KASPERSKY LAB

Kaspersky® Internet Security 6.0

MANUALE DELL'UTENTE

KASPERSKY INTERNET SECURITY 6.0

Manuale dell'utente

http://www.kaspersky.com

Data di revisione: ottobre 2006

Sommario

CAPITOLO 1. LE MINACCE ALLA SICUREZZA DEL COMPUTER

Poiché la tecnologia informatica si è sviluppata rapidamente penetrando in ogni aspetto dell'esistenza umana, la quantità di azioni illecite volte a minare la sicurezza delle informazioni si è moltiplicata.

I criminali informatici hanno mostrato un profondo interesse nelle attività di strutture governative e imprese commerciali. Essi cercano di impadronirsi di e diffondere informazioni riservate, danneggiando la reputazione di imprese, interrompendo la continuità di attività commerciali e, di conseguenza, violando le risorse informative di organizzazioni. Questi atti possono recare gravi danni a beni materiali e immateriali.

Ma non sono solo le grandi aziende a correre rischi. Anche gli utenti privati possono cadere vittima degli attacchi informatici. Servendosi di vari strumenti, i criminali accedono ai dati personali (numero di conto corrente e carta di credito, password, ecc.), provocano anomalie di funzionamento del sistema o ottengono l'accesso completo a computer altrui. Quei computer possono quindi essere utilizzati come elementi di una rete "zombie", cioè una rete di computer infetti usati dagli hacker per attaccare server, inviare spam, impadronirsi di informazioni riservate e diffondere nuovi virus e troiani.

Oggigiorno chiunque riconosce il valore dell'informazione ed è consapevole della necessità di proteggere i dati. Al tempo stesso l'informazione deve essere facilmente accessibile a determinati gruppi di utenti (per esempio dipendenti, clienti e partner di un'impresa). Ecco perché è necessario realizzare un vasto sistema di protezione dei dati. Questo sistema deve tenere conto di tutte le possibili minacce, siano esse umane, prodotte dall'uomo o conseguenze di catastrofi naturali, e applicare una serie completa di misure protettive a livello fisico, amministrativo e di software.

1.1. Le minacce potenziali

Singole persone, gruppi di persone o perfino fenomeni non correlati ad attività umane rappresentano potenziali minacce per la sicurezza dei dati. Le minacce potenziali possono essere suddivise in tre categorie:

- **Fattore umano**. Questo gruppo riguarda le azioni di persone autorizzate o non autorizzate ad accedere ai dati. Le minacce di questo gruppo possono essere:

- *Esterne*: criminali informatici, hacker, truffe via internet, partner sleali e strutture criminali.
- *Interne:* azioni del personale di un'azienda e degli utenti di PC ad uso domestico. Le azioni di questo gruppo possono essere deliberate o accidentali.

- **Fattore tecnologico**. Questo gruppo si riferisce a problemi tecnici: apparecchiature obsolete o software e hardware di scarsa qualità utilizzati per l'elaborazione delle informazioni. Questi fattori determinano il malfunzionamento delle apparecchiature e frequenti perdite di dati.
- **Fattore naturale**. Questo gruppo include qualsiasi evento naturale o altri eventi non dipendenti dall'attività dell'uomo.

Un sistema di protezione dati efficiente deve tener conto di tutti questi fattori. Questo manuale d'uso si riferisce esclusivamente a quelli di competenza diretta di Kaspersky Lab: le minacce esterne derivanti da attività umana.

1.2. La diffusione delle minacce

Man mano che la moderna tecnologia informatica e gli strumenti di comunicazione si evolvono, gli hacker possono contare su un numero crescente di opportunità per diffondere le loro minacce. Osserviamole più da vicino:

Internet

La rete Internet è unica in quanto non appartiene a nessuno e non è delimitata da confini geografici. Essa ha contribuito in molti modi allo sviluppo di innumerevoli risorse di rete e allo scambio di informazioni. Oggi tutti possono accedere ai dati disponibili su Internet o creare la propria pagina web.

Tuttavia proprio queste caratteristiche della rete offrono agli hacker la possibilità di commettere crimini via Internet, spesso senza essere individuati e puniti.

Gli hacker infettano i siti Internet con virus e altri programmi maligni facendoli passare come utili applicazioni gratuite (freeware). Inoltre gli script eseguiti automaticamente all'apertura di una pagina web sono in grado di eseguire azioni pericolose sul computer, fra cui la modifica del registro di sistema, il furto di dati personali e l'installazione di software nocivi.

Grazie alle tecnologie di rete, gli hacker possono attaccare PC e server aziendali remoti. Questi attacchi possono provocare il malfunzionamento di parte del sistema o fornire agli hacker l'accesso completo al sistema

stesso e alle informazioni in esso memorizzate. Il sistema può essere utilizzato anche come elemento di una rete "zombie".

Fin da quando è stato reso possibile l'uso delle carte di credito e di moneta elettronica su Internet per acquisti su negozi online, aste e pagine web di istituti di credito, le truffe online sono diventate uno dei crimini maggiormente diffusi.

Intranet

Intranet è una rete interna progettata specificamente per gestire le informazioni nell'ambito di un'azienda o di una rete domestica. Si tratta di uno spazio unificato per a cui tutti i computer della rete possono accedere per memorizzare, scambiare e consultare dati. Ciò significa che se un computer di tale rete è infetto, anche tutti gli altri corrono un grave rischio di infezione. Al fine di evitare una tale situazione, sia il perimetro della rete sia ogni singolo computer devono essere protetti.

E-mail

Poiché quasi tutti i computer hanno un client di posta elettronica installato e i programmi nocivi sfruttano i contenuti delle rubriche elettroniche, la diffusione di programmi nocivi può contare su condizioni ottimali. È possibile che l'utente di un computer infetto, ignaro di quanto sta avvenendo, invii e-mail infette ad amici e colleghi che, a loro volta, diffondono l'infezione. È molto comune che documenti infetti non individuati vengano inviati trasmettendo informazioni relative a grandi aziende. Quando ciò avviene, sono molti gli utenti che vengono infettati. Può trattarsi di centinaia o migliaia di persone che, a loro volta, inviano i file infetti a decine di migliaia di utenti.

Oltre alla minaccia dei programmi nocivi esiste quella della posta indesiderata, o spam. Sebbene questa non rappresenti una minaccia diretta per il computer, lo spam incrementa il carico sui server di posta, consuma larghezza di banda, riempie caselle elettroniche e determina la perdita di ore lavorative, provocando danni finanziari.

Gli hacker, inoltre, hanno iniziato a fare uso di programmi di mass mailing e di tecniche di social engineering per convincere gli utenti ad aprire messaggi e-mail o a fare clic su un determinato sito web. Le funzionalità di filtraggio antispam, di conseguenza, oltre a contrastare la posta spazzatura e i nuovi tipi di scansione online come il phishing, contribuiscono ad ostacolare la diffusione dei programmi nocivi.

Supporti di archiviazione esterni

I supporti esterni (floppy, CD-ROM e flash drive USB) sono molto usati per l'archiviazione e la trasmissione di informazioni.

All'apertura di un file contenente un codice maligno da un supporto di archiviazione esterno, è possibile che i file conservati nel computer si

infettino diffondendo il virus a tutte le altre unità del computer o agli altri computer della rete.

1.3. Tipi di minacce

Oggigiorno esistono numerosi tipi di minaccia che potrebbero pregiudicare il funzionamento di un computer. Questa sezione esamina le minacce bloccate da Kaspersky Internet Security.

Worm

Questa categoria di programmi nocivi si diffonde sfruttando in gran parte le vulnerabilità del sistema. Essi devono il loro nome alla capacità di "strisciare" come i vermi da un computer all'altro attraverso reti, posta elettronica e altri canali di informazione. Questa caratteristica consente ai worm di diffondersi con una velocità piuttosto elevata.

I worm penetrano all'interno di un computer, calcolano gli indirizzi di rete di altri computer e inviano loro una quantità di repliche di se stessi. Oltre agli indirizzi di rete, i worm utilizzano spesso i dati contenuti nelle rubriche dei client di posta elettronica. Alcuni di questi programmi maligni creano di quando in quando dei file di lavoro sui dischi di sistema, ma riescono a funzionare senza alcuna risorsa ad eccezione della RAM.

Virus

Programmi che infettano altri programmi aggiungendovi il proprio codice al fine di ottenere il controllo non appena un file infetto viene eseguito. Questa semplice definizione spiega il principio alla base della diffusione di un virus: l'*infezione*.

Troiani

Programmi che eseguono azioni non autorizzate, per esempio la cancellazione di dati sui drive provocando il blocco del sistema, il furto di informazioni confidenziali, ecc. Questa categoria di programmi nocivi non può essere definita virus nel senso tradizionale del termine in quanto non infetta altri computer o dati. I troiani non sono in grado di penetrare autonomamente in un computer ma vengono diffusi dagli hacker che li fanno passare per software regolare. I danni provocati dai troiani possono essere notevolmente superiori a quelli dei virus tradizionali.

Di recente, la categoria di programmi nocivi maggiormente diffusa è stata quella dei worm, seguita da virus e troiani. Alcuni programmi nocivi combinano le caratteristiche di due o addirittura tre di queste categorie.

Adware

Codice di programma incluso nel software, all'insaputa dell'utente, progettato per visualizzare messaggi pubblicitari. L'adware è solitamente incorporato nel software a distribuzione gratuita e il messaggio è situato nell'interfaccia del programma. Questi programmi spesso raccolgono anche dati personali relativi all'utente e li inviano allo sviluppatore, modificano le impostazioni del browser (pagina iniziale e pagine di ricerca, livello di sicurezza, ecc.) e creano un traffico che l'utente non è in grado di controllare. Tutto ciò può provocare la violazione delle regole di sicurezza e, in ultima analisi, perdite finanziarie.

Spyware

Software che raccoglie informazioni su un utente o azienda a loro insaputa. Talvolta esso si installa in un computer senza che l'utente se ne accorga. In generale gli obiettivi dello spyware sono:

- Ricostruire le azioni dell'utente su un computer
- Raccogliere informazioni sui contenuti del disco fisso; in tal caso, ciò comporta quasi sempre la scansione di numerose directory e del registro di sistema al fine di compilare un elenco dei software installati sul computer
- Raccogliere informazioni sulla qualità della connessione, larghezza di banda, velocità del modem, ecc.

Riskware

Software potenzialmente rischioso che non svolge una funzione nociva vera e propria ma che può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. In determinate condizioni, la presenza di tali programmi nel computer rappresenta una fonte di rischio per i proprio dati. Questi programmi includono, per esempio, alcune utilità di amministrazione remota, commutatori di tastiera, client IRC, server FTP e utilità multifunzione per interrompere processi o per nasconderne il funzionamento.

Esiste un altro tipo di programma nocivo trasmesso con adware, spyware e riskware: sono quei programmi che penetrano nel web browser e ridirigono il traffico. Chiunque abbia avuto l'esperienza di aprire un sito web credendo di caricarne uno diverso, quasi certamente ha incontrato uno di questi programmi.

Joke

Software che non reca alcun danno diretto ma visualizza messaggi secondo i quali il danno è già stato provocato o lo sarà in circostanze particolari. Questi programmi spesso comunicano all'utente la presenza di rischi inesistenti, per esempio sulla formattazione del disco fisso (anche

se non ha luogo alcuna formattazione) o l'individuazione di virus in file non infetti.

Rootkit

Utilità che celano attività nocive. Esse nascondono programmi nocivi che impediscono agli antivirus di individuarli. Le rootkit modificano il sistema operativo del computer e ne alterano le funzioni di base per nascondere la propria esistenza e le azioni intraprese dagli hacker sul computer infetto.

Altri programmi pericolosi

Programmi creati per lanciare attacchi DoS su server remoti e penetrare in altri computer, e programmi che fanno parte dell'ambiente di sviluppo dei programmi nocivi. Essi includono hack tool, virus builder, scanner di vulnerabilità, programmi di individuazione di password, e altri tipi di programma per penetrare in un sistema o utilizzare risorse di rete.

Attacchi di pirateria informatica

Gli attacchi di pirateria informatica possono essere avviati da hacker o da programmi nocivi. Essi hanno lo scopo di sottrarre informazioni da un computer remoto provocando il malfunzionamento del sistema, oppure di ottenere il controllo completo delle risorse del computer. Per una descrizione dettagliata dei tipi di attacco bloccati da Kaspersky Internet Security, consultare la sezione Elenco degli attacchi di rete rilevati.

Alcuni tipi di truffe online

Il **"phishing"** è una truffa online che impiega il mass mailing per carpire informazioni confidenziali, solitamente di natura confidenziale, sugli utenti. I messaggi inviati a tal fine sono concepiti in modo da indurre a credere che si tratti di e-mail informative da parte di istituti di credito e note aziende. Contengono dei link che aprono siti contraffatti, realizzati dagli hacker in modo da riprodurre il sito ufficiale dell'organizzazione che fingono di rappresentare. Il sito richiede all'utente di digitare, per esempio, il numero della carta di credito e altre informazioni confidenziali.

Dialer per siti a pagamento – tipo di truffa online basata sull'uso non autorizzato di servizi Internet a pagamento (solitamente siti web con contenuti pornografici). I dialer installati dagli hacker stabiliscono il contatto via modem tra il computer colpito e il numero telefonico del servizio a pagamento. Si tratta frequentemente di numeri con tariffe molto elevate che costringono l'ignaro utente al pagamento di bollette telefoniche costosissime.

Messaggi pubblicitari importuni

Ne fanno parte le finestre a comparsa (popup) e i banner pubblicitari che si aprono durante la navigazione. Le informazioni contenute in tali finestre

di solito non sono di alcun interesse per il navigatore comune. I popup e i banner distraggono l'utente dall'occupazione che stava svolgendo e consumano larghezza di banda.

Spam

Lo spam è posta "spazzatura" anonima, che comprende marketing, messaggi di natura politica e provocatoria o richieste di assistenza. Un'altra categoria di spam è costituita da proposte di investire ingenti somme di denaro o di entrare a far parte di strutture piramidali, e-mail volte a carpire password e numeri di carte di credito, e e-mail da trasmettere ad amici (catene di Sant'Antonio).

Kaspersky Internet Security adotta due categorie di metodi per individuare e bloccare questi tipi di minaccia:

- *Metodi reattivi* – basati sulla ricerca di file nocivi per mezzo di database delle firme regolarmente aggiornati. Questo metodo richiede l'inserimento delle firme coinvolte nel database e lo scaricamento degli aggiornamenti.
- *Metodi proattivi* – contrariamente ai metodi reattivi, non si basano sull'analisi di codici ma del comportamento del sistema. Questi metodi sono finalizzati all'individuazione di nuove minacce non ancora definite nelle firme.

Grazie all'applicazione di entrambi i metodi, Kaspersky Internet Security garantisce una protezione completa del computer contro le minacce già note e quelle ancora ignote.

1.4. Segnali di infezione

Vi sono numerosi segnali che indicano la presenza di un virus all'interno del computer. Di solito il computer si comporta in maniera strana, in particolare:

- Il video visualizza messaggi o immagini impreviste, oppure il computer emette suoni anomali;
- Il lettore CD/DVD-ROM si apre e si chiude inaspettatamente;
- Il computer apre arbitrariamente un programma non richiesto dall'utente;
- Il video visualizza messaggi pop up che informano che un determinato programma nel computer sta cercando di accedere a Internet, anche se tale azione non è stata richiesta dall'utente.

In tutti questi casi è molto probabile che il computer sia infetto da un virus.

Anche l'infezione attraverso la posta elettronica presenta numerosi tratti caratteristici:

- Amici e parenti sostengono di aver ricevuto messaggi che l'utente non ha mai inviato;
- La casella di posta elettronica contiene numerosi messaggi privi di mittente o intestazione.

Occorre specificare che questi segnali possono anche essere il risultato di problemi diversi dai virus. Talvolta hanno effettivamente altre cause. Per esempio, nel caso della posta elettronica, è possibile che i messaggi infetti vengano inviati con l'indirizzo di un mittente specifico ma non dal suo computer.

Vi sono anche sintomi indiretti che indicano una probabile infezione del computer:

- Il computer si blocca o ha crash frequenti
- Il computer carica i programmi con eccessiva lentezza
- Non si riesce a inizializzare il sistema operativo
- File e cartelle scompaiono o i loro contenuti risultano modificati
- Si osservano frequenti accessi al disco fisso (la spia lampeggia)
- Il browser web (per esempio Microsoft Internet Explorer) si blocca o ha comportamenti anomali (per esempio non si riesce a chiudere la finestra del programma).

Nel 90% dei casi, questi segnali indiretti sono provocati da anomalie di funzionamento dell'hardware o del software. Malgrado questi segnali dipendano raramente da un'infezione del computer, si raccomanda di effettuare una scansione completa del computer (cfr. 5.3 a pag. 61) con le impostazioni raccomandate dagli esperti di Kaspersky Lab.

1.5. Come comportarsi se il computer mostra segni di infezione

Se il computer ha un comportamento "sospetto":

1. Evitare il panico! Non lasciarsi prendere dal panico. È questa la regola principale da seguire in quanto può evitare la perdita di dati importanti e numerose seccature.
2. Scollegare il computer da Internet o da un'eventuale rete locale.

3. Se il sintomo riscontrato consiste nell'impossibilità di effettuare il boot dal disco fisso (il computer visualizza un messaggio d'errore all'accensione), provare ad avviare la macchina in modalità provvisoria o dal disco di boot di Windows creato durante l'installazione del sistema operativo.
4. Prima di eseguire qualsiasi operazione, effettuare una copia di backup del lavoro su un supporto esterno (floppy, CD, unità flash, ecc.).
5. Installare Kaspersky Internet Security, se non lo si è già fatto.
6. Aggiornare gli elenchi delle minacce del programma (cfr. 5.7 a pag. 65). Se possibile, procurarsi gli aggiornamenti accedendo a Internet da un computer non infetto, per esempio da un amico, in un Internet point o in ufficio. È consigliabile utilizzare un computer diverso, poiché connettendosi a Internet da un computer infetto è probabile che il virus invii informazioni importanti agli hacker o si diffonda agli indirizzi presenti nella rubrica. In altre parole, se si sospetta un'infezione, la precauzione migliore è scollegarsi immediatamente da Internet. È possibile procurarsi gli aggiornamenti degli elenchi delle minacce anche su un dischetto floppy da Kaspersky Lab o dai suoi distributori e aggiornare le proprie firme dal dischetto.
7. Selezionare il livello di sicurezza raccomandato dagli esperti di Kaspersky Lab.
8. Avviare una scansione completa del computer (cfr. 5.3 a pag. 61).

1.6. Prevenzione delle infezioni

Neanche le misure più affidabili e attente sono in grado di garantire una protezione assoluta dai virus e dai troiani, ma l'osservanza di queste regole riduce significativamente la probabilità di attacchi di virus e il livello di danno potenziale.

Come in medicina, una delle regole fondamentali per evitare le infezioni è la prevenzione. La profilassi del computer comporta poche regole che, se rispettate, possono ridurre in maniera considerevole la probabilità di incorrere in un virus e perdere dati.

Le regole di sicurezza fondamentali sono descritte di seguito. Osservandole è possibile evitare attacchi virulenti.

Regola 1: *Usare un software antivirus e programmi di sicurezza Internet*. Procedere come segue:

- Installare al più presto Kaspersky Internet Security.
- Aggiornare regolarmente (cfr. 5.7 a pag. 65) gli elenchi delle minacce del programma. È possibile aggiornare gli elenchi più volte al giorno durante

le epidemie di virus. In tali circostanze, gli elenchi delle minacce sui server di aggiornamento Kaspersky Lab vengono aggiornate istantaneamente.

- Selezionare le impostazioni di sicurezza raccomandate da Kaspersky Lab per il computer. Esse garantiscono una protezione costante dall'accensione del computer, ostacolando la penetrazione dei virus.
- Configurare le impostazioni di scansione completa raccomandate dagli esperti di Kaspersky Lab e pianificare scansioni almeno una volta la settimana. Se non si è installato Anti-Hacker, si raccomanda di provvedere in modo da proteggere il computer durante la navigazione.

Regola 2: *Usare cautela nella copia di nuovi dati sul computer*:

- Eseguire la scansione antivirus di tutte le unità di archiviazione esterne (cfr. 5.5 a pag. 62) (floppy, CD, unità flash, ecc.) prima di usarle.
- Trattare i messaggi e-mail con cautela. Non aprire alcun file arrivato per posta elettronica se non si ha la certezza di esserne l'effettivo destinatario, anche se il mittente è una persona nota.
- Trattare con prudenza qualsiasi informazione ottenuta tramite Internet. Se un sito web suggerisce di installare un nuovo programma, verificare che esso abbia un certificato di sicurezza. Se si copia un file eseguibile da Internet o da una rete locale, ricordarsi di esaminarlo con Kaspersky Internet Security.
- Selezionare con prudenza i siti web da visitare. Molti siti sono infetti da script pericolosi o worm di Internet.

Regola 3: *Prestare attenzione alle informazioni fornite da Kaspersky Lab.*

Nella maggior parte dei casi, Kaspersky Lab annuncia un'epidemia con largo anticipo rispetto al periodo di massima diffusione. In tal modo le probabilità di contrarre l'infezione sono esigue, e una volta scaricati gli aggiornamenti si disporrà di tempo a sufficienza per proteggersi dal nuovo virus.

Regola 4: *Non fidarsi delle bufale* come i programmi-scherzo (prank) e le e-mail relative a presunte infezioni.

Regola 5: *Usare lo strumento di aggiornamento di Windows* e installare regolarmente gli aggiornamenti del sistema operativo.

Regola 6: *Acquistare sempre software dotato di regolare licenza da rivenditori autorizzati.*

Regola 7: *Limitare il numero di persone che possono accedere al computer.*

Regola 8: *Contenere il rischio di conseguenze spiacevoli in caso di infezione*:

- Eseguire regolarmente una copia di backup dei dati. Se si perdono i dati, il sistema sarà in grado di ripristinarli piuttosto rapidamente se si dispone di copie di backup. Conservare in un luogo sicuro i dischetti floppy, i CD, le unità flash e altri supporti di archiviazione contenenti software e informazioni importanti.
- Creare un disco di ripristino (cfr. 17.10 a pag. 263) con il quale effettuare eventualmente il boot della macchina con un sistema operativo pulito.

Regola 9: C*ontrollare regolarmente l'elenco dei programmi installati sul computer*. A tal fine, aprire **Installazione applicazioni** in **Pannello di controllo** oppure aprire la cartella **Programmi**. È possibile scoprirvi applicazioni installate all'insaputa dell'utente, per esempio durante la navigazione in Internet o l'installazione di un programma. Alcune di esse sono quasi sempre programmi potenzialmente rischiosi.

CAPITOLO 2. KASPERSKY INTERNET SECURITY 6.0

Kaspersky Internet Security 6.0 è la nuova generazione dei prodotti per la sicurezza dei dati.

La caratteristica che contraddistingue Kaspersky Internet Security 6.0 rispetto ad altri software, perfino da altri prodotti Kaspersky Lab, è l'approccio complesso alla sicurezza dei dati conservati nel computer.

2.1. Le nuove funzioni di Kaspersky Internet Security 6.0

Kaspersky Internet Security 6.0 offre un approccio innovativo alla sicurezza dei dati. La caratteristica principale del programma è la combinazione in un'unica soluzione delle funzioni esistenti di tutti i prodotti dell'azienda, in versione potenziata. Il programma offre protezione sia contro i virus sia contro lo spam e gli attacchi di pirateria informatica. I nuovi moduli proteggono gli utenti da minacce, phishing e rootkits non ancora noti.

In altre parole, garantisce una sicurezza globale del computer senza la necessità di installare numerosi prodotti. Solo questo è un valido motivo per installare Kaspersky Internet Security 6.0.

Tutti i canali di accesso o uscita dei dati sono prottetti in maniera esauriente. Le impostazioni flessibili di ciascun componente del programma consentono di adattare in maniera ottimale Kaspersky Internet Security alle esigenze di ogni utente. È possibile inoltre impostare tutti i componenti di protezione da una singola postazione.

Esaminiamo in dettaglio le nuove funzioni di Kaspersky Internet Security 6.0.

Nuove funzionalità di protezione

- Kaspersky Internet Security protegge il computer da programmi nocivi noti e da programmi non ancora scoperti. La difesa proattiva (cfr. Capitolo 10 a pag. 123) è il vantaggio principale del programma. Esso è studiato per analizzare il comportamento delle applicazioni installate sul computer, monitorare le modifiche al registro di sistema, individuare le macro e combattere le minacce nascoste. Il componente si basa su un analizzatore euristico in grado di individuare vari tipi di programmi nocivi. Così facendo, compila una cronologia delle attività nocive grazie alla

quale è possibile retrocedere e ripristinare l'ultima versione sicuramente funzionante del sistema prima dell'attività nociva.

- Il programma protegge da rootkit e dialer, blocca i banner pubblicitari, i popup e gli script nocivi scaricati dalle pagine web, e individua i siti di phishing.
- La tecnologia antivirus è stata potenziata: adesso è possibile ridurre il carico e accelerare le scansioni dei file. Le tecnologie iCheck e iSwift contribuiscono a una maggiore velocità esaminando solo i file nuovi o modificati (cfr. 7.2.1 a pag. 93). Così facendo, il programma evita di effettuare scansioni ripetute di file che non hanno subito modifiche rispetto alla scansione precedente.
- Il processo di scansione si svolge adesso in modalità secondaria mentre l'utente continua a usare il computer. Una scansione può comportare un dispendio considerevole di tempo e di risorse di sistema, ma non è necessario che l'utente interrompa la propria attività con il computer. Se un'operazione richiede maggiori risorse di sistema, la scansione si interrompe fino a quando l'operazione sarà conclusa. La scansione riprende quindi dal punto in cui si era interrotta.
- Le aree critiche che potrebbero produrre gravi conseguenze in caso di infezione sono sottoposte a una scansione specifica. Questa attività può essere configurata in modo da iniziare a ogni avvio del sistema.
- La protezione della posta elettronica contro i programmi nocivi e lo spam è stata considerevolmente migliorata. Il programma esegue la scansione antivirus e antispam delle e-mail inviate con i seguenti protocolli:
    - IMAP, SMTP, POP3, indipendentemente dal client di posta utilizzato
    - NNTP (solo scansione antivirus), indipendentemente dal client di posta utilizzato
    - MAPI, HTTP (con i plug-in per MS Outlook e The Bat!)
- Sono disponibili plug-in specifici per i client di posta più comuni come Outlook, Microsoft Outlook Express e The Bat!, che consentono di configurare direttamente dal client la protezione antivirus e antispam della posta.
- La funzionalità di riconoscimento dello spam si espande man mano che la casella della posta in entrata si riempie, registrando le azioni dell'utente nei confronti della posta e garantendo così la massima flessibilità di configurazione. L'apprendimento progressivo da parte del programma si basa sull'algoritmo di Bayes. È possibile compilare liste bianche e liste nere di indirizzi di mittenti e di espressioni ricorrenti nei messaggi identificati come spam.

La funzione antispam fa uso di un database di phishing in grado di escludere tutte le e-mail studiate per procurare informazioni confidenziali di natura finanziaria.

- Il programma filtra la posta in arrivo e quella in uscita, individua e blocca le minacce da attacchi di rete comuni e consente di utilizzare Internet in modalità invisibile.
- In caso di lavoro in rete, è possibile inoltre specificare le reti attendibili al 100% e quelle da monitorare con estrema attenzione.
- La funzione di notifica dell'utente (cfr. 17.11.1 a pag. 267) è stata ampliata includendo determinati eventi che si verificano durante il funzionamento del programma. È possibile scegliere per ciascun evento uno dei seguenti metodi di notifica: e-mail, segnalazione acustica, messaggi a comparsa.
- È stata aggiunta la scansione per i dati trasmessi su connessioni SSL protette.
- Il programma è dotato di funzionalità di autodifesa: Protezione dall'amministrazione remota, e impostazioni protette da password. Queste funzioni impediscono ai programmi nocivi, agli hacker e agli utenti non autorizzati di disabilitare la protezione.
- Il programma utilizza una tecnologia di ripristino del sistema per rimuovere codici nocivi dal registro e dal file system del computer, e per ripristinare il sistema nell'ultima versione sicuramente funzionante prima delle attività nocive.

Nuove funzioni dell'interfaccia

- La nuova interfaccia di Kaspersky Internet Security agevola l'uso delle funzioni del programma. È possibile anche modificare l'aspetto del programma creando e utilizzando una grafica e uno schema cromatico personalizzati.
- Il programma offre regolarmente suggerimenti durante l'uso: Kaspersky Internet Security visualizza messaggi informativi sul livello di protezione, accompagna il proprio funzionamento con suggerimenti e consigli e offre un'esauriente guida.

Nuove funzioni di aggiornamento del programma

- Questa versione del programma introduce una nuova e più potente procedura di aggiornamento: Oggi Kaspersky Internet Security controlla automaticamente la disponibilità di aggiornamenti delle firme e dei moduli del programma necessari per il corretto funzionamento. Gli aggiornamenti vengono scaricati automaticamente alla prima occasione di connettersi ai server di Kaspersky Lab.

- Il programma scarica solo gli aggiornamenti non ancora installati. In tal modo il traffico verso i server di aggiornamento risulta ridotto fino a 10 volte.
- Durante la procedura viene determinata l'origine ideale dell'aggiornamento, che viene impostata come default per gli aggiornamenti futuri.
- Oggi è possibile scegliere di non utilizzare un server proxy se gli aggiornamenti del programma vengono scaricati da un'origine locale. Ciò riduce considerevolmente il carico sul server proxy.
- Il programma è dotato di una funzione di ripristino dello stato precedente, che consente di ripristinare l'ultima versione sicuramente funzionante delle firme se, per esempio, le firme installate risultano danneggiate o si è verificato un errore durante la copia.
- La funzione di aggiornamento comprende ora uno strumento che rende gli aggiornamenti accessibili agli altri computer della rete copiandoli in una cartella locale. Ciò riduce il traffico Internet.

2.2. Gli elementi della protezione di Kaspersky Internet Security

La protezione di Kaspersky Internet Security è stata studiata tenendo conto delle provenienze delle minacce. In altre parole, ogni tipo di minaccia è gestito da un componente distinto del programma, monitorato e affrontato con le misure necessarie a impedirne gli effetti nocivi sui dati dell'utente. Questa struttura rende flessibile la Security Suite, offrendo facili opzioni di configurazione per tutti i componenti in modo da soddisfare le esigenze di utenti specifici o aziende nella loro globalità.

Kaspersky Internet Security presenta:

- Componenti di protezione (cfr. 2.2.1 a pag. 25) per una difesa globale su tutti i canali di trasmissione e scambio dati del computer.
- Attività di scansione antivirus (cfr. 2.2.2 a pag. 27) che esaminano il computer o singoli file, cartelle, dischi o aree alla ricerca di virus.
- Strumenti di supporto (cfr. 2.2.3 a pag. 28) che offrono assistenza sul programma e ne estendono le funzionalità.

2.2.1. Componenti di protezione

I componenti di protezione garantiscono la sicurezza del computer in tempo reale:

File Anti-Virus

Un file system può contenere virus e altri programmi pericolosi. I programmi nocivi possono restare nel file system per anni dopo esservi stati introdotti attraverso un dischetto floppy o navigando in Internet, senza mostrare la propria presenza. Ma è sufficiente aprire il file infetto o, per esempio, provare a copiarlo su un disco, per attivare immediatamente il file.

File Antivirus è il componente che monitora il file system del computer. Esso esamina tutti i file che possono essere aperti, eseguiti o salvati sul computer e su tutte le unità disco collegate. Kaspersky Internet Security intercetta ogni file che viene aperto e lo esamina per escludere la presenza di virus noti. Il file esaminato potrà essere utilizzato solo se non infetto o se successivamente trattato mediante File Anti-Virus. Se per qualsiasi motivo non fosse possibile riparare un file infetto, esso viene eliminato dopo averne salvata una copia nella cartella Backup (cfr. 17.2 a pag. 234), o trasferito in Quarantena (cfr. 17.1 a pag. 231).

Mail Anti-Virus

La posta elettronica è molto utilizzata dagli hacker per diffondere programmi nocivi e rappresenta uno dei canali più diffusi per la diffusione di worm. Per questo è estremamente importante monitorare tutta la posta.

Mail Anti-Virus è il componente che esamina tutti i messaggi e-mail in entrata e in uscita dal computer, in cerca di programmi nocivi. Il programma consente al destinatario di aprire il messaggio solo se privo di oggetti pericolosi.

Web Anti-Virus

Ogni volta che si apre un sito web si corre il rischio di restare infettati dai virus presenti negli script eseguiti sui siti web, e di scaricare oggetti pericolosi sul proprio computer.

Web Anti-Virus è pensato specificamente per prevenire tali evenienze. Questo componente intercetta e blocca gli script dei siti web potenzialmente pericolosi, monitorando accuratamente tutto il traffico HTTP.

Difesa proattiva

Ogni giorno compaiono nuovi programmi nocivi in quantità crescente. Essi diventano sempre più complessi combinando più tipi di minaccia, e i metodi utilizzati per diffondersi sono sempre più difficili da scoprire.

Per individuare un nuovo programma nocivo prima che abbia il tempo di provocare danni, Kaspersky Lab ha sviluppato uno speciale componente dal nome *Difesa proattiva*. Esso è progettato per monitorare e analizzare il comportamento di tutti i programmi installati sul computer. Kaspersky Anti-Virus prende una decisione in base alle azioni eseguite da un'applicazione: il programma è pericoloso? Difesa proattiva protegge il computer sia dai virus noti sia da quelli non ancora scoperti.

Anti-Spy

I programmi che visualizzano messaggi pubblicitari senza che l'utente ne abbia fatto richiesta (banner e popup), programmi che si collegano con numeri telefonici per servizi Internet a pagamento senza l'autorizzazione dell'utente, strumenti di amministrazione remota e di monitoraggio, programmi joke, ecc., sono sempre più diffusi.

Anti-Spy individua queste azioni sul computer e le blocca. Per esempio, blocca i banner pubblicitari e i popup, autentiche seccature per chi naviga in Internet; blocca i programmi che cercano di collegarsi a numeri di telefono, e analizza le pagine web per escludere la presenza di contenuti di phishing.

Anti-Hacker

Gli hacker sfruttano ogni potenziale falla del sistema per invadere i computer, sia che facciano parte di una connessione di rete aperta, trasmettano dati da un computer all'altro, ecc.

Anti-Hacker è il componente studiato per proteggere il computer durante l'uso di Internet e di altre reti. Esso controlla le connessioni in entrata e in uscita ed esamina porte e pacchetti di dati.

Anti-Spam

Anche se non rappresenta una minaccia diretta per il computer, lo spam incrementa il carico sui server di posta, consuma larghezza di banda, riempie caselle elettroniche e determina la perdita di ore lavorative, provocando danni finanziari.

Il componente *Anti-Spam* si installa come plug-in del client di posta installato sul computer ed esamina tutta la posta in entrata per escludere la presenza di contenuti di spam. Tutti i messaggi e-mail contenenti spam vengono contrassegnati da un'intestazione particolare. Anti-Spam può essere configurato anche in modo da trattare lo spam in base a un'azione

predefinita dall'utente (cancellazione automatica, trasferimento in una cartella apposita, ecc.).

2.2.2. Attività di scansione antivirus

Oltre a monitorare costantemente i potenziali accessi di programmi nocivi, è estremamente importante eseguire periodicamente la scansione antivirus del computer. Ciò è necessario al fine di escludere la possibilità di diffondere programmi nocivi non ancora rilevati dai componenti di sicurezza a causa della protezione impostata su un livello basso o per altri motivi.

Kaspersky Internet Security offre tre attività di scansione antivirus:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del computer, fra cui: memoria di sistema, programmi caricati all'avvio, settori di boot del disco fisso, directory di sistema *Windows* e *system32*. L'obiettivo di questa attività è individuare rapidamente i virus attivi nel sistema senza eseguire una scansione completa del computer.

Risorse del computer

La scansione antivirus viene effettuata sull'intero computer, con un'analisi approfondita di tutte le unità disco, memoria e file.

Oggetti di avvio

La scansione antivirus viene effettuata su tutti i programmi caricati automaticamente all'avvio, sulla RAM e sui settori di boot dei dischi fissi.

È possibile inoltre creare altre attività di ricerca dei virus e pianificarne l'esecuzione. Per esempio, è possibile creare un'attività di scansione per i database della posta da eseguire una volta la settimana, o un'attività di scansione antivirus della cartella **Documenti**.

2.2.3. Strumenti del programma

Kaspersky Internet Security offre una serie di strumenti di supporto progettati per fornire assistenza software in tempo reale, espandendo le funzionalità del programma e assistendo l'utente durante la procedura.

Aggiornamento

Per poter essere sempre pronto ad affrontare gli attacchi hacher ed eliminare virus o altri programmi pericolosi, Kaspersky Internet Security necessita di assistenza in tempo reale. Lo strumento di *Aggiornamento* è progettato esattamente per questo. Esso si occupa di aggiornare gli elenchi delle minacce di Kaspersky Internet Security e i moduli del programma.

Aggiorna distribuzione

La funzione Aggiorna distribuzione consente di salvare gli aggiornamenti all'elenco dei virus ed ai moduli dell'applicazione recuperati dai server di Kaspersky Lab in una cartella locale. Gli altri computer della rete possono quindi accedere ad essi per risparmiare larghezza di banda Internet.

File di dati

Durante il funzionamento, ogni componente di sicurezza, attività di ricerca virus e aggiornamento del programma genera un report contenente informazioni sulle operazioni completate e sui rispettivi risultati. La funzione *Report* consente all'utente di restare sempre aggiornato sul funzionamento di tutti i componenti di Kaspersky Internet Security. In caso di problemi, è possibile inviare i report a Kaspersky Lab in modo da consentire ai nostri esperti di studiare la situazione in maniera approfondita e fornire una soluzione nella maniera più rapida possibile.

Kaspersky Internet Security invia tutti i file sospetti in una speciale area denominata *Quarantena*. Essi vengono salvati in forma codificata al fine di evitare di infettare il computer. Questi oggetti possono essere sottoposti a scansione antivirus, ripristinati nella posizione originaria, eliminati o trasferiti manualmente in Quarantena. Tutti i file che al termine della scansione antivirus non risultano infetti vengono automaticamente ripristinati nella posizione originaria.

Backup contiene le copie dei file ripuliti o eliminati dal programma. Queste copie vengono create per l'eventualità in cui si renda necessario ripristinare file o ottenere informazioni sull'infezione. Le copie di backup dei file sono salvate in forma codificata per evitare la diffusione dell'infezione.

I file contenuti nell'area Backup possono essere ripristinati nella posizione originale ed eliminati.

Disco di ripristino

Kaspersky Internet Security presenta una funzione speciale per la creazione di un disco di ripristino.

Il disco di ripristino offre un piano di backup in caso di danneggiamento dei file di sistema da parte di un'infezione che rende impossibile inizializzare il sistema operativo. In tal caso, il disco di ripristino consente di riavviare il computer e ripristinare il sistema nella configurazione in cui si trovava prima dell'infezione.

Supporto

Tutti gli utenti registrati di Kaspersky Internet Security possono avvalersi del nostro Servizio di assistenza tecnica. Per informazioni su come ottenere tale assistenza, usare la funzione *Supporto*.

Vi troverete un elenco delle domande più frequenti che potrebbero essere sufficienti a risolvere il problema. Ma è possibile anche accedere all'Assistenza tecnica online, e, naturalmente, i nostri esperti saranno disponibili telefonicamente o per e-mail per risolvere qualsiasi problema legato all'uso di Kaspersky Internet Security.

2.3. Requisiti di sistema hardware e software

Per garantire il corretto funzionamento di Kaspersky Internet Security 6.0, il computer deve possedere i seguenti requisiti minimi:

Requisiti di carattere generale:

- 50 MB di spazio disponibile sul disco fisso
- CD-ROM (per installare Kaspersky Internet Security 6.0 dal CD di installazione)
- Microsoft Internet Explorer 5.5 o successivo (per aggiornare gli elenchi delle minacce e i moduli del programma attraverso Internet)
- Microsoft Windows Installer 2.0

Microsoft Windows 98, Microsoft Windows Me, Microsoft Windows NT Workstation 4.0 (Service Pack 6a):

- Processore Intel Pentium 300 MHz o superiore
- 64 MB di RAM

Microsoft Windows 2000 Professional (Service Pack 3 o successiva), Microsoft Windows XP Home Edition, Microsoft Windows XP Professional (Service Pack 1 o successiva):

- Processore Intel Pentium 300 MHz o superiore
- 128 MB di RAM

2.4. Pacchetti software

Kaspersky Internet Security può essere acquistato presso i nostri rivenditori, nella versione in scatola, oppure via Internet (per esempio su www.kaspersky.com, nella sezione **eStore**).

La versione in scatola include:

- Una busta sigillata con CD di installazione contenente i file del programma
- Un manuale d'uso
- Il codice di attivazione del programma, applicato sulla busta del CD di installazione
- Il contratto di licenza con l'utente finale (EULA)

Prima di rompere il sigillo della busta contenente il CD di installazione, leggere attentamente l'EULA.

Chi acquista Kaspersky Internet Security attraverso Internet, copierà il prodotto dal sito web di Kaspersky Lab (**Downloads → Product Downloads**). Il manuale d'uso del prodotto può essere scaricato nella sezione **Downloads → Documentation**.

A pagamento avvenuto, l'utente riceverà per e-mail il codice di attivazione.

Il Contratto di licenza è un accordo con valore legale fra l'utente finale e Kaspersky Lab, volto a regolamentare le condizioni di utilizzo del prodotto acquistato.

Leggere attentamente l'EULA.

Se non si accettano i termini del Contratto di licenza, è possibile restituire il prodotto completo di scatola al distributore presso cui è stato effettuato l'acquisto, e ottenere il rimborso completo dell'importo pagato. Ciò è possibile a condizione che la busta sigillata contenente il CD di installazione sia ancora sigillata.

L'apertura della busta sigillata del CD di installazione comporta l'accettazione dei termini e delle condizioni del Contratto di licenza da parte dell'acquirente.

2.5. Assistenza per gli utenti registrati

Kaspersky Lab offre ai propri utenti registrati una serie di servizi volti ad ottimizzare l'efficacia di Kaspersky Internet Security.

Dopo l'attivazione del programma si diventa automaticamente utenti registrati e si ha diritto ai seguenti servizi fino alla scadenza della licenza:

- Nuove versioni del programma, a titolo gratuito

- Consullenza telefonica e via e-mail su problematiche relative all'installazione, alla configurazione e al funzionamento del programma
- Comunicazioni sui nuovi prodotti di Kaspersky Lab e sui nuovi virus (questo servizio è riservato agli utenti iscritti alla newsletter di Kaspersky Lab)

Kaspersky Lab non fornisce assistenza tecnica relativa all'uso e al funzionamento del sistema operativo o di qualsiasi altro prodotto di altri fabbricanti.

CAPITOLO 3. KASPERSKY INTERNET SECURITY 6.0

Kaspersky Internet Security può essere installato integralmente o parzialmente.

L'installazione parziale consente di selezionare i componenti da installare, oppure di installare automaticamente solo i componenti antivirus (cfr. Passo 9 della procedura di installazione). Gli altri componenti del programma potranno essere installati in seguito caricando di nuovo il CD di installazione. Si raccomanda di copiare il disco di installazione sul disco fisso o di avviare l'installazione per mezzo del prompt di comando:

```
msiexec /a <installation_file>
```

Nell'ultimo caso, Windows Installer copia automaticamente i file di installazione sul computer.

3.1. Procedura di installazione

Per installare Kaspersky Internet Security sul computer, aprire il file di Windows Installer (.msi) nel CD di installazione.

Nota:
La procedura di installazione per mezzo di un pacchetto scaricato da Internet è uguale a quella per mezzo del CD.

Si apre una procedura di installazione guidata del programma. Ogni finestra contiene dei pulsanti che consentono di completare il processo. Ecco una breve descrizione delle loro funzioni:

- **Avanti** – conferma un'azione e apre la fase successiva dell'installazione.
- **Indietro** – riporta alla fase precedente dell'installazione.
- **Annulla** – annulla l'installazione del prodotto.
- **Fine** – completa la procedura di installazione del programma.

Osserviamo in dettaglio le fasi della procedura di installazione.

Passaggio 1. Verificare i requisiti di sistema per l'installazione di Kaspersky Internet Security

Prima di installare il programma sul computer, l'installer controlla che il sistema operativo e i service pack necessari per l'installazione di Kaspersky Internet

Security. L'applicazione controlla inoltre che il computer disponga di altri programmi necessari e che l'utente possieda diritti sufficienti per l'installazione di software.

In assenza di uno qualsiasi dei requisiti necessari, il programma visualizza un messaggio informando l'utente dell'impossibilità di completare l'installazione. Prima di installare Kaspersky Internet Security si raccomanda di installare i service pack necessari attraverso **Windows Update** ed eventuali altri programmi.

Passaggio 2. Finestra di avvio dell'installazione

Se il sistema soddisfa tutti i requisiti necessari, non appena si esegue il file di installazione si apre una finestra che avvisa dell'inizio dell'installazione di Kaspersky Internet Security.

Per continuare l'installazione fare clic su **Avanti**. Per annullare l'installazione fare clic su Annulla.

Passaggio 3. Visualizzazione del Contratto di licenza con l'utente finale

La finestra di dialogo successiva contiene un Contratto di licenza tra l'acquirente e Kaspersky Lab. Leggere attentamente il contratto e, se si approvano le condizioni, fare clic su **Accetto i termini del contratto,** quindi premere il pulsante **Avanti**. L'installazione prosegue.

Passaggio 4. Scelta di una cartella di installazione

La fase successiva dell'installazione di Kaspersky Internet Security serve per stabilire la posizione in cui installare il programma sul computer. Il percorso predefinito è: **<Drive>\Programmi\Kaspersky Lab\Kaspersky Internet Security 6.0**.

Per specificare una cartella diversa, fare clic sul pulsante **Sfoglia** e selezionare la nuova cartella nella finestra di selezione che si apre, oppure digitare direttamente il percorso nel campo apposito.

Ricordare che, se si desidera digitare manualmente il percorso completo della cartella di installazione, esso non deve superare i 200 caratteri né contenere caratteri speciali.

Per continuare l'installazione fare clic su **Avanti**.

Passaggio 5. Scelta di un tipo di installazione

In questa fase si selezionano i componenti del programma che si desidera installare sul computer. Sono possibili tre opzioni:

Completa. Selezionando questa opzione, si installano tutti i componenti di Kaspersky Internet Security. Per vedere la fase successiva dell'installazione, cfr. Passaggio 7.

Personalizzata. Questa opzione consente di selezionare i componenti del programma che si desidera installare. Per ulteriori informazioni, cfr. Passaggio 6.

Funzioni antivirus. Questa opzione consente di installare solo i componenti che proteggono il computer dai virus. Anti-Hacker, Anti-Spam e Anti-Spy non saranno installati.

Per selezionare un tipo di installazione, fare clic sul pulsante appropriato.

Passaggio 6. Scelta dei componenti da installare

Questa fase si presenta solo se è stata selezionata l'opzione **Personalizzata**.

Se è stata selezionata l'installazione personalizzata, è necessario selezionare i componenti di Kaspersky Internet Security che si desidera installare. Le selezioni predefinite includono tutte le funzioni antivirus e i componenti di scansione antivirus. Anti-Hacker, Anti-Spam e Anti-Spy non vengono installati.

Per selezionare i componenti desiderati, fare clic con il pulsante destro del mouse sull'icona a fianco del nome di un componente e selezionare **Installare sul disco fisso** dal menu contestuale. Ulteriori informazioni sul tipo di protezione offerto da un determinato componente e sulla quantità di spazio su disco necessario per l'installazione sono disponibili nella parte inferiore della finestra del programma di installazione.

Se non si desidera installare un componente, selezionare **Questa funzionalità non sarà più disponibile** dal menu contestuale. Ricordare che, scegliendo di non installare un componente, ci si priva di un elemento di protezione da una vasta gamma di programmi pericolosi.

Dopo aver selezionato i componenti da installare, fare clic su **Avanti**. Per tornare all'elenco dei programmi predefiniti da installare, fare clic su **Reset**.

Passaggio 7. Disabilitazione della firewall di Microsoft Windows

Questa fase viene visualizzata solo se si sta installando Kaspersky Internet Security su un computer con la firewall abilitata e si è scelto di installare anche Anti-Hacker.

In questa fase, Kaspersky Internet Security chiede se si desidera disabilitare la firewall di Windows poiché Anti-Hacker, incluso in Kaspersky Internet Security, offre una protezione firewall completa e non richiede quindi ulteriori protezioni da parte del sistema operativo.

Se si desidera utilizzare Anti-Hacker come firewall predefinita, fare clic su **Avanti**. La firewall di Windows viene disabilitata automaticamente.

Se invece si desidera mantenere e utilizzare la firewall di Windows, selezionare **Mantieni firewall Windows abilitata**. Se si seleziona questa opzione, Anti-Hacker sarà installato ma disabilitato per evitare conflitti tra programmi.

Passaggio 8. Ricerca di programmi che interferiscono con la corretta installazione

In questa fase viene visualizzato un elenco di tutti i programmi in esecuzione sul computer. Se vi sono programmi aperti che potrebbero interferire con l'installazione di Kaspersky Internet Security, i loro nomi appaiono visualizzati sullo schermo. Il programma chiede se si desidera chiuderli e proseguire l'installazione.

Uno di questi programmi potrebbe essere Microsoft Office Outlook che, se aperto durante l'installazione di Kaspersky Internet Security, potrebbe ostacolare la corretta installazione di Anti-Spam. Durante l'installazione di questo componente, l'installer crea un plug-in per Microsoft Office Outlook, utilizzabile per "istruire" Anti-Spam con i messaggi e-mail presenti nella mailbox e per perfezionare l'intercettazione e l'elaborazione dello spam.

Dopo aver chiuso questi programmi, fare clic sul pulsante **Avanti** per proseguire l'installazione.

Passaggio 9. Ricerca di altri programmi antivirus

In questa fase, l'installer cerca altri programmi antivirus presenti sul computer, compresi altri prodotti Kaspersky Lab, che potrebbero provocare problemi di compatibilità con Kaspersky Internet Security.

Se l'installer individua questo tipo di programmi, ne visualizza un elenco sul video. Il programma chiede se si desidera disinstallarli prima di proseguire l'installazione.

È possibile selezionare la disinstallazione manuale o automatica nell'elenco delle applicazioni antivirus individuate.

Se l'elenco dei programmi antivirus contiene Kaspersky Anti-Virus® Personal o Kaspersky Anti-Virus® Personal Pro, si raccomanda di salvare le chiavi di licenza utilizzate prima di eliminarle. Esse infatti possono essere utilizzate anche per Kaspersky Internet Security 6.0. Si raccomanda inoltre di salvare gli oggetti della Quarantena e del Backup. Essi saranno trasferiti automaticamente nelle aree Quarantena e Backup di Kaspersky Internet Security da dove è possibile continuare a usarli.

Per continuare l'installazione fare clic su **Avanti**.

Passaggio 10. Completamento dell'installazione

In questa fase, il programma chiede di completare l'installazione del programma sul computer. Si può decidere di utilizzare le impostazioni di protezione, gli elenchi delle minacce e il database di Anti-Spam eventualmente salvati da una precedente versione di Kaspersky Internet Security (per esempio nel caso in cui si fosse installata la versione beta e si stesse passando alla versione commerciale).

Esaminiamo in dettaglio le opzioni sopra descritte.

Se precedentemente era stata installata sul computer un'altra versione o build di Kaspersky Internet Security salvandone le firme al momento della disinstallazione, è possibile utilizzarle anche nella nuova versione. Affinché ciò sia possibile, selezionare **Elenchi delle minacce**. In questo caso, gli elenchi delle minacce inclusi nell'installazione del programma non saranno copiati.

Per utilizzare le impostazioni di protezione configurate e salvate da una versione precedente, selezionare **Impostazioni di protezione**.

Si raccomanda inoltre di usare il database di Anti-Spam eventualmente salvato al momento di disinstallare la versione precedente del programma. In tal modo non sarà necessario istruire nuovamente Anti-Spam. Per utilizzare il database già creato in precedenza, selezionare **Database di Anti-Spam**.

Per continuare l'installazione fare clic su **Avanti**.

Passaggio 11. Lettura delle informazioni importanti sul programma

In questa fase, l'installer chiede se si desidera consultare le informazioni importanti relative al programma prima di iniziare a usare Kaspersky Internet Security. Questa finestra di dialogo riporta le funzioni di base di Kaspersky Internet Security, alcuni dati sul suo funzionamento, ecc.

Per passare alla fase successiva, fare clic sul pulsante **Avanti**.

Passaggio 12. Completamento della procedura di installazione

La finestra **Installazione completata** contiene informazioni su come portare a termine la procedura di installazione di Kaspersky Internet Security.

Per completare correttamente l'installazione è necessario riavviare il computer, seguendo il suggerimento del messaggio visualizzato sullo schermo. Dopo il riavvio del sistema, si apre automaticamente la finestra della procedura di ipostazione guidata di Kaspersky Internet Security.

Se non è richiesto il riavvio del sistema, fare clic su **Avanti** per passare alla procedura di impostazione guidata.

3.2. Impostazione guidata

La procedura di impostzione guidata di Kaspersky Internet Security 6.0 inizia al termine dell'installazione del programma e serve per agevolare la configurazione delle impostazioni iniziali del programma in base alle caratteristiche e agli usi del computer.

L'interfaccia della procedura guidata è analoga a quelle delle procedure guidate standard di Windows e consiste di una serie di passaggi tra i quali è possibile spostarsi per mezzo dei pulsanti **Indietro** e **Avanti**, o che è possibile portare a termine facendo clic sul pulsante **Fine.** Il pulsante **Annulla** serve per interrompere in qualsiasi momento la procedura.

È possibile omettere questa fase iniziale di impostazione durante l'installazione del programma chiudendo la finestra della procedura guidata. Sarà possibile eseguirla di nuovo in seguito dall'interfaccia del programma se si ripristinano le impostazioni predefinite di Kaspersky Internet Security (cfr. 6.6 a pag. 87).

3.2.1. Uso di oggetti salvati con la versione 5.0

Questa finestra si apre durante la procedura guidata se in precedenza si era installato Kaspersky Anti-Virus 5.0 sul computer salvandone Quarantena, Backup, licenza, impostazioni e oggetti al momento della disinstallazione.

Per utilizzare questi oggetti nella versione 6.0, selezionare le caselle appropriate.

3.2.2. Attivazione del programma

È possibile attivare il programma installando una chiave di licenza che Kaspersky Internet Security utilizzerà per verificare il contratto di licenza e determinarne la data di scadenza.

La chiave di licenza contiene informazioni di sistema necessarie per il corretto funzionamento del prodotto, oltre a informazioni relative a:

- Assistenza (chi la fornisce e come ottenerla)
- Nome, numero e data di scadenza della licenza

Attenzione!

Per attivare il programma è necessario disporre di una connessione Internet. Se durante l'installazione del programma non si è connessi a Internet, è possibile attivarlo (cfr. 17.5 a pag. 254) in seguito dall'interfaccia del programma stesso.

3.2.2.1. Scelta di un metodo di attivazione del programma

A seconda che si disponga di una chiave di licenza per Kaspersky Internet Security o sia necessario scaricarne una dal server Kaspersky Lab, è possibile scegliere varie opzioni di attivazione del programma:

- **Attivazione per mezzo di un codice**. Selezionare questa opzione di attivazione se è stata acquistata la versione completa del programma con codice di attivazione in dotazione. Questo codice consente di ottenere una chiave di licenza che garantisce l'accesso completo a tutte le funzionalità del programma fino alla scadenza della licenza.
- **Attivazione della versione di prova (30 giorni).** Selezionare questa opzione di attivazione se si desidera installare la versione di prova del programma prima di decidere se acquistare la versione commerciale. In questo caso l'utente riceverà una chiave di licenza gratuita della durata di 30 giorni.
- **Uso di una chiave di licenza precedentemente ottenuta**. Selezionare questa opzione di attivazione se già si dispone di un file chiave di licenza per Kaspersky Internet Security 6.0.
- **Activazione successiva**. Selezionando questa opzione si omette la fase di attivazione. Kaspersky Internet Security 6.0 viene installato sul computer e si potrà accedere a tutte le funzioni del programma ad eccezione degli aggiornamenti (è possibile aggiornare gli elenchi delle minacce solo dopo l'installazione del programma).

3.2.2.2. Inserimento del codice di attivazione

Per attivare il programma è necessario inserire il codice di attivazione fornito all'acquisto.

Digitare le proprie generalità nella parte inferiore della finestra: Nome completo, indirizzo e-mail, Paese e città di residenza. Queste informazioni potrebbero essere necessarie per l'identificazione dell'utente registrato, per esempio in caso di smarrimento o di furto della chiave di licenza. In questo caso, è possibile ottenere una nuova chiave di licenza utilizzando le proprie informazioni personali.

3.2.2.3. Ottenimento di una chiave di licenza

La procedura guidata stabilisce il collegamento con i server Kaspersky Lab ai quali invia i dati di registrazione (il codice di attivazione e le informazioni personali), che saranno quindi esaminati sul sever stesso.

Se il codice di attivazione supera l'esame, l'applicazione riceve un file con la chiave di licenza. Se si installa la versione demo del programma (con un periodo di prova di 30 giorni), la procedura guidata riceve un file chiave di prova senza codice di attivazione.

Esso viene installato automaticamente e, al termine della procedura, si apre una finestra di completamento dell'attivazione contenente informazioni dettagliate sulla licenza.

Se il codice di attivazione non supera l'esame, si apre sullo schermo un messaggio che informa l'utente. In questo caso occorre rivolgersi al rivenditore presso il quale si è acquistato il programma per ulteriori informazioni.

3.2.2.4. Selezione di un file chiave di licenza

Se si dispone di un file chiave di licenza per Kaspersky Internet Security 6.0, la procedura guidata chiede se si desidera installarlo. Se sì, servirsi del pulsante **Sfoglia** per selezionare il percorso del file della chiave di licenza, riconoscibile dall'estensione *.key,* nella finestra di selezione.

Al termine della procedura di installazione della chiave, nella parte inferiore della finestra vengono visualizzate tutte le informazioni relative alla licenza. il nome dell'utente a cui è intestata la registrazione del software, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della chiave.

3.2.2.5. Completamento dell'attivazione del programma

La procedura di impostazione guidata informa l'utente che il programma è stato attivato correttamente. Vengono visualizzate inoltre informazioni relative alla chiave di licenza installata: il nome dell'utente a cui è intestata la registrazione del software, il numero della licenza, il tipo di licenza (completa, beta-testing, demo, ecc.), e la data di scadenza della licenza.

3.2.3. Configurazione delle impostazioni di aggiornamento

La sicurezza del computer dipende direttamente dall'aggiornamento regolare degli firme delle minacce e dei moduli del programma. In questa finestra, la procedura guidata chiede di selezionare una modalità di aggiornamento del programma e di configurare un piano di aggiornamento.

- **Automatico**. Kaspersky Internet Security copia e installa gli aggiornamenti man mano che vengono messi a disposizione sui server di aggiornamento. È la modalità predefinita.
- **Ogni 1 giorno/i**.Gli aggiornamenti vengono eseguiti automaticamente in base alla programmazione impostata. Per configurare la programmazione fare clic su **Modifica**.
- **Manuale**. Questa opzione consente di eseguire manualmente gli aggiornamenti.

Osservare che, al momento dell'installazione del programma, gli elenchi delle minacce e i moduli del programma in dotazione con il software possono essere ormai obsoleti. Per questo motivo si raccomanda di scaricare gli ultimi aggiornamenti del programma. A tal fine, fare clic su **Aggiorna ora**. Kaspersky Internet Security scarica quindi gli aggiornamenti necessari dai server remoti dedicati e li installa sul computer.

Per configurare gli aggiornamenti (impostare le proprietà di rete, selezionare la risorsa da cui scaricare gli aggiornamenti o il server di aggiornamento più vicino), fare clic su **Impostazioni**.

3.2.4. Programmazione delle scansioni antivirus

La scansione di aree selezionate del computer in cerca di oggetti nocivi è una delle fasi più importanti della protezione del computer.

Al momento dell'installazione di Kaspersky Internet Security, vengono create tre attività di scansione antivirus predefinite. In questa finestra, viene richiesto di scegliere un'impostazione per l'attività di scansione:

Esaminare gli oggetti all'avvio

- **Esegui all'avvio** – esamina automaticamente gli oggetti di avvio ogni volta che si accende il computer. Questo è il valore predefinito.
- **Esegui dopo ogni aggiornamento** – esamina automaticamente gli oggetti all'avvio dopo aver scaricato gli aggiornamenti del programma.

È possibile abilitare la scansione automatica degli oggetti all'avvio con qualsiasi opzione. A tal fine, selezionare le caselle corrispondenti all'opzione desiderata.

Scansione delle aree critiche

Per eseguire automaticamente la scansione antivirus delle aree critiche del sistema (memoria di sistema, oggetti all'avvio, settori di boot, cartelle di sistema di Windows) selezionare la casella corrispondente viruses

automatically, check the appropriate box. Per configurare la programmazione fare clic su **Modifica**.

Per impostazione predefinita, questa scansione automatica è disabilitata.

Scansione completa del computer

Per eseguire automaticamente una scansione completa del computer, selezionare la casella appropriata. Per configurare la programmazione fare clic su **Modifica**.

Per impostazione predefinita, l'esecuzione di questa attività in base alla programmazione è disabilitata. Tuttavia, si raccomanda di eseguire una scansione completa del computer subito dopo l'installazione del programma.

3.2.5. Restrizioni di accesso al programma

Poiché è possibile che più persone facciano uso di uno stesso computer (famigliari, per esempio) senza essere necessariamente utenti avanzati, e poiché è possibile disabilitare la protezione per mezzo di programmi nocivi, esiste un'opzione di protezione dell'accesso a Kaspersky Internet Security mediante password. L'uso di una password è utile per proteggere il programma da tentativi non autorizzati di disabilitare la protezione o modificare le impostazioni.

Per abilitare la protezione con password, selezionare **Abilita protezione con password** e compilare i campi **Digita password** e **Conferma password**.

Selezionare sotto l'area alla quale si desidera applicare la protezione con password:

- **Tutte le funzioni (ad eccezione dei prompt).** Richiede la password se l'utente cerca di eseguire qualsiasi azione con il programma, ad eccezione delle risposte alle notifiche in caso di rilevamento di oggetti pericolosi.
- **Funzioni selezionate:**
  - **Salvataggio impostazioni** – richiede la password quando un utente cerca di salvare delle modifiche alle impostazioni del programma.
  - **Uscita applicazione** – richiede la password se un utente cerca di chiudere il programma.
  - **Interruzione / pausa attività** – richiede la password se l'utente cerca di sospendere o disabilitare qualsiasi componente di protezione o attività di scansione antivirus.

3.2.6. Configurazione delle impostazioni di Anti-Hacker

Anti-Hacker è il componente di Kaspersky Internet Security che protegge il computer sulle reti locali e durante la navigazione in Internet. In questa fase, la procedura di configurazione guidata chiede di creare un elenco di regole per guidare Anti-Hacker durante l'analisi dell'attività di rete del computer.

3.2.6.1. Determinazione dello status di una zona di sicurezza

In questa fase, la procedura guidata analizza l'ambiente di rete del computer. In base a questa analisi, l'intero spazio di rete viene suddiviso in zone:

Internet – il World Wide Web. In questa zona, Kaspersky Internet Security agisce come una firewall personale. Così facendo, le regole predefinite di filtraggio pacchetti e delle applicazioni regolano l'intera attività di rete per garantire la massima sicurezza. Durante una sessione di lavoro in questa zona non è possibile modificare le impostazioni di protezione ma solo abilitare la modalità invisibile per una maggiore sicurezza del computer.

Zone di sicurezza – alcune zone, per lo più sottoreti delle quali fa parte il computer (per esempio sottoreti a casa o al lavoro). Per impostazione predefinita, queste zone sono definite "a medio rischio". È possibile modificare lo status di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole per il filtraggio pacchetti e le applicazioni.

Tutte le zone individuate vengono visualizzate in un elenco. Ciascuna di esse è accompagnata da una descrizione, dalla maschera dell'indirizzo e della sottorete, e dallo status con il quale ogni determinata attività di rete sarà autorizzata o bloccata da Anti-Hacker.

- **Internet**. È lo status predefinito assegnato a Internet, poiché durante la navigazione il computer è soggetto a tutti i tipi di minacce potenziali. Questo status è raccomandato anche per le reti non protette da programmi antivirus, firewall, filtri, ecc. Selezionando questo status, il programma garantisce la massima sicurezza durante l'uso di questa zona, in particolare:
    - Blocco di qualsiasi attività di rete NetBios all'interno della sottorete
    - Blocco delle regole delle applicazioni e di filtraggio dei pacchetti che consentono un'attività NetBios all'interno della sottorete

Anche se è stata creata una directory ad accesso libero, le informazioni in essa contenute saranno disponibili solo agli utenti di sottoreti con questo status. Inoltre, quando si seleziona questo status, non è possibile accedere a file e stampanti di altre reti di computer.

- **LAN**. Il programma assegna questo status alla maggior parte delle zone di sicurezza rilevate durante l'analisi dell'ambiente di rete del computer, con l'eccezione delle zone Internet. Si raccomanda di applicare questo status alle zone caratterizzate da un fattore di rischio medio (per esempio LAN aziendali). Selezionando questo status, il programma consente:
  - qualsiasi attività di rete NetBios all'interno della sottorete
  - regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBios all'interno della sottorete

  Selezionare questo status se si desidera garantire l'accesso a determinate cartelle del computer, bloccando al tempo stesso qualsiasi altra attività esterna. Gli utenti ai quali si desidera concedere l'accesso ai file del computer possono utilizzarli, ma non possono installare un troiano nel computer.
- **Affidabile (consenti tutte le connessioni)** – una rete che si ritiene assolutamente sicura per il computer, il quale non è soggetto ad attacchi e tentativi di accesso ai dati durante la sua presenza in tale rete. In questo caso, ogni attività di rete è consentita. Anche se in precedenza si è selezionato il massimo livello di protezione creando regole di blocco, questi sistemi di sicurezza non vengono applicati per i computer remoti provenienti da una rete affidabile.

Per una maggiore sicurezza durante l'uso di reti indicate come **LAN** o **Internet** è possibile attivare la *modalità invisibile*. Questa funzione consente esclusivamente le attività di rete avviate da utenti o applicazioni autorizzati. In altre parole, il computer diventa invisibile per il resto dell'ambiente. Questa modalità non pregiudica le prestazioni del computer su Internet.

La modalità invisibile è sconsigliata se il computer funziona da server (per esempio un server di posta o HTTP). In tal caso infatti i computer che si connettono al server non riuscirebbero a vederlo.

Per modificare lo status di una zona o abilitare/disabilitare la modalità invisibile, selezionarla dall'elenco e seguire i collegamenti appropriati nel riquadro **Descrizione regola** sotto l'elenco. È possibile eseguire attività simili e modificare indirizzi e maschere di sottoreti nella finestra **Impostazioni zona** che si apre facendo clic su **Modifica**.

È possibile aggiungere una nuova zona all'elenco durante la visualizzazione. A tal fine, fare clic su **Trova**. Anti-Hacker cerca le potenziali zone di registrazione,

chiedendo eventualmente di selezionare uno status da assegnare loro. È possibile inoltre aggiungere manualmente nuove zone all'elenco (per esempio se si connette il laptop a una nuova rete). Per fare questo, usare il pulsante **Aggiungi** e inserire le informazioni necessarie nella finestra **Impostazioni zona**.

Per eliminare una rete dall'elenco, fare clic sul pulsante **Elimina**.

3.2.6.2. Creazione di un elenco di applicazioni di rete

La procedura di configurazione guidata analizza il software installato sul computer e crea un elenco di applicazioni che usano una connessione di rete.

Anti-Hacker crea una regola volta a controllare l'attività di rete per ciascuna di queste applicazioni. Le regole vengono applicate in base a modelli per applicazioni comuni che usano connessioni di rete, creati da Kaspersky Lab e in dotazione con il software.

È possibile visualizzare l'elenco delle applicazioni di rete e le rispettive regole nella finestra delle impostazioni di Anti-Hacker, accessibile facendo clic su **Elenco**.

Per una maggiore sicurezza, è possibile disabilitare la funzione di cache DNS durante l'uso di risorse Internet. Questa funzione riduce drasticamente il tempo di connessione del computer alla risorsa Internet necessaria; al tempo stesso rappresenta però una pericolosa vulnerabilità, sfruttando la quale gli hacker possono creare falle di dati non individuabili per mezzo della firewall. Per questo motivo, per aumentare il livello di sicurezza del computer, si raccomanda di disabilitare questa funzione e di non salvare informazioni sui nomi dei domini nella cache (questa impostazione è selezionata per default).

3.2.7. Selezione di una modalità di sicurezza

In questa finestra, la procedura guidata chiede di selezionare la modalità di sicurezza da applicare al programma:

Base. È l'impostazione predefinita, studiata per utenti dotati di scarsa esperienza con il computer o con l'uso di software antivirus. Essa imposta tutti i componenti del programma sui livelli di sicurezza raccomandati e informa l'utente solo in caso di eventi pericolosi, per esempio l'intercettazione di codici nocivi o l'esecuzione di azioni rischiose.

Interattiva. Questa modalità offre una protezione dei dati del computer più personalizzata rispetto alla modalità Base. Essa è in grado di intercettare tentativi di modifica delle impostazioni di sistema, attività sospette a livello di

sistema e attività non autorizzate a livello di rete. Tutte le attività sopra elencate possono indicare la presenza di programmi nocivi o semplicemente dipendere da attività standard di programmi in uso sul computer. Spetta all'utente stabilire per ogni singolo caso se consentire o bloccare tali attività.
Se si sceglie questa modalità, occorre specificare quando applicarla:

- **Abilita modalità di training Anti-Hacker** – viene chiesto l'intervento dell'utente ogni volta che i programmi installati sul computer cercano di connettersi a una determinata risorsa di rete. L'utente può consentire la connessione o bloccarla e configurare una regola Anti-Hacker per il programma in questione. Se si disabilita la modalità di training, Anti-Hacker funziona con un livello di protezione minimo, vale a dire che consente a tutte le applicazioni di accedere alle risorse di rete.

Se il computer utilizzato esegue Microsoft Windows XP Professional x64 Edition, le impostazioni elencate di seguito per l'interattività non saranno disponibili.

- **Abilita monitoraggio del registro di sistema** – viene richiesto l'intervento dell'utente ogni volta che si rilevano tentativi di modificare le chiavi del registro di sistema.
- **Abilita difesa proattiva estesa** – questa modalità analizza tutte le attività sospette delle applicazioni del sistema, compresi l'apertura di un browser con impostazioni di riga di comando, inserimenti in processi di applicazioni e intercettori di hook di finestre (disabilitati per impostazione predefinita).

3.2.8. Completamento della procedura di configurazione guidata

L'ultima finestra della procedura guidata chiede se si desidera riavviare il computer per completare l'installazione del programma. Il riavvio è necessario affinché i driver di alcuni componenti di Kaspersky Internet Security vengano registrati correttamente.

È possibile posticipare il riavvio, ma in tal caso alcuni componenti del programma non funzioneranno.

CAPITOLO 4. INTERFACCIA DEL PROGRAMMA

Kaspersky Internet Security è dotato di un'interfaccia semplice e intuitiva. Questo capitolo ne descrive le caratteristiche principali:

- Icona della barra delle applicazioni (cfr. 4.1 a pag. 47)
- Menu contestuale (cfr. 4.2 a pag. 48)
- Finestra principale (cfr. 4.3 a pag. 49)
- Finestra delle impostazioni del programma (cfr. 4.4 a pag. 52)

Oltre all'interfaccia principale del programma, vi sono plugin per le seguenti applicazioni:

- Microsoft Office Outlook – scansioni antivirus (cfr. 8.2.2 a pag. 108) e scansioni antispam (cfr. 13.3.9 a pag. 194)
- Outlook Express (cfr. 13.3.10 a pag. 198)
- The Bat! – scansioni antivirus (cfr. 8.2.3 a pag. 110) e scansioni antispam (cfr. 13.3.11 a pag. 199)
- Microsoft Internet Explorer (cfr. Capitolo 11 a pag. 141)
- Microsoft Windows Explorer (cfr. 14.2 a pag. 202)

I plug-in estendono le funzionalità di questi programmi consentendo la gestione e l'impostazione di Kaspersky Internet Security dalle loro interfacce.

4.1. L'icona della barra delle applicazioni

Subito dopo l'installazione di Kaspersky Internet Security, nella barra delle applicazioni viene visualizzata un'iconache funge da indicatore delle funzioni di Kaspersky Internet Security e che riflette lo stato della protezione e mostra una serie di funzioni di base eseguite dal programma.

Se l'icona è attiva  (colorata), il computer è protetto. Se l'icona è inattiva  (bianco e nero), la protezione è stata disabilitata oppure alcuni dei componenti di protezione (cfr. 2.2.1 a pag. 25) sono stati messi in pausa.

L'icona di Kaspersky Internet Security cambia in relazione all'operazione eseguita:

 Scansione posta elettronica.

 Scansione degli script.

 Scansione in corso di un file in fase di apertura, salvataggio o esecuzione da parte dell'utente o di un programma.

 Gli elenchi delle minacce di Kaspersky Internet Security e i moduli del programma sono in fase di aggiornamento.

L'icona consente inoltre di accedere alle funzioni di base dell'interfaccia del programma: il menu contestuale (cfr. 4.2 a pag. 48) e la finestra principale (cfr. 4.3 a pag. 49).

Per aprire il menu contestuale, fare clic con il pulsante destro del mouse sull'icona del programma.

Per aprire la finestra principale di Kaspersky Internet Security nella sezione **Protezione** (la prima schermata predefinita del programma), fare doppio clic sull'icona del programma. Se si fa clic una volta sola, la finestra principale si apre sulla sezione che era attiva l'ultima volta che il programma è stato chiuso.

4.2. Il menu contestuale

È possibile eseguire semplici attività di protezione dal menu contestuale (cfr. Figura 1).

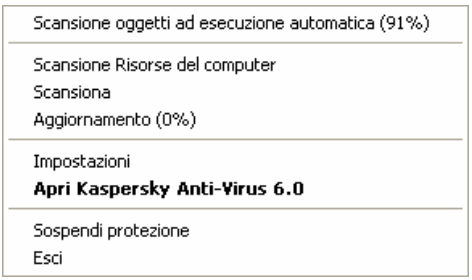


Figura 1. Il menu contestuale

Il menu di Kaspersky Internet Security contiene i seguenti elementi:

Scansione Risorse del computer – avvia una scansione completa del computer in cerca di oggetti pericolosi. Durante l'operazione vengono esaminati i file di tutte le unità, inclusi i supporti di archiviazione esterni.

Scansiona – seleziona gli oggetti e ne esegue la scansione antivirus. L'elenco predefinito contiene una serie di file come quelli della cartella **Documenti**, la cartella Avvio, i database di posta, tutte le unità del computer, ecc. È possibile aggiungere elementi all'elenco, selezionare file da esaminare e avviare scansioni antivirus.

Aggiornamento – consente di scaricare gli aggiornamenti dei moduli del programma e gli elenchi delle minacce di Kaspersky Internet Security, e di installarli sul computer.

Network Monitor – consente di visualizzare l'elenco delle connessioni di rete stabilite, delle porte aperte e del traffico.

Attiva – serve per attivare il programma. Questo elemento di menu è disponibile solo se il programma non è attivato.

Impostazioni – consente di visualizzare e configurare le impostazioni di Kaspersky Internet Security.

Apri Kaspersky Internet Security 6.0 – apre la finestra principale del programma (cfr. 4.3 a pag. 49).

Sospendi protezione / Riprendi protezione – disabilita temporaneamente o abilita i componenti della protezione (cfr. 2.2.1 a pag. 25). Questo elemento di menu non influisce sugli aggiornamenti del programma o sulle attività di scansione antivirus.

Esci – chiude Kaspersky Internet Security.

Durante un'attività di scansione antivirus, il menu contestuale visualizza il nome dell'attività accompagnato da un indicatore della percentuale di avanzamento. Selezionando l'attività, è possibile portarsi sulla finestra dei report per visualizzare i risultati correnti.

4.3. La finestra principale del programma

La finestra principale di Kaspersky Internet Security (cfr. Figura 2) è caratterizzata da un'interfaccia semplice e intuitiva per interagire con il programma. Essa può essere suddivisa in due parti:

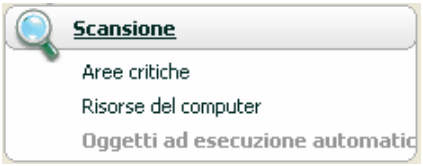
- La parte sinistra della finestra, il pannello di navigazione, consente di aprire in maniera semplice e veloce qualsiasi componente e di visualizzare i risultati di scansioni antivirus o gli strumenti di supporto del programma;

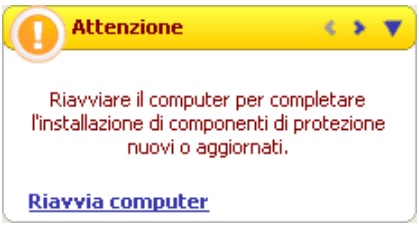
- La parte destra della finestra, il pannello informativo, contiene informazioni sul componente di protezione selezionato nella parte sinistra della finestra e visualizza le impostazioni dei componenti, fornendo gli strumenti per effettuare scansioni antivirus, lavorare con i file in quarantena e le copie di backup, gestire le chiavi di licenza, ecc.

Figura 2. La finestra principale di Kaspersky Internet Security

Dopo aver selezionato una sezione o un componente nella parte sinistra della finestra, nella parte destra vengono visualizzate le informazioni relative alla selezione.

Esaminiamo adesso gli elementi del pannello di navigazione della finestra principale.

Sezione della finestra principale	Scopo
Questa finestra fornisce principalmente informazioni sullo stato di protezione del computer. La sezione **Protezione** è progettata esattamente per questo. 	Vi si trovano informazioni sulle operazioni di Kaspersky Internet Security: verificare che tutti i componenti funzionino correttamente ed esaminare le statistiche generali. Da qui è possibile inoltre abilitare/disabilitare i componenti di protezione. Per visualizzare statistiche e impostazioni di un componente di protezione specifico, è sufficiente selezionare il nome del componente sul quale si desidera ottenere informazioni nella sezione **Protezione**.
Per effettuare la scansione del computer in cerca di file o programmi nocivi, usare la sezione speciale **Scansione** nella finestra principale. 	Questa sezione contiene un elenco di oggetti che possono essere sottoposti a scansione antivirus. In questa sezione è possibile anche creare attività di scansione antivirus che saranno visualizzate nel pannello di navigazione. Questa funzione semplifica considerevolmente l'avvio delle scansioni antivirus. Le attività che, secondo gli esperti Kaspersky Lab, è necessario eseguire con maggiore frequenza, sono configurate e incluse nella sezione. Tra queste vi sono le attività di scansione antivirus delle aree critiche, dei programmi all'avvio e le scansioni complete del computer.

La sezione **Strumenti** comprende ulteriori funzioni di Kaspersky Internet Security. 	Qui è possibile aggiornare il programma, configurare le impostazioni dello strumento Aggiorna distribuzione per i computer della rete, visualizzare i report sulle prestazioni di qualsiasi componente di Kaspersky Internet Security, lavorare con gli oggetti contenuti nella cartella di Quarantena e lecopie di backup, controllare le informazioni di supporto tecnico, creare il disco di emergenza, e gestire le chiavi di licenza.
La sezione **Commenti e suggerimenti** accompagna l'utente durante l'uso del programma. 	In questa sezione è possibile leggere suggerimenti su come incrementare il livello di sicurezza del computer. Vi si trovano inoltre commenti sulle prestazioni correnti del programma e sulle sue impostazioni. Per mezzo dei link di questa sezione, è possibile eseguire le azioni raccomandate per una sezione particolare o visualizzare informazioni più dettagliate.

Ogni elemento del pannello di navigazione è accompagnato da uno speciale menu contestuale. Esso contiene punti per i componenti di protezione e strumenti che agevolano l'utente nella configurazione e gestione dei componenti e nella visualizzazione dei report. Esiste un ulteriore elemento di menu per le attività di scansione antivirus, utilizzabile per creare la propria attività sulla base di una selezionata.

È possibile anche modificare l'aspetto del programma creando e utilizzando una grafica e uno schema cromatico personalizzati.

4.4. Finestra delle impostazioni del programma

La finestra delle impostazioni di Kaspersky Internet Security (cfr. 4.3 a pag. 49) può essere aperta dalla finestra principale facendo clic su Impostazioni nella parte superiore.

La finestra delle impostazioni (cfr. Figura 3) ha la stessa struttura della finestra principale:

- La parte sinistra della finestra consente di accedere in maniera facile e veloce alle impostazioni di ciascun componente del programma, alle attività di scansione antivirus e agli strumenti del programma;
- La parte destra della finestra contiene un elenco di impostazioni del componente, attività, ecc., selezionato nella parte sinistra della finestra.

Quando si seleziona qualsiasi sezione, componente o attività nella parte sinistra della finestra delle impostazioni, la parte destra ne visualizza le impostazioni di base. Per configurare le impostazioni avanzate, è possibile aprire le finestre delle impostazioni di secondo e terzo livello. Per una descrizione dettagliata delle impostazioni del programma, consultare le sezioni corrispondenti del manuale dell'utente.

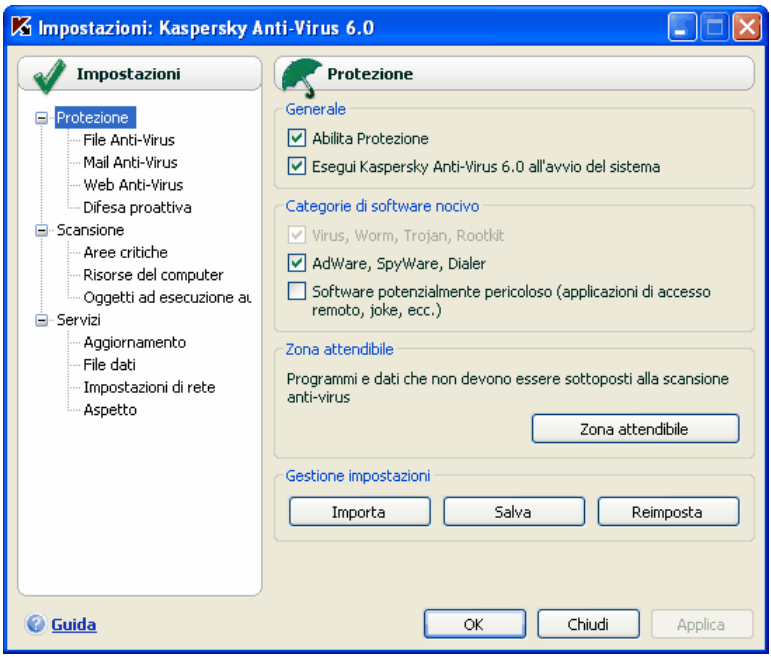


Figura 3. La finestra delle impostazioni di Kaspersky Internet Security

CAPITOLO 5. GUIDA INTRODUTTIVA

Uno dei principali obiettivi di Kaspersky Lab con Kaspersky Internet Security era fornire una configurazione ottimale per tutte le opzioni del programma. Ciò consente agli utenti a qualsiasi livello di conoscenza del computer di proteggere il PC subito dopo l'installazione, senza sprecare tempo con la configurazione.

È possibile tuttavia che il computer o il tipo di lavoro per il quale lo si utilizza richiedano delle configurazioni specifiche. Ecco perché si raccomanda di eseguire una configurazione preliminare in modo da ottenere l'approccio più flessibile e personalizzato possibile alla protezione del computer.

Per facilitare al massimo la messa in funzione del programma, abbiamo combinato tutte le fasi di configurazione preliminare in una procedura di configurazione guidata (cfr. 3.2 a pag. 37) che si avvia al termine dell'installazione del programma. Seguendo le istruzioni della procedura guidata è possibile attivare il programma, configurare le impostazioni degli aggiornamenti e delle scansioni antivirus, proteggere l'accesso al programma mediante password e configurare Anti-Hacker in modo da soddisfare i requisiti della rete.

Dopo aver installato e avviato il programma, si raccomanda di eseguire i seguenti passaggi:

- Controllare lo stato corrente della protezione (cfr. 5.1 a pag. 54) per garantire che Kaspersky Internet Security funzioni al livello appropriato.
- Configurare le regole di Anti-Hacker (cfr. 5.2 a pag. 60) per i programmi che richiedono una connessione di rete.
- "Istruire" Anti-Spam (cfr. 5.6 a pag. 64) in base alle e-mail ricevute.
- Aggiornare il programma (cfr. 5.7 a pag. 65) (se la procedura guidata non ha provveduto automaticamente dopo l'installazione del programma).
- Eseguire la scansione antivirus del computer (cfr. 5.3 a pag. 61).

5.1. Come determinare lo stato della protezione del computer

La finestra principale di Kaspersky Internet Security nella sezione **Protezione** riporta informazioni globali sulla protezione del computer. Lo *stato corrente della*

protezione del computer e le *statistiche generali delle prestazioni* del programma sono visualizzati lì.

Status protezione visualizza lo stato corrente della protezione del computer per mezzo di speciali indicatori (cfr. 5.1.1 a pag. 55). Le Statistiche (cfr. 5.1.2 a pag. 58) contengono i dati relativi all'operazione corrente del programma.

5.1.1. Indicatori della protezione

Lo **Status protezione** è determinato da tre indicatori che riflettono il grado di protezione del computer in un momento dato e mostrano eventuali problemi nelle impostazioni del programma e nel suo funzionamento.

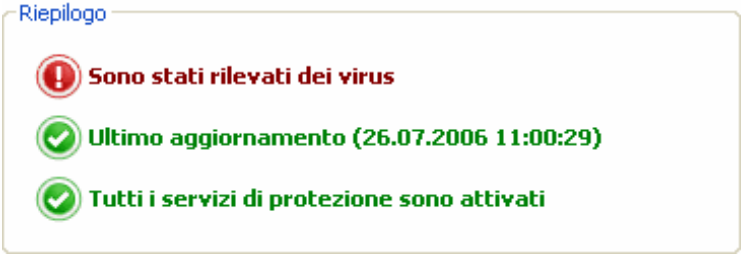


Figura 4. Gli indicatori che riflettono lo stato di protezione del computer

Il grado di importanza degli eventi riportato dall'indicatore può avere uno dei seguenti valori:

– *l'indicatore è di natura informativa*; esso consente di sapere che il livello di protezione del computer è corretto e che non sono stati rilevati problemi di impostazione o di funzionamento del programma o dei suoi componenti.

– *l'indicatore richiama l'attenzione su diverse deviazioni* di funzionamento di Kaspersky Internet Security rispetto al livello di prestazioni raccomandato, con potenziali conseguenze sulla sicurezza dei dati. Prestare attenzione alle raccomandazioni degli esperti di Kaspersky Lab. Le azioni raccomandate sono indicate in forma di collegamenti.

– *l'indicatore riflette situazioni critiche* nella protezione del computer. Seguire attentamente le raccomandazioni. Esse infatti sono tutte volte a garantire una protezione ottimale del computer. Le azioni raccomandate sono indicate in forma di collegamenti.

Esaminiamo adesso gli indicatori della protezione e le situazioni che ciascuno di essi riflette.

Il primo indicatore segnala la presenza di file e programmi nocivi nel computer. L'indicatore può assumere uno dei seguenti valori:

Nessun oggetto nocivo rilevato

Kaspersky Internet Security non ha rilevato alcun file o programma pericoloso nel computer.

Tutti gli oggetti nocivi riparati

Kaspersky Internet Security ha trattato tutti i file e programmi infetti da virus e ha eliminato quelli impossibili da trattare.

Attacco hacker bloccato

Kaspersky Internet Security ha intercettato e bloccato un tentativo di attacco alla rete.

Sono state rilevate minacce

Il computer è a rischio di infezione. Kaspersky Internet Security ha individuato programmi nocivi (virus, troiani, worm, ecc.) che è necessario neutralizzare. Per fare ciò, utilizzare il collegamento Neutralizza tutto. Fare clic sul collegamento Dettagli per visualizzare informazioni più particolareggiate sugli oggetti nocivi.

Necessario riavviare il computer

Per trattare i file o programmi nocivi è necessario riavviare il computer. Salvare e chiudere i file sui quali si sta lavorando e usare il collegamento Riavvia computer.

Il secondo indicatore mostra il livello di efficacia della protezione del computer. L'indicatore può assumere uno dei seguenti valori:

Le firme sono caricate (data, ora)

Il programma non necessita di aggiornamenti. Tutti i database utilizzati da Kaspersky Internet Security eseguono le firme correnti per la protezione del computer.

Le firme non sono aggiornate

I moduli del programma e il database di Kaspersky Internet Security non vengono aggiornati da diversi giorni. L'utente corre il rischio di infettare il computer con nuovi programmi nocivi apparsi dopo l'ultimo aggiornamento del programma. Si raccomanda caldamente di aggiornare Kaspersky Internet

Security. Per fare ciò, utilizzare il collegamento Aggiorna.

Necessario riavviare il computer

Per garantire il corretto funzionamento del programma è necessario riavviare il sistema. Salvare e chiudere i file sui quali si sta lavorando e usare il collegamento Riavvia computer.

Le firme sono obsolete

Kaspersky Internet Security non è stato aggiornato per diverso tempo. I dati presenti nel computer corrono gravi rischi. Aggiornare il programma al più presto. Per fare ciò, utilizzare il collegamento Aggiorna.

Le firme sono danneggiate o parzialmente danneggiate

Gli elenchi delle minacce sono completamente o parzialmente danneggiati. Se ciò si verifica, si raccomanda di eseguire di nuovo l'aggiornamento del programma. Se si ripresenta lo stesso messaggio d'errore, rivolgersi al servizio di assistenza tecnica Kaspersky Lab.

Il terzo indicatore riflette la funzionalità corrente del programma. L'indicatore può assumere uno dei seguenti valori:

Tutti i componenti della protezione sono abilitati

Kaspersky Internet Security protegge il computer su tutti i canali attraverso i quali potrebbero penetrare programmi nocivi. Tutti i componenti della protezione sono abilitati.

Protezione non installata

Al momento dell'installazione di Kaspersky Internet Security non è stato installato nessuno dei componenti di monitoraggio. Questo significa che è possibile solo eseguire la scansione antivirus. Per la massima sicurezza è necessario installare i componenti di protezione sul computer.

Alcuni componenti di protezione sono sospesi

Uno o più componenti di protezione sono stati sospesi. Per ripristinare il componente disattivato, selezionarlo dall'elenco e fare clic su ▶.

Tutti i componenti della protezione sono sospesi

Tutti i componenti di protezione sono stati sospesi. Per ripristinare i componenti, selezionare **Riprendi protezione** dal menu contestuale facendo clic sull'icona della barra delle applicazioni.

Alcuni componenti di protezione sono interrotti

Uno o più componenti di protezione sono stati interrotti. In conseguenza di questo dato, il computer potrebbe infettarsi provocando la perdita di dati. Si raccomanda vivamente di abilitare la protezione. A tal fine, selezionare un componente attivo dall'elenco e fare clic su ▶.

Tutti i componenti della protezione sono interrotti

La protezione è completamente disabilitata. Nessun componente di protezione è in funzione. Per ripristinare i componenti, selezionare **Riprendi protezione** dal menu contestuale facendo clic sull'icona della barra delle applicazioni.

Alcuni componenti di protezione hanno provocato un errore

Uno o più componenti di Kaspersky Internet Security hanno provocato un errore. Si raccomanda in questo caso di abilitare i componenti interessati o di riavviare il computer (è possibile che i driver dei componenti debbano essere registrati dopo l'aggiornamento).

5.1.2. Status dei componenti di Kaspersky Internet Security

Per capire in che modo Kaspersky Internet Security sta proteggendo file system, e-mail, traffico HTTP e altre aree a rischio, o per visualizzare le attività di scansione antivirus o l'avanzamento dell'aggiornamento delle firme, è sufficiente aprire la sezione corrispondente della finestra principale del programma.

Per esempio, per visualizzare lo stato corrente di File Anti-Virus, selezionare **File Anti-Virus** dalla parte sinistra della finestra principale e, per vedere se il computer è protetto dai nuovi virus, selezionare **Difesa proattiva**. La parte destra della finestra visualizzerà informazioni complete sul funzionamento del componente.

Per i componenti di protezione, essa è suddivisa in **barra di stato**, casella **Stato** (**Impostazioni** nel caso delle attività di scansione antivirus e di aggiornamento) e casella **Statistiche**.

Consideriamo File Anti-Virus come esempio di *barra di stato*:

- *File Anti-Virus: In funzione* – la protezione dei file è attiva al livello selezionato (cfr. 7.1 a pag. 91).
- *File Anti-Virus: In pausa* – File Anti-Virus è temporaneamente disabilitato. Il componente ricomincerà a funzionare automaticamente alla scadenza del periodo stabilito o dopo aver riavviato il programma. La protezione dei file può anche essere ripristinata manualmente facendo clic sul pulsante ▶ ubicato sulla barra di stato.
- *File Anti-Virus: Interrotto* – il componente è stato interrotto dall'utente. La protezione dei file può essere ripristinata manualmente facendo clic sul pulsante ▶ ubicato sulla barra di stato.
- *File Anti-Virus: Non in funzione* – la protezione dei file non è disponibile perché, per esempio, non si dispone di una chiave di licenza per il programma.
- *File Anti-Virus: Disabilitato (errore)* – il componente ha provocato un errore. Se ciò si verifica, rivolgersi al servizio di assistenza tecnica Kaspersky Lab.

Se il componente contiene più moduli, la sezione **Stato** conterrà informazioni sull'abilitazione di ciascuno di essi. Per i componenti non composti da moduli singoli, vengono visualizzati lo status, il livello di sicurezza e, per alcuni, la risposta ai programmi pericolosi.

La casella **Stato** non è disponibile per le attività di scansione antivirus e di aggiornamento. Il livello di sicurezza, l'azione applicata ai programmi pericolosi per le attività di scansione antivirus, e la modalità operativa per gli aggiornamenti sono elencati nel riquadro **Impostazioni**.

Il riquadro **Statistiche** contiene informazioni sul funzionamento dei componenti di protezione, gli aggiornamenti o le attività di scansione antivirus.

5.1.3. Statistiche sulle prestazioni del programma

Le **statistiche sul programma** sono accessibili nel riquadro **Statistiche** della sezione **Protezione** della finestra principale del programma e visualizzano informazioni di carattere generale sulla protezione del computer, a partire dall'installazione di Kaspersky Internet Security.

Figura 5. Il riquadro statistiche generali del programma

Fare clic con il pulsante sinistro del mouse su un punto qualsiasi del riquadro per visualizzare un report con informazioni dettagliate. Le schede visualizzano:

- Informazioni sugli oggetti trovati (cfr. 17.3.2 a pag. 241) e sullo status assegnato a ciascuno
- Registro degli eventi (cfr. 17.3.3 a pag. 241)
- Statistiche generali sulla scansione (cfr. 17.3.4 a pag. 243).
- Statistiche sulle prestazioni del programma (cfr. 17.3.5 a pag. 243)

5.2. Controllo integrità delle applicazioni

In questa fase, la procedura guidata di Kaspersky Internet Security analizza le applicazioni installate sul computer (file librerie dinamiche, firme digitali di fabbricazione), conta i file delle checksum delle applicazioni e crea un elenco di programmi attendibili dal punto di vista della sicurezza antivirus. Per esempio, questo elenco include automaticamente tutte le applicazioni con firma digitale di Microsoft.

In un momento successivo, Kaspersky Internet Security utilizzerà le informazioni ottenute analizzando la struttura dell'applicazione al fine di prevenire l'integrazione di codici maligni nei moduli dell'applicazione.

L'analisi delle applicazioni installate sul computer può richiedere qualche tempo.

5.3. Come creare regole antihacker

Generalmente, subito dopo l'avvio del sistema operativo, alcuni programmi presenti nel computer cercano di stabilire una connessione di rete con una determinata risorsa: MS Outlook cerca di connettersi con il server di posta per scaricare nuove e-mail, ICQ cerca di connettersi a Internet in modo da consentire la comunicazione con amici e colleghi, ecc.

Anti-Hacker tiene sotto controllo tutta l'attività di rete del computer. Kaspersky Internet Security contiene regole Anti-Hacker predefinite per la maggior parte delle applicazioni di sistema il cui funzionamento richiede una connessione di rete. In assenza di regole appropriate, Anti-Hacker informa l'utente che è stato rilevato un tentativo di stabilire una connessione con la rete da parte di un programma.

Se il computer si connette alla rete all'avvio del sistema, il programma informa l'utente e chiede si specificare se la rete è ritenuta affidabile.

I messaggi relativi all'attività di un determinato programma sul computer (cfr. Figura 6) contengono brevi informazioni sulla connessione e sulle opzioni di interazione con quel programma:

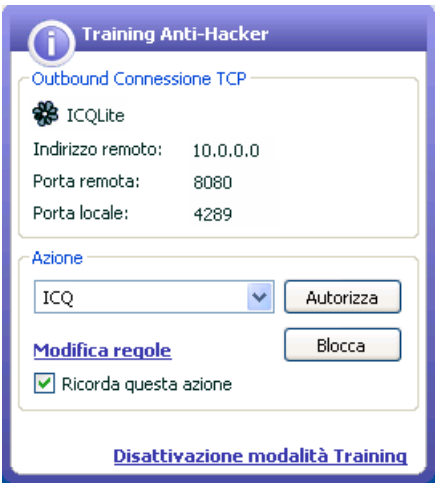


Figura 6. Informazione di Anti-Hacker relativa al rilevamento di attività di rete di ICQ

- Consenti attività di rete
- Blocca attività di rete
- Configura in dettaglio il comportamento di Anti-Hacker per questo programma

Se si desidera che Anti-Hacker ricordi l'azione prescelta, selezionare **Ricorda questa azione**. In seguito, quando il programma cerca di connettersi alla risorsa specificata con queste impostazioni, il componente non avvertirà più l'utente.

Se si desidera creare in un secondo momento le regole per i programmi installati nel computer, fare clic su Disable training mode. Così facendo, Anti-Hacker avvia la Modalità di protezione minima e consente ai programmi specificati di stabilire connessioni di rete o di caricare o scaricare pacchetti di dati dalla rete.

5.4. Come eseguire la scansione antivirus del computer

Dopo l'installazione, il programma comunica all'utente con un messaggio speciale che il computer non è ancora stato esaminato e raccomanda di eseguire immediatamente una scansione antivirus.

Kaspersky Internet Security include un'attività di scansione antivirus predefinita. Essa si trova nella finestra principale del programma nella sezione **Scansione**.

Dopo aver selezionato l'attività dal nome **Risorse del computer**, è possibile visualizzare le statistiche relative alla scansione più recente nella parte destra della finestra principale, oltre alle impostazioni dell'attività: il livello di protezione selezionato e le azioni da intraprendere nei confronti degli oggetti pericolosi.

Per eseguire la scansione del computer in cerca di programmi nocivi,

Fare clic sul pulsante **Scan** nella parte destra dello schermo.

Il programma avvia la scansione del computer visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.5. Come eseguire la scansione di aree critiche del computer

Vi sono aree del computer particolarmente critiche dal punto di vista della sicurezza. Esse sono prese di mira dai programmi nocivi volti a danneggiare il sistema operativo, il processore, la memoria, ecc.

È estremamente importante garantire la sicurezza di queste aree per il corretto funzionamento del computer. Abbiamo quindi programmato un'attività di scansione antivirus specifica per queste aree. Essa si trova nella finestra principale del programma nella sezione **Scansione**.

Dopo aver selezionato l'attività dal nome **Aree critiche**, è possibile visualizzare le statistiche relative alla scansione più recente di queste aree nella parte destra della finestra principale, oltre alle impostazioni dell'attività: il livello di protezione selezionato e le azioni da intraprendere incaso di minacce alla sicurezza. Da qui è possibile selezionare le aree critiche da esaminare e avviare immediatamente una scansione antivirus delle aree selezionate.

Per eseguire la scansione delle aree critiche del computer in cerca di programmi nocivi,

Fare clic sul pulsante **Scansione** nella parte destra dello schermo.

Il programma avvia la scansione delle aree selezionate visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.6. Come eseguire la scansione antivirus di un file, una cartella o un disco

Vi sono situazioni in è necessario eseguire la scansione antivirus di singoli oggetti anziché dell'intero computer, per esempio del disco fisso in cui si trovano programmi, giochi, database di posta portati a casa dall'ufficio, file archiviati ricevuti come allegati, ecc. È possibile selezionare l'oggetto da esaminare per mezzo degli strumenti standard del sistema operativo Windows (per esempio dalla finestra di **Explorer** o dal **Desktop**, ecc.).

Per eseguire la scansione di un oggetto,

posizionare il cursore sopra al nome dell'oggetto selezionato, aprire il menu contestuale di Windows facendo clic con il pulsante destro del mouse e selezionare **Scansione anti-virus** (cfr. Figura 7).

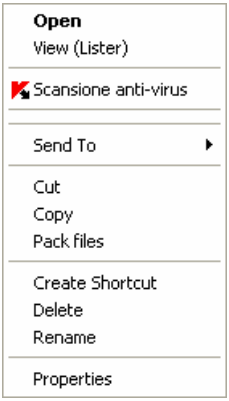


Figura 7. Scansione antivirus di un oggetto selezionato per mezzo degli strumenti di Windows

Il programma avvia quindi la scansione dell'oggetto selezionato visualizzando i dettagli in una finestra apposita. È possibile nascondere la finestra delle informazioni sulla scansione semplicemente chiudendola. La scansione non sarà interrotta.

5.7. Come istruire Anti-Spam

Una delle fasi essenziali prima di usare Anti-Spam consiste nell'istruire il programma sulla base delle e-mail. Lo spam è posta indesiderata, anche se è molto difficile stabilire cosa sia spam per ogni singolo utente. Naturalmente vi sono categorie di posta che possono essere definite spam con un elevato grado di precisione (per esempio il mass mailing, annunci pubblicitari, e-mail codificate in cinese), ma alcune di esse in realtà potrebbero essere gradite a determinati utenti.

Pertanto è necessario che ciascun utente stabilisca autonomamente quali tipi di messaggio rientrano tra lo spam e quali no. Dopo l'installazione, Kaspersky Internet Security chiede se si desidera addestrare Anti-Spam a distinguere tra spam e e-mail gradite. Ciò è possibile per mezzo degli appositi pulsanti che vengono integrati nel client di posta (Outlook, Outlook Express, The Bat!) oppure servendosi della procedura guidata di addestramento.

Attenzione!

Questa versione di Kaspersky Internet Security non offre plug-in Anti-Spam per le versioni a 64 bit dei client di posta elettronica Microsoft Office Outlook, Microsoft Outlook Express e The Bat!

Per istruire Anti-Spam con gli appositi pulsanti,

1. Aprire il client di posta predefinito del computer (p. es. Microsoft Office Outlook). Nella barra degli strumenti sono comparsi due pulsanti: **Spam** e **Accetta**.
2. Selezionare un messaggio o gruppo di messaggi contenente e-mail gradite e fare clic su **Accetta**. Da questo momento, le e-mail provenienti dagli indirizzi selezionati non saranno mai trattate come spam.
3. Selezionare un'e-mail considerata spam, un gruppo di e-mail o una cartella contenenti spam e fare clic su **Spam**. Anti-Spam analizza i contenuti di questi messaggi e in futuro considererà spam tutte le e-mail dai contenuti simili.

Per istruire Anti-Spam con la procedura guidata,

1. Selezionare Anti-Spam nella sezione **Protezione** della finestra principale del programma e fare clic su **Impostazioni**.

2. Nella parte destra della finestra delle impostazioni, fare clic su **Training Wizard**.
3. Nella prima fase, selezionare le cartelle del client di posta contenenti le e-mail non considerate spam. Fare clic sul pulsante **Avanti**.
4. Nella seconda fase, specificare le cartelle contenenti lo spam. Fare clic sul pulsante **Avanti**.

Il processo di addestramento si basa sulle cartelle specificate.

Quando un'e-mail arriva nella casella della posta in entrata, Anti-Spam ne analizza il contenuto e aggiunge la dicitura [Spam] alla riga dell'oggetto dei messaggi spam. È possibile configurare nel proprio client di posta una regola specifica per questi messaggi in modo da eliminarli o trasferirli in una cartella apposita.

5.8. Come aggiornare il programma

Kaspersky Lab aggiorna gli elenchi delle minacce di Kaspersky Internet Security e i moduli del programma per mezzo di appositi server di aggiornamento.

I server di aggiornamento di Kaspersky Lab sono siti Internet di Kaspersky Lab Internet in cui vengono archiviati gli aggiornamenti dei programmi.

Attenzione!

Per aggiornare Kaspersky Internet Security è necessario disporre di un collegamento Internet.

Kaspersky Internet Security verifica automaticamente la presenza di aggiornamenti sui server di Kaspersky Lab servers. Se Kaspersky Lab ha reso pubblici degli aggiornamenti del programma, Kaspersky Internet Security li scarica e li installa in modalità invisibile.

Per aggiornare Kaspersky Internet Security manualmente,

Selezionare il componente **Aggiornamenti** nella sezione **Servizi** della finestra principale del programma e fare clic sul pulsante **Aggiorna subito!** nella parte destra della finestra.

Kaspersky Internet Security avvia così il processo di aggiornamento. Tutti i dettagli del processo vengono visualizzati in un'apposita finestra.

5.9. Come comportarsi in presenza di oggetti pericolosi

In presenza di oggetti pericolosi nella posta, nei file aperti o nei programmi avviati, viene visualizzato sul video un messaggio apposito (cfr. Figura 8).

Figura 8. Avviso di rilevamento di un virus

L'avviso può essere dei seguenti tipi:

- *Avvertimento* – indica il rilevamento di un oggetto potenzialmente infetto. Se possibile, viene indicato anche il nome del programma probabilmente nocivo che potrebbe aver infettato il file.
- *Allarme* – indica il rilevamento di un programma nocivo.

L'avviso contiene:

- Il nome del programma nocivo che ha infettato l'oggetto. Link a www.viruslist.com, dove sono disponibili informazioni dettagliate sul tipo di minaccia individuato nel computer.
- Nome completo dell'oggetto pericoloso.
- Breve descrizione e azioni possibili per gestire l'oggetto. La descrizione indica il tipo di programma nocivo che ha infettato l'oggetto e specifica se sia possibile neutralizzarlo.

Se il programma è in grado di ripulire l'oggetto, l'utente può scegliere tra le seguenti opzioni:

- **Disinfect** – il programma cerca di riparare l'oggetto infetto. Prima del trattamento, viene effettuata una copia di backup dell'oggetto per

l'eventualità in cui si renda necessario ripristinare l'oggetto stesso o una copia dell'infezione.

- **Elimina** – il programma elimina l'oggetto. Prima del trattamento, viene effettuata una copia di backup dell'oggetto per l'eventualità in cui si renda necessario ripristinare l'oggetto stesso o una copia dell'infezione.
- **Ignora** – il programma non esegue alcuna azione sull'oggetto e si limita a registrare l'evento nel report. Se si seleziona questa opzione, l'oggetto resta disponibile per l'uso.

Se l'oggetto non è riparabile, Kaspersky Internet Security chiede se si desidera eliminarlo o ignorarlo.

Se si sospetta che l'oggetto sia infetto, il programma chiede se si desidera ignorarlo o metterlo in quarantena.

Per eseguire un'azione, fare clic sul pulsante appropriato.

È possibile applicare l'azione selezionata a tutti gli oggetti caratterizzati dallo stesso status rilevati nella sessione corrente del programma selezionando la casella **Applica a tutti**.

È possibile che si presentino situazioni in cui l'oggetto sospetto rivelato non sia tale per l'utente. È il caso, per esempio, di un file creato dall'utente e che il programma considera pericoloso anche se l'utente è assolutamente certo della sua affidabilità. L'utente infatti utilizza regolarmente quel file ed è sicuro che non può recare alcun danno al computer. In tal caso, si raccomanda di aggiungere questo file all'elenco delle esclusioni. È possibile eseguire questa operazione dall'apposita finestra (cfr. 6.3 a pag. 75) o direttamente dalla finestra di avviso facendo clic su Aggiungi a zona attendibile.

5.10. Come comportarsi in caso di protezione non funzionante

Se si verificano problemi o errori di funzionamento di qualsiasi componente di protezione, è bene verificarne lo status.

Se lo status del componente è *<nome del componente> : non funzionante* o *<nome del componente> : errore di funzionamento*, cercare di riavviare il programma.

Se il problema non si risolve riavviando il programma, si raccomanda di rivolgersi al servizio di assistenza tecnica. Salvare un report sul funzionamento del componente e inviarlo a Kaspersky Lab. Questo aiuterà gli esperti del servizio di assistenza tecnica a comprendere a fondo il problema.

Per salvare il report su un file:

1. Selezionare il componente nella sezione **Protezione** della finestra principale del programma e fare clic con il pulsante sinistro su un punto qualsiasi del riquadro **Statistiche**.
2. Fare clic sul pulsante **Salva con nome** e specificare nella finestra che si apre il nome del file per il report sulle prestazioni del componente.

Per salvare in una sola volta un report su tutti i componenti di Kaspersky Internet Security (componenti di protezione, attività di scansione antivirus, funzioni di supporto):

1. Selezionare la sezione **Protezione** della finestra principale del programma e fare clic con il pulsante sinistro su un punto qualsiasi del riquadro **Statistiche**.

   OPPURE

   Fare clic su Elenco di tutti i report nella finestra dei report per ogni componente. La scheda **Report** visualizza quindi un elenco dei report su tutti i componenti del programma.
2. Fare clic sul pulsante **Salva con nome** e specificare nella finestra che si apre il nome del file per il report sulle prestazioni del programma.

CAPITOLO 6. SISTEMA DI GESTIONE DELLA PROTEZIONE

Kaspersky Internet Security consente al sistema di gestione sicurezza del computer multitasking di:

- Abilitare, disabilitare e sospendere (cfr. 6.1 a pag. 69) il programma
- Definire i tipi di programmi pericolosi (cfr. 6.2 a pag. 74) dai quali Kaspersky Internet Security deve proteggere il computer
- Creare un elenco di esclusioni (cfr. 6.3 a pag. 75) per la protezione
- Creare attività di scansione antivirus e di aggiornamento personalizzate (cfr. 6.4 a pag. 84).
- Programmare una serie di scansioni antivirus (cfr. 6.5 a pag. 85).
- Importare ed esportare impostazioni (cfr. 6.6 a pag. 87) per il programma.

6.1. Interruzione e ripristino della protezione del computer

Per impostazione predefinita, Kaspersky Internet Security viene caricato all'avv del sistema e protegge il computer per tutto il tempo che resta in uso. Il messaggio *Protetto da Kaspersky Internet Security* nell'angolo superiore destro dell schermo informa l'utente che tutti i componenti di protezione (cfr. 2.2.1 a pag. 25) sono in funzione.

È possibile disabilitare completamente o parzialmente la protezione offerta da Kaspersky Internet Security.

Attenzione!

Kaspersky Lab raccomanda caldamente di **non disabilitare la protezione**, poiché ciò potrebbe provocare l'infezione del computer e la perdita dei dati.

Osservare che in questo caso la protezione è descritta nel contest dei componeni di protezione. Disabilitare o sospendere i componenti di protezione non pregiudica le prestazioni delle attività di scansione antivirus o aggiornamento del programma.

6.1.1. Sospensione della protezione

Sospendere la protezione significa disabilitare temporaneamente tutti i componenti di protezione che monitorano i file del computer, la posta in arrivo e in uscita, gli script eseguibili, il comportamento delle applicazioni, Anti-Hacker e Anti-Spam.

Per sospendere un'operazione di Kaspersky Internet Security:

1. Selezionare **Interrompi protezione** nel menu contestuale del programma (cfr. 4.2 a pag. 48).
2. Nella finestra Interrompi protezione che si apre (cfr. Figura 9), specificare quando si desidera ripristinare la protezione:
   - **N minuti/ore** – la protezione sarà ripristinata allo scadere dei minuti/ore indicati.
   - **On next Internet connection** – la protezione sarà ripristinata non appena il computer si connetterà a Internet.
   - **Al successivo riavvio** – la protezione sarà ripristinata aprendo il programma dal menu Start o dopo aver riavviato il computer (a condizione che il programma sia impostato in modo da aprirsi automaticamente all'avvio (cfr. 6.1.5 a pag. 73).
   - **Mai** – la protezione sarà ripristinata solo se avviata manualmente dall'utente. Per abilitare la protezione, selezionare **Riprendi protezione** dal menu contestuale del programma.

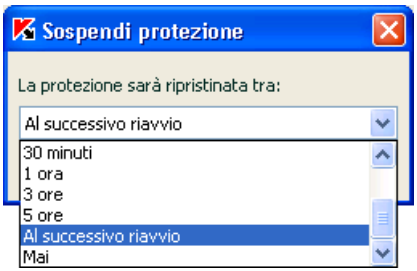


Figura 9. Finestra di sospensione della protezione

Suggerimento:
È possibile inoltre interrompere la protezione del computer fino alla successiva inizializzazione del sistema con uno dei seguenti metodi:

- Fare clic sul pulsante nella sezione **Protezione**.
- Selezionare **Esci** dal menu contestuale. Il programma si chiude.

Se si sospende la protezione, si sospendono tutti i componenti. Questo status è indicato da:

- Nomi inattivi (di colore grigio) dei componenti disabilitati nella sezione Protezione della finestra principale.
- Icona della barra delle applicazioni inattiva (di colore bianco e nero).
- Il terzo indicatore di protezione (cfr. 5.1.1 a pag. 55) del computer, che segnala che **Tutti i componenti della protezione sono sospesi**.

6.1.2. Interruzione della protezione

Interrompere la protezione significa disabilitare completamente i componenti della protezione. Le attività di scansione antivirus e di aggiornamento continuano a funzionare in questa modalità.

Se la protezione è interrotta, essa può essere ripristinata esclusivamente dall'utente. Se la protezione è stata interrotta, i suoi componenti non si ripristinano automaticamente al riavvio del sistema o del programma. Ricordare che se Kaspersky Internet Security è in conflitto con altri programmi installati sul computer, è possibile sospendere i singoli componenti o creare un elenco di esclusioni (cfr. 6.3 a pag. 75).

Per interrompere la protezione:

1. Aprire la finestra principale di Kaspersky Internet Security.
2. Selezionare la sezione **Protezione** e fare clic su **Impostazioni**.
3. Nella finestra delle impostazioni del programma, deselezionare **Abilita Protezione**.

Disabilitando la protezione, tutti i suoi componenti si interrompono. Questo status è indicato da:

- Nomi inattivi (di colore grigio) dei componenti disabilitati nella sezione Protezione della finestra principale.
- Icona della barra delle applicazioni inattiva (di colore bianco e nero).

- Il terzo indicatore di protezione (cfr. 5.1.1 a pag. 55) del computer, che segnala che  **Tutti i componenti della protezione sono disabilitati**.

6.1.3. Sospensione/interruzione dei componenti della protezione, delle scansioni antivirus e delle attività di aggiornamento

Esistono molti modi per interrompere un componente di protezione, una scansione antivirus o un aggiornamento. Tuttavia, prima di farlo, si raccomanda di chiarirsi le idee sui motivi per cui si desidera interromperli. È probabile infatti che esista una soluzione diversa al problema, per esempio modificare il livello di sicurezza. Se, per esempio, si lavora con un database che sicuramente non contiene virus, è sufficiente aggiungerne i file tra le esclusioni (cfr. 6.3 a pag. 75).

Per sospendere componenti della protezione, scansioni antivirus e attività di aggiornamento:

Selezionare il componente o l'attività dalla parte sinistra della finestra principale e fare clic sul pulsante  nella barra di stato.

Lo status del componente/attività diventa *sospeso*. Il componente o attività resterà sospeso fino a quando l'utente li ripristinerà facendo clic sul pulsante  .

Per interrompere componenti della protezione, scansioni antivirus e attività di aggiornamento:

Fare clic sul pulsante  nella barra di stato. È possibile interrompere i componenti della protezione anche dalla finestra delle impostazioni del programma deselezionando  **Abilita <component name>** nella sezione **Generale** relativa al componente.

Lo status del componente/attività diventa *interrotto (disabilitato)*. Il componente o attività resterà interrotto fino a quando l'utente li abiliterà facendo clic sul pulsante  . Per le scansioni antivirus e le attività di aggiornamento, è possibile scegliere tra le seguenti opzioni: Continuare l'attività che è stata interrotta o riavviarla.

Le differenze tra le due opzioni di interruzione delle attività e dei componenti sono le seguenti:

- Quando si *sospende* un componente o attività (pulsante ), le statistiche relative alla sessione corrente di Kaspersky Internet Security vengono

salvate e continueranno ad essere registrate se la funzione viene ripristinata.

- Quando si interrompe la protezione (pulsante ■), tutte le statistiche vengono azzerate e ricominciate al riavvio del componente.

6.1.4. Ripristino della protezione del computer

Se l'utente ha sospeso o interrotto la protezione del computer, potrà ripristinarla mediante uno dei seguenti metodi:

- Dal menu contestuale.

  Selezionare **Riprendi**.

- Dalla finestra principale del programma.

  Fare clic sul pulsante ▶ della barra di stato nella sezione **Protezione** della finestra principale.

Lo status della protezione diventa immediatamente *attivo*. L'icona della barra delle applicazioni diventa attiva (colorata). Anche il terzo indicatore della protezione (cfr. 5.1.1 a pag. 55) informa l'utente che **Tutti i componenti della protezione sono in esecuzione**.

6.1.5. Spegnimento del programma

Per spegnere Kaspersky Internet Security, selezionare **Esci** dal menu contestuale del programma (cfr. 4.2 a pag. 48). Il programma si chiude lasciando il computer privo di protezione.

Se le connessioni di rete monitorate dal programma sono attive sul computer nel momento in cui il programma viene chiuso, viene visualizzato un messaggio che informa che queste connessioni saranno interrotte. Ciò è necessario per consentire al programma di chiudersi correttamente. Le connessioni vengono interrotte automaticamente dopo dieci secondi oppure facendo clic su **Sì**. La maggior parte delle connessioni sarà ripristinata automaticamente dopo qualche tempo.

Osservare che, se si sta scaricando un file senza un download manager, al termine della connessione il file parzialmente scaricato andrà perduto e occorrerà scaricarlo nuovamente.

Si può scegliere di non interrompere le connessioni facendo clic su **No** nella finestra dell'avviso. Così facendo, il programma continuerà a funzionare.

Se il programma è stato chiuso, è possibile abilitare nuovamente la protezione del computer aprendo Kaspersky Internet Security (**Start→ Programmi → Kaspersky Internet Security 6.0 → Kaspersky Internet Security 6.0.**

È possibile inoltre ripristinare automaticamente la protezione dopo il riavvio del sistema operativo. Per abilitare questa funzione, selezionare la sezione **Protezione** nella finestra delle impostazioni del programma e selezionare **Lancia Kaspersky Internet Security 6.0 all-avvio**.

6.2. Selezione dei programmi monitorati

Kaspersky Internet Security protegge il computer da vari tipi di programmi nocivi. Indipendentemente dalle impostazioni prescelte, il programma esamina sempre e neutralizza virus, troiani e backdoor. Questi programmi sono in grado di danneggiare gravemente il computer. Per migliorare la sicurezza del computer, è possibile accrescere l'elenco delle minacce che il programma sarà in grado di intercettare abilitando il monitoraggio di diversi programmi potenzialmente pericolosi.

Per specificare da quali programmi nocivi Kaspersky Internet Security proteggerà il computer, selezionare la sezione **Protezione** nella finestra delle impostazioni del programma (cfr. 4.4 a pag. 52).

Il riquadro **Categorie di software nocivo** contiene i tipi di minaccia:

- **Virus, Worm, Trojan, Rootkit**. Questo gruppo combina le categorie più comuni e pericolose di programmi nocivi. Questo è il livello di sicurezza minimo ammissibile, e disabilitarlo incrementerebbe drasticamente le probabilità del computer di incorrere in un'infezione. Secondo le raccomandazioni degli esperti Kaspersky Lab, non è possibile rimuovere questi oggetti dall'elenco di quelli esaminati da Kaspersky Internet Security.
- **AdWare, SpyWare, Dialer**. Questo gruppo si riferisce a software potenzialmente pericoloso che potrebbe costituire una fonte di rischio.
- **Software potenzialmente pericoloso (applicazioni di accesso remoto, joke, ecc.)**. Questo gruppo include programmi che di per sé non sono nocivi o pericolosi, ma che in determinate circostanze potrebbero essere utilizzati per danneggiare il computer.

I gruppi sopra elencati comprendono la serie completa degli elenchi delle minacce per la scansione di oggetti in tempo reale e la scansione antivirus del computer.

Se tutti i gruppi sono selezionati, Kaspersky Internet Security garantisce la massima protezione antivirus del computer. Se il secondo e il terzo gruppo sono

disabilitati, il programma protegge solo dai programmi nocivi più comuni. Fra questi non sono compresi i programmi potenzialmente pericolosi che potrebbero essere installati sul computer e danneggiare i file, provocare perdite finanziarie e rubare tempo.

Gli esperti di Kaspersky Lab raccomandano di disabilitare i gruppi di minacce solo se assolutamente necessario. Se, per esempio, si desidera disabilitare il monitoraggio dei programmi potenzialmente pericolosi del secondo gruppo solo perché Kaspersky Internet Security interferisce con altri programmi classificandoli come potenzialmente pericolosi, è sufficiente aggiungerli all'elenco delle esclusioni (cfr. 6.3 a pag. 75).

6.3. Creazione di una zona attendibile

Una *zona attendibile* è un elenco di oggetti creato dall'utente, che Kaspersky Internet Security non esamina. In altre parole, si tratta di una serie di programmi esclusi dalla protezione.

L'utente crea una zona protetta sulla base delle proprietà dei file che usa e dei programmi installati sul computer. Questo elenco di esclusioni può tornare utile, per esempio, se Kaspersky Internet Security blocca l'accesso a un oggetto o programma della cui sicurezza l'utente è assolutamente sicuro.

È possibile escludere file dalla scansione in base al formato, oppure usare una maschera, escludere una determinata area (per esempio una cartella o un programma), processi di programmi o oggetti in base allo status che il programma assegna agli oggetti durante una scansione.

Per creare un elenco di esclusioni,

1. Aprire la finestra delle impostazini di Kaspersky Internet Security e selezionare la sezione **Protezione**.
2. Fare clic sul pulsante **Zona attendibile** nella sezione Zona attendibile.
3. Configurare le regole di esclusione degli oggetti e creare un elenco di applicazioni attendibili nella finestra che si apre (cfr. Figura 10).

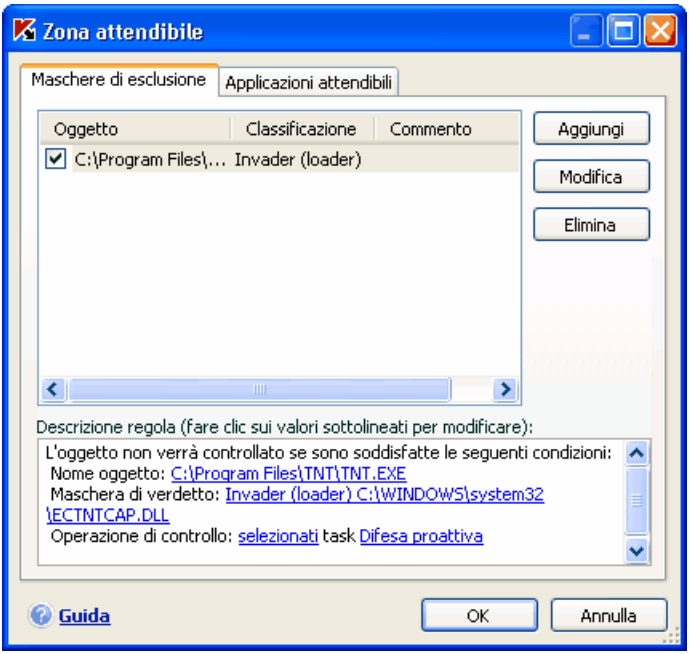


Figura 10. Creazione di una zona attendibile

6.3.1. Regole di esclusione

Le regole di esclusione sono delle condizioni in base alle quali Kaspersky Internet Security stabilisce quali oggetti non sottoporre a scansione.

È possibile escludere i file dalla scansione in base al formato, usare una maschera, escludere una determinata area (per esempio una cartella o un programma), processi di programmi o oggetti in base al “verdetto”,

cioè lo status che Kaspersky Internet Security assegna a un oggetto durante la scansione. Un verdetto si basa sulla classificazione dei programmi nocivi e potenzialmente pericolosi presenti nell’enciclopedia dei virus di Kaspersky Lab.

Il Software potenzialmente pericoloso non svolge una funzione nociva vera e propria ma può essere utilizzato dagli hacker come componente ausiliario di un codice maligno in quanto contiene errori e vulnerabilità. Di questa categoria fanno parte, per esempio, programmi di amministrazione remota, client IRC, servizi FTP, utilità multifunzione per interrompere o nascondere i processi, keylogger, macro per la decodifica di password, autodialer, ecc. Questi programmi non sono classificati come viruses. Essi possono essere suddivisi in diverse categorie, per esempio adware, scherzi, riskware, ecc. (per ulteriori

informazioni sui programmi potenzialmente pericolosi individuati da Kaspersky Internet Security, vedere Virus Encyclopedia su www.viruslist.com). Dopo la scansione, questi programmi possono essere bloccati. Poiché molti di essi sono estremamente comuni, l'utente ha la possibilità di escluderli dalla scansione specificando il verdetto assegnato al programma come esclusione.

Poniamo per esempio di utilizzare frequentemente un programma di amministrazione remota. Si tratta di un sistema di accesso remoto che consente di lavorare da un altro computer. Kaspersky Internet Security visualizza questo tipo di applicazione come potenzialmente pericolosa e la blocca. Per evitare il blocco dell'applicazione, è necessario creare una regola di esclusione che specifichi Remote Admin come verdetto.

Quando si aggiunge un'esclusione, viene creata una regola che in seguito sarà utilizzata da numerosi componenti del programma e attività di scansione antivirus (File Anti-Virus, Mail Anti-Virus, **Difesa proattiva**). Per creare le regole di esclusione, esiste una finestra specifica accessibile dalla finestra delle impostazioni del programma, dall'avviso di intercettazione dell'oggetto e dalla finestra dei report.

*Per aggiungere esclusioni nella scheda **Regola di esclusione**:*

1. Fare clic sul pulsante **Aggiungi** nella scheda **Regola di esclusione**.
2. Nella finestra che si apre (cfr. Figura 11), fare clic sulla sezione **Impostazioni**:

   - **Oggetto** – esclusione dalla scansione di un oggetto, directory o file corrispondente a una determinata maschera.
   - **Verdetto** – esclusione dalla scansione di oggetti in base allo status assegnato loro dall'enciclopedia dei virus.

Figura 11. Creazione di una regola di esclusione

Se si selezionano subito entrambe le caselle, si crea una regola con un determinato verdetto per l'oggetto in questione. In tal caso vale la seguente regola:

- Se si specifica un determinato file come **Oggetto** e un determinato status nella sezione **Verdetto**, il file specificato sarà escluso solo se classificato come il tipo di minaccia selezionata.
- Se si seleziona un'area o cartella come **Oggetto** e lo status (o maschera dei verdetti) come **Verdetto**, gli oggetti con quello status saranno esclusi solo dalla scansione di quell'area o cartella.

3. Assegnare dei valori ai tipi di esclusione selezionati. A tal fine, fare clic con il pulsante sinistro del mouse nella sezione **Descrizione regola** sul link specifica ubicato a fianco del tipo di esclusione:
   - Per il tipo di oggetto, digitare il nome nella finestra che si apre (può trattarsi di un file, di una directory o di una maschera di file, cfr. A.2 a pag. 293). Selezionare la casella **Includi sottocartelle** per l'oggetto (file, maschera di file, cartella) da escludere ogni volta dalla scansione. Per esempio, se si specifica **C:\Program Files\winword.exe** come esclusione selezionando l'opzione sottocartelle, il file **winword.exe** sarà escluso dalla scansione se presente in qualsiasi sottocartella di **C:\Programmi**.

- Digitare il nome completo della minaccia che si desidera escludere dalle scansioni come indicato nell'enciclopedia dei virus, oppure utilizzare una maschera (cfr. A.3 a pag. 293) per il **Verdetto**.

  Per alcuni verdetti, è possibile assegnare condizioni avanzate per l'applicazione delle esclusioni nel campo **Impostazioni avanzate**. Nella maggior parte dei casi, il programma compila automaticamente questo campo quando si aggiunge una regola di esclusione da un avviso di difesa proattiva.

  È possibile aggiungere impostazioni avanzate per i seguenti verdetti in particolare:

  - *Invader* (si inserisce nei processi dei programmi). Per questo verdetto, è possibile assegnare all'oggetto interessato (per esempio un file .dll) un nome, una maschera o percorso completo come condizione di esclusione supplementare.
  - *Opening Internet Browser*. Per questo verdetto è possibile elencare le impostazioni di apertura del browser come impostazioni di esclusione supplementari. Per esempio, si è deciso di bloccare i browser dall'apertura con determinate impostazioni nell'analisi dell'attività dell'applicazione **Difesa proattiva**. Tuttavia, si desidera consentire al browser di aprirsi per il dominio *www.kasperky.com* con un link da Microsoft Office Outlook come regola di esclusione. Per fare questo, selezionare Outlook come **Oggetto** di esclusione e *Opening Internet Browser* come **Verdetto**, e digitare una maschera di dominio consentito nel campo **Impostazioni avanzate**.

4. Definire quali componenti di Kaspersky Internet Security devono applicare questa regola. Se si seleziona tutti, la regola sarà applicata a tutti i componenti. Se si desidera limitare la regola a uno o più componenti, fare clic su tutti che cambia in selezionati. Nella finestra che si apre, selezionare le caselle relative ai componenti ai quali si desidera applicare questa regola di esclusione.

Per creare una regola di esclusione dall'avviso di un programma che avverte dell'individuazione di un oggetto pericoloso:

1. Usare il link Aggiungi a zona attendibile nella finestra della notifica (cfr. Figura 12).

Figura 12. Avviso di intercettazione di oggetto pericoloso

2. Nella finestra che si apre, verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome dell'oggetto e il tipo di minaccia in base alle informazioni ottenute dalla notifica. Per creare la regola, fare clic su **OK**.

Per creare una regola di esclusione dalla finestra dei report:

1. Selezionare nel report l'oggetto che si desidera aggiungere alle esclusioni.
2. Aprire il menu contestuale e selezionare **Aggiungi a zona attendibile** (cfr. Figura 13).
3. Si apre quindi la finestra delle impostazioni delle esclusioni. Verificare che tutte le impostazioni delle regole di esclusione corrispondano alle proprie esigenze. Il programma inserisce automaticamente il nome dell'oggetto e il tipo di minaccia in base alle informazioni ottenute dal report. Per creare la regola, fare clic su **OK**.

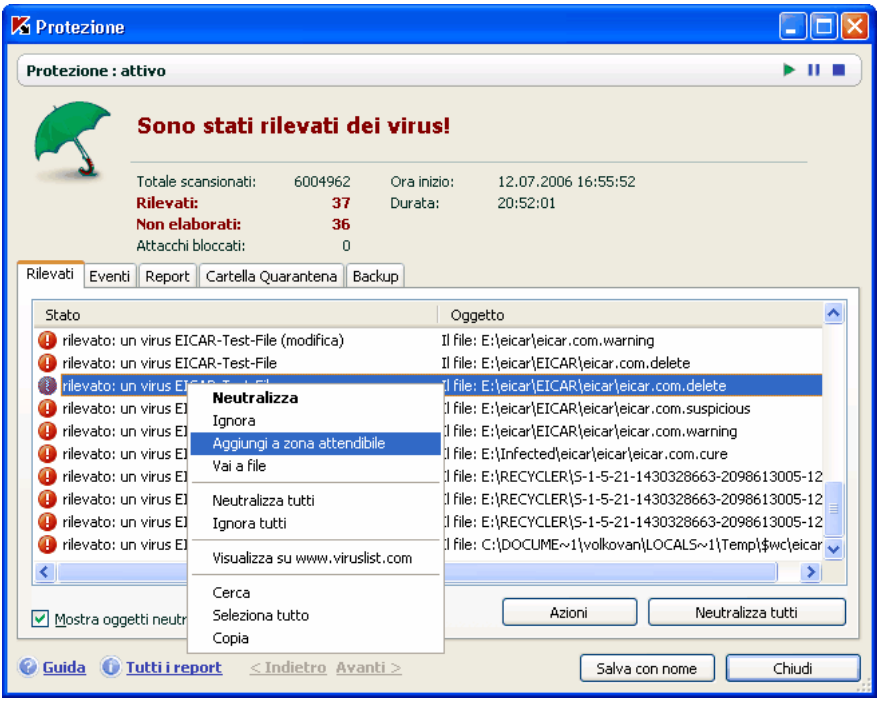


Figura 13. Creazione di una regola di esclusione da un report

6.3.2. Applicazioni attendibili

Kaspersky Internet Security è in grado di creare un elenco di applicazioni attendibili di cui non è necessario monitorare le attività dei file o di rete, siano esse sospette oppure no.

Per esempio, si può ritenere che gli oggetti utilizzati da Windows Notepad siano sicuri e non necessitino di scansione. In altre parole, ci si fida dei processi di questo programma. Per escludere dalla scansione gli oggetti utilizzati da questo processo, aggiungere Notebook all'elenco delle applicazioni attendibili. Tuttavia, il file eseguibile e il processo dell'applicazione affidabile saranno sottoposti a scansione antivirus come in precedenza. Per escludere completamente l'applicazione dalla scansione, è necessario utilizzare le regole di esclusione (cfr. 6.3.1 a pag. 76).

Inoltre, è possibile che alcune azioni classificate come pericolose siano in realtà perfettamente normali per le funzioni di determinati programmi. Per esempio, i programmi di commutazione del layout di tastiera intercettano regolarmente il testo digitato sulla tastiera. Per giustificare le operazioni specifiche di tali

programmi ed escludere dal monitoraggio le loro attività, si raccomanda di aggiungerli all'elenco delle applicazioni attendibili.

Grazie alle esclusioni delle applicazioni attendibili è possible inoltre risolvere potenziali conflitti di compatibilità tra Kaspersky Internet Security e altre applicazioni (per esempio il traffico di rete da un altro computer che è appena stato esaminato dall'applicazione antivirus) e incrementare la produttività del computer, particolarmente importante quando si utilizzano applicazioni server.

Per impostazione predefinita, Kaspersky Internet Security esamina gli oggetti aperti, eseguiti o salvati da qualsiasi processo di programma e monitora l'attività di tutti i programmi e il traffico di rete che creano.

È possibile creare un elenco di applicazioni attendibili nella scheda specifica **Applicazioni attendibili** (cfr. Figura 14). È possibile aggiungere elementi e modificare l'elenco servendosi dei pulsanti **Aggiungi, Modifica** ed **Elimina** sulla destra.

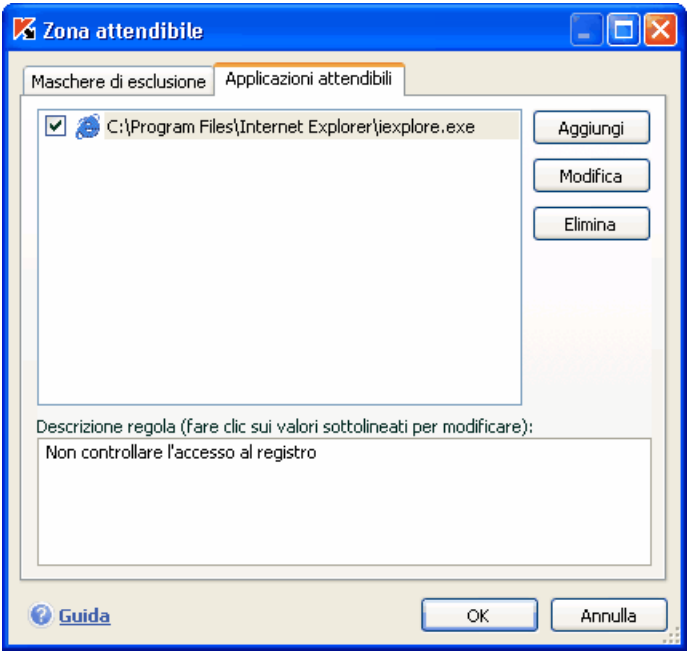


Figura 14. Elenco delle applicazioni attendibili

Per aggiungere un programma all'elenco delle applicazioni attendibili:

1. Fare clic sul pulsante **Aggiungi** nella parte destra della finestra.

2. Nella finestra **Applicazione attendibile** (cfr. Figura 15) che si apre, selezionare l'applicazione per mezzo del pulsante **Sfoglia**. Si apre un menu contestuale. Facendo clic su **Sfoglia** è possibile aprire la finestra di selezione dei file e selezionare il percorso del file eseguibile. In alternative, facendo clic su **Applicazioni** è possibile aprire un elenco delle applicazioni correntemente in funzione e selezionare quelle desiderate.

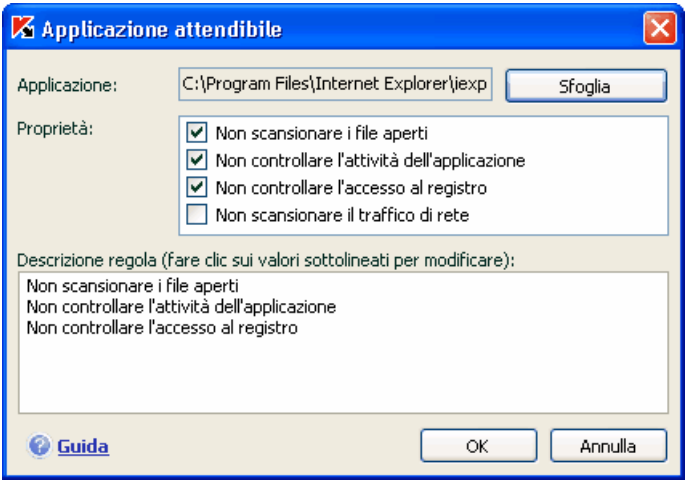


Figura 15. Aggiunta di un'applicazione all'elenco delle applicazioni attendibili

Quando si seleziona un programma, Kaspersky Internet Security ricorda gli attributi interni del file eseguibile e li usa per identificare il programma come affidabile durante le scansioni.

Il percorso del file viene inserito automaticamente quando se ne seleziona il nome. È possibile tuttavia modificarlo manualmente.

> Usare il percorso completo del file eseguibile o una maschera *. In caso di uso di una maschera, un processo avviato viene considerato affidabile indipendentemente dalla cartella che contiene il file eseguibile.

3. Specificare quindi le azioni eseguite da questo processo che Kaspersky Internet Security non deve monitorare:

   Non scansionare i file aperti – esclude dalla scansione tutti i file che il processo dell'applicazione affidabile apre.

- **Non controllare l'attivita dell'applicazione** – esclude dal monitoraggio di **Difesa proattiva** qualsiasi attività, sospetta o no, che un'applicazione affidabile sta eseguendo.
- **Non controllare l'accesso al registro** – esclude dalla scansione i tentativi di accesso al registro di sistema avviati dalle applicazioni attendibili.
- **Non scansionare il traffico di rete** – esclude dale scansioni antivirus e antispam il trattico di rete avviato dalle applicazioni attendibili. È possibile escludere dalla scansione il traffico di rete o quello protetto (SSL) generato da tali applicazioni. A tal fine, usare il collegamento tutto**.** Questo sarà modificato in crittografato. È inoltre possibile limitare l'esclusione assegnando una porta remota o un host remoto. Per creare una limitazione, fare clic su tutti, che diventa selezionati, e digitare un valore per la porta/host remoto.

Osservare che se la casella **Do not scan network traffic** è selezionata, il traffico relativo all'applicazione sarà sottoposto alla sola scansione antivirus e antispam. Questo tuttavia non influisce sulla scansione del traffico da parte di Anti-Hacker. Le impostazioni di Anti-Hacker influiscono sull'analisi dell'attività di rete dell'applicazione in questione.

6.4. Avvio di attività di scansione antivirus e aggiornamento con un altro profilo

Kaspersky Internet Security 6.0 è dotato di una funzione che consente di esaminare le attività sotto un altro profilo. Questa funzione è normalmente disabilitata e le attività vengono eseguite con il profilo con cui l'utente si è collegato al sistema.

Così, per esempio, possono essere necessari i diritti di accesso a un determinato oggetto durante una scansione. Utilizzando questa funzione, è possibile configurare le attività in modo da essere eseguite con il profilo di un utente in possesso dei privilegi richiesti.

È possibile che gli aggiornamenti del programma debbano essere eseguiti da un'origine alla quale non si ha accesso (per esempio la cartella aggiornamenti di rete) o da un server proxy per il quale non si hanno diritti. È possible quindi utilizzare questa funzione per eseguire l'Updater con un profilo diverso in possesso dei diritti necessari.

Per configurare un'attività di scansione da eseguire con un profilo utente diverso:

1. Selezionare il nome dell'attività nella scheda **Scansione (Aggiornamento)** della finestra principale e usare il link Impostazioni per aprire la finestra delle impostazioni.
2. Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni dell'attività e aprire la scheda **Account** nella finestra che si apre (cfr. Figura 16).

Per abilitare questa funzione, selezionare la casella ☑ **Esegui questa operazione come**. Inserire i dati di login del profilo con cui si desidera avviare l'attività: nome utente e password.

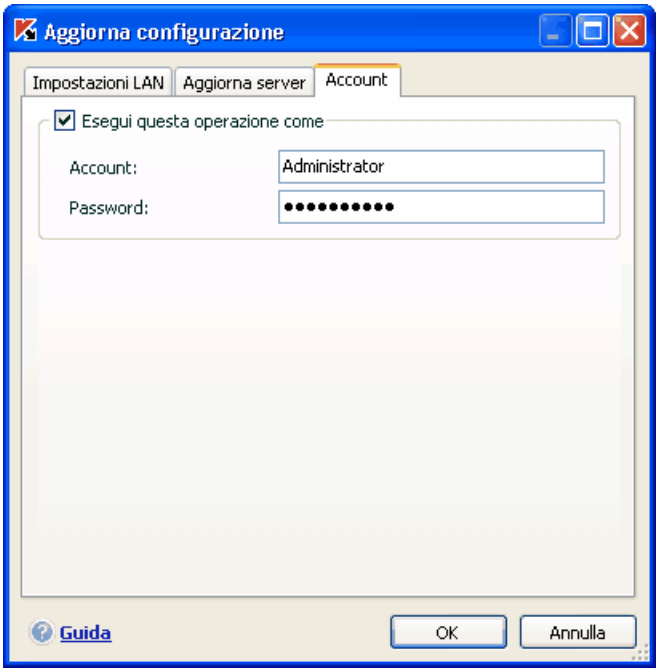


Figura 16. Configurazione di un'attività di aggiornamento da un altro profilo

6.5. Programmazione delle scansioni antivirus e degli aggiornamenti

È possibile eseguire le scansioni antivirus e gli aggiornamenti manualmente o automaticamente per mezzo di una pianificazione.

L'impostazione predefinita per la programmazione delle attività di scansione antivirus create all'installazione del programma è "disabilitato". Fanno eccezione gli elementi di avvio, che vengono esaminati ogni volta che si avvia il computer. L'impostazione predefinita per la programmazione delle attività di aggiornamento create all'installazione del programma è anch'essa "disabilitato". L'Updater viene eseguito automaticamente ogni volta che vengono messi a disposizione nuovi aggiornamenti sui server di Kaspersky Lab.

Se le impostazioni dell'attività di scansione automatica non sono soddisfacenti, modificarle selezionando il nome dell'attività nella finestra principale del programma, sezione **Scansione** (per la scansione antivirus) o sezione **Servizi** (per le attività di aggiornamento), e aprire la finestra delle impostazioni facendo clic su Impostazioni.

Per fare avviare le attività in base a una pianificazione, selezionare la casella dell'avvio automatico delle attività nella sezione **Modalità di esecuzione**. È possibile modificare le condizioni di avvio dell'attività di scansione nella finestra **Programmazione** (cfr. Figura 17), che si apre facendo clic su **Modifica**.

Figura 17. Pianificazione delle attività

Il passaggio più importante consiste nel determinare la frequenza di avvio dell'attività. È possibile selezionare una delle seguenti opzioni:

- **Una volta**. L'attività sarà eseguita una volta nel giorno e nell'ora specificati.
- **Ogni minuto**. L'intervallo tra le scansioni sarà del numero di minuti specificato nelle impostazioni di pianificazione. Non deve essere superiore a 59 minuti.

Ogni ora. L'intervallo tra le scansioni è calcolato in ore. Digitare il numero di ore nelle impostazioni di pianificazione: **Ogni *n* ore**, specificare il valore di *n*. Per esempio, digitare **Ogni 1 ore** se si desidera eseguire la scansione ogni ora.

Giornalmente – l'intervallo tra le scansioni è calcolato in giorni. Specificare la frequenza della scansione nelle impostazioni di pianificazione:

- Selezionare l'opzione **Ogni *n* giorno(i)** e digitare un valore per *n*. Digitare *Ogni 2 giorni* se si desidera avviare la scansione a giorni alterni.
- Selezionare **Tutti i giorni feriali** se si desidera eseguire la scansione tutti i giorni dal lunedì al venerdì.
- Selezionare **Tutti i giorni festivi** per avviare l'attività solo il sabato e la domenica.

  Oltre alla frequenza è necessario specificare nel campo **Ora** l'ora del giorno o della notte in cui si desidera avviare la scansione.

Settimanalmente – l'attività di scansione viene eseguita solo determinati giorni della settimana. Se si seleziona questa opzione, mettere nelle impostazioni di pianificazione un segno di spunta accanto ai giorni della settimana in cui si desidera eseguire la scansione. Specificare inoltre l'ora in cui sarà eseguita l'attività nel campo *Ora*.

Mensilmente – l'attività di scansione sarà eseguita una volta al mese all'ora specificata.

Osservare che l'attività di scansione per gli oggetti di avvio ha una pianificazione specifica. È possibile configurarne l'esecuzione automatica ogni volta che si accende il computer e/o si scaricano gli aggiornamenti degli elenchi delle minacce. È sufficiente selezionare le caselle corrispondenti nella sezione **Modalità di esecuzione** della finestra delle impostazioni dell'attività.

Se per qualsiasi motivo una scansione viene omessa (per esempio all'ora prevista il computer era spento), è possibile configurare l'attività saltata in modo da iniziare automaticamente non appena possibile. A tal fine, selezionare la casella **Esegui operazione se ignorata** nella finestra delle pianificazioni.

6.6. Importazione ed esportazione delle impostazioni di Kaspersky Internet Security

Kaspersky Internet Security offre la possibilità di importare ed esportare le impostazioni.

Questa funzione risulta particolarmente utile nei casi in cui, per esempio, il programma è installato sia nel computer di casa sia in quello dell'ufficio. È possibile configurare le impostazioni preferite del programma sul computer di casa, salvare queste impostazioni su un disco e, servendosi della funzione di importazione, caricarle sul computer in ufficio. Le impostazioni vengono salvate in uno speciale file di configurazione.

Per esportare le impostazioni correnti del programma:

1. Aprire la finestra principale di Kaspersky Internet Security.
2. Selezionare la sezione Protezione e fare clic su **Impostazioni**.
3. Fare clic sul pulsante **Salva** nella sezione **Gestione impostazioni**.
4. Digitare un nome per il file di configurazione e selezionare una destinazione in cui salvarlo.

Per importare le impostazioni da un file di configurazione:

1. Aprire la finestra principale di Kaspersky Internet Security.
2. Selezionare la sezione **Protezione** e fare clic su Impostazioni.
3. Fare clic sul pulsante **Carica** e selezionare il file da cui si desidera importare le impostazioni di Kaspersky Internet Security.

6.7. Ripristino delle impostazioni predefinite

È possibile ripristinare le impostazioni raccomandate del programma in qualsiasi momento. Esse infatti sono considerate ottimali e sono quindi consigliate dagli esperti di Kaspersky Lab. Per ripristinare le impostazioni predefinite servirsi della procedura di configurazione guidata.

Per ripristinare le impostazioni di protezione:

1. Selezionare la sezione **Protezione** e fare clic su Impostazioni per aprire la finestra di configurazione del programma.
2. Fare clic sul pulsante **Reimposta** nella sezione **Gestione impostazioni**.

La finestra che si apre chiede di definire le impostazioni da salvare per ciascun componente e quali invece abbandonare una volta ripristinato il livello di sicurezza raccomandato.

L'elenco visualizza i componenti del programma con le impostazioni modificate dall'utente o configurate man mano dal programma stesso durante l'autoapprendimento (Anti-Hacker o Anti-Spam). Qualora fossero state create

impostazioni speciali per uno o più componenti, anch'esse saranno visualizzate nell'elenco.

Esempi di impostazioni speciali sono le liste bianche e nere di espressioni e indirizzi utilizzati da Anti-Spam, elenchi di indirizzi e di numeri di ISP affidabili utilizzati da Web Anti-Virus e Anti-Spy, regole di esclusione create exclusion rules create per componenti del programma, regole di applicazioni e filtraggio di pacchetti per Anti-Hacker, e regole di applicazioni per Difesa proattiva.

Questi elenchi vengono creati man mano che si utilizza il programma, in base alle attività individuali e ai requisiti di sicurezza. Questo processo di solito richiede tempo, pertanto si consiglia di salvare tali impostazioni prima di ripristinare le impostazioni predefinite del programma.

Il programma salva per impostazione predefinita tutte le impostazioni personalizzate dell'elenco (se deselezionate). Se non si desidera salvare una delle impostazioni, selezionare la casella corrispondente.

Al termine della configurazione delle impostazioni, premere il pulsante **Avanti**. Si apre la procedura di configurazione guidata. Seguire le istruzioni.

Al termine della procedura di configurazione guidata, per tutti i componenti viene impostato il livello di protezione **Raccomandato**, con l'eccezione delle impostazioni salvate prima di effettuare il ripristino delle impostazioni predefinite. Vengono applicate inoltre le impostazioni configurate con la procedura di configurazione guidata.

CAPITOLO 7. FILE ANTI-VIRUS

Kaspersky Internet Security contiene un componente speciale per la protezione antivirus dei file presenti nel computer, *File Anti-Virus.* Esso viene caricato all'avvio del sistema operativo ed eseguito nella RAM del computer ed esamina tutti i file aperti, salvati o eseguiti dall'utente o da altri programmi.

L'indicatore di funzionamento del componente è l'icona della barra delle applicazioni di Kaspersky Internet Security, che durante la scansione di un file assume questo aspetto  .

Per impostazione predefinita, File Anti-Virus esamina soltanto i *file nuovi o modificati*. In altre parole, esamina i file che sono stati aggiunti o modificati successivamente alla scansione precedente, grazie alle tecnologie iChecker™ e iSwift™ basate su tabelle di checksum dei file. I file vengono esaminati con il seguente algoritmo:

1. Ogni file con cui l'utente o un programma lavora viene intercettato dal componente.
2. File Anti-Virus esamina i database di iChecker e iSwift in cerca di informazioni sul file intercettato. A questo punto vi sono le seguenti possibilità:
    - In assenza di informazioni nel database sul file intercettato, esso viene sottoposto a un'approfondita scansione antivirus. La checksum del file esaminato viene registrata nel database.
    - In assenza di informazioni nel database sul file in questione, File Anti-Virus ne confronta lo status corrente con lo status registrato nel database in occasione della scansione precedente. Se le informazioni corrispondono esattamente, il file viene reso accessibile all'utente senza necessità di scansione. Se il file è stato modificato, sarà sottoposto a una scansione approfondita e le nuove informazioni saranno registrate nel database.

Il processo di scansione si svolge come segue:

1. Il file viene sottoposto a scansione antivirus. Gli oggetti nocivi vengono individuati operando un confronto con gli *elenchi delle minacce* usati dal programma. Gli elenchi contengono le descrizioni di tutti i programmi nocivi, le minacce e gli attacchi di rete noti nonché dei metodi per neutralizzarli.
2. Dopo l'analisi è possibile agire come segue:

a. In caso di rilevamento di un codice nocivo, File Anti-Virus blocca il file interessato, ne salva una copia nel *Backup* e cerca di ripararlo. Se la riparazione ha esito positivo, il file viene reso nuovamente accessibile. In caso contrario il file viene eliminato.

b. Se il codice viene rilevato in un file sospettato di essere nocivo ma senza alcuna prova di ciò, il file viene inviato in *Quarantena*.

c. Se nel file non viene rilevato alcun codice nocivo, il file viene immediatamente ripristinato.

7.1. Selezione di un livello di sicurezza dei file

File Anti-Virus protegge i file in uso ad uno dei seguenti livelli (cfr. Figura 18):

Elevato – il livello di monitoraggio più approfondito dei file aperti, salvati o eseguiti.

Raccomandato. Kaspersky Lab raccomada questo livello. Esso esegue la scansione delle seguenti categorie di oggetti:

- Programmi e file in base ai contenuti
- Solo gli oggetti nuovi e gli oggetti modificati dopo l'ultima scansione
- Archivi inferiori a 8 MB
- Pacchetti di installazione e oggetti OLE incorporati

Basso – livello che consente di utilizzare le applicazioni che richiedono considerevoli risorse di sistema, grazie alla limitazione del numero di file esaminati.

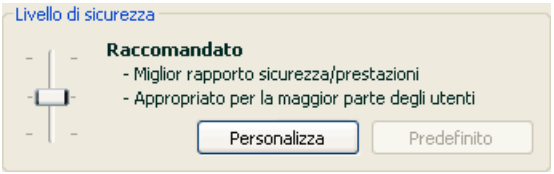


Figura 18. Livello di sicurezza di File Anti-Virus

Per impostazione predefinita, File Anti-Virus è impostato su **Raccomandato**.

È possibile aumentare o ridurre il livello di protezione dei file di lavoro selezionando il livello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Regolando il livello di sicurezza, si definisce il rapporto tra la velocità di scansione e il numero totale di file esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di file esaminati.

Se nessuno dei livelli di sicurezza è ritenuto soddisfacente, è possibile personalizzarne le impostazioni di protezione. Selezionare a tal fine il livello che più si approssima alle esigenze di sicurezza del computer e utilizzarlo come modello per modificare le impostazioni. In tal caso il livello diventa **Personalizzato**. Osserviamo un esempio in cui un livello di sicurezza dei file definito dall'utente può essere particolarmente utile.

Esempio:

Il lavoro svolto sul computer comporta numerosi di tipi di file, alcuni dei quali di dimensioni piuttosto elevate. L'utente non desidera correre il rischio di omettere nella scansione eventuali file a causa delle dimensioni o dell'estensione, anche se ciò potrebbe influire sulla produttività del computer.

Suggerimento per selezionare un livello:

In base ai dati sulla provenienza, si potrebbe concludere che il rischio di infezione da parte di un programma nocivo sia piuttosto elevato. Le dimensioni e il tipo dei file gestiti sono molto eterogenei e l'eventuale esclusione di qualsiasi file dalla scansione comporterebbe un rischio elevato per i dati del computer. L'utente desidera esaminare i file utilizzati in base al contenuto, non in base all'estensione.

Si raccomanda quindi di selezionare inizialmente il livello di sicurezza **Raccomandato** e di apportare le seguenti modifiche: rimuovere le restrizioni sui file eliminati e ottimizzare il funzionamento di File Anti-Virus esaminando solo i file nuovi e modificati. In tal modo la scansione non influirà eccessivamente sulle risorse di sistema e sarà possibile continuare a usare senza problemi altre applicazioni.

Per modificare le impostazioni di un livello di sicurezza:

Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di File Anti-Virus. Modificare le impostazioni di File Anti-Virus nella finestra che si apre e fare clic su **OK**.

Viene quindi creato un quarto livello di sicurezza, **Personalizzato**, che contiene le impostazioni di protezione configurate dall'utente.

7.2. Configurazione di File Anti-Virus

Il modo in cui File Anti-Virus proteggerà il computer su cui è installato dipendono dalla configurazione. Le impostazioni del programma possono essere suddivise nei seguenti gruppi:

- Impostazioni che definiscono i tipi di file (cfr. 7.2.1 a pag. 93) sottoporre alla scansione antivirus
- Impostazioni che definiscono l'ampiezza della protezione (cfr. 7.2.2 a pag. 95)
- Impostazioni che definiscono le reazioni del programma agli oggetti pericolosi individuati (cfr. 7.2.5 a pag. 100).

La presente sezione prende in esame questi gruppi di impostazioni.

7.2.1. Definizione dei tipi di file da esaminare

Selezionando i tipi di file da esaminare, si specificano i formati di file, le dimensioni e le unità da sottoporre alla scansione antivirus all'apertura, esecuzione o salvataggio.

Al fine di agevolare la configurazione, tutti i file sono stati suddivisi in due gruppi: *semplici* e *complessi*. I file semplici non contengono oggetti (per esempio i file .txt). I file complessi possono contenere numerosi oggetti, ciascuno dei quali a sua volta può avere diversi livelli di nidificazione. Gli esempi sono numerosi: archivi, file che contengono macro, fogli di calcolo, e-mail con allegati, ecc.

I tipi di file esaminati vengono definiti nella sezione **Tipi di file** (cfr. Figura 19). Selezionare una delle seguenti opzioni:

Tutti. Con questa opzione selezionata tutti gli oggetti del file system che vengono aperti, eseguiti o salvati saranno esaminati senza eccezioni.

Programmi e documenti (per contenuto). Se è stato selezionato questo gruppo di file, File Anti-Virus esaminerà solo i file potenzialmente infetti, cioè i file che possono contenere virus.

> Nota:
> Vi sono file nei quali non possono annidarsi virus, poiché il codice di tali file non contiene alcun elemento a cui il virus possa attaccarsi, per esempio i file .txt.

Prima di cercare virus in un file, viene analizzata l'intestazione interna del file stesso al fine di individuare il formato (txt, doc, exe, ecc.). Se dall'analisi risulta che il formato del file non consente infezioni, il file viene

escluso dalla scansione e messo immediatamente a disposizione dell'utente. Se il formato file è infettabile, il file viene sottoposto a scansione antivirus.

Programmi e documenti (per estensione). Se è stata selezionata questa opzione, File Anti-Virus esamina solo i file potenzialmente infetti determinando il formato file in base all'estensione. Per mezzo del link estensione [possibile consultare un elenco delle estensioni (cfr. A.1 a pag. 290) esaminate con questa opzione.

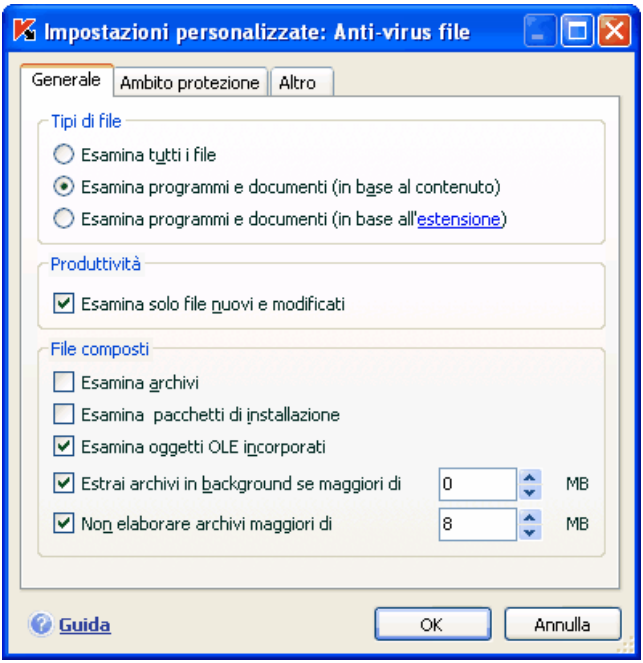


Figura 19. Selezione dei tipi di file sottoposti a scansione antivirus

Suggerimento:
Ricordare che è possibile inviare virus all'interno di file con estensione .txt che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione **Programmi e documenti (per estensione)**, tale file sarebbe escluso dalla scansione. Selezionando invece l'opzione **Programmi e documenti (per contenuto)** ignorando le estensioni, File Anti-Virus analizzerebbe in primo luogo le intestazioni dei file, rivelando il falso file .txt come un file .exe. Il file sarebbe quindi sottoposto a un'approfondita scansione antivirus.

Nella sezione **Efficienza operativa**, è possibile specificare che si desidera sottoporre a scansione antivirus i soli file nuovi o modificati. Questa modalità

riduce considerevolmente la durata della scansione e aumenta la velocità del programma. Per attivare questa modalità, selezionare la casella **Scansiona solo file nuovi e modificati**. Questa modalità si applica sia ai file semplici sia a quelli complessi.

Nella sezione **File compositi**, specificare quali file complessi sottoporre alla scansione antivirus:

- **Scansiona tutti/solo nuovi archivi** – vengono esaminati archivi .zip, .cab, .rar, e .arj, compresi quelli protetti da password.
- **Scansiona tutti/solo nuovi pacchetti di installazione** – vengono sottoposti alla scansione antivirus gli archivi autoestraenti.
- **Scansiona tutti/solo nuovi oggetti OLE incorporati** – vengono esaminati gli oggetti incorporati all'interno di file (per esempio fogli di calcolo Excel o una macro incorporata in un file di MS Word, allegati alle e-mail, ecc.).

Per ogni tipo di file complesso è possibile selezionare ed esaminare tutti i file o solo quelli nuovi usando il link a fianco del nome dell'oggetto. Facendovi clic sopra con il pulsante sinistro del mouse, il suo valore cambia. Se la sezione **Efficienza operativa** è stata impostata in modo da esaminare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file complesso da sottoporre a scansione.

Per specificare quali file complessi non devono essere sottoposti alla scansione antivirus utilizzare le seguenti impostazioni:

- **Non elaborare archivi maggiori di ... MB**. Se le dimensioni di un oggetto complesso superano questo limite, il programma lo esamina come se fosse un oggetto singolo (analizzando l'intestazione) e lo restituisce all'utente. Gli oggetti in esso contenuti saranno esaminati in un secondo momento. Se questa opzione non è stata selezionata, l'accesso ai file di dimensioni superiori sarà bloccato fino a quando saranno stati esaminati.
- **Estrai in background archivi maggiori di ... MB**. Se è stata selezionata questa opzione, i file di dimensioni superiori a quella specificata saranno esclusi dalla scansione.

7.2.2. Definizione dell'ambito della protezione

File Anti-Virus esamina per impostazione predefinita tutti i file che vengono usati, indipendentemente dalla loro posizione, sia essa un disco fisso, un CD-ROM o un'unità flash.

È possibile limitare l'ambito della protezione procedendo come segue:

1. Selezionare **File Anti-Virus** nella finestra principale e aprire la finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Personalizza** e selezionare la scheda **Ambito della protezione** (cfr. Figura 20) nella finestra che si apre.

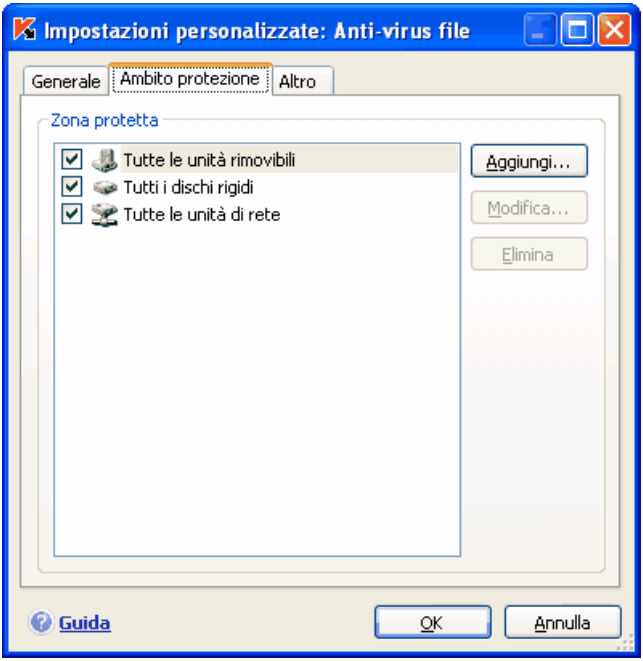


Figura 20. Definizione dell'ambito della protezione

La scheda visualizza un elenco di oggetti che File Anti-Virus analizzerà. La protezione è abilitata per impostazione predefinita per tutti gli oggetti presenti sui dischi fissi, su supporti esterni e su unità di rete connesse al computer. È possibile aggiungere elementi e modificare l'elenco servendosi dei pulsanti **Aggiungi, Modifica** ed **Elimina**.

Se si desidera proteggere un numero minore di oggetti, è possibile procedere come segue:

- Specificare solo le cartelle, le unità e i file che necessitano di protezione.
- Creare un elenco di oggetti che non necessitano di protezione.
- Combinare i metodi uno e due per creare una protezione il cui ambito esclude una serie di oggetti.

Attenzione!

Ricordare che File Anti-Virus esamina solo i file inclusi nell'ambito della protezione creato. I file non inclusi in quell'ambito saranno disponibili per l'uso senza essere sottoposti a scansione antivirus. Ciò incrementa il rischio di infezione del computer.

7.2.3. Configurazione delle impostazioni avanzate

È possibile specificare come impostazioni avanzate Anti-Virus file la modalità di scansione del sistema, nonché configurare le condizioni per mettere temporaneamente in pausa il componente.

Per configurare le impostazioni avanzate Anti-Virus file:

1. Selezionare **Anti-Virus file** nella finestra principale e passare alla finestra delle impostazioni del componente facendo clic sul collegamento Impostazioni.
2. Fare clic sul pulsante **Personalizza** e selezionare la scheda **Altro** nella finestra che si apre (cfr. Figura 21).

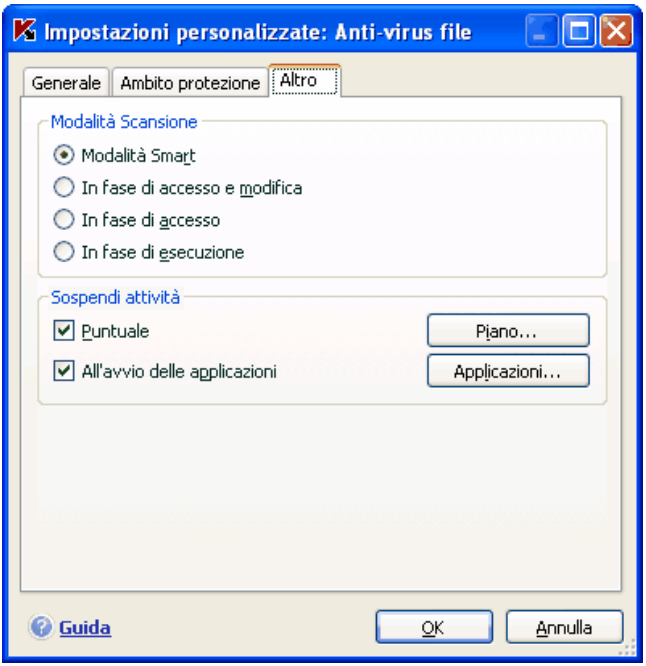


Figura 21. Configurazione delle impostazioni supplementari Anti-Virus file

La modalità di scansione dei file determina le condizioni di elaborazione Anti-Virus file. Sono disponibili le seguenti opzioni:

- **Modalità Smart**. Questa modalità mira ad accelerare l'elaborazione dei file per restituirli all'utente. Quando è selezionata, la decisione di scansione viene presa analizzando le operazioni eseguite col file.

  Ad esempio, quando si utilizza un file di Microsoft Office, Kaspersky Internet Security esamina il file all'apertura iniziale ed alla chiusura finale. Tutte le operazioni che sovrascrivono il file comprese tra queste due operazioni non vengono esaminate.

  La modalità Smart è quella predefinita.

- **In fase di accesso e modifica** – Anti-Virus file esamina i file quando vengono aperti o modificati.

- **In fase di accesso** – i file vengono esaminati solo quando si cerca di aprirli.

- **In fase di esecuzione** – i file vengono esaminati solo quando si cerca di eseguirli.

Potrebbe essere necessario sospendere l'attività di Anti-Virus file quando si eseguono attività che richiedano una grande quantità di risorse del sistema. Per diminuire il carico e fare in modo che l'utente riottenga rapidamente l'accesso ai file, si consiglia di configurare il componente per la disattivazione ad una certa ora o quando vengono utilizzati determinati programmi.

Per sospendere l'attività del componente per un certo tempo, selezionare **Puntuale**, fare clic su **Piano** e assegnare un intervallo per la disattivazione del componente nella finestra che si apre (cfr. Figura 9). Per fare ciò, inserire una valore in formato HH:MM nei campi corrispondenti.

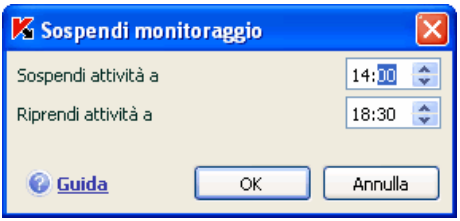


Figura 22. Sospensione dell'attività del componente

Per disattivare il componente quando si lavora con programmi che utilizzano una grande quantità di risorse del sistema, selezionare **All'avvio delle applicazioni** e modificare l'elenco di programmi nella finestra che si apre (cfr. Figura 23) facendo clic su **Applicazioni**.

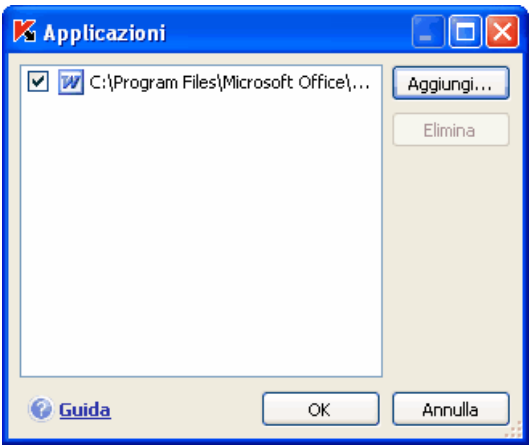


Figura 23. Creazione di un elenco di applicazioni

Per aggiungere un'applicazione all'elenco, utilizzare il pulsante **Aggiungi**. Si apre un menu sensibile al contesto, dal quale, facendo clic su **Sfoglia** si

raggiunge la finestra standard di selezione file per specificare il file eseguibile dell'applicazione da aggiungere; oppure, è possibile passare all'elenco delle applicazioni attualmente in esecuzione scegliendo **Applicazioni** e selezionare quella desiderata.

Per eliminare un'applicazione, selezionarla dall'elenco e fare clic su **Elimina**.

È possibile disabilitare temporaneamente la sospensione dell'attività di Anti-Virus file con un'applicazione specifica, deselezionandone il nome. Non è necessario eliminarla dall'elenco.

7.2.4. Ripristino delle impostazioni di File Anti-Virus

Durante la configurazione di File Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di sicurezza **Raccomandato**.

Per ripristinare le impostazioni predefinite di File Anti-Virus:

1. Selezionare **File Anti-Virus** nella finestra principale e aprire la finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

7.2.5. Selezione delle azioni da applicare agli oggetti

Se durante la scansione antivirus File Anti-Virus rileva o sospetta la presenza di un'infezione all'interno di un file, le fasi successive dipendono dallo status dell'oggetto e dall'azione selezionata.

File Anti-Virus applica agli oggetti i seguenti status:

- Programma nocivo (per esempio, *virus, troiano*).
- *Probabilmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il codice del file contiene una sezione che sembra essere la variante di un virus noto o ricorda la struttura di una sequenza virale.

Per impostazione predefinita, tutti i file infetti sono sottoposti a un tentativo di riparazione e se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

Selezionare **File Anti-Virus** nella finestra principale e aprire la finestra delle impostazioni del componente facendo clic su Impostazioni. Tutte le azioni potenziali sono visualizzate nelle sezioni appropriate (cfr. Figura 24).

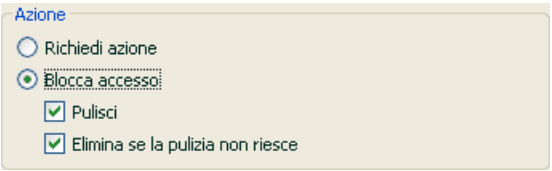


Figura 24. Azioni possibili di File Anti-Virus in caso di oggetti pericolosi

Se l'azione selezionata è	Quando viene rilevato un oggetto pericoloso
Richiedi azione	File Anti-Virus visualizza un avvertimento contenente informazioni sul programma nocivo che ha o potrebbe aver infettato il file e propone una serie di azioni da scegliere. Tali azioni dipendono dallo status dell'oggetto.
Blocca accesso	File Anti-Virus blocca l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel report (cfr. 17.3 a pag. 237). In un secondo momento sarà possibile tentare di riparare l'oggetto.
Blocca accesso **Pulisci**	File Anti-Virus blocca l'accesso all'oggetto e cerca di ripararlo. Se la riparazione ha esito positivo, il file viene ripristinato per l'uso. Se la riparazione non è stata possibile, l'oggetto viene spostato in Quarantena (cfr. 17.1 a pag. 231). Le informazioni relative all'evento vengono registrate nel report. In un secondo momento sarà possibile tentare di riparare l'oggetto.
Blocca accesso **Pulisci** **Elimina se la pulizia non riesce**	File Anti-Virus blocca l'accesso all'oggetto e cerca di ripararlo. Se la riparazione ha esito positivo, il file viene ripristinato per l'uso. Se la riparazione non riesce, l'oggetto viene eliminato. Una copia dell'oggetto viene

Se l'azione selezionata è	Quando viene rilevato un oggetto pericoloso
	conservata nel Backup (cfr. 17.2 a pag. 234).
Blocca accesso **Pulisci** **Elimina**	File Anti-Virus blocca l'accesso all'oggetto e lo elimina.

Indipendentemente dallo status dell'oggetto (infetto o potenzialmente infetto), prima di cercare di riparare l'oggetto o di eliminarlo Kaspersky Internet Security crea una copia di backup e la invia nell'area di Backup, da dove potrà essere recuperata qualora si renda necessario il ripristino dell'oggetto o si presenti un'opportunità di ripararlo.

7.3. Riparazione posticipata

Se l'azione da applicare ai programmi nocivi è **Blocca accesso**, l'accesso agli oggetti viene bloccato e la riparazione non viene eseguita.

Se l'azione selezionata fosse

Blocca accesso
Pulisci

sarebbe bloccato l'accesso anche a tutti gli oggetti non trattati.

Per poter accedere di nuovo agli oggetti bloccati è necessario prima ripararli. Procedere come segue:

1. Selezionare **File Anti-Virus** nella finestra principale del programma e fare clic con il pulsante sinistro su un punto qualsiasi del riquadro **Statistiche**.
2. Selezionare gli oggetti desiderati nella scheda **Rilevati** e fare clic sul pulsante **Azioni → Neutralizza tutti**.

Se riparato con successo, l'oggetto sarà messo di nuovo a disposizione dell'utente. Se la riparazione non riesce, è possibile *eliminare* l'oggetto o *ignorarlo*. In quest'ultimo caso, l'accesso al file sarà ripristinato. Questo tuttavia incrementa considerevolmente il rischio di infezione del computer, pertanto si raccomanda di non ignorare gli oggetti nocivi.

CAPITOLO 8. MAIL ANTI-VIRUS

Kaspersky Internet Security comprende uno speciale componente che protegge la posta in arrivo e in uscita dagli oggetti pericolosi: *Mail Anti-Virus*. Esso viene eseguito all'avvio del sistema, rimane attivo nella memoria di sistema ed esamina tutta la posta basata sui protocolli POP3, SMTP, IMAP, MAPI[1] e NNTP, nonché la crittografia per POP3 e IMAP (SSL).

L'indicatore di funzionamento del componente è l'icona della barra delle applicazioni di Kaspersky Internet Security, che durante la scansione di un messaggio di posta elettronica assume questo aspetto  .

La configurazione predefinita di Mail Anti-Virus è la seguente:

1. Mail Anti-Virus intercetta ciascun messaggio ricevuto o inviato dall'utente.
2. Il messaggio viene suddiviso nelle parti che lo compongono: intestazioni e-mail header, corpo del messaggio, allegati.
3. Il corpo del messaggio e gli allegati (inclusi gli allegati OLE) vengono esaminati per escludere la presenza di oggetti pericolosi. Gli oggetti nocivi vengono individuati per mezzo degli *elenchi delle minacce* incluse nel programma e con l'algoritmo euristico. Gli elenchi contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti negli elenchi.
4. Dopo la scansione antivirus è possibile scegliere tra le seguenti azioni:
    - Se il corpo del messaggio o gli allegati contengono codici nocivi, Mail Anti-Virus blocca il messaggio, salva una copia dell'oggetto infetto nella cartella *Backup* e cerca di riparare l'oggetto. Se la riparazione del messaggio ha esito positivo, esso viene reso nuovamente disponibile per l'utente. In caso contrario, l'oggetto infetto all'interno del messaggio viene eliminato. Dopo la scansione antivirus, nel campo dell'oggetto del messaggio viene inserito un testo che dichiara che il messaggio è stato esaminato da Kaspersky Internet Security.
    - Se nel corpo del messaggio o in un allegato viene individuato un codice che sembra nocivo ma senza alcuna certezza, la

[1] Emails sent with MAPI are scanned using a special plug-in for Microsoft Office Outlook and The Bat!

parte sospetta del messaggio viene trasferita nella cartella *Quarantena*.

- Se all'interno del messaggio non viene individuato alcun codice nocivo, il messaggio viene reso nuovamente disponibile.

Il programma è dotato di uno speciale plug-in (cfr. 8.2.2 a pag. 108) per MS Outlook in grado di configurare le scansioni della posta con maggior precisione.

Se il client di posta utilizzato è The Bat!, è possibile usare Kaspersky Internet Security in aggiunta ad altre applicazioni antivirus. Le regole di trattamento del traffico e-mail (cfr. 8.2.3 a pag. 110) sono configurate direttamente da The Bat! e sostituiscono le impostazioni di protezione della posta di Kaspersky Internet Security.

Quando si lavora con altri programmi di posta (fra cui Outlook Express, Mozilla Thunderbird, Eudora, Incredimail), Mail Anti-Virus esamina la posta basata sui protocolli SMTP, POP3, IMAP, MAPI e NNTP.

Osservare che i messaggi trasmessi mediante il protocollo IMAP non vengono esaminati in Thunderbird se si fa uso di filtri che li trasferiscono fuori dalla casella di posta in arrivo.

Mail Anti-Virus, inoltre, non esamina i messaggi trasmessi mediante il protocollo SSL.

8.1. Selezione di un livello di protezione della posta elettronica

Kaspersky Internet Security protegge la posta elettronica in base a uno dei seguenti livelli (cfr. Figura 25):

Elevato – il livello che garantisce il monitoraggio più approfondito della posta in entrata e in uscita. Il programma esamina approfonditamente gli allegati di posta, inclusi gli archivi, indipendentemente dalla durata della scansione.

Raccomandato. È il livello consigliato dagli esperti Kaspersky Lab. A questo livello di protezione vengono esaminati gli stessi oggetti del livello **Elevato**, con l'eccezione degli allegati o dei messaggi la cui scansione richiederebbe più di 3 minuti.

Basso – livello di sicurezza le cui impostazioni consentono di utilizzare applicazioni che assorbono risorse considerevoli, grazie alla limitazione dell'ambito della scansione. In base a queste impostazioni, viene esaminata solo la posta in entrata, escludendo però gli archivi e gli oggetti (e-mail) allegati la cui scansione richiederebbe più di tre minuti. Questo livello è consigliato se nel computer sono installate altre applicazioni di protezione della posta elettronica.

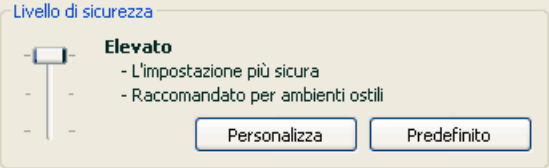


Figura 25. Selezione di un livello di protezione della posta elettronica

Per impostazione predefinita, la protezione della posta elettronica è impostata su **Raccomandato**.

È possibile aumentare o ridurre il livello di protezione della posta selezionando il livello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Modificando il livello di protezione, si definisce il rapporto tra la velocità di scansione e il numero totale di oggetti esaminati: La velocità di scansione è inversamente proporzionale al numero di oggetti e-mail esaminati.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile modificarne le impostazioni. In questo caso il livello diventa **Impostazioni personalizzate**. Osserviamo un esempio in cui un livello di protezione della posta elettronica definito dall'utente può essere particolarmente utile.

Esempio:

Il computer si trova all'esterno della LAN e si connette a Internet mediante connessione remota. Il client installato per ricevere e inviare la posta elettronica è Outlook Express e il servizio utilizzato è gratuito. Per varie ragioni, il traffico di posta elettronica prevede un certo numero di archivi allegati. Come garantire una protezione ottimale del computer dalle infezioni trasmesse attraverso la posta elettronica?

Suggerimento per selezionare un livello:

Analizzando la situazione, si potrebbe concludere che il rischio di infezione attraverso la posta elettronica sia piuttosto elevato (a causa dell'assenza di una protezione centralizzata della posta elettronica e del metodo di connessione a Internet).

Il livello di protezione consigliato è quindi **Elevato**, apportando le seguenti modifiche: Si consiglia di ridurre il tempo di scansione degli allegati, per esempio a 1-2 minuti. La maggior parte degli archivi allegati sarà così sottoposta a scansione antivirus ma la velocità di elaborazione non sarà pregiudicata.

Per modificare un livello di protezione predefinito:

Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di Mail Anti-Virus. Modificare le impostazioni di protezione nella finestra che si apre e fare clic su **OK**.

8.2. Configurazione di Mail Anti-Virus

Le modalità di scansione della posta dipendono da una serie di impostazioni che possono essere suddivise nei seguenti gruppi:

- Impostazioni che definiscono il gruppo di messaggi protetto (cfr. 8.2.1 a pag. 106)
- Impostazioni di scansione della posta per MS Outlook (cfr. 8.2.2 a pag. 108) e The Bat! (cfr. 8.2.3 a pag. 110)

> Attenzione!
>
> Questa versione di Kaspersky Internet Security non offre plug-in Mail Anti-Virus per le versioni a 64 bit dei client di posta elettronica.

- Impostazioni che definiscono le azioni da eseguire in caso di oggetti di posta pericolosi (cfr. 8.2.4 a pag. 112).

La presente sezione prende in esame queste impostazioni.

8.2.1. Selezione di un gruppo di messaggi protetto

Mail Anti-Virus consente di selezionare i gruppi di messaggi da esaminare per escludere la presenza di oggetti pericolosi.

Per impostazione predefinita, il componente protegge la posta elettronica al livello di protezione **Raccomandato**, esaminando cioè sia i messaggi in arrivo sia quelli in uscita. La prima volta che si lavora con il programma è consigliabile esaminare la posta in uscita in quanto è probabile che il computer nasconda worm che si servono della posta elettronica come canale di diffusione. Questo

accorgimento eviterà il rischio che il computer invii inavvertitamente mailing di massa con oggetti infetti.

Se si è certi che i messaggi che si inviano non contengano oggetti pericolosi, è possibile disabilitare la scansione della posta in uscita procedendo come segue:

1. Fare clic sul pulsante **Personalizza** nella finestra di configurazione di Mail Anti-Virus.
2. Nella finestra delle impostazioni di Mail Anti-Virus che si apre (cfr. Figura 26), selezionare **I messaggi in entrata** nella sezione **Portata**.

Figura 26. Impostazioni di Mail Anti-Virus

Oltre a selezionare un gruppo di messaggi, è possibile specificare se sottoporre alla scansione anche gli archivi allegati e impostare la durata massima della scansione di un oggetto di posta. Queste impostazioni vengono configurate nella sezione **Limitazioni**.

Se il computer non è protetto da alcun software di rete locale e la connessione a Internet non prevede l'uso di un server proxy o di una firewall, si raccomanda di non disabilitare la scansione degli archivi allegati e di non impostare una limitazione temporale alla scansione.

Se invece si lavora in un ambiente protetto, è possibile modificare le limitazioni temporali alla scansione in modo da incrementare la velocità.

È possibile configurare anche le condizioni di filtraggio degli oggetti allegati a un messaggio nella sezione **Filtro allegati**:

- **Disabilita filtro** – consente di non utilizzare ulteriori filtri per gli allegati.
- **Rinomina i tipi di file selezionati** – consente di escludere gli allegati di formati specifici e di sostituire l'ultimo carattere del nome di un file con un trattino di sottolineatura. Per selezionare il tipo di file, fare clic sul pulsante **Tipi di file**.
- **Elimina i tipi di file selezionati** – consente di escludere ed eliminare gli allegati di formati specifici. Per selezionare il tipo di file, fare clic sul pulsante **Tipi di file**.

Per ulteriori informazioni sui tipi di allegati filtrati, consultare la sezione A.1 a pag. 290.

L'uso del filtro rappresenta un'ulteriore sicurezza per il computer, poiché nella maggior parte dei casi i programmi nocivi si diffondono attraverso la posta in forma di allegati. Rinominando o eliminando determinati tipi di allegati, si previene l'apertura automatica degli allegati all'arrivo di un messaggio e si evitano altri rischi potenziali.

8.2.2. Configurazione del trattamento della posta in Microsoft Office Outlook

Se il client di posta utilizzato è Outlook, è possibile impostare una configurazione personalizzata delle scansioni antivirus.

Durante l'installazione di Kaspersky Internet Security, viene installato in Outlook uno speciale plug-in in grado di accedere rapidamente alle impostazioni di Mail Anti-Virus e di impostare l'ora di avvio della scansione antivirus dei messaggi.

Attenzione!

Questa versione di Kaspersky Internet Security non offre plug-in Mail Anti-Virus per la versione a 64 bit di Microsoft Office Outlook.

Il plug-in ha l'aspetto di una scheda di **Mail Anti-Virus** ubicata in **Strumenti** → **Impostazioni** (cfr. Figura 27).

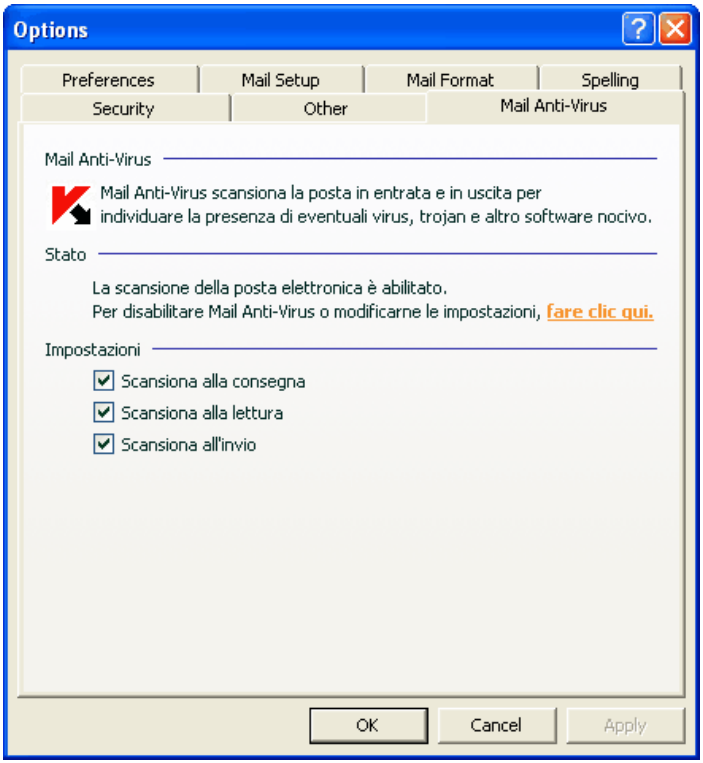


Figura 27. Configurazione delle impostazioni di Mail Anti-Virus in MS Outlook

Selezionare una modalità di scansione della posta:

- **Scansiona alla consegna** – consente di analizzare ogni messaggio nel momento in cui viene consegnato.
- **Scansiona alla lettura** – consente di esaminare i messaggi nel momento in cui vengono aperti.
- **Scansiona all'invio** – consente di eseguire la scansione antivirus dei messaggi in uscita nel momento dell'invio.

Attenzione!

Se si utilizza Outlook per connettersi al server di posta mediante protocollo IMAP, si raccomanda di non utilizzare la modalità **Scansiona alla consegna**. Se si abilita questa modalità, i messaggi di posta elettronica vengono copiati sul computer locale alla consegna al server, perdendo di conseguenza il vantaggio principale del protocollo IMAP, cioè la riduzione del traffico e la gestione della posta indesiderata direttamente sul server senza copiarla sul computer dell'utente.

L'azione da eseguire sugli oggetti di posta pericolosi è definita tra le impostazioni di Mail Anti-Virus. Per configurarle, fare clic qui.

8.2.3. Configurazione delle scansioni di posta in The Bat!

Le azioni da eseguire sugli oggetti di posta infetti in The Bat! sono definite per mezzo degli strumenti del programma.

Attenzione!

Le impostazioni di Mail Anti-Virus che determinano se esaminare i messaggi in arrivo e in uscita, nonché le azioni da eseguire sugli oggetti di posta pericolosi e le esclusioni, sono ignorate. Gli unici elementi di cui The Bat! tiene conto sono la scansione degli archivi allegati e le limitazioni temporali della scansione dei messaggi (cfr. 8.2.1 a pag. 106).

Questa versione di Kaspersky Internet Security non offre plug-in Mail Anti-Virus per la versione a 64 bit di The Bat!

Per impostare le regole di protezione della posta in The Bat!:

1. Selezionare **Impostazioni** dal menu **Proprietà** del programma di posta.
2. Selezionare **Protezione virus** dalla struttura ad albero delle impostazioni.

Le impostazioni di protezione visualizzate (cfr. Figura 28) valgono per tutti i moduli antivirus installati nel computer che supportano The Bat!

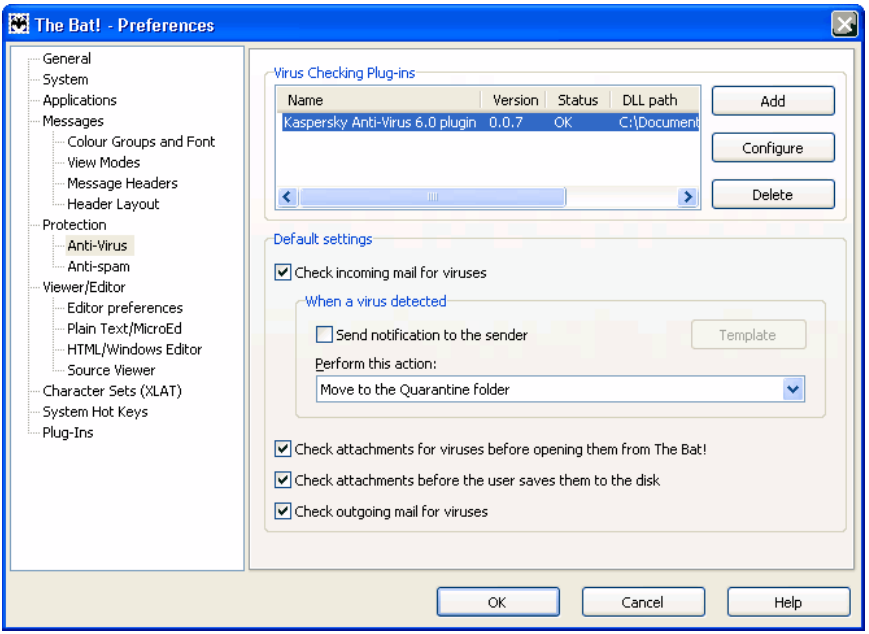


Figura 28. Configurazione delle scansioni di posta in The Bat!

A questo punto occorre stabilire:

- Quali gruppi di messaggi saranno sottoposti alla scansione antivirus (in arrivo, in uscita)
- In quale momento saranno gli oggetti di posta saranno sottoposti alla scansione antivirus (all'apertura del messaggio o prima di salvarlo sul disco)
- Le azioni da eseguire in caso di intercettazione di oggetti pericolosi nei messaggi. Per esempio, è possibile selezionare:

  Prova a curare le parti infettate – consente di riparare l'oggetto di posta infetto; se la riparazione non riesce, l'oggetto resta nel messaggio. Kaspersky Internet Security informa sempre l'utente ogni volta che viene individuato un messaggio infetto. Ma anche selezionando **Elimina** nella finestra degli avvisi di Mail Anti-Virus, l'oggetto rimane nel messaggio poiché l'azione selezionata in The Bat! ha la precedenza su quelle di Mail Anti-Virus.

  Rimuovi le parti infettate – consente di eliminare l'oggetto pericoloso dal messaggio, sia esso effettivamente infetto o solo sospettato di esserlo.

Per impostazione predefinita, The Bat! trasferisce tutti gli oggetti di posta infetti nella cartella Quarantena senza ripararli.

Attenzione!

The Bat! non evidenzia con intestazioni speciali i messaggi contenenti oggetti pericolosi.

8.2.4. Ripristino delle impostazioni predefinite di Mail Anti-Virus

Durante la configurazione di Mail Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di sicurezza **Raccomandato**.

Per ripristinare le impostazioni predefinite di Mail Anti-Virus:

1. Selezionare **Mail Anti-Virus** nella finestra principale e aprire la finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

8.2.5. Selezione delle azioni da eseguire sugli oggetti di posta pericolosi

Se una scansione della posta evidenzia messaggi o parti di messaggio (intestazione, corpo, allegati) infetti o sospetti, le operazioni successive di Mail Anti-Virus dipendono dallo status dell'oggetto e dall'azione selezionata.

Dopo la scansione, agli oggetti di posta possono essere associati i seguenti status:

- Status di programma nocivo (per esempio, *virus, troiano*; per ulteriori informazioni, cfr. 1.1 a pag. 11).
- *Probabilmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il codice del file contiene una sezione che sembra essere la variante di un virus noto o ricorda la struttura di una sequenza virale.

Per impostazione predefinita, quando Mail Anti-Virus rileva un oggetto pericoloso o potenzialmente infetto, visualizza un avviso e invita l'utente di selezionare un'azione.

Per modificare un'azione da applicare a un oggetto:

Aprire la finestra delle impostazini di Kaspersky Internet Security e selezionare la sezione **Mail Anti-Virus**. Tutte le azioni possibili per gli oggetti pericolosi sono elencate nella casella **Azione** (cfr. Figura 29).

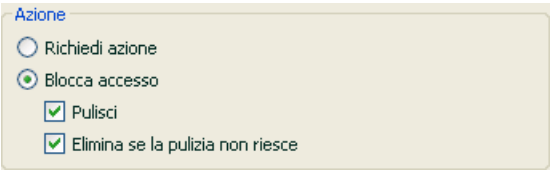


Figura 29. Selezione delle azioni da eseguire sugli oggetti di posta pericolosi

Osserviamo adesso in dettaglio le possibili opzioni di trattamento degli oggetti di posta pericolosi.

Se l'azione selezionata è	**Quando viene rilevato un oggetto pericoloso**
Richiedi azione	Mail Anti-Virus visualizza un avviso (cfr. 5.8 a pag. 65) con informazioni sul programma nocivo che ha infettato *probabilmente) il file e offre l-opzione di unoa delle seguenti azioni.
Blocca accesso	Mail Anti-Virus non elabora l'oggetto. Le informazioni relative all'evento vengono registrate nel report (cfr. 17.3 a pag. 237). In un secondo momento sarà possibile tentare di riparare l'oggetto.
Blocca accesso **Pulisci**	Mail Anti-Virus esegue una delle seguenti azioni: • Cerca di trattare l'oggetto infetto. Se la riparazione ha esito positivo, il file viene reso disponibile per l'uso. Se la riparazione non è possibile, l'accesso all'oggetto viene bloccato. Le informazioni relative all'evento vengono registrate nel report. In un secondo momento sarà possibile tentare di riparare l'oggetto. • Trasferisce l'oggetto potenzialmente infetto in Quarantena. In seguito sarà

	possibile cercare di riparare l'oggetto o ripristinarlo nella posizione originaria.
Blocca accesso **Pulisci** **Elimina se la pulizia non è riesce**[2]	Mail Anti-Virus esegue una delle seguenti azioni: • Cerca di trattare l'oggetto infetto. Se la riparazione ha esito positivo, il file viene reso disponibile per l'uso. Se la riparazione non riesce, l'oggetto viene eliminato. • Trasferisce l'oggetto potenzialmente infetto in Quarantena (cfr. 17.1 a pag. 231).
Blocca accesso **Pulisci** **Elimina**	Quando Mail Anti-Virus individua un oggetto infetto o potenzialmente infetto, lo elimina senza informare l'utente.

Indipendentemente dallo status dell'oggetto (infetto o potenzialmente infetto), prima di cercare di riparare l'oggetto o di eliminarlo Kaspersky Internet Security crea una copia di backup e la invia nella cartella Backup (cfr. 17.2 a pag. 234) da dove potrà essere recuperato qualora si renda necessario il ripristino dell'oggetto o si presenti un'opportunità di ripararlo.

[2] Se il client in uso è The Bat!, gli oggetti di posta pericolosi vengono riparati o eliminati quando Mail Anti-Virus esegue questa azione (a seconda dell'azione selezionata in The Bat!).

CAPITOLO 9. WEB ANTI-VIRUS

Ogni volta che si usa Internet, si espongono le informazioni custodite nel computer al rischio di infezione da parte di programmi pericolosi. Questi possono essere caricati nel computer aprendo un determinato sito web o leggendo un articolo su Internet.

Kaspersky Internet Security include uno speciale componente per la protezione del computer durante la navigazione su Internet: Web Anti-Virus. Esso protegge le informazioni che entrano nel computer attraverso il protocollo HTTP e impedisce il caricamento di script pericolosi sul computer.

Attenzione!

Web Anti-Virus controlla solo il traffico HTTP che passa attraverso le porte elencate nell'elenco delle porte monitorate (cfr. 17.7 a pag. 258). Il pacchetto del programma include un elenco delle porte più comunemente utilizzate per la trasmissione della posta e del traffico HTTP. Se si utilizzano porte non presenti in questo elenco è necessario aggiungerle al fine di proteggere il traffico che passa attraverso di esse.

Se si lavora in uno spazio non protetto o si accede a Internet via modem, si raccomanda di utilizzare Web Anti-Virus per proteggere il computer durante l'uso di Internet. Se il computer è collegato a una rete protetta da firewall o da filtri per il traffico HTTP, Web Anti-Virus offre un'ulteriore protezione durante la navigazione sul Web.

L'indicatore di funzionamento del componente è l'icona della barra delle applicazioni di Kaspersky Internet Security, che durante la scansione di uno script assume questo aspetto  .

Osserviamo in dettaglio il funzionamento del componente.

Web Anti-Virus si compone di due moduli che gestiscono:

- *Scansione traffico* – scansione degli oggetti che entrano nel computer mediante HTTP.
- *Scansione browser* – scansione di tutti gli script Java e Visual Basic caricati durante l'uso del computer e la navigazione Internet.

Attenzione!

Questa versione dell'applicazione non prevede la scansione degli script per le applicazioni a 64 bit.

- È presente inoltre uno speciale plug-in per Microsoft Internet Explorer che viene installato con Kaspersky Internet Security. L'icona nel pannello strumenti del browser significa che esso è installato. Facendo clic sull'icona, si apre una finestra contenente le statistiche di Web Anti-Virus sul numero di script esaminati e bloccati.

Web Anti-Virus monitora il traffico HTTP con le seguenti modalità:

1. Ogni pagina web o file accessibile all'utente o a un determinato programma via HTTP viene intercettata e analizzata da Web Anti-Virus per escludere la presenza di codici nocivi. Gli oggetti nocivi vengono individuati per mezzo degli *elenchi delle minacce* inclusi in Kaspersky Internet Security e con l'algoritmo euristico. Gli elenchi contengono le descrizioni di tutti i programmi nocivi noti e dei metodi per neutralizzarli. L'algoritmo euristico è in grado di rilevare nuovi virus non ancora inseriti negli elenchi.
2. Dopo l'analisi è possibile agire come segue:
    a. Se la pagina web o l'oggetto a cui l'utente sta cercando di accedere contengono un codice nocivo, il programma li blocca. Viene quindi visualizzato un messaggio che informa che l'oggetto o pagina è infetto.
    b. Se il file o la pagina web non contengono codici nocivi, il programma li rende immediatamente accessibili all'utente.

Gli script vengono esaminati secondo il seguente algoritmo:

1. Web Anti-Virus intercetta ogni script eseguito in una pagina web e lo esamina per escludere la presenza di codici nocivi.
2. Se uno script contiene un codice nocivo, Web Anti-Virus lo blocca e informa l'utente con un avviso a comparsa.
3. Se nello script non viene rilevato alcun codice nocivo, esso viene eseguito.

9.1. Selezione del livello di protezione web

Kaspersky Internet Security protegge il computer durante la navigazione in Internet in base a uno dei seguenti livelli (cfr. Figura 30):

Elevato – il livello che garantisce il monitoraggio più approfondito di script e oggetti in arrivo mediante HTTP. Il programma esegue un'accurata scansione di tutti gli oggetti utilizzando l-intero elenco delle minacce.

Questo livello di protezione è consigliato per gli ambienti sensibili in cui non si utilizzano altri strumenti di sicurezza HTTP.

Raccomandato. È il livello consigliato dagli esperti Kaspersky Lab. Questo livello esamina gli stessi oggetti presi in considerazione dal livello **elevato**, ma applica una limitazione del tempo di caching per i frammenti di file, accelerando la scansione e rendendo disponibili gli oggetti più rapidamente.

Basso – è un livello di protezione le cui impostazioni consentono di utilizzare applicazioni che assorbono risorse considerevoli, grazie alla restrizione dell'ambito della scansione ottenuta utilizzando un elenco di minacce limitato. Questo livello è consigliato se nel computer sono installate altre applicazioni di protezione web.

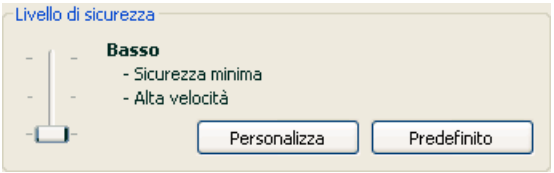


Figura 30. Selezione di un livello di protezione web

Per impostazione predefinita, la protezione è impostata sul livello **Raccomandato**.

È possibile aumentare o ridurre il livello di protezione selezionando quello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Modificando il livello di protezione, si definisce il rapporto tra la velocità di scansione e il numero totale di oggetti esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di oggetti esaminati.

Se nessuno dei livelli preimpostati risulta soddisfacente, è possibile crearne uno personalizzato. Osserviamo un esempio in cui la creazione di un livello personalizzato risulta utile.

Esempio:

Il computer dell'utente si connette a Internet via modem. Non è connesso a una LAN aziendale e non è protetto da alcuna misura antivirus per il traffico HTTP in entrata.

A causa della natura stessa del suo lavoro, l'utente scarica regolarmente file di grandi dimensioni da Internet. La scansione di file di questo genere, di norma, richiede tempi piuttosto lenti.

Come garantire quindi una protezione ottimale del computer contro le infezioni trasmesse attraverso il traffico HTTP o gli script?

Suggerimento per selezionare un livello:

Da queste informazioni basilari, possiamo concludere che il computer lavora in un ambiente sensibile e che il rischio di contrarre infezioni attraverso il traffico HTTP è elevato (nessuna protezione web centralizzata, metodo di connessione a Internet).

Il livello di protezione consigliato è quindi **Elevato**, apportando le seguenti modifiche: Si raccomanda di ridurre il tempo di caching dei frammenti di file durante la scansione.

Per modificare un livello di protezione predefinito:

Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di Web Anti-Virus. Modificare le impostazioni di protezione web (cfr. 9.2 a pag. 118) nella finestra che si apre e fare clic sul pulsante **OK**.

9.2. Configurazione di Web Anti-Virus

Web Anti-Virus esamina tutti gli oggetti caricati nel computer tramite HTTP e monitora tutti gli script Java o Visual Basic eseguiti.

Per accelerare la velocità del componente è possibile configurare alcune impostazioni, in particolare:

- Impostare l'algoritmo di scansione selezionando un set di elenchi di minacce completo o ridotto.
- Creare un elenco di indirizzi attendibili.

Inoltre è possibile selezionare le azioni che Web Anti-Virus eseguirà ogni volta che rileva oggetti HTTP pericolosi.

La presente sezione prende in esame queste impostazioni.

9.2.1. Impostazione di un metodo di scansione

È possibile esaminare i dati provenienti da Internet in base a uno dei seguenti algoritmi:

- *Scansione di flussi (database anti-virus limitato)* – tecnologia di rilevamento dei codici nocivi per il traffico di rete, che esamina i dati in tempo reale. Per esempio, durante lo scaricamento di un file da Internet, Web Anti-Virus esamina i file man mano che se ne scaricano porzioni nel

computer. Questa tecnologia consente all'utente di disporre con maggiore rapidità dell'oggetto scansionato. Al tempo stesso, le scansioni in streaming applicano un elenco di firme ridotto (che comprende solo le firme più attive), riducendo in maniera significativa il livello di sicurezza della navigazione iInternet.

- *Scansione di buffer (database anti-virus completo)* – tecnologia di rilevamento dei codici nocivi per il traffico di rete, che esamina gli oggetti solo dopo che sono stati scaricati completamente nel buffer. A questo punto, l'oggetto viene sottoposto alla scansione antivirus e, in base ai risultati, messo a disposizione dell'utente o bloccato.
  Questo tipo di scansione applica l'elenco completo delle firme, massimizzando il rilevamento di codici nocivi. Questo algoritmo, tuttavia, rallenta i tempi di elaborazione e posticipa l'accesso dell'utente agli oggetti, e può provocare problemi durante la copia e l'elaborazione di oggetti di grandi dimensioni in seguito all'interruzione della connessione con il client HTTP.
  Per risolvere questo problema si suggerisce di ridurre il tempo di caching dei frammenti di oggetto scaricati da Internet. Allo scadere di questo limite temporale, l'utente riceve la parte scaricata del file non scansionata; l'oggetto sarà sottoposto a scansione antivirus solo dopo essere stato scaricato completamente. In tal modo l'utente è in grado di accedere all'oggetto con maggiore rapidità risolvendo il problema dell'interruzione della connessione senza ridurre la sicurezza d'uso di Internet.

Per selezionare l'algoritmo di scansione utilizzato da Web Anti-Virus:

1. Fare clic sul pulsante **Personalizza** nella finestra di configurazione di Web Anti-Virus.
2. Nella finestra che si apre (cfr. Figura 31), selezionare l'opzione desiderata nella sezione **Metodo di scansione**.

Per impostazione predefinita, Web Anti-Virus esamina i dati provenienti da Internet per mezzo di un buffer e utilizza l'elenco completo delle firme. Il tempo di caching dei frammenti di file è ridotto a un secondo.

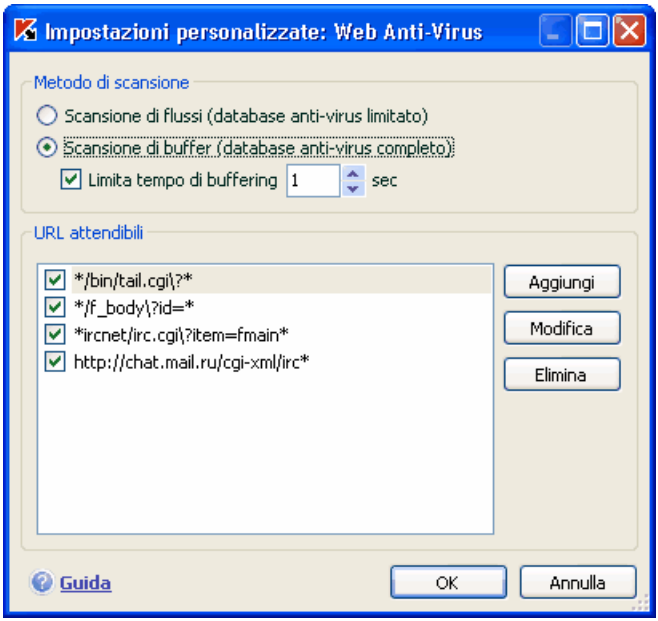


Figura 31. Configurazione di Web Anti-Virus

Attenzione!
In caso di problemi di accesso a risorse quali radio Internet, video streaming o Internet conferencing, utilizzare la scansione in streaming.

9.2.2. Creazione di un elenco di indirizzi attendibili

È possibile creare un elenco di indirizzi i cui contenuti sono ritenuti attendibili. Web Anti-Virus non analizzerà i dati provenienti da quegli indirizzi. Questa opzione può essere utilizzata nei casi in cui Web Anti-Virus interferisce con il normale uso di Internet, per esempio durante lo scaricamento di un file specifico che viene bloccato da Web Anti-Virus ogni volta che si tenta di scaricarlo.

Per creare un elenco degli indirizzi attendibili:

1. Fare clic sul pulsante **Personalizza** nella finestra di configurazione di Web Anti-Virus.
2. Nella finestra che si apre (cfr. Figura 31), creare un elenco dei server attendibili nella sezione **URL attendibili**. A questo scopo utilizzare i pulsanti sulla destra dell'elenco.

Al momento di digitare un indirizzo affidabile, è possibile creare delle maschere con i seguenti caratteri jolly:

***** – qualsiasi combinazione di caratteri.
Esempio: Se si è creata la maschera ***abc***, non verrà esaminata alcuna URL contenente la sequenza **abc**. Ad esempio: www.virus.com/download_virus/page_0-9abcdef.html

? – qualsiasi carattere singolo.
Esempio: Se si è creata la maschera **Patch_123?.com**, le URL contenenti la sequenza indicata seguita da qualsiasi carattere in sostituzione del punto interrogativo non saranno esaminate. Ad esempio: **Patch_1234.com** Tuttavia l'URL **patch_12345.com** sarà esaminata.

Se i caratteri * o ? fanno effettivamente parte dell'URL da aggiungere all'elenco, digitare una barra inversa per ignorare il carattere * o ? che segue.

Esempio: Si desidera aggiungere questa URL all'elenco degli indirizzi attendibili: www.virus.com/download_virus/virus.dll?virus_name=

Per evitare che Kaspersky Internet Security consideri il **?** come un carattere jolly, è necessario farlo precedere da una barra inversa (\ ). Di conseguenza, l'URL aggiunta all'elenco delle esclusioni sarà come segue: www.virus.com/download_virus/virus.dll\?virus_name=

9.2.3. Ripristino delle impostazioni di Web Anti-Virus

Durante la configurazione di Web Anti-Virus, è possibile ripristinare in qualsiasi momento le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di sicurezza **Raccomandato**.

Per ripristinare le impostazioni predefinite di Web Anti-Virus:

1. Selezionare **Web Anti-Virus** nella finestra principale e aprire la finestra delle impostazioni del componente facendo clic su Impostazioni.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

9.2.4. Selezione delle reazioni agli oggetti pericolosi

Se l'analisi di un oggetto HTTP evidenzia la presenza di un codice nocivo, la reazione di Web Anti-Virus dipende dall'azione selezionata dall'utente.

Per configurare le reazioni di Web Anti-Virus in presenza di un oggetto pericoloso:

Aprire la finestra delle impostazini di Kaspersky Internet Security e selezionare la sezione **Web Anti-Virus**. Tutte le azioni possibili per gli oggetti pericolosi sono elencate nella casella **Azione** (cfr. Figura 32).

Per impostazione predefinita, in presenza di un oggetto HTTP pericoloso Web Anti-Virus visualizza un avviso e propone una scelta di azioni da eseguire sull'oggetto.

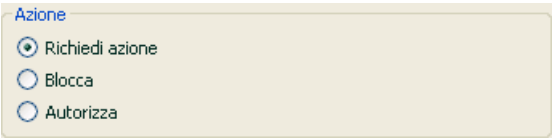


Figura 32. Selezione di azioni da eseguire su script pericolosi

Osserviamo adesso in dettaglio le possibili opzioni di trattamento degli oggetti HTTP pericolosi.

Se l'azione selezionata è	Se viene intercettato un oggetto pericoloso nel traffico HTTP
Richiedi azione	Web Anti-Virus visualizza un avviso contenente informazioni sul codice nocivo che potrebbe aver infettato l'oggetto e offre una serie di opzioni.
Blocca	Web Anti-Virus blocca l'accesso all'oggetto e visualizza un avviso in merito. Le informazioni relative all'evento vengono registrate nel report (cfr. 17.3 a pag. 237).
Autorizza	Web Anti-Virus consente l'accesso all'oggetto. Le informazioni relative all'evento vengono registrate nel report.

Per quanto riguarda gli script pericolosi, Web Anti-Virus li blocca sempre e visualizza messaggi che avvisano l'utente dell'azione eseguita. Non è possibile modificare la reazione a uno script pericoloso; l'unica alternativa consiste nel disabilitare il modulo di scansione degli script.

CAPITOLO 10. DIFESA PROATTIVA

Attenzione!

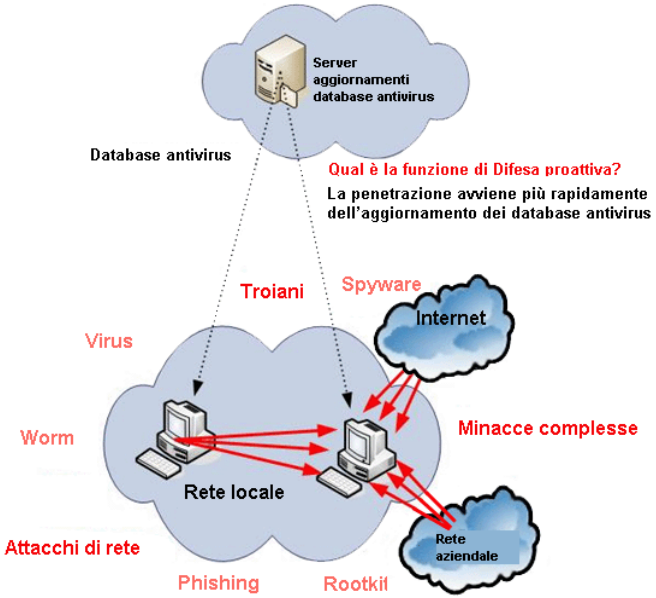
Questa versione di Kaspersky Internet Security non offre la Difesa proattiva sui computer che eseguono Microsoft Windows XP Professional x64 Edition.

Kaspersky Internet Security protegge sia dalle minacce note sia da quelle sulle quali non si possiedono ancora informazioni negli appositi elenchi. Questa protezione è garantita da un componente appositamente sviluppato, *Difesa proattiva.*

La necessità di un componente come Difesa proattiva si è fatta più pressante man mano che i programmi nocivi hanno iniziato a diffondersi più rapidamente degli aggiornamenti antivirus necessari per neutralizzarli. La tecnica di reazione sulla quale si basano le difese antivirus tradizionali richiede che almeno un computer sia infettato dalla nuova minaccia e comporta il dispendio temporale necessario per analizzare il codice nocivo e aggiungerlo agli elenchi delle minacce e aggiornare il database dei computer degli utenti. A quel punto è possibile che la nuova minaccia abbia già provocato danni notevoli.

Le tecnologie preventive fornite da Difesa proattiva di Kaspersky Internet Security sono in grado di evitare perdite di tempo e neutralizzare le nuove minacce prima che possano danneggiare il computer. Come è possibile? Contrariamente alle tecnologie reattive che analizzano i codici, le tecnologie preventive riconoscono una nuova minaccia nel computer in base alle sequenze di azioni eseguite da una determinata applicazione o processo. L'installazione del programma include una serie di criteri in grado di identificare il livello di pericolosità delle attività. Se l'attività di un'applicazione somiglia alle azioni tipiche delle attività pericolose, l'applicazione viene immediatamente classificata come pericolosa e vengono eseguite le azioni specificate nelle regole relative a quel tipo di attività. Fra gli esempi di attività pericolose figurano:

- Modifiche al file system
- Moduli che vengono incorporati in altri processi
- Processi di mascheratura
- Modifiche alle chiavi del registro di sistema di Microsoft Window



Difesa proattiva intercetta e blocca tutte le operazioni pericolose.

Inoltre individua tutte le macro VBA eseguite nelle applicazioni Microsoft Office. Il programma fa uso di elenchi di virus per analizzare le macro.

In funzione, Difesa proattiva applica una serie di regole incluse con il programma e con le esclusioni create. Una *regola* è un insieme di criteri che definiscono il grado di minaccia da parte di un'attività e la reazione del programma a tale attività.

Esistono regole individuali per l'attività dell'applicazione e per il monitoraggio delle modifiche al registro di sistema, delle macro e dei processi avviati sul computer. È possibile modificare l'elenco di regole a discrezione dell'utente aggiungendone o eliminando e modificando quelle esistenti. Le regole possono bloccare azioni o concedere autorizzazioni.

Esaminiamo gli algoritmi di Difesa proattiva:

1. Subito dopo l'avvio del computer, Difesa proattiva analizza i seguenti fattori:

    - *Azioni di ogni applicazione in esecuzione sul computer*. Difesa proattiva registra una cronologia delle azioni eseguite in sequenza e la confronta alle sequenze caratteristiche delle attività pericoloso (con il programma è fornito un database dei

tipi di attività pericolose che viene aggiornato con gli elenchi dei virus).

- *Azioni di ogni macro VBA eseguita*. Il programma le analizza a fronte dell'lenco delle azioni pericolose incluso nel programma stesso.
- *Integrità dei moduli di programma* dei programmi installati nel computer, che aiuta a impedire la sostituzione dei moduli delle applicazione con versioni contenenti codici nocivi e l'apertura di queste applicazioni da parte di programmi nocivi.
- *Ogni tentativo di modificare il registro di sistema* (eliminando o aggiungendo chiavi di registro di sistema, assegnando strani valori alle chiavi, ecc.).

2. L'analisi applica le regole di Difesa proattiva e le esclusioni assegnate.
3. Dopo l'analisi è possibile agire come segue:
   - Se l'attività soddisfa le condizioni delle regole di autorizzazione di Difesa proattiva, non viene bloccata.
   - Se le regole di blocco corrispondono all'attività, le azioni successive eseguite dal computer corrisponderanno alle istruzioni specificate nelle regole. Tali attività vengono solitamente bloccate. Sul video viene visualizzato un messaggio che specifica l'applicazione, il tipo di attività svolta dalla stessa e una cronologia delle azioni eseguite. L'utente deve accettare la decisione, bloccare o consentire questa attività. È possibile inoltre creare una regola per tale attività e annullare gli effetti delle azioni eseguite sul sistema.
   - Se per la sequenza di eventi eseguiti sul computer non esiste alcuna regola, allora è consentita.

10.1. Impostazioni di Difesa proattiva

Difesa proattiva prevede impostazioni proprie (cfr. Figura 33) che definiscono:

- Se l'attività dell'applicazione è monitorata sul computer

  Questa modalità di Difesa proattiva è controllata da ☑ **Abilita Rilevamento Attività Applicazione**. Per impostazione predefinita questa modalità è abilitata, garantendo un attento monitoraggio delle azioni di qualsiasi programma aperto sul computer. È specificato un elenco di

attività pericolose. È possibile configurare l'ordine di elaborazione dell'applicazione (cfr. 10.1.1 a pag. 127) per serie di quell'attività. Inoltre è possibile creare esclusioni di Difesa proattiva che escludono dal monitoraggio l'attività di applicazioni selezionate.

- Se il controllo dell'integrità dell'applicazione è abilitato

  Questa funzione tiene sotto controllo l'integrità dei moduli delle applicazioni installate sul computer e viene abilitata selezionando la casella **Controllo dell'integrità dell'applicazione**. L'integrità viene monitorata grazie alla composizione dei moduli e alle checksum dell'applicazione. È possibile creare regole di controllo dell'integrità per i moduli delle applicazioni. Se una determinata applicazione non si trova nell'elenco delle applicazioni controllate, la funzione di controllo dell'integrità non è attiva per tale applicazione.

Figura 33. Impostazioni di Difesa proattiva

- Se le variazioni ai registri di sistema vengono monitorate

Per impostazione predefinita, l'opzione **Abilita Registry Guard** è selezionata, consentendo a Kaspersky Internet Security di analizzare approfonditamente qualsiasi tentativo di modificare le chiavi di registro del sistema operativo.

È possibile creare regole di monitoraggio personalizzate (cfr. 10.1.4.2 a pag. 139) in base alle chiavi di registro.

- Se le macro vengono esaminate

  Il monitoraggio delle macro presenti nel computer viene abilitato selezionando la casella **Abilita Office Guard**. Per impostazione predefinita, questa opzione è selezionata e Difesa proattiva controlla approfonditamente tutte le azioni delle macro di Visual Basic of Applications.

  È possibile specificare quali macro considerare pericolose e quali azioni eseguire (cfr. 10.1.3 a pag. 133).

È possibile inoltre configurare esclusioni (cfr. 6.3.1 a pag. 76) per i moduli di Difesa proattiva e creare un elenco delle applicazioni attendibili (cfr. 6.3.2 a pag. 81).

La presente sezione prende in esame gli aspetti sopra elencati.

10.1.1. Regole di controllo delle attività

Kaspersky Internet Security monitora tutte le applicazioni presenti sul computer. Il monitoraggio dell'attività può essere attivato o disattivato tramite **Attiva analisi attività applicazione**. L'applicazione comprende un insieme di azioni tipiche di un'attività pericolosa. Se un'attività di qualsiasi applicazione è classificata come pericolosa, Difesa proattiva si atterrà alla reazione specificata nella regola per contrastare l'attività.

Osserviamo alcuni tipi di attività pericolosa:

- *Comportamento pericoloso*. Kaspersky Internet Security analizza l'attività delle applicazioni installate sul computer, e rileva le azioni pericolose o sospette da parte dei programmi in base alle regole create da Kaspersky Lab. Tali azioni includono, per esempio, l'installazione dissimulata di un programma, o i programmi che si replicano.
- *Avvio del browser Internet con parametri*. Questa attività è tipica dell'apertura del browser Web da parte di un'applicazione che trasmette determinati parametri al browser. Per esempio, questo avviene se si fa clic sul collegamento a una determinata URL in un messaggio e-mail a carattere pubblicitario. Analizzando questo tipo di attività, è possibile rilevare i tentativi di apertura del browser Web con parametri.

- *Intrusione nel processo*. Consiste nell'aggiungere codice eseguibile o un flusso supplementare al processo di un determinato programma. Questa attività è tipica dei troiani.
- *Processi nascosti (rootkit)*. I rootkit sono un insieme di programmi utilizzati per nascondere i programmi nocivi ed i loro processi nel sistema. Kaspersky Internet Security analizza il sistema operativo alla ricerca di processi nascosti.
- *Invasori*. È un'attività utilizzata nei tentativi di lettura di password ed altre informazioni riservate visualizzate nelle finestre di dialogo del sistema operativo. Kaspersky Internet Security identifica tali attività, in caso di tentativi di intercettare i dati trasferiti dal sistema operativo alla finestra di dialogo.
- *Valori sospetti nel registro*. Il registro di sistema è un database che conserva le impostazioni di sistema e dell'utente per controllare il funzionamento di Windows, come anche qualsiasi utility stabilita sul computer. I programmi nocivi, cercando di nascondere la loro presenza nel sistema, copiano valori errati nelle chiavi di registro. Kaspersky Internet Security analizza le voci del registro di sistema alla ricerca di valori sospetti.
- *Attività di sistema sospetta*. L'applicazione analizza le azioni eseguite dal sistema operativo Windows.
- *Keylogger*. È un'attività utilizzata dai programmi nocivi per tentare di leggere password ed altre informazioni riservate digitate per mezzo della tastiera.
- *Protezione di Microsoft Windows Task Manager*. Kaspersky Internet Security protegge Task Manager dai moduli nocivi che s'iniettano al suo interno allo scopo di bloccarne il funzionamento.

L'elenco delle attività pericolose viene aggiornato automaticamente durante l'aggiornamento di Kaspersky Internet Security e non può essere modificato. È possibile:

- Disabilitare il monitoraggio di una o più attività deselezionando la casella ☑ a fianco del nome dell'attività desiderata
- Modificare la regola utilizzata da Difesa proattiva quando viene intercettata un'attività pericolosa
- Creare un elenco di esclusioni (cfr. 6.3 a pag. 75) includendovi le applicazioni con attività che non si considerano pericolose.

Per configurare il monitoraggio delle attività,

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic su Impostazioni nella finestra principale del programma.

2. Selezionare **Difesa proattiva** nella struttura ad albero delle impostazioni.
3. Fare clic sul pulsante **Impostazioni** nella sezione **Rilevamento Attività Applicazione**.

I tipi di attività monitorati da Difesa proattiva sono elencati tra le **Impostazioni: Rilevamento Attività Applicazione** (cfr. Figura 34).

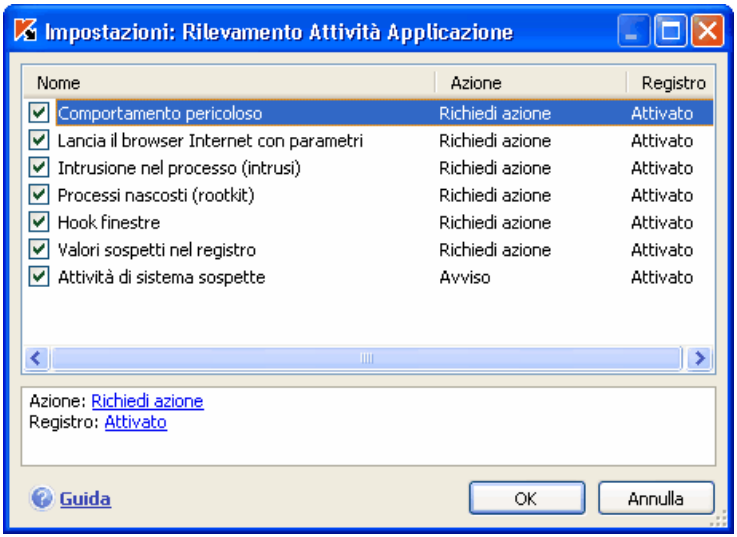


Figura 34. Configurazione del controllo delle attività delle applicazioni

Per modificare un'attività pericolosa, selezionarla dall'elenco e assegnare le impostazioni della regola nella parte inferiore della scheda:

- Assegnare la reazione di Difesa proattiva all'attività pericolosa.
- Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: autorizza, richiedi azione e termina. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata. Oltre a terminare il processo è possibile metterlo in Quarantena usando il link Attivato / Disativato dall'impostazione prescelta.
- Stabilire se si desidera generare un report sull'operazione eseguita, usando il link Attivato / Disativato.

Per disabilitare il monitoraggio di un'attività pericolosa, deselezionare la casella ☑ accanto al nome dell'attività in questione nell'elenco. Difesa proattiva non analizzerà più il tipo di attività deselezionato.

10.1.2. Controllo integrità delle applicazioni

Esistono diversi programmi che, se contenenti un codice nocivo, possono provocare gravi conseguenze come per esempio violazioni dell'integrità del sistema. Di norma si tratta di applicazioni e processi di sistema utilizzati per accedere a Internet e per lavorare con la posta elettronica e con altri documenti. È per questo motivo che tali applicazioni sono considerate *critiche* ai fini del controllo delle attività.

Difesa proattiva svolge la funzione di monitorare scrupolosamente tali applicazioni, analizzarne le attività e osservare altri processi avviati dalle applicazioni critiche. Kaspersky Internet Security propone un elenco di applicazioni critiche e una regola di monitoraggio creata per ciascuna di esse. È possibile aggiungere all'elenco altre applicazioni che l'utente considera critiche, e modificare le regole relative alle applicazioni presenti nell'elenco.

Esiste inoltre un elenco di moduli attendibili, per esempio moduli dotati di firma digitale di Microsoft Corporation. È altamente improbabile che le attività di applicazioni con tali moduli possano essere nocive, pertanto non è necessario monitorarle approfonditamente. Kaspersky Lab ha creato un elenco di questi moduli per alleggerire il carico sul computer durante l'uso di Difesa proattiva.

I componenti con la firma di Microsoft sono aggiunti automaticamente all'elenco delle applicazioni attendibili. Se necessario, è possibile aggiungere o eliminare componenti dall'elenco.

I processi di monitoraggio del sistema possono essere disattivati selezionando la casella  **Controllo dell'integrità dell'applicazione**. L'impostazione è deselezionata per impostazione predefinita. Se si abilita questa funzione, ogni applicazione o modulo di applicazione aperta viene esaminata a fronte dell'elenco delle applicazioni critiche e attendibili. Se l'applicazione è presente nell'elenco delle applicazioni critiche, la sua attività sarà sottoposta a un approfondito monitoraggio da parte di Difesa proattiva in base alla regola creata per tale attività.

Per configurare il controllo dell'integrità delle applicazioni:

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **Difesa proattiva** nella struttura ad albero delle impostazioni.
3. Fare clic sul pulsante **Impostazioni** nella casella **Controllo dell'integrità dell'applicazione**.

Esaminiamo il lavoro con i processi critici e attendibili.

10.1.2.1. Configurazione delle regole di controllo dell'integrità delle applicazioni

Le *applicazioni critiche* sono file eseguibili di programmi il cui monitoraggio è estremamente importante poiché, se infettati da codici nocivi, provocano conseguenze estremamente gravi.

La scheda **Applicazioni critiche** (cfr. Figura 35) contiene un elenco di applicazioni critiche creato da Kaspersky Lab e incluso nel programma. Per ciascuna di tali applicazioni viene creata una regola di monitoraggio. Tali regole possono essere modificate oppure è possibile crearne di nuove.

Difesa proattiva analizza le seguenti operazioni che coinvolgono applicazioni critiche: esecuzione, modifica dei contenuti dei moduli dell'applicazione e avvio di un'applicazione come processo secondario. È possibile selezionare la reazione di Difesa proattiva a ciascuna delle operazioni elencate (autorizzazione o blocco dell'operazione) e specificare inoltre se registrare l'attività nel report delle operazioni del componente. In pratica, per impostazione predefinita tutte le operazioni critiche possono essere avviate, modificate o avviate come processi secondari.

Per aggiungere un'applicazione critica all'elenco e creare una regola di monitoraggio apposita:

1. Fare clic su **Aggiungi** nella scheda **Applicazioni critiche**. Si apre un menu contestuale. Facendo clic su **Sfoglia** è possible aprire la finestra di selezione dei file. In alternativa, facendo clic su **Applicazioni** è possible aprire un elenco delle applicazioni correntemente in funzione e selezionare quelle desiderate. L'applicazione viene aggiunta in cima all'elenco. Per impostazione predefinita viene creata per tale applicazione una regola di autorizzazione. La prima volta che questa applicazione viene avviata, viene creato un elenco dei moduli utilizzati all'avvio del programma, ai quali è garantita l'autorizzazione.

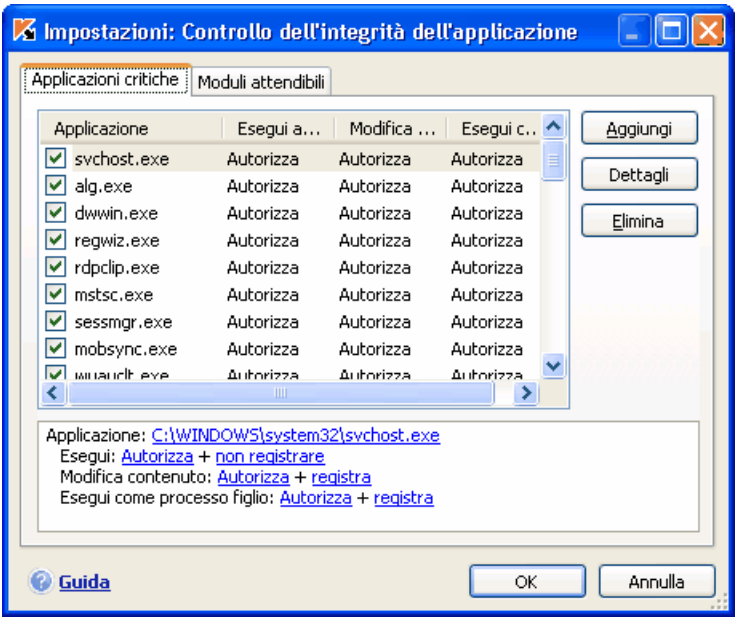


Figura 35. Controllo dell'integrità delle applicazioni

2. Selezionare una regola dall'elenco e assegnare le impostazioni necessarie nella parte inferiore della scheda:

   - Definire la reazione di Difesa proattiva ai tentativi di apertura, modifica dei contenuti o avvio di un'applicazione critica come processo secondario.

     Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: autorizza, richiedi azione e blocca. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata.

   - Stabilire se si desidera generare un report sull'operazione eseguita, facendo clic su registra / non registrare.

Per disabilitare il monitoraggio dell'attività di un'applicazione, deselezionare la casella ☑ accanto al nome.

10.1.2.2. Creazione di un elenco di componenti condivisi

Kaspersky Internet Security include un elenco di componenti condivisi che possono essere aperti in tutte le applicazioni controllate. Questo elenco è consultabile nella scheda **Moduli attendibili** (cfr. Figura 36). L'elenco contiene i moduli utilizzati da Kaspersky Internet Security, i componenti con firma di Microsoft e i componenti aggiunti dall'utente.

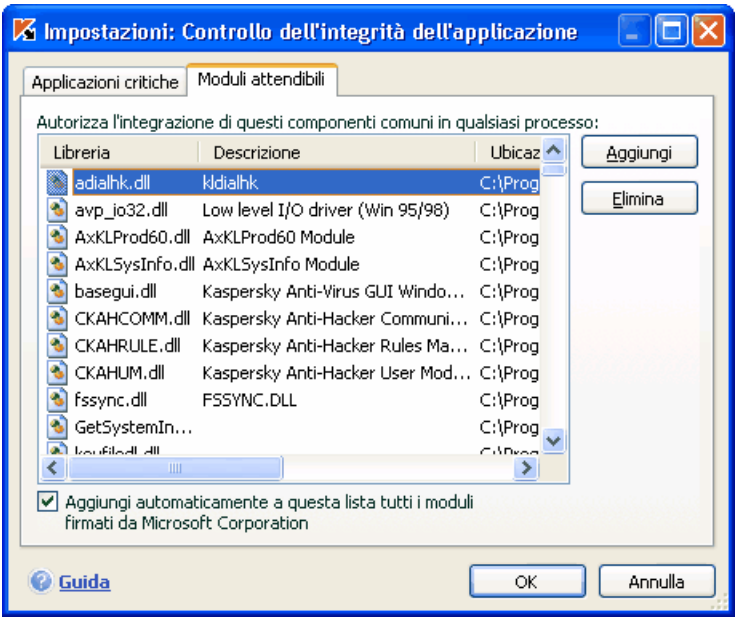


Figura 36. Configurazione dell'elenco dei moduli attendibili

È possibile installare sul computer vari programmi e aggiungere automaticamente quelli con i moduli firmati da Microsoft nell'elenco dei moduli attendibili selezionando la casella ☑ **Aggiungi automaticamente a questa lista tutti i moduli firmati da Microsoft Corporation**. Poi, se l'applicazione controllata apre un modulo firmato da Microsoft, il programma ne consente automaticamente il caricamento e il modulo viene inserito nell'elenco di componenti condivisi.

Per aggiungere un elemenco all'elenco dei moduli attendibili, fare clic su **Aggiungi** e selezionare il modulo nella finestra standard di selezione file.

10.1.3. Office Guard

È possibile abilitare la scansione e l'elaborazione delle macro pericolose sul computer selezionando ☑ **Abilita Office Guard**. La casella è selezionata per impostazione predefinita. Ogni macro eseguita viene esaminata e, se presente nell'elenco delle macro pericolose, viene elaborata come segue:

Esempio:

> La macro *PDFMaker* è un plug-in della barra degli strumenti di Adobe Acrobat in Microsoft Office Word in grado di convertire qualsiasi documento in file .pdf. Difesa proattiva classifica l'incorporazione di elementi nel software come azioni pericolose. Se Kaspersky Internet Security Office Guard è abilitato, durante il caricamento di una macro Difesa proattiva visualizza un messaggio che informa che è stato individuato un comando macro pericoloso. L'utente può scegliere di terminare la macro o di consentirne l'esecuzione.

È possibile stabilire quali azioni eseguire durante l'esecuzione di macro con determinate azioni, e anche creare un elenco di esclusioni contenente le macro che l'utente non ritiene pericolose. Tali macro non saranno esaminate da Difesa proattiva.

Per configurare Office Guard:

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **Difesa proattiva** nella struttura ad albero delle impostazioni.
3. Fare clic sul pulsante **Impostazioni** nella casella **Office Guard**.

Le regole di elaborazione delle macro pericolose sono configurate nella finestra **Impostazioni: Office Guard** (cfr. Figura 37). Essa contiene le regole predefinite delle macro che Kaspersky Lab classifica come pericolose. Tali azioni includono, per esempio, l'incorporazione di moduli all'interno di programmi e l'eliminazione di file.

Le azioni che Kaspersky Internet Security esegue quando individua una macro sono elencate per ogni macro.

Se non si considera pericolosa una determinata azione di macro, deselezionare la casella corrispondente al nome dell'azione. È il caso, per esempio, di un utente che lavora frequentemente con un programma che fa uso di macro per aprire diversi file (non come sola lettura), e sicuro dell'attendibilità di questa operazione.

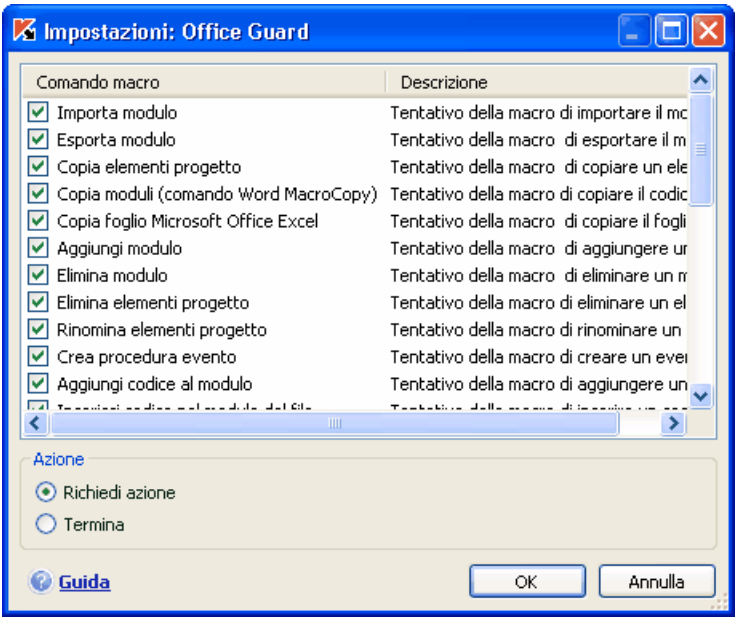


Figura 37. Configurazione delle impostazioni di Office Guard

Per evitare che Kaspersky Internet Security blocchi la macro:

Deselezionare la casella a fianco dell'azione. Il programma non considererà più la macro tra quelle pericolose e la esegue immediatamente.

Per impostazione predefinita, ogni volta che il programma rileva una macro pericolosa sul computer, si apre una finestra che chiede all'utente se desidera autorizzare o bloccare la macro.

Per far sì che il programma blocchi automaticamente tutte le macro senza interrogare l'utente:

Nella finestra dell'elenco delle macro, selezionare **Termina**.

10.1.4. Registry Guard

L'obiettivo dei programmi nocivi è spesso modificare i registri del sistema operativo del computer. Può trattarsi di innocui programmi-scherzo come di programmi realmente nocivi che presentano un'autentica minaccia per il computer.

Per esempio, gli scherzi possono copiare le proprie informazioni sulle chiavi di registro che determinano l'apertura automatica delle applicazioni all'avvio. Oppure, all'apertura del sistema operativo potrebbe aprirsi una finestra che informa che il computer è infetto, anche se ciò non corrisponde a realtà.

I troiani modificano i registri per accedere alle risorse del computer e danneggiare l'integrità di sistema del computer.

Difesa proattiva agevola l'individuazione di nuove minacce non ancora note che cercano di modificare il sistema del computer; a ciò contribuisce in particolare lo speciale modulo che può essere abilitato facendo clic sulla casella ☑ **Abilita Registry Guard**.

Per configurare il monitoraggio dei registri di sistema:

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **Difesa proattiva** nella struttura ad albero delle impostazioni.
3. Fare clic sul pulsante **Impostazioni** nella sezione **Registry Guard**.

Kaspersky Lab ha già creato un elenco di regole per controllare le operazioni relative alle chiavi di registro e lo ha incluso nel programma. Le operazioni relative alle chiavi di registro possono essere suddivise in gruppi logici come *System security*, *Internet security*, ecc. Ognuno di tali gruppi include chiavi di registro del sistema e regole di lavoro. Ogni volta che il programma viene aggiornato, l'elenco si arricchisce di nuovi gruppi di regole per le chiavi.

La finestra **Registro gruppi di chiavi** (cfr. Figura 38) contiene un elenco completo di regole.

Ad ogni gruppo di regole è assegnata una priorità di esecuzione che è possibile modificare per mezzo dei pulsanti **Sposta su** e **Sposta giù**. Se le stesse chiavi di registro sono presenti in più gruppi, la prima regola applicata alla chiave è quella del gruppo con la priorità più elevata.

Per smettere di usare qualsiasi gruppo di regole agire come segue:

- Deselezionare la casella ☑ accanto al nome del gruppo. Il gruppo di regole rimane presente nell'elenco ma Difesa proattiva non lo utilizza.
- Eliminare il gruppo di regole dall'elenco. Si sconsiglia di eliminare i gruppi creati da Kaspersky Lab poiché contengono le regole ottimali.

Figura 38. Gruppi chiavi di registro controllati

Se i gruppi di regole delle chiavi non soddisfano i criteri di monitoraggio del registro di sistema dell'utente, è possibile creare regole personalizzate facendo clic su **Aggiungi** nella finestra dei gruppi di chiavi.

Nella finestra che si apre eseguire questi passaggi:

1. Digitare il nome del nuovo gruppo di regole per il monitoraggio delle chiavi di registro del sistema nel campo **Nome**.
2. Creare un elenco di chiavi (cfr. 10.1.4.1 a pag. 137) dal registro di sistema per il quale si desidera creare la regola nella scheda **Chiavi**. Può trattarsi di una o più chiavi.
3. Creare una regola (cfr. 10.1.4.2 a pag. 139) per le chiavi di registro nella scheda **Regole**. È possibile creare più regole e impostarne l'ordine di applicazione.

10.1.4.1. Selezione delle chiavi di registro per creare una regola

Quando si aggiungono chiavi di registro del sistema a un gruppo, è possibile specificare una chiave o un gruppo di chiavi. È possibile creare una regola per una chiave o per il suo valore specifico.

La scheda **Chiavi** contiene un elenco di chiavi per la regola.

Per aggiungere una chiave di registro del sistema:

1. Fare clic sul pulsante **Aggiungi** nella finestra **Modifica gruppo** (cfr. Figura 39).
2. Nella finestra che si apre selezionare una chiave di registro del sistema o un gruppo di chiavi per cui si desidera creare la regola di monitoraggio.
3. Specificare il valore della chiave o una maschera per un gruppo di chiavi a cui si desidera applicare la regola nel campo **Valore**.
4. Selezionare la casella **Includi sottochiavi** per la regola da applicare a tutte le chiavi collegate alla chiave di registro selezionata.

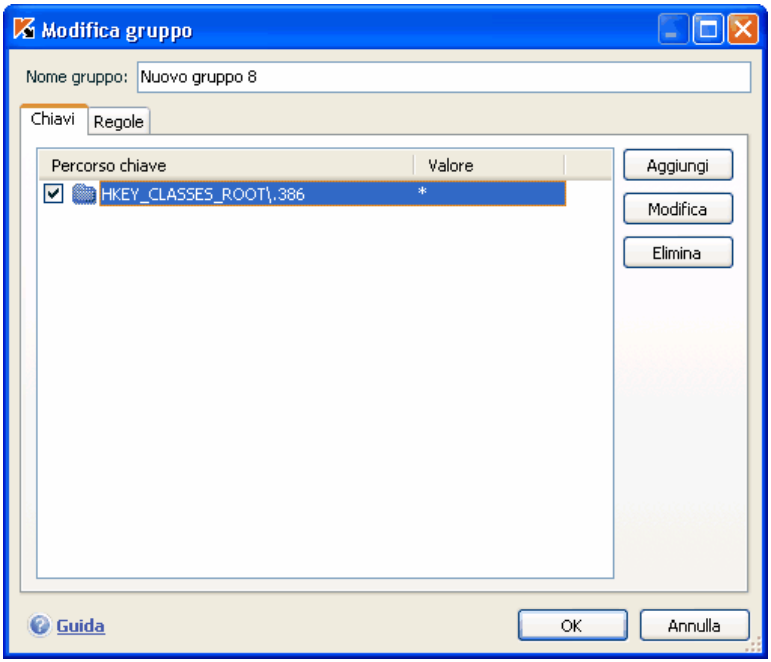


Figura 39. Aggiunta di chiavi di registro controllate

Se per il nome della chiave sono stati utilizzati caratteri jolly, sono necessarie solo le maschere con un asterisco e un punto interrogativo come funzione **Includi sottochiavi**.

Se si seleziona un gruppo di chiavi che fa uso di maschera e si specifica un valore corrispondente, la regola sarà applicata a quel valore per tutte le chiavi del gruppo selezionato.

10.1.4.2. Creazione di una regola per Registry Guard

Una regola di Registry Guard contiene le seguenti definizioni:

- L'applicazione a cui si applica la regola se cerca di accedere alle chiavi di registro del sistema
- La reazione del programma a un'applicazione che cerca di eseguire un'operazione con una chiave di registro del sistema

Per creare una regola per le chiavi di registro del sistema selezionate:

1. Fare clic su **Nuova** nella scheda **Regole**. La regola generale sarà aggiunta alla prima posizione dell'elenco delle regole (cfr. Figura 40).

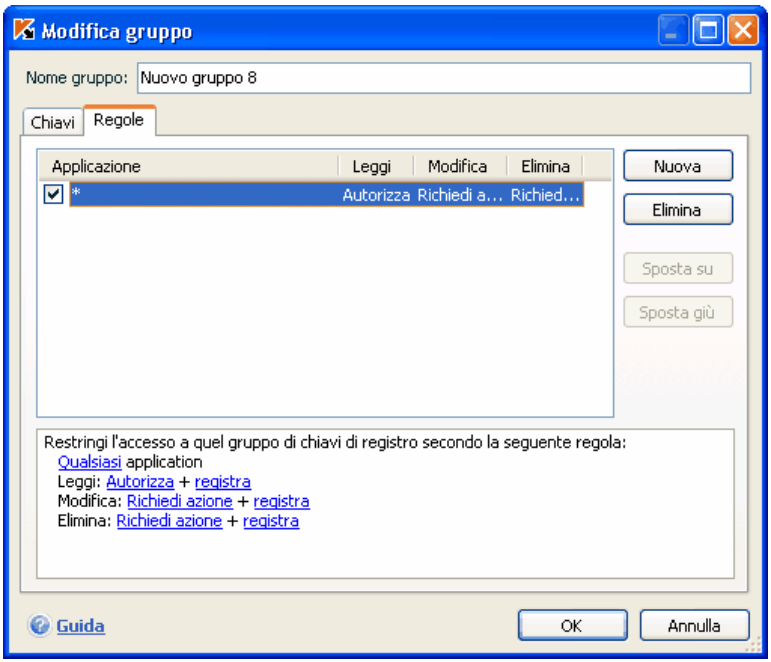


Figura 40. Creazione di una regola di monitoraggio delle chiavi di registro

2. Selezionare una regola dall'elenco e assegnare le impostazioni necessarie nella parte inferiore della scheda:

   - Specificare l'applicazione.

     La regola viene creata per qualsiasi applicazione per impostazione predefinita. Se si desidera applicare la regola a un'applicazione specifica, fare clic con il pulsante sinistro del mouse su qualsiasi che diventa questa. Seguire quindi l'apposito collegamento specifica il nome dell'applicazione. Si apre un menu contestuale. Facendo clic su **Sfoglia** è possibile aprire la finestra di selezione dei file. In alternativa, facendo clic su **Applicazioni** è possibile aprire un elenco delle applicazioni correntemente in funzione e selezionare quelle desiderate.

   - Definire la reazione di Difesa proattiva all'applicazione selezionata che cerca di leggere, modificare o eliminare le chiavi di registro del sistema.

     Come reazione è possibile assegnare qualsiasi azione tra quelle elencate di seguito: autorizza, richiedi azione e blocca. Fare clic con il pulsante sinistro del mouse sul link dell'azione fino a visualizzare quella desiderata.

   - Stabilire se si desidera generare un report sull'operazione eseguita, facendo clic su registra / non registrare.

È possibile creare diverse regole e modificarne la priorità per mezzo dei pulsanti **Sposta su** e **Sposta giù**.

È possibile inoltre creare una regola di autorizzazione per una chiave di registro del sistema dall'avviso a comparsa che informa che un programma sta cercando di eseguire un'operazione con la chiave. Per fare questo, fare clic su Crea regola di autorizzazione nell'avviso e selezionare nella finestra che si apre la regola da applicare.

CAPITOLO 11. ANTI-SPY

Recentemente, la categoria del malware si è arricchita di un numero crescente di programmi volti a:

- Impadronirsi di informazioni confidenziali (password, numeri di carte di credito, documenti importanti, ecc.)
- Intercettare le operazioni dell'utente al computer e analizzare il software installato
- Visualizzare contenuti pubblicitari importuni in browser, popup e banner in vari programmi
- Accedere a Internet senza autorizzazione da computer altrui e aprire vari siti web

Il phishing e i keylogger sono programmati specificamente per impadronirsi di informazioni confidenziali; gli autodialer, gli scherzi e gli adware possono provocare perdite di tempo e denaro. Anti-Spy è concepito appositamente per proteggere l'utente da questi programmi.

Anti-Spy comprende i seguenti moduli:

- *Anti-Phishing* per proteggere dal phishing.

  Il phishing consiste solitamente di messaggi e-mail inviati da sedicenti istituzioni finanziarie, e contenenti collegamenti ai loro siti web. Il testo del messaggio invita l'utente a seguire un link e inserire i propri dati nella finestra che si apre, per esempio il numero di carta di credito o il nome utente e la password per accedere a un sito di Internet banking da cui eseguire operazioni finanziarie.

  Un esempio comune di phishing è un messaggio e-mail dalla banca dell'utente, con un link al sito ufficiale. Facendo clic sul link, si accede a una copia esatta del sito web della banca che riporta perfino l'indirizzo nella barra del browser, anche se si tratta di un sito contraffatto. Da questo momento in poi, tutte le operazioni eseguite dal sito possono essere ricostruite e utilizzate per prelevare denaro dal conto dell'utente.

  I link a siti di phishing vengono solitamente inviati in messaggi e-mail o con mezzi diversi, per esempio tramite programmi di instant messaging. Anti-Phishing intercetta i tentativi di aprire siti di phishing e li blocca.

  Gli elenchi delle minacce di Kaspersky Internet Security includono tutti i siti attualmente noti come siti di phishing. Gli esperti Kaspersky Lab lo arricchiscono man mano con gli indirizzi ottenuti dall'Anti-Phishing Working Group, un'organizzazione internazionale che si occupa del

problema. Questo elenco viene aggiornato automaticamente insieme agli elenchi delle minacce.

- *Popup Blocker* blocca i popup pubblicitari che si aprono su vari siti web.

  Le informazioni contenute in tali finestre di solito non sono di alcun interesse per il navigatore comune. Tali finestre si aprono automaticamente all'apertura di un determinato sito web o portano su una finestra diversa per mezzo di un ipertesto. Essi contengono pubblicità e altre informazioni non richieste. Popup Blocker blocca queste finestre, e un apposito messaggio sopra la barra delle applicazioni ne informa l'utente. È possibile determinare direttamente in questo messaggio se si desidera bloccare la finestra oppure no.

  > Popup Blocker funziona correttamente con il modulo di bloccaggio dei popul di Microsoft Internet Explorer incluso nel Service Pack 2 di Microsoft Windows XP. Quando si installa il programma, viene installato anche un plug-in nel browser che consente di autorizzare l'apertura dei popup durante l'uso di Internet.

  Alcuni siti usano i popup per fornire informazioni in maniera più rapida e accessibile. Se si utilizzano tali siti con frequenza e le informazioni riportate nel popup sono di estrema importanza per l'utente, questi può aggiungerle all'elenco dei siti attendibili (cfr. 11.1.1 a pag. 143). In tal modo i popup non vengono bloccati.

  Durante l'uso di Microsoft Internet Explorer, viene visualizzata l'icona  nella barra di stato del browser ogni volta che viene bloccato un popup. È possibile sbloccare tale popup o aggiungerlo all'elenco degli indirizzi attendibili facendoci clic sopra.

- *Anti-Banner* blocca i banner pubblicitari in rete o incorporati nell'interfaccia di vari programmi installati nel computer.

  I banner pubblicitari sono totalmente privi di informazioni utili. Essi distraggono l'utente dal suo lavoro e incrementano il traffico sul computer. Anti-Banner blocca i banner pubblicitari più diffusi. Kaspersky Internet Security include maschere per questo scopo. È possibile disabilitare il blocco dei banner o creare degli elenchi di banner autorizzati e bloccati.

  > Per integrare Anti-Banner in **Opera**, aggiungere la seguente riga a *standard_menu.ini*, sezione **[Image Link Popup Menu]**:
  > Item, "New banner" = Copy image address & Execute program, "…\Program Files\Kaspersky Lab\Kaspersky Internet Security 6.0\opera_banner_deny.vbs", "//nologo %C"

- *Anti-Dialer* protegge il computer dai servizi Internet a pagamento non autorizzati dall'utente.

Anti-Dialer funziona solo con Microsoft Windows XP e Microsoft Windows 2000.

Questi servizi conducono generalmente a siti web a carattere pornografico. Appositi programmi nocivi (dialer) inizializzano la connessione con tali siti via modem. L'utente quindi è costretto a pagare costose tariffe telefoniche per un traffico non desiderato o utilizzato. Se si desidera escludere un numero qualsiasi dall'elenco dei numeri bloccati, aggiungerlo all'elenco dei numeri attendibili (cfr. 11.1.3 a pag. 147).

11.1. Configurazione di Anti-Spy

Anti-Spy protegge il computer da tutti i programmi noti agli esperti Kaspersky Lab studiati per trafugare informazioni confidenziali o sottrarre denaro. È possibile configurare più specificamente il componente nei seguenti modi:

- Creando un elenco dei siti web attendibili (cfr. 11.1.1 a pag. 143) i cui popup non si desidera bloccare.
- Creando liste bianche e liste nere dei banner (cfr. 11.1.2 a pag. 145)
- Creando elenchi dei numeri telefonici attendibili (cfr. 11.1.3 a pag. 147) per le connessioni remote autorizzate.

11.1.1. Creazione di elenchi di indirizzi attendibili per Popup Blocker

Attenzione!

Questa versione di Kaspersky Internet Security non offre Popup Blocker sui computer che eseguono Microsoft Windows XP Professional x64 Edition.

Anti-Spy blocca per impostazione predefinita la maggior parte dei popup visualizzati automaticamente senza richiedere l'intervento dell'utente. Fanno eccezione i popup dei siti web aggiunti all'elenco dei siti attendibili in Microsoft Internet Explorer e i siti Intranet a cui l'utente risulta iscritto in quel momento.

Se si esegue Windows XP con Service Pack 2, Internet Explorer dispone già di un'applicazione che blocca i popup. È possibile configurarla selezionando le finestre specifiche che si desidera bloccare e quelle che invece si desidera autorizzare. Anti-Spy è compatibile con questa applicazione in base ai seguenti principi: Quando un popup cerca di aprirsi, viene sempre data la precedenza a una regola di bloccaggio. Per esempio, l'indirizzo di un determinato popup compare nell'elenco delle finestre autorizzate per Internet Explorer ma non per

Popup Blocker. Questa finestra sarà bloccata, e viceversa, se il browser è configurato in modo da bloccare tutti i popup, un popup sarà bloccato anche se il relativo indirizzo non compare nell'elenco degli indirizzi attendibili di Popup Blocker. Per questo motivo, se si esegue Microsoft Windows XP Service Pack 2, si raccomanda di configurare insieme il browser e Popup Blocker.

Se per qualsiasi motivo si desidera consentire la visualizzazione di un popup, è necessario aggiungerlo all'elenco degli indirizzi raccomandati procedendo come segue:

1. Aprire la finestra delle impostazioni di Kaspersky Internet Security e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic su **Siti attendibili** nella sezione di Popup Blocker.
3. Nella finestra che si apre, fare clic su **Aggiungi** (cfr. Figura 41) e digitare una maschera per i siti di cui non si desidera visualizzare i popup.

Suggerimento:
Quando si digita la maschera di un indirizzo attendibile, è possibile usare i caratteri * o ?.
Per esempio, la maschera http://www.test* esclude i popup di qualsiasi sito che inizia con la serie di caratteri indicata.

4. Specificare se gli indirizzi della zona attendibile di Internet Explorer o quelli della LAN devono essere esclusi dalla scansione. Il programma li considera attendibili per impostazione predefinita e non blocca i popup di questi indirizzi.

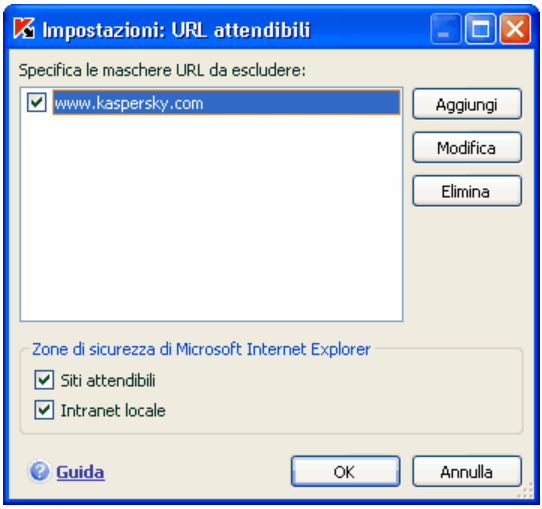


Figura 41. Creazione di un elenco di siti attendibili

La nuova esclusione sarà aggiunta all'inizio dell'elenco dei siti attendibili. Per sospendere l'esclusione aggiunta, è sufficiente deselezionare la casella accanto al nome. Se si desidera eliminare definitivamente un'esclusione, selezionarla dall'elenco e fare clic su **Elimina**.

Se si desidera bloccare i popup della propria rete intranet o dei siti web inclusi nell'elenco dei siti attendibili di Microsoft Internet Explorer, deselezionare le caselle corrispondenti nella sezione **Zone di sicurezza di Microsoft Internet Explorer**.

Quando un popup non incluso nell'elenco dei siti attendibili cerca di aprirsi, viene visualizzato un messaggio sopra l'icona del programma che informa dell'avvenuto blocco della finestra. Seguendo i collegamenti all'interno del messaggio è possibile eliminare il blocco e aggiungere l'indirizzo della finestra all'elenco dei siti attendibili.

È possibile eseguire azioni simili anche con la versione di Internet Explorer inclusa in Windows XP Service Pack 2 utilizzando il menu contestuale che si apre facendo clic sull'icona del programma nella parte inferiore del browser quando vengono bloccati dei popup.

11.1.2. Elenco di blocco dei banner pubblicitari

Gli esperti Kaspersky Lab hanno compilato un elenco di maschere dei più comuni banner pubblicitari sulla base di ricerche specifiche, e l'hanno incluso nel programma. Il programma blocca i banner pubblicitari compresi nelle maschere dell'elenco, a meno che il blocco non sia disabilitato.

Inoltre è possibile creare liste bianche e liste nere dei banner pubblicitari, in base alle quali autorizzare o bloccare la visualizzazione degli stessi.

Osservare che se una maschera di dominio è presente nell'elenco dei banner bloccati o in una lista nera è possibile continuare ad accedere al sito root.
Per esempio, se l'elenco dei banner bloccati include una maschera per **truehits.net**, è possibile accedere a **http://truehits.net**, mentre l'accesso a **http://truehits.net/a.jpg** è bloccato.

11.1.2.1. Configurazione dell'elenco di blocco dei banner pubblicitari standard

Kaspersky Internet Security include un elenco di maschere per i più comuni banner pubblicitari sui siti web e le interfacce dei programmi. Questo elenco è stato compilato dagli esperti Kaspersky Lab e viene aggiornato con gli elenchi delle minacce.

È possibile selezionare quali banner pubblicitari standard si desidera usare durante l'esecuzione di Anti-Banner procedendo come segue:

1. Aprire la finestra delle impostazioni di Kaspersky Internet Security e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic sul pulsante **Impostazioni** nella sezione dei banner bloccati.
3. Aprire la scheda **Comune** (cfr. Figura 42). Anti-Banner blocca le maschere dei banner pubblicitari elencate nella scheda. È possibile utilizzare la stringa della maschera in qualsiasi punto dell'indirizzo del banner.

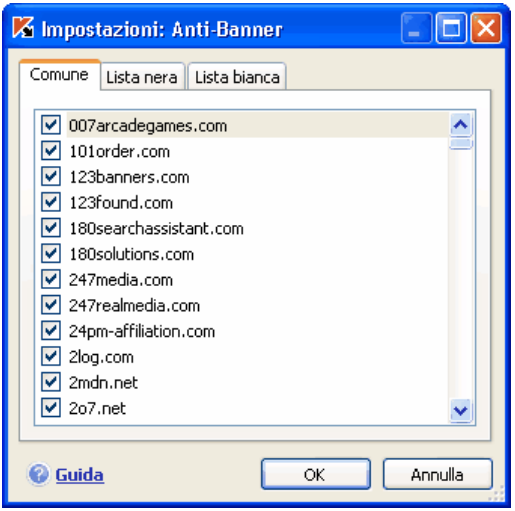


Figura 42. Elenco dei banner bloccati

L'elenco delle maschere standard bloccate non è modificabile. Se non si desidera bloccare un banner compreso in una maschera standard, deselezionare la casella ☑ accanto alla maschera stessa.

Per analizzare i banner pubblicitari che non corrispondono alle maschere incluse negli elenchi standard, selezionare ☑ **Usa metodi di analisi euristica**. L'applicazione analizzerà le immagini caricate alla ricerca di segnali tipici dei banner pubblicitari. Grazie a tale analisi, l'immagine può essere identificata come banner e quindi bloccata.

È possibile inoltre creare elenchi personalizzati di banner autorizzati e bloccati per mezzo delle schede **Lista bianca** e **Lista nera**.

11.1.2.2. Liste bianche dei banner pubblicitari

Durante l'uso del programma, è possibile creare liste bianche di banner pubblicitari se non si desidera bloccare determinati banner. Le liste bianche contengono le maschere dei banner pubblicitari autorizzati.

Per aggiungere una nuova maschera alla lista bianca:

1. Aprire la finestra delle impostazioni di Kaspersky Internet Security e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic sul pulsante **Impostazioni** nella sezione dei banner bloccati.
3. Aprire la scheda **Lista bianca**.

Aggiungere la maschera del banner autorizzato per mezzo del pulsante **Aggiungi**. È possibile specificare l'URL del banner o una serie di caratteri. In quest'ultimo caso, quando un banner tenta di aprirsi, il programma lo esamina per stabilire se contenga la stringa di caratteri specificata.

Per sospendere l'uso di una maschera creata dall'utente, non è necessario eliminarla dall'elenco. È sufficiente deselezionare la casella ☑ accanto alla maschera. I banner che rientrano nella maschera deselezionata, quindi, non saranno più trattati come esclusioni.

Per mezzo dei pulsanti **Importa** ed **Esporta**, è possibile copiare da un computer all'altro i propri elenchi di banner autorizzati.

11.1.2.3. Liste nere dei banner pubblicitari

Oltre all'elenco standard dei banner bloccati (cfr. 11.1.2.1 a pag. 145) da Anti-Banner, è possibile creare elenchi personalizzati procedendo come segue:

1. Aprire la finestra delle impostazioni di Kaspersky Internet Security e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic sul pulsante **Impostazioni** nella sezione dei banner bloccati.
3. Aprire la scheda **Lista nera**.

Per mezzo del pulsante **Aggiungi**, digitare una maschera per il banner che si desidera bloccare. È possibile specificare l'URL del banner o una serie di caratteri. In quest'ultimo caso, quando un banner tenta di aprirsi, il programma lo esamina per stabilire se contenga la stringa di caratteri specificata.

Per sospendere l'uso di una maschera creata dall'utente, non è necessario eliminarla dall'elenco. È sufficiente deselezionare la casella ☑ accanto alla maschera.

Per mezzo dei pulsanti **Importa** ed **Esporta**, è possibile copiare da un computer all'altro i propri elenchi di banner bloccati.

11.1.3. Creazione di un elenco di numeri attendibili per Anti-Autodialer

Questa versione di Kaspersky Internet Security non offre Anti-Autodialer sui computer che eseguono Microsoft Windows XP Professional x64 Edition.

Il modulo *Anti-Autodialer* monitora i numeri di telefono utilizzati per connettersi segretamente a Internet. Una connessione è considerata segreta se configurata in modo da non informare l'utente della connessione in corso o se non è inizializzata dall'utente stesso.

Ogni qualvolta venga eseguito un tentativo di connessione segreta, il programma informa l'utente visualizzando un messaggio specifico. L'utente deve quindi decidere se autorizzare o bloccare tale connessione nel messaggio stesso. Se non è stato l'utente a inizializzare la connessione, è molto probabile che la causa sia un programma nocivo.

Se si desidera autorizzare le connessioni a determinati numeri senza che il programma chieda ogni volta l'autorizzazione dell'utente, è necessario aggiungerli all'elenco dei numeri attendibili procedendo come segue:

1. Aprire la finestra delle impostazioni di Kaspersky Internet Security e selezionare Anti-Spy nella struttura ad albero.
2. Fare clic su **Numeri attendibili** nella sezione Anti-Dialer.
3. Nella finestra che si apre, fare clic su **Aggiungi** (cfr. Figura 43) e digitare un numero o una maschera per i numeri ai quali non si desidera bloccare la connessione.

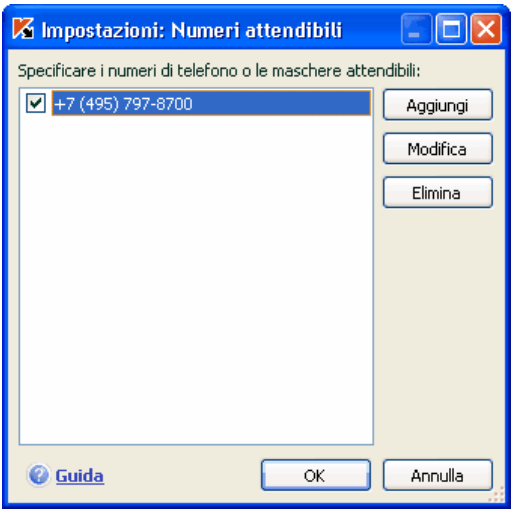


Figura 43. Creazione di un elenco di indirizzi attendibili

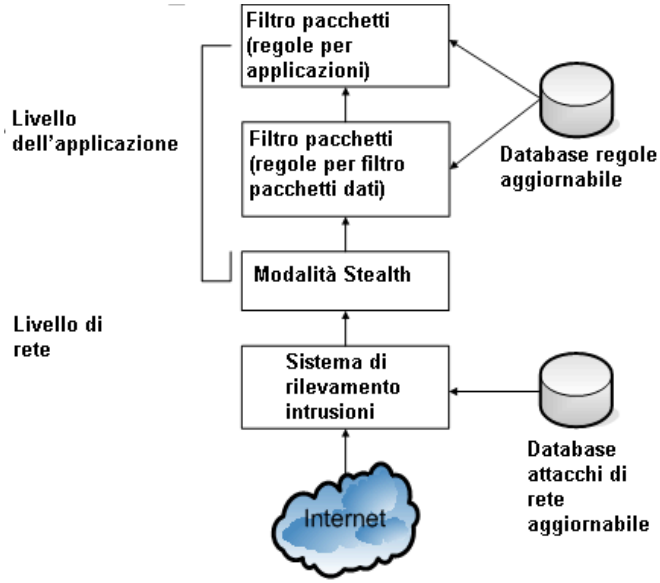
Suggerimento:
Quando si digita la maschera di un numero attendibile, è possibile usare i caratteri ***** o **?**.
Per esempio, la maschera 8????79787* copre qualsiasi numero che inizi con 79787 e con prefisso di tre cifre.

La nuova esclusione sarà aggiunta all'inizio dell'elenco dei numeri attendibili. Per sospendere l'esclusione aggiunta, è sufficiente deselezionare la casella accanto al numero nell'elenco. Per rimuovere definitivamente un'esclusione, selezionarla dall'elenco e fare clic su **Elimina**.

CAPITOLO 12. ANTI-HACKER

I computer di oggi sono diventati estremamente vulnerabili durante la navigazione in Internet. Essi sono soggetti a infezioni virali e ad altri tipi di attacco che sfruttano le vulnerabilità dei sistemi operativi e del software.

Kaspersky Internet Security contiene uno speciale componente, *Anti-Hacker*, che garantisce la sicurezza nelle reti locali e in Internet. Questo componente protegge il computer a livello di rete e di applicazioni e maschera il computer nella rete al fine di evitare attacchi. Osserviamo in dettaglio il funzionamento di Anti-Hacker.



Il computer è protetto a livello di rete grazie a regole di filtraggio pacchetti che autorizzano o bloccano l'attività di rete in base all'analisi delle impostazioni quali la direzione di un pacchetto, il protocollo di trasferimento del pacchetto dati e la porta del pacchetto in uscita. Le regole dei pacchetti dati stabiliscono l'accesso alla rete indipendentemente dalle applicazioni installate sul computer che fanno uso della rete.

Oltre alle regole di filtraggio pacchetti, anche Intrusion Detection System (IDS) offre una protezione supplementare a livello di rete. L'obiettivo del sistema è analizzare le connessioni in entrata, rilevare le scansioni delle porte del computer e filtrare i pacchetti di rete volti a sfruttare le vulnerabilità del software.

Quando è in esecuzione, Intrusion Detection System blocca tutte le connessioni in entrata provenienti da un determinato computer per un tempo specificato, e l'utente riceve un messaggio che informa del tentativo di attacco di rete subito dal computer.

Intrusion Detection System si basa sull'uso di uno speciale database degli attacchi di rete per l'analisi, aggiornato regolarmente dal nostro team. Esso viene aggiornato con gli elenchi delle minacce.

Il computer è protetto a livello di applicazioni grazie alle regole sull'uso delle risorse di rete per le applicazioni installate sul computer. Come per la sicurezza a livello di rete, la sicurezza a livello di applicazioni si basa sull'analisi dei pacchetti dati dal punto di vista di direzione, protocollo di trasferimento e porte utilizzate. Tuttavia, a livello di applicazioni, vengono presi in considerazione anche le caratteristiche del pacchetto dati e l'applicazione specifica che invia e riceve il pacchetto.

L'uso delle regole delle applicazioni agevola la configurazione più specifica della protezione quando, per esempio, un determinato tipo di connessione viene precluso ad alcune applicazioni ma non ad altre.

Esistono due tipi di regole per Anti-Hacker, basati sui due livelli di sicurezza di Anti-Hacker:

- *Regole per filtro pacchetti* (cfr. 12.3 a pag. 158). Utilizzate per creare restrizioni di carattere generale all'attività di rete, a prescindere dalle applicazioni installate. Esempio: Se si crea una regola di filtraggio pacchetti che blocca le connessioni in entrata sulla porta 21, nessuna delle applicazioni che utilizza quella porta (un server ftp, per esempio) sarà accessibile dall'esterno.

- *Regole per applicazioni* (cfr. 12.2 a pag. 154). Utilizzate per creare restrizioni all'attività di rete per applicazioni specifiche. Esempio: Se sono attive delle regole di bloccaggio delle connessioni sulla porta 80 per tutte le applicazioni, è possibile creare una regola che consenta le connessioni su tale porta a Firefox (o a un altro browser).

Esistono due tipi di regole per applicazioni e filtro pacchetti: *autorizza* e *blocca*. L'installazione del programma include una serie di regole volte a regolare l'attività di rete per la maggior parte delle applicazioni, che utilizza i protocolli e le porte più comuni. Kaspersky Internet Security include inoltre una serie di regole di autorizzazione per applicazioni attendibili la cui attività di rete non dà adito a sospetti.

Kaspersky Internet Security suddivide l'intero spazio di rete in zone in modo da semplificare le impostazioni e le regole: *Internet* e *zone di sicurezza*, che corrispondono in gran parte alle sottoreti di cui il computer fa parte. È possibile assegnare uno status a ogni zona (*Internet, Local Area Network, attendibile*), dal quale dipenderà l'applicazione delle regole e il monitoraggio delle attività di rete nelle singole zone (cfr. 12.5 a pag. 163).

Una speciale funzione di Anti-Hacker, la *modalità Stealth* (modalità invisibile), impedisce il rilevamento del computer dall'esterno, privando così gli hacker da un obiettivo da attaccare. Questa modalità non influisce sulle prestazioni del computer in Internet, presupponendo che esso non sia utilizzato come server.

12.1. Selezione di un livello di protezione di Anti-Hacker

Kaspersky Internet Security protegge il computer durante la navigazione in Internet in base a uno dei seguenti livelli (cfr. Figura 44):

Blocca tutti – blocca qualsiasi attività di rete sul computer. Se si è selezionato questo livello di sicurezza, non sarà possibile utilizzare nessuna risorsa di rete o programma che richiedano una connessione in rete. Si raccomanda di selezionare questo livello solo in caso di attacco di rete o durante l'uso di una rete pericolosa.

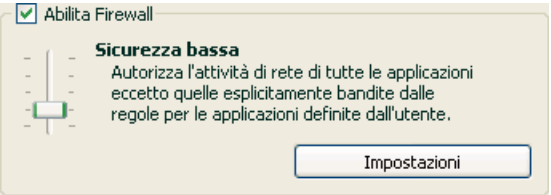


Figura 44. Selezione di un livello di protezione di Anti-Hacker

Sicurezza alta – l'attività di rete è possibile nella misura consentita dalle regole di autorizzazione. Anti-Hacker utilizza regole preimpostate o personalizzate. La serie di regole predefinite di Kaspersky Internet Security include regole di autorizzazione per applicazioni la cui attività di rete non è sospetta e per pacchetti dati assolutamente sicuri da inviare e da ricevere. Se tuttavia nell'elenco delle regole esiste una regola di blocco per un'applicazione con priorità più elevata rispetto a quella di autorizzazione, il programma blocca ogni attività di rete dell'applicazione.

> Attenzione!
>
> Se si seleziona questo livello di sicurezza, tutte le attività di rete non registrate in una regola di autorizzazione di Anti-Hacker saranno bloccate. Si raccomanda quindi di utilizzare questo livello solo se si è certi che tutti i programmi di cui si necessita sono autorizzati dalle regole e se non si progetta di installare nuovo software.

Modalità Training – consente di determinare per ogni singolo caso quali attività di rete autorizzare e quali bloccare. Fanno eccezione le connessioni di rete, le cui regole sono già incluse nel programma. A questo livello, ogni volta che un programma tenta di utilizzare una risorsa di rete o di trasmettere un pacchetto dati, Anti-Hacker controlla se esiste una regola per tale connessione. In presenza di una regola, Anti-Hacker la mette in pratica. In assenza di regole, viene visualizzato un messaggio contenente una descrizione della connessione di rete (il programma che l'ha iniziata, la porta utilizzata, il protocollo, ecc.). L'utente deve decidere se autorizzare la connessione oppure no. Per mezzo di un apposito pulsante nella finestra del messaggio, è possibile creare una regola per tale connessione in modo che, in futuro, Anti-Hacker applicherà le condizioni della regola senza più avvertire l'utente.

Sicurezza bassa – blocca le attività di rete non autorizzate. Anti-Hacker blocca le attività di rete in base alle regole di blocco incluse nel programma o create dall'utente. L'elenco delle regole incluse con Kaspersky Internet Security comprende anche regole di blocco per applicazioni la cui attività di rete è considerata pericolosa e per pacchetti dati che mettono a rischio il computer. Se tuttavia nell'elenco delle regole esiste una regola di autorizzazione per un'applicazione con priorità più elevata rispetto a quella di blocco, il programma autorizza ogni attività di rete dell'applicazione.

Autorizza tutte – autorizza qualsiasi attività di rete sul computer. Si raccomanda di limitare l'uso di questo livello a casi estremamente rari in cui non si osservino attacchi attivi di rete e sia quindi possibile ritenere affidabile ogni attività.

È possibile aumentare o ridurre il livello di sicurezza della rete selezionando quello desiderato o modificando le impostazioni del livello corrente.

Per modificare il livello di sicurezza della rete:

1. Selezionare **Anti-Hacker** nella finestra delle impostazioni di Kaspersky Internet Security.
2. Nella parte destra della finestra, regolare il cursore nella sezione Firewall.

Per configurare il livello di sicurezza della rete:

1. Selezionare il livello di sicurezza che meglio soddisfa le esigenze dell'utente.
2. Fare clic sul pulsante **Impostazioni** e modificare le impostazioni di sicurezza di rete nella finestra che si apre.

12.2. Regole delle applicazioni

Kaspersky Internet Security include una serie di regole per le applicazioni Windows più comuni. È possibile creare più regole di autorizzazione e di blocco per lo stesso programma. Si tratta solitamente di programmi con attività di rete che sono state analizzate in dettaglio dagli esperti Kaspersky Lab e definite come decisamente pericolose o attendibili.

A seconda del livello di sicurezza (cfr. 12.1 a pag. 152) selezionato per la Firewall e del tipo di rete (cfr. 12.5 a pag. 163) di cui fa parte il computer, l'elenco delle regole per i programmi può essere utilizzato in vari modi, per esempio applicando solo regole di autorizzazione con il livello di **Sicurezza alta**. Tutte le attività di rete delle applicazioni che non corrispondono alle regole vengono bloccate.

Per lavorare con l'elenco delle regole per applicazioni:

1. Fare clic su **Impostazioni** nella sezione Firewall della finestra delle impostazioni di Anti-Hacker.
2. Nella finestra che si apre, selezionare la scheda **Regole per applicazioni** (cfr. Figura 45).

Tutte le regole di questa scheda possono essere raggruppate secondo i seguenti criteri:

- *Regole per applicazioni* – Se l'opzione **Raggruppa regole per applicazione** è selezionata, l'elenco delle regole è visualizzato in base alle applicazioni. La scheda contiene in questo caso un elenco di applicazioni per le quali sono state create delle regole. Per ogni applicazione sono riportate le seguenti informazioni: nome e icona dell'applicazione, prompt di comando, root directory in cui si trova il file eseguibile dell'applicazione e il numero di regole create.

  Per mezzo del pulsante **Modifica**, è possibile aprire l'elenco delle regole per l'applicazione selezionata e modificarlo: aggiungere una nuova regola, modificare le regole esistenti e cambiare le priorità.

  Per mezzo del pulsante **Aggiungi**, è possibile aggiungere una nuova applicazione all'elenco e creare una regola apposita.

  I pulsanti **Esporta** e **Importa** sono progettati per consentire di trasferire le regole create da un computer a un altro e accelerare la configurazione di Anti-Hacker.

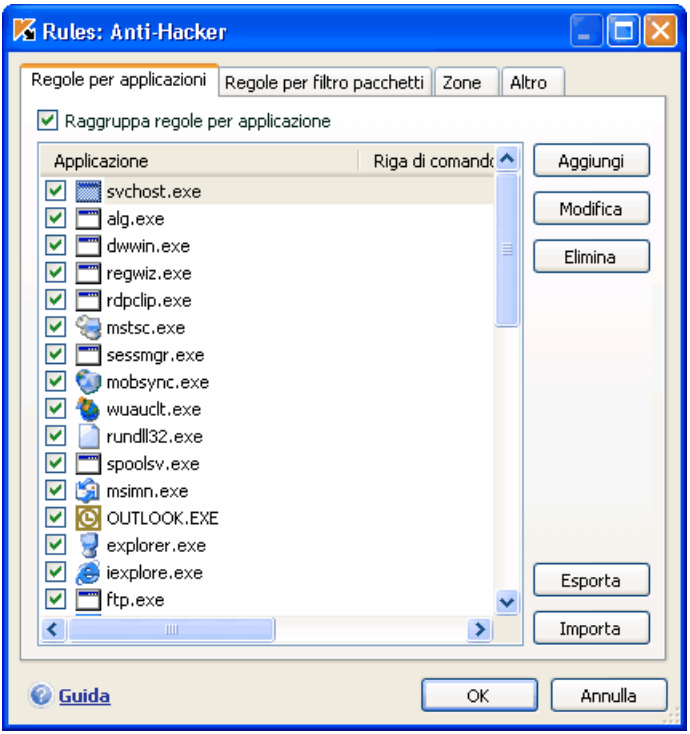


Figura 45. Elenco di regole per le applicazioni installate sul computer

- *Elenco di regole generali* non raggruppate in base al nome dell'applicazione. È possibile visualizzare l'elenco delle regole in questo modo deselezionando ☑ **Raggruppa regole per applicazione**. L'elenco delle regole generali visualizza informazioni complete su una regola: oltre al nome dell'applicazione e al comando per avviarla, è visualizzata l'azione della regola (autorizzazione o blocco dell'attività di rete), con il protocollo di trasferimento dati, la direzione dei dati (in entrata o in uscita) e altre informazioni.

  Il pulsante **Aggiungi** consente di creare nuove regole, mentre per modificare una regola selezionata dall'elenco è possibile usare il pulsante **Modifica**. È possibile inoltre modificare le impostazioni base nella parte inferiore della scheda.

  Servirsi dei pulsanti **Sposta su** e **Sposta giù** per cambiare la priorità delle regole.

12.2.1. Creazione manuale delle regole

Per creare manualmente una regola per applicazioni:

1. Selezionare l'applicazione facendo clic sul pulsante **Aggiungi** o sulla scheda **Regole per applicazioni**. Nella finestra che si apre, selezionare il file eseguibile dell'applicazione per la quale si desidera creare una regola. Si apre un elenco di regole per l'applicazione selezionata. Se esistono già delle regole per l'applicazione, esse sono elencate nella parte superiore della finestra. In assenza di regole, la finestra appare vuota.

   È possibile selezionare un'applicazione in seguito durante la configurazione delle condizioni della regola.

2. Fare clic sul pulsante **Aggiungi** nella finestra delle regole delle applicazioni.

Nella finestra **Nuova regola** che si apre è presente un modulo utilizzabile per affinare una regola (cfr. 12.4 a pag. 164).

12.2.2. Creazione di regole da un modello

Il programma include modelli di regola predefiniti che possono essere utilizzati per la creazione di regole personalizzate. Questi modelli prevedono le operazioni tipiche per le applicazioni, esaminate in maniera approfondita dagli esperti Kaspersky Lab. Per esempio, se un'applicazione è un client di posta, esegue una serie di operazioni standard quali l'invio e la ricezione di messaggi. Per eseguire queste attività vengono stabilite delle connessioni di rete con il server di posta attraverso porte standard e protocolli standard. In situazioni standard come questa è possibile evitare di creare una regola fin dalla base utilizzando un modello.

Per creare una regola per applicazioni da un modello:

1. Se non è già selezionata, selezionare la casella **Raggruppa regole per applicazione** nella scheda **Regole per applicazioni**, e fare clic sul pulsante **Aggiungi**.
2. Nella finestra che si apre, selezionare il file eseguibile dell'applicazione per la quale si desidera creare una regola. Si apre una finestra contenente le regole per l'applicazione selezionata. Se esistono già delle regole per l'applicazione, esse sono elencate nella parte superiore della finestra. In assenza di regole, la finestra appare vuota.
3. Fare clic su **Predefinisci**
4. Nella finestra delle regole per le applicazioni e selezionare uno dei modelli di regola dal menu contestuale (cfr. Figura 46).

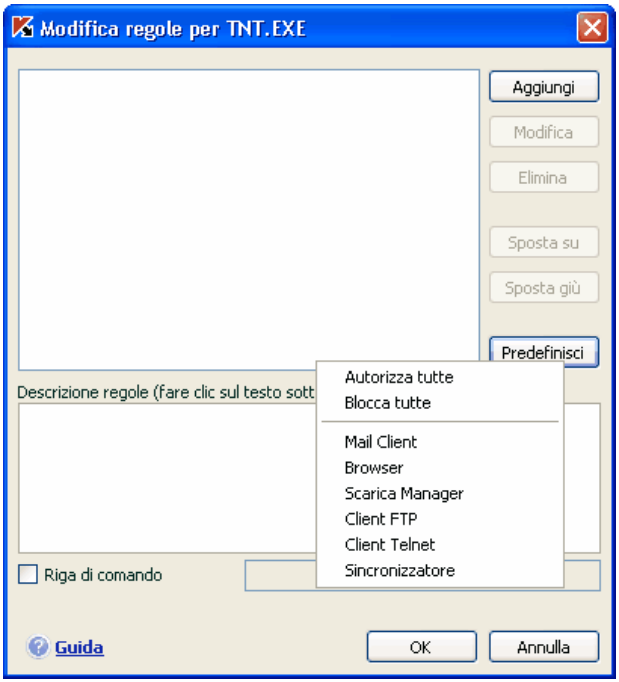


Figura 46. Selezione di un modello per la creazione di una nuova regola

Autorizza tutte è una regola che autorizza qualsiasi attività di rete per l'applicazione. **Blocca tutte** è una regola che blocca qualsiasi attività di rete per l'applicazione. Qualsiasi tentativo di stabilire una connessione di rete da parte dell'applicazione in questione sarà bloccato senza informare l'utente.

Altri modelli elencati nel menu contestuale creano regole tipiche per i programmi corrispondenti. Per esempio, il modello **Mail Client** crea una serie di regole che autorizzano attività di rete standard per client di posta, come l'invio di messaggi.

4. Se necessario, modificare le regole create per l'applicazione. È possibile modificare azioni, direzione della connessione di rete, indirizzo remoto, porte (locale e remota) e l'intervallo temporale da assegnare alla regola.

5. Se si desidera applicare la regola a un'applicazione aperta con determinate impostazioni nella riga di comando, selezionare la casella ☑ **Riga di comando** e digitare la stringa nel campo a destra.

La regola o serie di regole creata sarà aggiunta alla fine dell'elenco con la priorità più bassa. È possibile tuttavia aumentare la priorità della regola (cfr. 12.5 a pag. 163).

È possibile creare una regola dalla finestra di allarme di individuazione di un'attività di rete (cfr. 12.10 a pag. 172).

12.3. Regole di filtraggio pacchetti

Kaspersky Internet Security include una serie di regole utilizzate per filtrare i pacchetti dati in arrivo e in uscita dal computer. Il trasferimento dei pacchetti dati può essere iniziato dall'utente stesso o da un'applicazione installata sul computer. Il programma include regole di filtraggio di pacchetti analizzati scrupolosamente dagli esperti Kaspersky Lab e definiti pericolosi o attendibili.

A seconda del livello di sicurezza selezionato per la Firewall e del tipo di rete di cui fa parte di computer, l'elenco delle regole può essere utilizzato in vari modi. per esempio applicando solo regole di autorizzazione con il livello di **Sicurezza alta**. I pacchetti non coperti da una regola di autorizzazione vengono bloccati.

Per lavorare con l'elenco delle regole di filtraggio dei pacchetti:

1. Fare clic su **Impostazioni** nella sezione Firewall della finestra delle impostazioni di Anti-Hacker.
2. Nella finestra che si apre, selezionare la scheda **Regole per filtro pacchetti** (cfr. Figura 47).

Per ogni regola di filtraggio pacchetti sono riportate le seguenti informazioni: nome della regola, azione (autorizzazione o blocco del trasferimento del pacchetto), protocollo di trasferimento dati, direzione del pacchetto e impostazioni della connessione di rete utilizzate per il trasferimento del pacchetto.

Se il nome della regola di filtraggio del pacchetto è selezionato, essa sarà applicata.

È possibile lavorare con l'elenco delle regole utilizzando i pulsanti a destra dell'elenco.

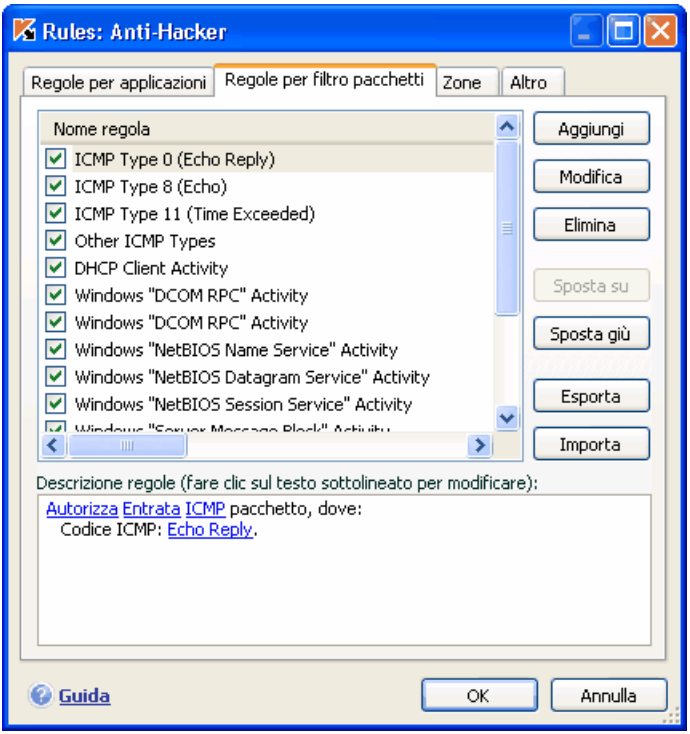


Figura 47. Elenco delle regole di filtraggio pacchetti

Per creare una nuova regola di filtraggio pacchetti:

Fare clic sul pulsante **Aggiungi** nella scheda **Regole per filtro pacchetti**.

Nella finestra **Nuova regola** che si apre è presente un modulo utilizzabile per affinare una regola (cfr. 12.4 a pag. 159).

12.4. Aggiustamento delle regole per applicazioni e filtro pacchetti

La finestra **Nuova regola** per le impostazioni avanzate delle regole è praticamente identica a quella per le applicazioni e il filtro pacchetti (cfr. Figura 48).

Figura 48. Creazione di una nuova regola per applicazioni

Passaggio 1:

- Digitare un nome per la regola. Il programma usa un nome standard che è possibile sostituire.
- Selezionare le impostazioni della connessione di rete per la regola: indirizzo remoto, porta remota, indirizzo locale, ora. Verificare tutte le impostazioni che si desidera applicare alla regola.
- Configurare le altre impostazioni per le notifiche all'utente. Se si desidera visualizzare un messaggio a comparsa con un breve commento ogni volta che si usa una regola, selezionare la casella **Visualizza avviso**. Se si desidera che il programma registri le informazioni relative alle prestazioni della regola nel report Anti-Hacker, selezionare la casella **Registra evento**. Per impostazione predefinita, al momento della creazione della regola la casella non è selezionata. Si raccomanda di utilizzare impostazioni supplementari durante la creazione di regole di blocco.

Passaggio 2: assegnare dei valori ai parametri delle regole e selezionare le azioni. Queste operazioni si eseguono nella sezione **Descrizione regole**.

1. L'azione di ogni regola creata è *autorizza*. Per modificare questa azione in una regola di blocco, fare clic con il pulsante sinistro del mouse sul link

Autorizza nella sezione della descrizione della regola. L'azione diventa Blocca.

2. Se non si era selezionata un'applicazione prima di creare la regola, è necessario farlo adesso facendo clic su seleziona applicazione. Fare clic con il pulsante sinistro del mouse sul link e, nella finestra standard di selezione dei file che si apre, selezionare il file eseguibile dell'applicazione per la quale si sta creando la regola.

3. Quindi è necessario determinare la direzione della connessione di rete per la regola. Il valore predefinito è una regola per una connessione di rete sia in entrata che in uscita. Per modificare la direzione, fare clic con il pulsante sinistro del mouse su in entrata e in uscita e selezionare la direzione della connessione di rete nella finestra che si apre:

   - **Entrata (flusso)**. La regola si applica solo alle connessioni di rete aperte da un computer remoto che invia informazioni al computer dell'utente.
   - **Entrata**. La regola si applica a tutti i pacchetti dati provenienti da un computer remoto, eccezion fatta per i pacchetti TCP.
   - **Entrata ed Uscita**. La regola si applica al traffico in entrata e in uscita, indipendentemente dal computer (dell'utente o remoto) che ha iniziato la connessione di rete.
   - **Uscita (flusso)**. La regola si applica solo alle connessioni di rete aperte dal computer dell'utente che invia informazioni a un computer remoto.
   - **Uscita**. La regola si applica a tutti i pacchetti dati in entrata inviati dal computer dell'utente, eccezion fatta per i pacchetti TCP.

   Se è importante impostare la direzione dei pacchetti specificamente nella regola, selezionare se si tratta di pacchetti in entrata o in uscita. Se si desidera creare una regola per il trasferimento dei dati in streaming, selezionare stream: in entrata, in uscita o entrambi.

   La differenza tra la *direzione di streaming* e la *direzione del pacchetto* è che quando si crea una regola di streaming, si definisce la direzione in cui viene aperta la connessione. La direzione dei pacchetti durante il trasferimento dei dati su questa connessione non viene considerata.

   Per esempio, se si configura una regola per lo scambio di dati con un servizio eseguito in modalità FTP passiva, è necessario autorizzare uno streaming in uscita. Per scambiare dati con un server in modalità FTP attiva, si raccomanda di consentire streaming sia in uscita che in entrata.

4. Se è stato selezionato un indirizzo remoto come proprietà di una connessione di rete, fare clic con il pulsante sinistro del mouse su specifica indirizzo e digitare l'indirizzo IP della regola nella finestra che si apre. È possibile usare uno o più tipi di indirizzo IP per una regola. Possono essere specificati più indirizzi di ciascun tipo.

5. Quindi è necessario impostare il protocollo usato dalla connessione di rete. TCP è il protocollo predefinito per la connessione. Quindi è necessario impostare il protocollo usato dalla connessione di rete. TCP è il protocollo predefinito per la connessione. Se si sta creando una regola per applicazioni, è possibile selezionare il protocollo TCP o l'UDP facendo clic con il pulsante sinistro del mouse sul link con il nome del protocollo fino a visualizzare quello desiderato. Se si sta creando una regola per filtro pacchetti e si desidera change the default protocol, fare clic sul nome e selezionare il protocollo desiderato nella finestra che si apre. Se si seleziona ICMP, può essere necessario indicate the type.

   Per esempio, per parlare con amici tramite ICQ, è necessario creare una regola di autorizzazione per uno streaming UDP in uscita. Tali pacchetti dati servono per le query DNS.

   Se durante l'uso di ICQ si desidera bloccare banner e popup, è necessario creare una regola per quell'applicazione che blocchi l'attivitè TCP in entrata e in uscita (è possibile farlo anche attraverso Anti-Spy: per ulteriori informazioni cfr. Capitolo 11 a pag. 141).

6. Se si sono selezionate le impostazioni della connessione di rete (indirizzo, porta, intervallo temporale), è necessario assegnare loro anche dei valori esatti.

Dopo aver aggiunto la regola all'elenco delle regole per applicazioni, è possibile configurarla ulteriormente (cfr. Figura 49). Se si desidera applicare la regola a un'applicazione aperta con determinate impostazioni nella riga di comando, selezionare la casella **Riga di comando** e digitare la stringa nel campo a destra. Questa regola non sarà valida per le applicazioni avviate con un diverso prompt di comando.

Microsoft Windows 98 non offre l'opzione delle impostazioni iniziali della riga di comando.

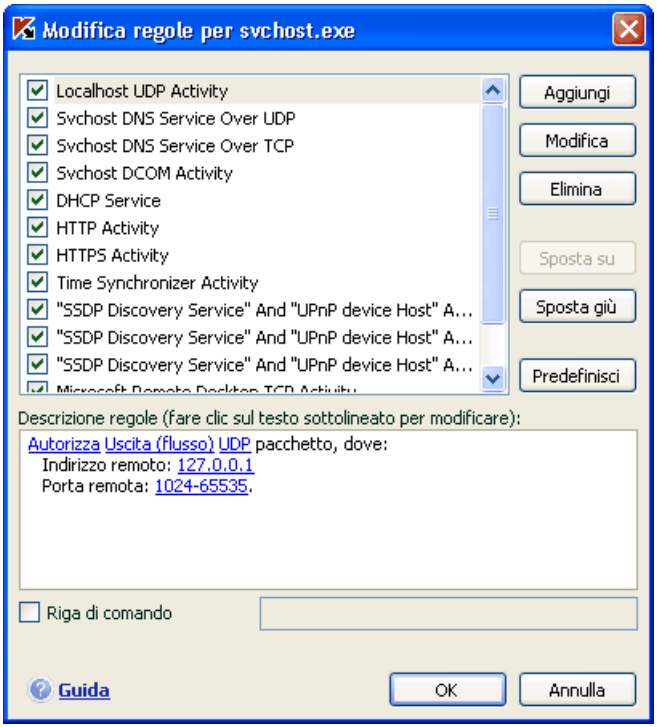


Figura 49. Impostazioni avanzate della nuova regola

È possibile creare una regola dalla finestra di allarme di individuazione di un'attività di rete (cfr. 12.10 a pag. 172).

12.5. Assegnazione della priorità alle regole

Ogni regola creata per un'applicazione o un pacchetto ha una determinata priorità. A parità di altre condizioni (per esempio le impostazioni della connessione di rete), l'azione applicata all'attività del programma sarà quella della regola con la priorità più elevata.

La priorità di una regola dipende dalla sua posizione nell'elenco delle regole. La prima regola dell'elenco è quella con la massima priorità. Ogni regola creata manualmente viene aggiunta all'inizio dell'elenco. Le regole create da modelli o da un avviso vengono aggiunte alla fine dell'elenco delle regole.

Per assegnare una priorità alle regole per applicazioni procedere come segue:

1. Selezionare il nome dell'applicazione nella scheda **Regole per applicazione**.
2. Usare i pulsanti **Sposta su** e **Sposta giù** nella finestra delle regole per applicazioni che si apre per spostare la posizione delle regole nell'elenco, modificando in tal modo l'ordine delle priorità.

Per assegnare una priorità alle regole di filtraggio dei pacchetti procedere come segue:

1. Selezionare la regola nella scheda **Regole per filtro pacchetti**.
2. Usare i pulsanti **Sposta su** e **Sposta giù** nella finestra delle regole per applicazioni che si apre per spostare la posizione delle regole nell'elenco, modificando in tal modo l'ordine delle priorità.

12.6. Regole per zone di sicurezza

Dopo l'installazione, Anti-Hacker analizza l'ambiente di rete del computer. In base ai risultati dell'analisi, l'intero spazio di rete viene suddiviso in zone:

Internet – il World Wide Web. In questa zona, Kaspersky Internet Security agisce come una firewall personale. Così facendo, le regole predefinite di filtraggio pacchetti e delle applicazioni regolano l'intera attività di rete per garantire la massima sicurezza. Durante una sessione di lavoro in questa zona non è possibile modificare le impostazioni di protezione ma solo abilitare la modalità invisibile per una maggiore sicurezza del computer.

Zone di sicurezza – alcune zone, per lo più sottoreti delle quali fa parte il computer (per esempio sottoreti a casa o al lavoro). Per impostazione predefinita, queste zone sono definite "a medio rischio". È possibile modificare lo status di queste zone in base a quanto si ritiene affidabile una determinata sottorete, e configurare regole per il filtraggio pacchetti e le applicazioni.

Se è abilitata la modalità Training di Anti-Hacker, si apre una finestra ogni volta che il computer si connette a una nuova zona, visualizzandone una breve descrizione. È necessario assegnare uno status alla zona: in base ad esso l'attività di rete sarà autorizzata oppure no.

- **Internet**. È lo status predefinito assegnato a Internet, poiché durante la navigazione il computer è soggetto a tutti i tipi di minacce potenziali. Questo status è raccomandato anche per le reti non protette da programmi antivirus, firewall, filtri, ecc. Selezionando questo status, il programma garantisce la massima sicurezza durante l'uso di questa zona, in particolare:

- Blocco di qualsiasi attività di rete NetBios all'interno della sottorete
- Blocco delle regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBios all'interno della sottorete

Anche se è stata creata una directory ad accesso libero, le informazioni in essa contenute saranno disponibili solo agli utenti di sottoreti con questo status. Inoltre, quando si seleziona questo status, non è possibile accedere a file e stampanti di altre reti di computer.

- **LAN**. Il programma assegna questo status a tutte le zone rilevate durante l'analisi dell'ambiente di rete del computer, con l'eccezione delle zone Internet. Si raccomanda di applicare questo status alle zone caratterizzate da un fattore di rischio medio (per esempio LAN aziendali). Selezionando questo status, il programma consente:
  - Qualsiasi attività di rete NetBios all'interno della sottorete
  - Regole per applicazioni e filtraggio pacchetti che consentono un'attività NetBios all'interno della sottorete

  Selezionare questo status se si desidera garantire l'accesso a determinate cartelle del computer, bloccando al tempo stesso qualsiasi altra attività esterna. Gli utenti ai quali si desidera concedere l'accesso ai file del computer possono utilizzarli, ma non possono installare un troiano nel computer.
- **Attendibile**. Questo status è raccomandato solo per le zone ritenute assolutamente sicure, in cui il computer non è esposto ad attacchi o tentativi di accesso ai dati in esso custoditi. Se si seleziona questo status, tutte le attività di rete sono consentite. Anche se in precedenza si è selezionato il massimo livello di protezione creando regole di blocco, questi sistemi di sicurezza non vengono applicati per i computer remoti provenienti da una zona attendibile.

Osservare che qualsiasi restrizione o autorizzazione all'accesso ai file ha valore solo all'esterno di questa sottorete.

Per una maggiore sicurezza durante l'uso di reti indicate come **LAN** o **Internet** è possibile attivare la *modalità invisibile*. Questa caratteristica consente solo le attività di rete iniziate dall'utente o da un'applicazione autorizzata. In altre parole, il computer diventa invisibile per il resto dell'ambiente. Questa modalità non pregiudica le prestazioni del computer su Internet.

La modalità invisibile è sconsigliata se il computer funziona da server (per esempio un server di posta o HTTP). In tal caso infatti i computer che si connettono al server non riuscirebbero a verderlo.

L'elenco delle zone delle quali il computer fa parte è visualizzato nella scheda **Zone** (cfr. Figura 50). Per ciascuna di esse sono indicati lo status, una breve descrizione della rete e l'eventuale uso della modalità Stealth.

Per modificare lo status di una zona o abilitare/disabilitare la modalità invisibile, selezionarla dall'elenco e seguire i collegamenti appropriati nel riquadro **Descrizione regole** sotto l'elenco. È possibile eseguire attività simili e modificare indirizzi e maschere di sottoreti nella finestra **Proprietà zona** che si apre facendo clic su **Modifica**.

È possibile aggiungere una nuova zona all'elenco durante la visualizzazione. A tal fine, fare clic su **Aggiorna**. Anti-Hacker cerca le potenziali zone di registrazione, chiedendo eventualmente di selezionare uno status da assegnare loro. È possibile inoltre aggiungere manualmente nuove zone all'elenco (per esempio se si connette il laptop a una nuova rete). Per fare questo, usare il pulsante **Aggiungi** e inserire le informazioni necessarie nella finestra **Proprietà zona**.

Per eliminare una rete dall'elenco, fare clic sul pulsante **Elimina**.

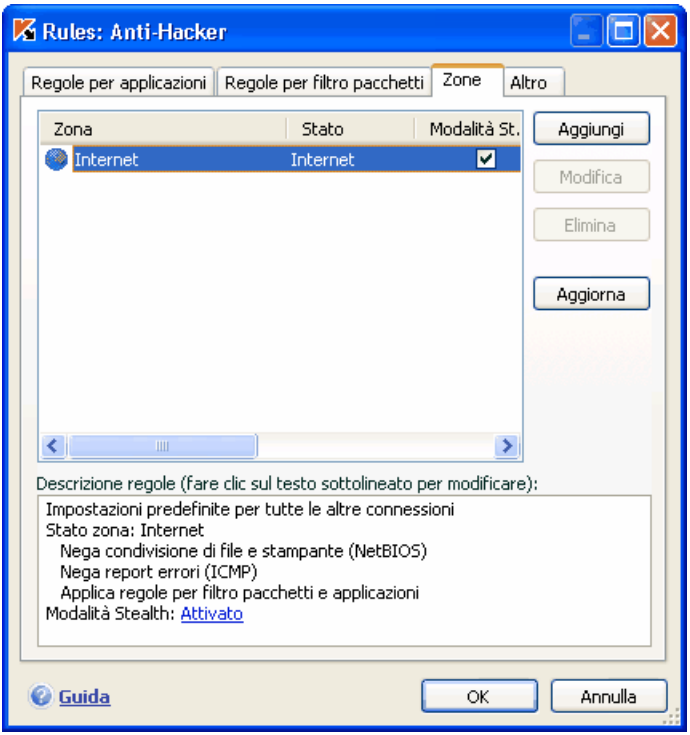


Figura 50. Elenco delle regole per le zone

12.7. Modalità Firewall

La modalità Firewall (cfr. Figura 51) controlla la compatibilità di Anti-Hacker con i programmi che stabiliscono connessioni di rete multiple e con giochi in rete.

Massima compatibilità – il firewall garantisce il funzionamento ottimale di Anti-Hacker con i programmi che stabiliscono connessioni di rete multiple (client di rete per la condivisione di file). Questa modalità tuttavia può comportare un rallentamento del tempo di reazione nei giochi in rete. In presenza di tali problemi si raccomanda di applicare la Massima velocità.

Massima velocità – il firewall garantisce un tempo di reazione ottimale durante i giochi in rete. Tuttavia questa opzione può provocare dei conflitti con client di condivisione file o altre applicazioni di rete. Per risolvere il problema disabilitare la modalità Stealth.

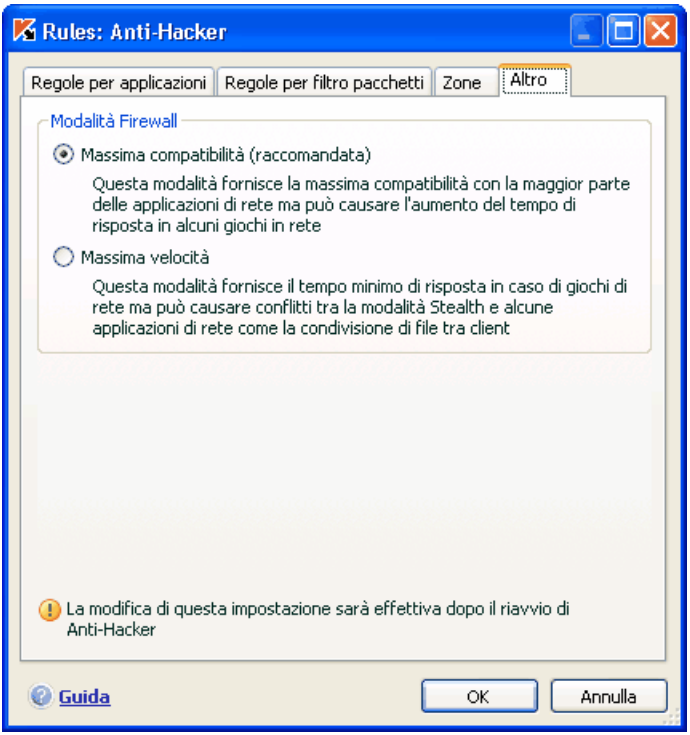


Figura 51. Selezione di una modalità Anti-Hacker

Per selezionare una modalità Firewall:

1. Fare clic su **Impostazioni** nella sezione Firewall della finestra delle impostazioni di Anti-Hacker.
2. Selezionare la scheda **Altro** nella finestra che si apre e selezionare la modalità desiderata, Massima compatibilità o Massima velocità.

Le modifiche alla modalità Firewall avranno effetto solo dopo aver riavviato Anti-Hacker.

12.8. Configurazione del sistema di intercettazione intrusioni

Tutti gli attacchi di rete noti che potrebbero mettere in pericolo il computer sono presenti nell'elenco delle minacce. Il **sistema di intercettazione intrusioni** di Anti-Hacker si basa su un elenco di tali attacchi. L'elenco degli attacchi che possono essere intercettati da Intrusion Detector viene aggiornato durante il processo di aggiornamento delle firme (cfr. Capitolo 15 a pag. 215).

Il sistema di intrusione attacchi intercetta le attività di rete tipiche degli attacchi, e se intercetta un tentativo di attaccare il computer ne blocca qualsiasi attività di rete per un'ora. In questo caso viene visualizzato un messaggio che informa dell'avvenuto tentativo di attacco, con informazioni specifiche sul computer da cui l'attacco è partito.

È possibile configurare il sistema di intercettazione attacchi procedendo come segue:

3. Aprire la finestra delle impostazioni di Anti-Hacker.
4. Fare clic su **Impostazioni** nella finestra **Intrusion Detector**.
5. Nella finestra che si apre (cfr. Figura 52), specificare se si desidera bloccare un computer pirata e, se sì, per quanto tempo. Per impostazione predefinita, il computer viene bloccato per 60 minuti. È possibile aumentare o ridurre questo periodo modificando il valore nel campo accanto a ☑ **Blocca il computer da cui proviene l'attacco per… min**. Se si desidera interrompere il blocco dell'attività di rete di un computer pirata nei confronti del proprio computer, deselezionare questa casella.

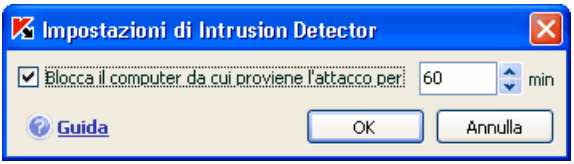


Figura 52. Configurazione del tempo di blocco di computer pirata

12.9. Elenco degli attacchi di rete intercettati

Esistono attualmente numerosi attacchi di rete che sfruttano le vulnerabilità dei sistemi operativi e di altri software, sistemi o altro, installati sul computer. I pirati informatici sviluppano costantemente nuovi metodi di attacco, imparando come trafugare informazioni confidenziali, provocando anomalie di funzionamento del sistema o "impadronendosi" del computer per utilizzarlo come elemento di una rete fantasma da cui lanciare nuovi attacchi.

Per garantire la sicurezza del computer, è necessario conoscere i tipi di attacchi di rete possibili. Gli attacchi di rete noti possono essere suddivisi in tre categorie principali:

- **Scansione di porte** – questa minaccia non costituisce di per sé un attacco, ma di solito ne precede uno poiché si tratta di uno dei metodi più comuni per ottenere informazioni su un computer remoto. Le porte UDP/TCP utilizzate dagli strumenti di rete sull'indirizzo in questione vengono scansionate per capire se sono chiuse o aperte.

  Dalla scansione delle porte, un pirata è in grado di capire quali tipi di attacco funzioneranno sul sistema e quali no. Inoltre, le informazioni ottenute dalla scansione (un modello del sistema) consentono di identificare il sistema operativo utilizzato dal computer remoto. Questo, a sua volta, circoscrive ulteriormente il numero degli attacchi possibili e, di conseguenza, il tempo necessario a lanciarli. Inoltre consente al pirata di sfruttare le vulnerabilità specifiche del sistema operativo.

- **Attacchi DoS (Denial of Service)** – si tratta di attacchi volti a rendere instabile o completamente inoperativo il sistema. Le conseguenze di questi attacchi sono il danneggiamento o la corruzione delle risorse dati a cui sono rivolti e l'impossibilità di utilizzare quelle risorse.

  Esistono due tipi principali di attacchi DoS:

  - L'invio al computer attaccato di pacchetti appositamente creati per provocare il riavvio o l'arresto del sistema.

- L'invio al computer attaccato di numerosi pacchetti in un lasso temporale estremamente breve che non consente al computer di elaborarli, esaurendo le risorse di sistema.

Quelli descritti di seguito sono esempi comuni di attacchi di questa categoria:

- *Ping of death* – consiste nell'invio di un pacchetto ICMP di dimensioni superiori a quelle massime di 64 KB. Questo attacco è in grado di bloccare completamente alcuni sistemi operativi.
- *Land* – consiste nell'inviare a una porta aperta del computer una richiesta di connessione con se stessa. Il computer entra in un circolo vizioso che incrementa il carico sul processore e può provocare il blocco di alcuni sistemi operativi.
- *ICMP Flood* – consiste nell'invio di un numero elevato di pacchetti ICMP al computer attaccato. L'attacco costringe il computer a rispondere a ciascun pacchetto in entrata, sovraccaricando gravemente il processore.
- *SYN Flood* – consiste nell'invio di un numero elevato di query al computer per stabilire una falsa connessione. Il sistema riserva determinate risorse a ciascuna di queste connessioni, assorbendo totalmente le risorse disponibili. In conseguenza di questo attacco, il computer non reagisce più ad altri tentativi di connessione.

- **Intrusioni**, volte a impadronirsi del computer attaccato. Si tratta del tipo di attacco più pericoloso di tutti poiché, se portato a buon fine, offre al pirata il controllo completo del computer.

  I pirati utilizzano questo tipo di attacco per ottenere informazioni confidenziali con un computer remoto (per esempio, numeri di carte di credito o password) o per controllare il sistema al fine di utilizzarne in seguito le risorse per fini illeciti (il sistema catturato sarà usato come elemento di reti fantasma o come piattaforma per nuovi attacchi).

  Questo gruppo comprende più attacchi di qualsiasi altro. Essi possono essere suddivisi in tre sottogruppi a seconda del sistema operativo: attacchi a Microsoft Windows, attacchi a Unix e attacchi efficaci con entrambi i sistemi operativi.

  I tipi di attacco più comuni che utilizzano strumenti del sistema operativo sono:

  - *Attacchi di overflow del buffer* – tipo di vulnerabilità del software che si manifesta a causa del controllo insufficiente o assente sulla gestione di massicci quantitativi di dati. È uno dei primi tipi di vulnerabilità scoperti dai pirati e il più facile da sfruttare.

- *Attacchi di stringhe di formato* – tipo di vulnerabilità che deriva da un controllo insufficiente dei valori di input per le funzioni I/O, quali printf(), fprintf(), scanf() e altri della libreria C standard. Se un programma presenta questa vulnerabilità, un pirata può ottenere il controllo completo del sistema servendosi di query create con una tecnica speciale.

Intrusion Detector analizza e blocca automaticamente i tentativi di sfruttare queste vulnerabilità dei più comuni strumenti di rete (FTP, POP3, IMAP) eseguiti sul computer dell'utente.

Gli *attacchi a Microsoft Windows* si basano sullo sfruttamento delle vulnerabilità dei software installati sul computer (per esempio, di programmi come Microsoft SQL Server, Microsoft Internet Explorer, Messenger e di componenti del sistema accessibili attraverso la rete come DCom, SMB, Wins, LSASS, IIS5).

Per esempio, Anti-Hacker protegge il computer da attacchi che sfruttano le seguenti vulnerabilità del software (questo elenco di vulnerabilità è tratto dal sistema di numerazione della Microsoft Knowledge Base):

(**MS03-026**) Vulnerabilità DCOM RPC (worm Lovesan)

(**MS03-043**) Sovraccarico buffer servizio Microsoft Messenger

(**MS03-051**) Overflow del buffer delle estensioni del server di Microsoft Frontpage 2000

(**MS04-007**) Vulnerabilità ASN.1 Microsoft Windows

(**MS04-031**) Overflow del buffer remoto non autenticato del servizio Microsoft NetDDE

(**MS04-032**) Overflow di heap metafile (.emf) Microsoft Windows XP

(**MS05-011**) Gestione delle risposte transazioni client Microsoft Windows SMB

(**MS05-017**) Vulnerabilità overflow del buffer di accodamento messaggi Microsoft Windows

(**MS05-039**) Overflow remoto del servizio Plug-and-Play di Microsoft Windows

(**MS04-045**) Overflow dell'heap remoto di Microsoft Windows Internet Naming Service (WINS)

(**MS05-051**) Modifica della memoria del coordinatore transazioni distribuite di Microsoft Windows

Esistono inoltre casi isolati di intrusioni mediante script maligni, fra cui gli script elaborati da Microsoft Internet Explorer e worm di tipo Helkern. Questo tipo di attacco consiste essenzialmente nell'invio di speciali pacchetti UDP a un computer remoto in grado di eseguire il codice nocivo.

Ricordare che, quando è connesso in rete, il computer è esposto ogni giorno al rischio di attacchi di pirateria informatica. Per garantire la protezione del computer, è necessario abilitare Anti-Hacker durante l'uso di Internet e aggiornare regolarmente gli elenchi degli attacchi (cfr. 15.3.2 a pag. 221).

12.10. Blocco e autorizzazione di attività di rete

Se il livello di sicurezza del firewall è impostato su **Modalità training**, ogni volta che viene tentata una connessione di rete priva di regole viene visualizzato un apposito messaggio.

Per esempio, se il client di posta utilizzato è MS Outlook, esso scarica la posta da un Exchange server remoto. Per visualizzare la casella di posta in arrivo, il programma si connette al server di posta. Anti-Hacker intercetta sempre questo tipo di attività di rete e visualizza un messaggio (cfr. Figura 53) contenente:

- *La descrizione dell'attività* – il nome dell'applicazione e le caratteristiche della connessione che sta avviando. Generalmente vengono indicati aaanche il tipo di connessione, la porta locale da cui essa è avviata, la porta remota e l'indirizzo a cui ci si connette. Fare clic con il pulsante sinistro del mouse su un punto qualsiasi del messaggio per ottenere informazioni più dettagliate sull'attività di rete. La finestra che si apre contiene informazioni sulla connessione, sul processo che l'ha iniziata e sullo sviluppatore dell'applicazione.
- *L'azione* – le operazioni che Anti-Hacker eseguirà relative all'attività di rete individuata. La configurazione di questo parametro è a scelta dell'utente.

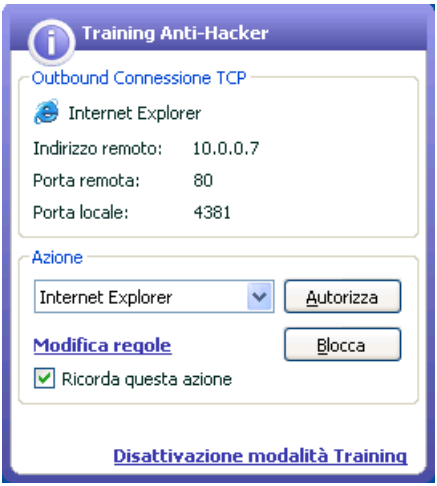


Figura 53. Notifica di attività di rete

Consultare con attenzione le informazioni sull'attività di rete e solo dopo selezionare le azioni di Anti-Hacker. Si raccomanda di decidere tenendo conto dei seguenti suggerimenti:

1. Prima di procedere, stabilire se autorizzare o bloccare l'attività di rete. È possibile che nella situazione specifica una serie di regole già create per l'applicazione o pacchetto possa essere di aiuto (supponendo che sia stata creata). Per fare ciò, utilizzare il collegamento **Modifica regole**. Si apre quindi una finestra contenente un elenco completo delle regole create per l'applicazione o pacchetto dati.
2. Decidere quindi se eseguire l'azione una sola volta o automaticamente ogni volta che viene intercettata questa attività.

Per eseguire l'azione una sola volta:

Deselezionare la casella ☑ **Ricorda questa azione** e fare clic sul pulsante con il nome dell'azione, per esempio **Autorizza**.

Per eseguire automaticamente l'azione selezionata ogni volta che questa attività viene iniziata sul computer:

1. Selezionare la casella ☑ **Ricorda questa azione**.
2. Selezionare il tipo di attività che si desidera eseguire dall'elenco a discesa nella sezione **Azione**:
   - **Tutte le attività** – qualsiasi attività di rete iniziata dall'applicazione.

- **Personalizzato** – attività specifiche che l'utente dovrà definire in un'apposita finestra come per la creazione di una regola (cfr. 12.2.1 a pag. 156).
- **<Modello>** – il nome del modello che include la serie di regole tipiche dell'attività di rete dell'applicazione. Questo tipo di attività è incluso nell'elenco se Kaspersky Internet Security possiede un modello appropriato per l'applicazione che ha iniziato l'attività di rete (cfr. 12.2.2 a pag. 156). In tal caso non è necessario personalizzare le attività da autorizzare o da bloccare. È sufficiente usare il modello per creare automaticamente una serie di regole per l'applicazione.

3. Fare clic sul pulsante con il nome dell'azione (**Autorizza** o **Blocca**).

Ricordare che la regola creata sarà usata solo quando tutti i parametri della connessione corrispondono a quelli indicati. Per esempio, questa regola non viene applicata a connessioni stabilite da una porta locale diversa.

CAPITOLO 13. ANTI-SPAM

Kaspersky Internet Security 6.0 include uno speciale componente che intercetta lo spam e lo elabora in base alle regole del client di posta, consentendo all'utente di risparmiare tempo durante l'uso della posta elettronica.

La posta elettronica viene sottoposta a scansione antispam in base al seguente metodo:

1. L'indirizzo del mittente viene confrontato con le liste bianche e le liste nere degli indirizzi.
    - Se è presente nella lista bianca, il messaggio viene classificato come *accettato*.
    - Se è presente nella lista nera, il messaggio viene classificato come *spam*. Ulteriori analisi dipendono dall'azione selezionata (cfr. 13.3.8 a pag. 194).
2. Se l'indirizzo del mittente non è presente né nella lista bianca né in quella nera, il messaggio viene analizzato per mezzo della tecnologia PDB (cfr. 13.3.2 a pag. 183) in cerca di espressioni tipiche dello spam. L'analisi si basa sul database creato addestrando Anti-Spam.
3. Anti-Spam esamina in dettaglio il testo del messaggio e cerca frasi presenti nelle liste bianca o nera.
    - Se il testo contiene frasi presenti nella lista bianca delle frasi, il messaggio è classificato come *accettato*.
    - In presenza di frasi contenute nella lista nera, il messaggio è classificato come *spam*. L'ulteriore elaborazione dipende dall'azione selezionata.
4. Se il messaggio non contiene frasi presenti nella lista bianca o nella lista nera, viene sottoposto a scansione anti-phishing. Se il testo contiene un indirizzo presente nel database anti-phishing, il messaggio è classificato come *spam*. L'ulteriore elaborazione dipende dall'azione selezionata.
5. Se il messaggio non contiene elementi di phishing, viene sottoposto a scansione antispam utilizzando speciali tecnologie:
    - Analisi grafica mediante tecnologia GSG
    - Analisi del testo mediante l'algoritmo di Bayes per il riconoscimento dello spam

6. Quindi il messaggio viene scansionato alla ricerca di fattori di filtraggio spam avanzati (cfr. 13.3.5 a pag. 191) impostati dall'utente al momento dell'installazione di Anti-Spam. Questa fase potrebbe includere l'analisi dei tag HTML, delle dimensioni dei caratteri o degli eventuali caratteri nascosti.

Ciascuna delle fasi sopra elencate a cui viene sottoposto il messaggio durante l'analisi antispam può essere disabilitata.

Sono disponibili plug-in Anti-Spam per i seguenti client di posta:

- MS Outlook (cfr. 13.3.9 a pag. 194)
- Outlook Express (cfr. 13.3.10 a pag. 198)
- The Bat! (cfr. 13.3.11 a pag. 199)

Attenzione!

Questa versione di Kaspersky Internet Security non offre plug-in Anti-Spam per le versioni a 64 bit di Microsoft Office Outlook, Microsoft Outlook Express e The Bat!

Il pannello delle attività di MS Outlook e Outlook Express presenta due pulsanti, **Spam** e **Accettato**, che consentono di configurare Anti-Spam in modo da individuare lo spam direttamente nella casella della posta. Questi pulsanti non sono presenti in The Bat!, ma il programma può essere addestrato utilizzando gli speciali elementi **Segna come spam** e **Segna come NON spam** nel menu **Speciale**. Inoltre, alle impostazioni del client di posta vengono aggiunti speciali parametri di elaborazione antispam (cfr. 13.3.1 a pag. 183).

Anti-Spam fa uso di un algoritmo di Bayes modificato per l'autoistruzione, che consente al componente di imparare a distinguere tra *spam* e *non spam*. Gli esperti Kaspersky Lab hanno perfezionato l'algoritmo di Bayes in modo da garantire una configurazione più flessibile per l'intercettazione della posta indesiderata. L'algoritmo preleva i dati dal contenuto della lettera.

Si presentano situazioni in cui l'algoritmo di Bayes modificato per l'autoapprendimento non è in grado di classificare un determinato messaggio come spam o accettato con precisione. Questi messaggi vengono classificati come *probabile spam*.

Per ridurre il numero di messaggi classificati come probabile spam, si raccomanda di effettuare l'ulteriore training Anti-Spam (cfr. 13.2 a pag. 178) per tali messaggi, specificando quali di essi devono essere classificati come *spam* e quali come *non spam*.

I messaggi riconosciuti come *spam* o *probabile spam* vengono modificati: alla riga dell'oggetto vengono aggiunte le annotazioni **[!! SPAM]** o **[?? Probabile spam]**.

Le regole per l'elaborazione dei messaggi classificati come spam o probabile spam in MS Outlook, Outlook Express o The Bat! possono essere configurate in speciali plug-in creati appositamente per questi client. Per altri client di posta, è possibile creare delle regole di filtraggio che prendano in considerazione la riga dell'oggetto e, per esempio, configurarli in modo da spostare i messaggi in cartelle apposite a seconda che contengano **[!! SPAM]** o **[?? Probabile spam]**. Per una descrizione più dettagliata del meccanismo di filtraggio, consultare la documentazione del client di posta usato.

13.1. Selezione di un livello di sensibilità per Anti-Spam

Kaspersky Internet Security protegge il computer dallo spam in base a uno dei seguenti livelli (cfr. Figura 54):

Blocca tutto – il livello di sensibilità più severo, che classifica come spam tutti i messaggi che non contengono frasi presenti nella lista bianca delle frasi (cfr. 13.3 a pag. 182) e i cui mittenti non sono elencati nella lista bianca. A questo livello, i messaggi vengono esaminati solo a fronte della lista bianca. Tutte le altre funzioni sono disabilitate.

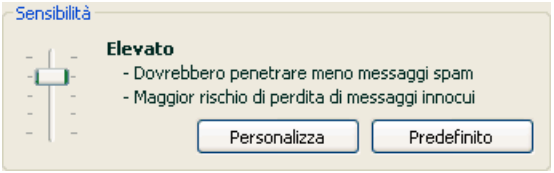


Figura 54. Selezione di un livello di sicurezza per Anti-Spam

Elevato – un livello severo che, se attivato, aumenta la probabilità che alcuni messaggi effettivamente accettabili vengano classificati come *spam*. A questo livello, il messaggio viene esaminato a fronte delle liste bianca e nera, mediante le tecnologie PDB e GSG e in base all'algoritmo modificato di Bayes (cfr. 13.3.2 a pag. 183).

Questo livello deve essere adottato solo nei casi in cui la probabilità che l'indirizzo del destinatario sia ignoto agli spammer è elevata, per esempio quando il destinatario non è iscritto a nessuna mailing list e non possiede un indirizzo e-mail su server gratuiti/non aziendali.

Raccomandato – il livello ottimale per classificare i messaggi.

A questo livello è possibile che alcuni messaggi spam non siano intercettati, segnalando così un training di Anti-Spam insufficiente. Si raccomanda di effettuare il training supplementare del modulo utilizzando la procedura

guidata di Training (cfr. 13.2.1 a pag. 179) o il pulsante **Spam**/**NON Spam** (elementi di menu di The Bat!) per i messaggi classificati in maniera erronea.

Basso – il livello più permissivo. Può essere raccomandato per gli utenti la cui corrispondenza, per qualsiasi motivo, contiene un numero significativo di parole riconosciute come spam da Anti-Spam, senza essere tali. Ciò può essere dovuto all'attività professionale del destinatario, che richiede per la corrispondenza con i colleghi l'uso di un linguaggio ampiamente diffuso tra gli spammer. Tutte le tecnologie di intercettazione dello spam sono utilizzate per analizzare i messaggi a questo livello.

Autorizza tutto – lowest sensitivity level. A questo livello sono riconosciuti come spam solo i messaggi che contengono frasi presenti nella lista nera delle frasi e i cui mittenti sono presenti nell'elenco nero degli indirizzi. I messaggi vengono esaminati solo a fronte della lista nera. Tutte le altre funzioni sono disabilitate.

Per impostazione predefinita, la protezione antispam è impostata sul livello **Raccomandato**.

È possibile tuttavia aumentare o ridurre il livello di protezione oppure modificare le impostazioni del livello corrente.

Per modificare un livello di protezione:

Regolare i cursori della sensibilità. Regolando il livello di sensibilità si definisce la correlazione tra i fattori di spam, probabile spam e messaggi accettabili (cfr. 13.3.3 a pag. 185).

Per modificare le impostazioni del livello corrente:

Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni di Anti-Spam. Modificare il fattore spam nella finestra che si apre e fare clic su **OK**.

Il livello di sicurezza diventa quindi **Impostazioni personalizzate**, con impostazioni configurate dall'utente.

13.2. Addestramento di Anti-Spam

Anti-Spam è dotato di un database di posta preinstallato contenente cinquanta esempi di spam. Si raccomanda tuttavia di sottoporre il modulo Anti-Spam a un ulteriore addestramento basato sui messaggi ricevuti.

Esistono diversi approcci di addestramento di Anti-Spam:

- Usare la Procedura guidata di training (cfr. 13.2.1 a pag. 179)
- Addestrare Anti-Spam (cfr. 13.2.2 a pag. 180) in base alle e-mail inviate.

- Addestrare il programma direttamente mentre si lavora con la posta elettronica (cfr. 13.2.3 a pag. 180) utilizzando gli appositi pulsanti nel pannello strumenti o nei menu del client.
- Addestrare Anti-Spam con i report (cfr. 13.2.4 a pag. 181)

L'addestramento mediante procedura guidata è il migliore fin dal primo utilizzo di Anti-Spam. La procedura guidata è in grado di addestrare Anti-Spam in base a un numero molto elevato di messaggi.

Osservare che non è possibile addestrare Anti-Spam con più di 50 messaggi per cartella. In presenza di cartelle contenenti un numero superiore di messaggi, il programma ne utilizzerà solo 50 ai fini del training.

Il training supplementare utilizzando gli speciali pulsanti nell'interfaccia del client è preferibile quando si sceglie di lavorare direttamente sui messaggi.

13.2.1. Procedura guidata di training

La Procedura guidata di training consente di addestrare Anti-Spam indicando le cartelle di posta che contengono spam e messaggi accettabili.

Per avviare la Procedura guidata di training:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni.
2. Fare clic sul pulsante **Procedura guidata di training** nella parte destra della finestra.

La Procedura guidata di training guida l'utente passo passo nell'addestramento di Anti-Spam. Facendo clic sul pulsante **Avanti** si apre la fase successiva dell'addestramento, mentre il pulsante **Indietro** consente di tornare alla fase precedente.

La fase 1 della Procedura guidata di training richiede la selezione delle cartelle contenenti la posta accettabile. In questa fase è sufficiente selezionare le cartelle i cui contenuti sono ritenuti assolutamente attendibili.

La fase 2 della Procedura guidata di training consiste nella selezione delle cartelle contenenti lo spam.

Nella fase 3 Anti-Spam viene addestrato automaticamente sulle cartelle selezionate. I messaggi presenti in queste cartelle costituiranno il database di Anti-Spam. I mittenti dei messaggi accettabili vengono inseriti automaticamente nella lista bianca degli indirizzi.

Nella fase 4 è necessario salvare i risultati dell'addestramento applicando uno dei seguenti metodi: Aggiungere i risultati dell'addestramento al database corrente o sostituire il database corrente con i risultati dell'addestramento. Ricordare che, affinché il meccanismo di intercettazione dello spam funzioni correttamente, è necessario addestrare il programma su un minimo di 50

messaggi accettabili e 50 messaggi di spam. In caso contrario l'algoritmo di Bayes non funzionerà.

Per risparmiare tempo, la Procedura guidata di training limita l'addestramento a 50 messaggi tra quelli presenti in ciascuna cartella selezionata.

13.2.2. Addestramento con i messaggi in uscita

È possibile addestrare Anti-Spam con i messaggi in uscita direttamente dal client di posta. La lista bianca degli indirizzi di Anti-Spam viene integrata con gli indirizzi dei messaggi in uscita. Per il training vengono utilizzati solo i primi 50 messaggi, dopodiché la procedura è completa.

Per addestrare Anti-Spam con i messaggi in uscita:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni.
2. Selezionare la casella ☑ **Training sui messaggi di posta in uscita** nella sezione **Training**.

Attenzione!

Se si seleziona la casella ☑ **Scansiona all-invio** del plug-in di Microsoft Outlook E-mail Anti-Virus (cfr. 13.3.9 a pag. 194), Anti-Spam utilizza per l'addestramento solo i messaggi in uscita inviati tramite il protocollo MAPI.

13.2.3. Training mediante il client di posta

Per addestrare il programma direttamente dalla casella di posta, è possibile utilizzare gli appositi pulsanti sul pannello degli strumenti del client.

Al momento dell'installazione sul computer, Anti-Spam installa i plug-in dei seguenti client di posta:

- MS Outlook
- Outlook Express
- The Bat!

Attenzione!

Questa versione di Kaspersky Internet Security non offre plug-in Anti-Spam per le versioni a 64 bit di Microsoft Office Outlook, Microsoft Outlook Express e The Bat!

In Outlook compaiono due pulsanti, **Spam** e **Accettati**, nel pannello delle attività, e la scheda **Anti-Spam** con le azioni da selezionare (cfr. 13.3.9 a pag. 194) nel

menu **Guida→ Impostazioni**. Oltre ai pulsanti **Spam** e **Accettati**, Outlook Express aggiunge un pulsante **Impostazioni** nel pannello delle attività, che apre una finestra contenente le azioni da eseguire sullo spam (cfr. 13.3.10 a pag. 198). Questi pulsanti non sono presenti in The Bat!, ma il programma può essere addestrato utilizzando gli speciali elementi **Segna come spam** e **Segna come NON spam** nel menu **Speciale**.

Se si decide di classificare come spam il messaggio selezionato, fare clic sul pulsante **Spam**. Se il messaggio non è da considerare spam, fare clic su **Accettato**. Anti-Spam esegue quindi il training sull'ultimo messaggio selezionato. Se si selezionano diversi messaggi, essi vengono tutti utilizzati per il training.

Attenzione!

Nei casi in cui si abbia necessità di selezionare immediatamente più messaggi, o si sia assolutamente certi che una determinata cartella contiene solo messaggi appartenenti a un unico gruppo (spam o non spam), è possibile adottare un approccio di training più complesso per mezzo della Procedura guidata di training (cfr. 13.2.1 a pag. 179).

13.2.4. Training nei report di Anti-Spam

Esiste inoltre l'opzione di training di Anti-Spam attraverso i report.

Per visualizzare i report del componente:

1. Selezionare Anti-Spam nella sezione **Protezione** della finestra principale del programma.
2. Fare clic con il pulsante sinistro del mouse su casella **Statistiche** (cfr. Figura 55).

In base ai report del componente è possibile trarre conclusioni sull'accuratezza della configurazione e, se necessario, apportare determinate correzioni ad Anti-Spam.

Per classificare un determinato messaggio come spam o non spam:

1. Selezionare il messaggio dell'elenco dei report nella scheda **Eventi** e usare il pulsante **Azioni**.
2. Selezionare una delle quattro opzioni seguenti:
   - **Segna come spam**
   - **Segna come non spam**
   - **Aggiungi alla lista bianca**
   - **Aggiungi alla lista nera**

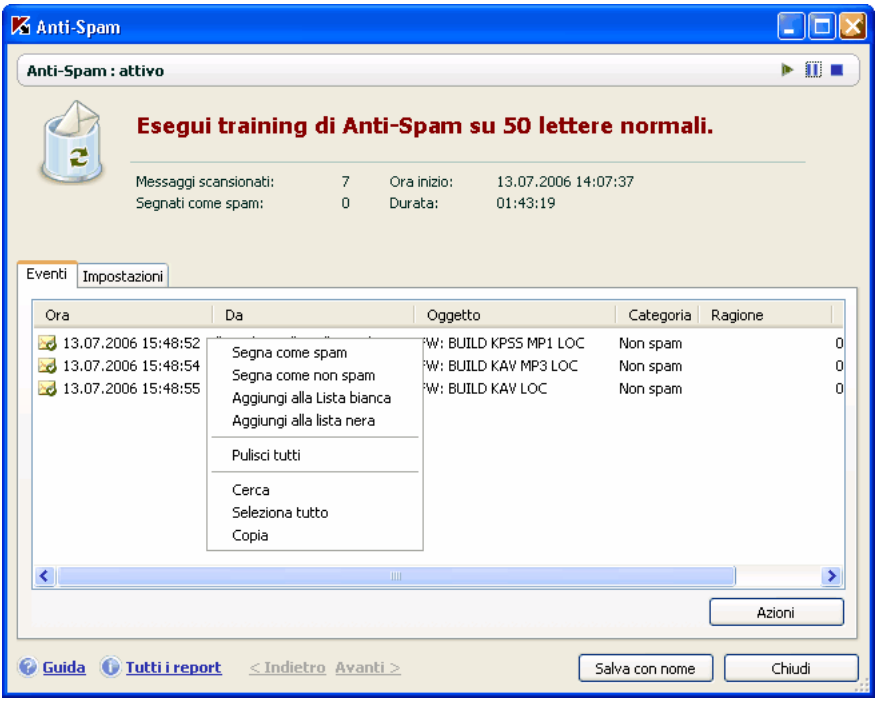


Figura 55. Addestramento di Anti-Spam dai report

Anti-Spam esegue un ulteriore training sulla base di questo messaggio.

13.3. Configurazione di Anti-Spam

La configurazione di precisione di Anti-Spam è essenziale ai fini di un'efficace intercettazione dello spam. Tutte le impostazioni per il funzionamento del componente si trovano nella finestra delle impostazioni di Kaspersky Internet Security e consentono di:

- Determinare i dettagli del funzionamento di Anti-Spam (cfr. 13.3.1 a pag. 183)
- Scegliere quali tecnologie di filtraggio antispam utilizzare (cfr. 13.3.2 a pag. 183)
- Regolare l'accuratezza di riconoscimento dello spam e del probabile spam (cfr. 13.3.3 a pag. 185)

- Creare liste bianche e liste nere di mittenti e frasi ricorrenti (cfr. 13.3.4 a pag. 186)
- Configurare ulteriori funzioni di filtraggio antispam (cfr. 13.3.5 a pag. 191).
- Ridurre al minimo la quantità di spam nella casella di posta in entrata grazie alla visualizzazione in anteprima con Mail Dispatcher (cfr. 13.3.7 a pag. 193)

La presente sezione prende in esame queste impostazioni.

13.3.1. Configurazione delle impostazioni di scansione

È possibile configurare le seguenti impostazioni di scansione:

- Inclusione del traffico tramite protocolli POP3 IMAP nella scansione. Kaspersky Internet Security esamina per impostazione predefinita i messaggi trasferiti mediante questi protocolli con l'eccezione dei messaggi codificati con SSL.
- Attivazione dei plug-in per Outlook, Outlook Express e The Bat!

Attenzione!

Questa versione di Kaspersky Internet Security non offre plug-in Anti-Spam per le versioni a 64 bit di Microsoft Office Outlook, Microsoft Outlook Express e The Bat!

- Visualizzazione dei messaggi mediante POP3 con Mail Dispatcher (cfr. 13.3.7 a pag. 193) prima di scaricarla dal server di posta nella casella della posta in entrata dell'utente.

Per configurare le impostazioni sopra elencate:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni di Kaspersky Internet Security.
2. Selezionare le caselle nella sezione **Attiva il plug-in di Microsoft Office Outlook / The Bat!** (cfr. Figura 56).
3. Se necessario modificare le impostazioni di rete.

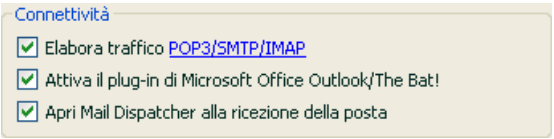


Figura 56. Configurazione delle impostazioni di scansione

13.3.2. Selezione delle tecnologie di filtraggio antispam

I messaggi vengono sottoposti alla scansione antispam mediante tecnologie di filtraggio all'avanguardia:

- **iBayes**, basata sul teorema di Bayes, analizza il testo dei messaggi per individuare frasi ricorrenti nello spam. L'analisi si basa sui dati statistici ottenuti mediante il training di Anti-Spam (cfr. 13.2 a pag. 178).
- **GSG**, analizza gli elementi grafici nei messaggi per mezzo di speciali firme grafiche per individuare lo spam in formati non di testo.
- **PDB**, analizza le intestazioni dei messaggi e le classifica come spam sulla base di una serie di regole eurisitche.

Il programma utilizza le tecnologie di filtraggio Per impostazione predefinita, sottoponendo i messaggi a una scansione antispam più completa possibile.

Per disabilitare una o più tecnologie di filtraggio:

1. Aprire la finestra delle impostazioni di Anti-Spam dal link Impostazioni nella finestra principale.
2. Fare clic su **Personalizza** nella sezione **Sensibilità**, e nella finestra che si apre selezionare la scheda **Riconoscimento spam** (cfr. Figura 57).

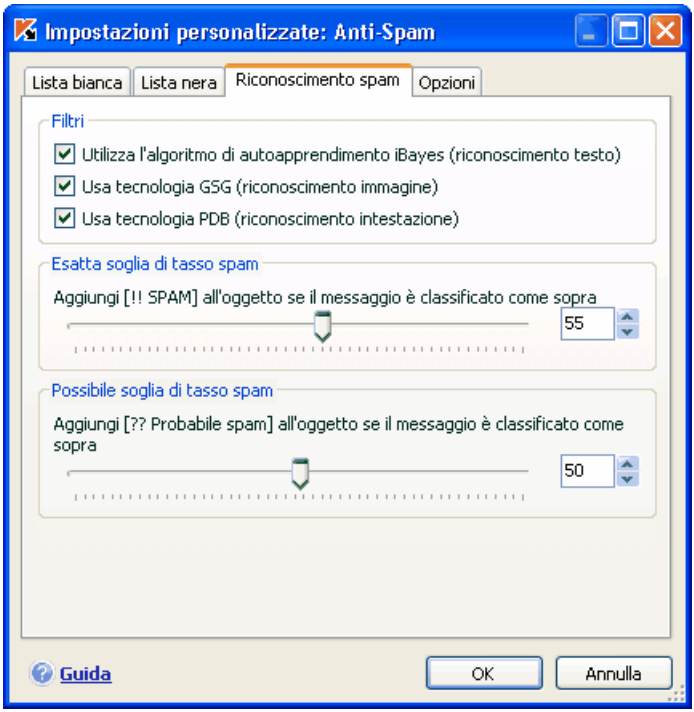


Figura 57. Configurazione del riconoscimento dello spam

3. Deselezionare le caselle a fianco delle tecnologie di filtraggio che non si desidera utilizzare ai fini del riconoscimento.

13.3.3. Definizione dei fattori di spam e probabile spam

Gli esperti Kaspersky Lab hanno configurato Anti-Spam in maniera ottimale per riconoscere lo spam e il probabile spam.

Il riconoscimento dello spam si basa su tecnologie di filtraggio all'avanguardia (cfr. 13.3.2 a pag. 183) che addestrano Anti-Spam all'identificazione di spam, probabile spam e non spam con un elevato grado di precisione utilizzando un certo numero di messaggi presenti nella casella della posta in entrata.

L'addestramento di Anti-Spam può essere eseguito per mezzo della Procedura guidata di training oppure sulla base dei messaggi elaborati dai client di posta. Così facendo, ad ogni singolo elemento dei messaggi accettati o dello spam viene assegnato un fattore. Quando un messaggio entra nella casella dei

messaggi in entrata, Anti-Spam lo esamina con iBayes cercando eventuali elementi di spam e di messaggi accettati. I fattori di ciascun elemento vengono sommati ottenendo un *fattore di spam* e un *fattore di non spam.*

Il fattore di probabile spam definisce la probabilità che il messaggio sia classificato come tale. Se si sta utilizzando il livello **Raccomandato**, ogni messaggio è caratterizzato da una probabilità di essere considerato *probabile spam* compresa tra il 50% e il 59%. La posta che, in seguito alla scansione, ottiene una probabilità inferiore al 50% viene considerata non spam.

Il fattore di spam determina la probabilità che Anti-Spam classifichi un messaggio come spam. Qualsiasi messaggio con probabilità superiori a quella sopra indicata saranno classificate come spam. Per impostazione predefinita, il fattore di spam al livello **Raccomandato** è del 59%. Questo significa che qualsiasi messaggio con una probabilità superiore al 59% sarà considerato *spam*.

Esistono in tutto cinque livelli di sensibilità (cfr. 13.1 a pag. 177), tre dei quali (**Elevato, Raccomandato** e **Basso**) si basano su diversi valori del fattore di spam e probabile spam.

È possibile modificare autonomamente l'algoritmo Anti-Spam procedendo come segue:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni di Kaspersky Internet Security.
2. Nella sezione **Sensibilità** sul lato destro della finestra fare clic su **Personalizza**.
3. Nella finestra che si apre, regolare i fattori di spam e probabile spam nelle sezioni corrispondenti della scheda **Riconoscimento spam** (cfr. Figura 57).

13.3.4. Creazione manuale di liste bianche e liste nere

L'utente può creare manualmente liste bianche e liste nere utilizzando Anti-Spam con i propri messaggi di posta elettronica. Queste liste contengono informazioni sugli indirizzi che l'utente considera sicuri o spam, e su varie parole chiave e frasi che identificano i messaggi come spam o non spam.

L'applicazione principale delle liste di espressioni chiave, in particolare la lista bianca, è la possibilità di coordinare con i destinatari attendibili, per esempio i colleghi, firme contenenti una determinata frase. Può trattarsi di una frase qualsiasi. Per esempio è possibile utilizzare come firma una firma PGP. È possibile utilizzare caratteri jolly nelle firme e negli indirizzi: ***** e **?**. L'asterisco * rappresenta una sequenza qualsiasi di caratteri di lunghezza non definita. Il punto interrogativo rappresenta un carattere singolo qualsiasi.
Se la firma contiene asterischi e punti interrogativi, per evitare errori durante l'elaborazione da parte di Anti-Spam essi devono essere preceduti da una barra inversa. Così al posto di un solo carattere ne vengono utilizzati due: ***** e **?**.

13.3.4.1. Liste bianche di indirizzi e frasi

Una lista bianca contiene frasi ricorrenti individuate nei messaggi catalogati come *non spam*, e gli indirizzi dei mittenti dai quali si è certi che non potrebbe mai provenire un messaggio di spam. La lista bianca viene compilata manualmente, mentre l'elenco degli indirizzi dei mittenti viene creato automaticamente durante il training del componente Anti-Spam. L'elenco può essere modificato dall'utente.

Per configurare la lista bianca:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni di Kaspersky Internet Security.
2. Fare clic sul pulsante **Personalizza** nella parte destra della finestra.
3. Aprire la scheda **Lista bianca** (cfr. Figura 58).

La tabella è suddivisa in due sezioni: quella superiore, contenente gli indirizzi dei mittenti di messaggi accettabili, e quella inferiore, contenente le frasi ricorrenti nei loro messaggi.

Per abilitare le liste bianche di frasi e indirizzi durante il filtraggio dello spam, selezionare le caselle corrispondenti nelle sezioni **Mittenti autorizzati** e **Frasi autorizzate**.

È possibile modificare le liste servendosi degli appositi pulsanti in ciascuna sezione.

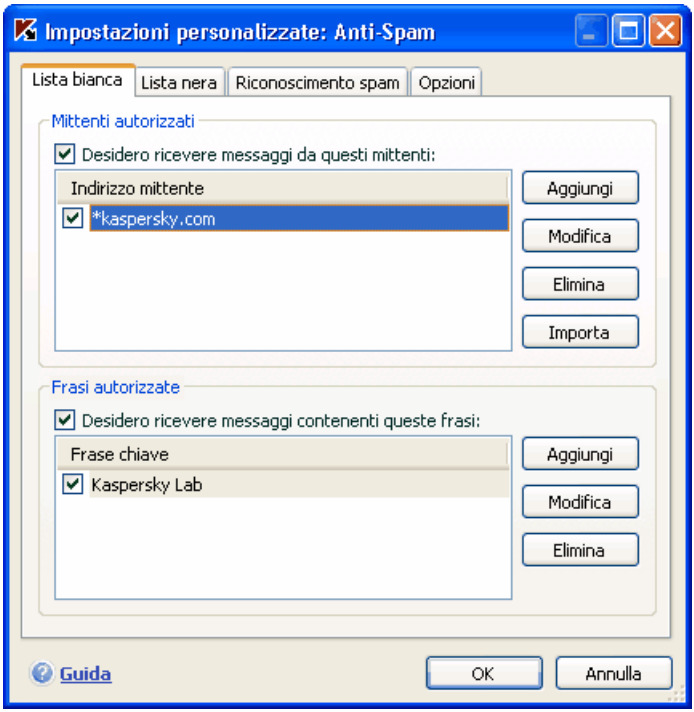


Figura 58. Configurazione delle liste bianche di indirizzi e frasi

È possibile assegnare alla lista degli indirizzi sia indirizzi completi sia maschere di indirizzi. Durante l'inserimento di un indirizzo, il registro non viene tenuto in considerazione. Osserviamo alcuni esempi di maschere di indirizzi:

- *ivanov@test.ru* – i messaggi provenienti da questo indirizzo saranno sempre classificati come accettabili.
- **@test.ru* – i messaggi provenienti da qualsiasi indirizzo del dominio *test.ru* sono considerati accettabili, per esempio: *petrov@test.ru*, *sidorov@test.ru*;
- *ivanov@** – un mittente con questo nome, indipendentemente dal dominio di posta, è considerato sempre accettabile, per esempio: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – i messaggi provenienti da qualsiasi mittente di un dominio che inizia per *test* non vengono considerati spam, per esempio: *ivanov@test.ru*, *petrov@test.com*;

- *ivan.*@test.???* – i messaggi provenienti da un mittente il cui nome inizia con ivan. e il cui dominio inizia con *test* e finisce con qualsiasi sequenza di tre caratteri viene sempre considerato accettabile, per esempio: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

È possibile utilizzare maschere anche per le frasi. Durante l'inserimento di una frase, il registro non viene tenuto in considerazione. Ecco alcuni esempi:

- *Caro Ivan!* -- un messaggio contenente solo questo testo è considerato accettabile. Si sconsiglia di utilizzare questa frase per una lista bianca.
- *Caro Ivan!** -- un messaggio che inizia con *Caro Ivan!* È considerato accettabile.
- *Caro *! ** – i messaggi che iniziano con *Caro* e un punto esclamativo in qualsiasi punto del messaggio non sono considerati spam.
- ** Ivan? ** – il messaggio si rivolge a un utente di nome *Ivan*, il cui nome è seguito da qualsiasi carattere, e non è considerato spam.
- ** Ivan\? ** – i messaggi contenenti il gruppo *Ivan?* sono considerati accettabili.

Se si desidera annullare la classificazione di un determinato indirizzo o frase come attributi accettabili, non è necessario eliminarli dalla lista, ma è sufficiente deselezionarne i nomi.

L'utente può scegliere di importare file di formato CSV nella lista bianca degli indirizzi.

13.3.4.2. Liste nere di indirizzi e frasi

La lista nera dei mittenti contiene frasi ricorrenti individuate nei messaggi classificati come *spam* nonché gli indirizzi di provenienza. L'elenco viene compilato manualmente.

Per compilare la lista nera:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni di Kaspersky Internet Security.
2. Fare clic sul pulsante **Personalizza** nella parte destra della finestra.
3. Aprire la scheda **Lista nera** (cfr. Figura 59).

La tabella è suddivisa in due sezioni: quella superiore, contenente gli indirizzi dei mittenti di messaggi spam, e quella inferiore, contenente le frasi ricorrenti nei loro messaggi.

Per abilitare le liste nere di frasi e indirizzi durante il filtraggio dello spam, selezionare le caselle corrispondenti nelle sezioni **Mittenti bloccati** e **Frasi bloccate**.

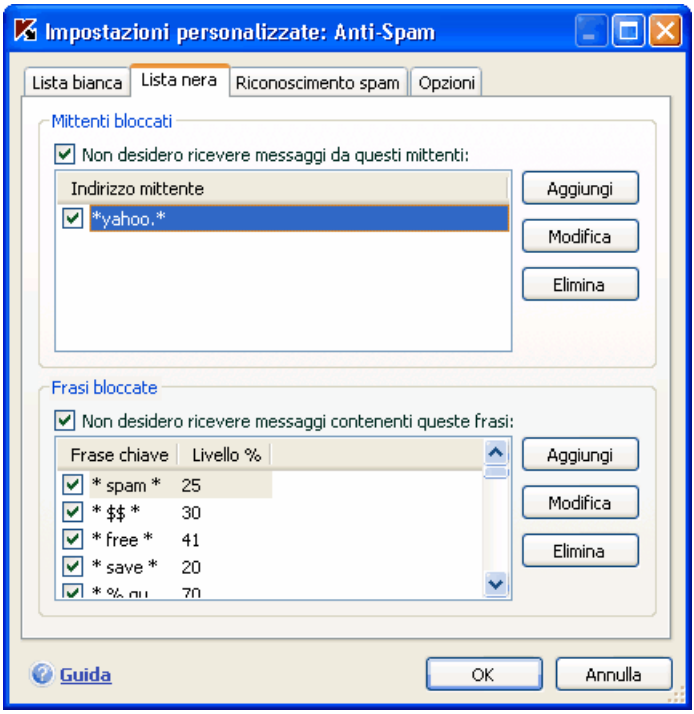


Figura 59. Configurazione delle liste nere di indirizzi e frasi

È possibile modificare le liste servendosi degli appositi pulsanti in ciascuna sezione.

È possibile assegnare alla lista degli indirizzi sia indirizzi completi sia maschere di indirizzi. Durante l'inserimento di un indirizzo, il registro non viene tenuto in considerazione. Osserviamo alcuni esempi di maschere di indirizzi:

- *ivanov@test.ru* – i messaggi provenienti da questo indirizzo saranno sempre classificati come spam.
- **@test.ru* – i messaggi provenienti da qualsiasi indirizzo del dominio *test.ru* sono considerati spam, per esempio: *petrov@test.ru*, *sidorov@test.ru*;

- *ivanov@** – un mittente con questo nome, indipendentemente dal dominio di posta, è considerato sempre spam, per esempio: *ivanov@test.ru*, *ivanov@mail.ru*;
- **@test** – i messaggi provenienti da qualsiasi mittente di un dominio che inizia per *test* vengono considerati spam, per esempio: *ivanov@test.ru*, *petrov@test.com*;
- *ivan.*@test.???* – i messaggi provenienti da un mittente il cui nome inizia con ivan. e il cui dominio inizia con *test* e finisce con qualsiasi sequenza di tre caratteri viene sempre considerato spam, per esempio: *ivan.ivanov@test.com*, *ivan.petrov@test.org*.

È possibile utilizzare maschere anche per le frasi. Durante l'inserimento di una frase, il registro non viene tenuto in considerazione. Ecco alcuni esempi:

- *Caro Ivan!* -- un messaggio contenente solo questo testo è considerato spam. Si sconsiglia di utilizzare questa frase per una lista.
- *Caro Ivan!** -- un messaggio che inizia con *Caro Ivan!* È considerato spam.
- *Caro *! ** – i messaggi che iniziano con *Caro* e un punto esclamativo in qualsiasi punto del messaggio sono considerati spam.
- ** Ivan? ** – il messaggio si rivolge a un utente di nome *Ivan*, il cui nome è seguito da qualsiasi carattere, ed è considerato spam.
- ** Ivan\? ** – i messaggi contenenti il gruppo *Ivan?* sono considerati spam.

Se non si desidera classificare un determinato indirizzo o frase come spam, non è necessario eliminarli dall'elenco, ma è sufficiente deselezionarne i nomi.

13.3.5. Ulteriori funzioni di filtraggio antispam

Oltre alle principali funzioni utilizzate per il filtraggio dello spam (creazione di liste bianche e liste nere, analisi antiphishing, tecnologie di filtraggio), è possibile avvalersi di funzioni avanzate.

Per configurare le funzioni avanzate di filtraggio antispam:

1. Selezionare **Anti-Spam** nella finestra delle impostazioni di Kaspersky Internet Security.
2. Fare clic sul pulsante **Personalizza** nella parte destra della finestra.
3. Aprire la scheda **Opzioni** (cfr. Figura 60).

Essa contiene una serie di indicatori che classificano un messaggio come probabile spam.

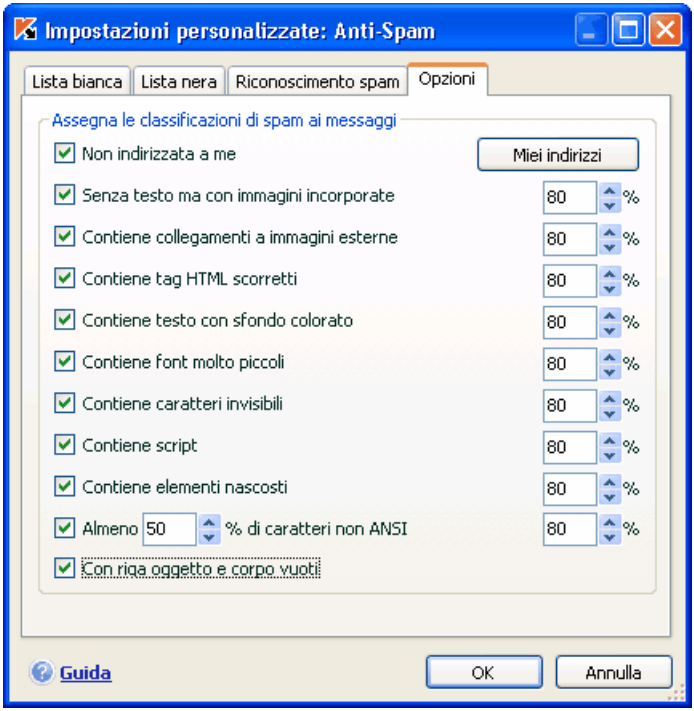


Figura 60. Impostazioni avanzate di riconoscimento dello spam

Per utilizzare eventuali indicatori supplementari di filtraggio, selezionare la casella corrispondente. Ciascuno degli indicatori richiede inoltre l'impostazione di un fattore di spam (in punti percentuali) che definisce la probabilità che un messaggio sia classificato come spam. Il valore predefinito del fattore di spam è 80%. Il messaggio sarà classificato come spam se la somma delle probabilità di tutti i fattori supplementari supera il 100%.

Se si abilita il filtraggio della posta "Non indirizzata a me", è necessario specificare l'elenco dei propri indirizzi nella finestra che si apre facendo clic su **Miei indirizzi**.

13.3.6. Creazione di un elenco di indirizzi attendibili

Se si abilita il filtraggio antispam della posta “Non indirizzata a me," è necessario specificare i propri indirizzi di posta attendibili.

L’indirizzo del destinatario viene scansionato durante l’analisi del messaggio. Se l’indirizzo non corrisponde a nessuno di quelli presenti nella lista, il messaggio viene classificato come spam.

È possibile creare e modificare una lista di indirizzi nella finestra **Miei indirizzi di posta elettronica** servendosi dei pulsanti **Aggiungi**, **Modifica** ed **Elimina**.

13.3.7. Mail Dispatcher

Attenzione!

Mail Dispatcher è disponibile solo se si riceve posta per mezzo del protocollo POP3.

Mail Dispatcher è progettato per visualizzare l’elenco dei messaggi presenti sul server senza scaricarli sul computer. In tal modo è possibile rifiutare dei messaggi, risparmiando tempo e denaro e riducendo la probabilità di scaricare spam e virus sul computer.

Mail Dispatcher si apre se è stata selezionata la casella **Apri Mail Dispatcher alla ricezione della posta** nelle impostazioni di Anti-Spam.

Per eliminare messaggi dal server senza scaricarli sul computer:

Selezionare le caselle sulla sinistra dei messaggi da eliminare e fare clic sul pulsante **Elimina**. I messaggi selezionati saranno eliminati dal server. Il resto della posta sarà scaricato sul computer dopo la chiusura della finestra di Mail Dispatcher.

Talvolta può essere difficile decidere se accettare un determinato messaggio solo sulla base del mittente e dell’oggetto. In certi casi Mail Dispatcher offre ulteriori informazioni scaricando anche le intestazioni dei messaggi.

Per visualizzare le intestazioni dei messaggi:

Selezionare il messaggio dall’elenco della posta in arrivo. Le intestazioni vengono visualizzate nella parte inferiore del modulo.

Esse non presentano dimensioni considerevoli, limitandosi il più delle volte a poche decine di byte, e non possono contenere codici nocivi.

Ecco un esempio in cui la visualizzazione delle intestazioni può essere utile: gli spammer hanno installato un programma nocivo sul computer di un collega che

invia spam con il proprio nome utilizzando la rubrica del proprio client di posta. La probabilità di trovarsi nella rubrica del collega è estremamente elevata, rendendo quindi il computer bersaglio frequente di spam proveniente da lui. È impossibile stabilire a priori, sulla base del solo indirizzo del mittente, se il messaggio sia stato inviato dal collega o da uno spammer. È quindi utile consultare le intestazioni del messaggio per controllare attentamente chi ha inviato il messaggio, quando e quali sono le sue dimensioni, oltre a ricostruire il percorso compiuto dal messaggio tra il mittente e il server di posta del destinatario. Tutte queste informazioni dovrebbero essere presenti nell'intestazione del messaggio. In base ad esse è possibile decidere se sia veramente necessario scaricare quel messaggio dal server o se in effetti sia consigliabile eliminarlo.

Nota:
È possibile ordinare i messaggi in base a qualsiasi colonna dell'elenco. Per ordinarli fare clic sull'intestazione della colonna. Le righe vengono quindi riorganizzate in ordine crescente. Per modificare l'ordine di visualizzazione, fare di nuovo clic sull'intestazione della colonna.

13.3.8. Azioni da eseguire sui messaggi di spam

Se dopo la scansione si scopre che un messaggio è spam o probabile spam, le fasi successive della procedura di Anti-Spam dipendono dallo status dell'oggetto e dall'azione selezionata. Per impostazione predefinita, i messaggi riconosciuti come *spam* o *probabile spam* vengono modificati: alla riga dell'oggetto vengono aggiunte le annotazioni **[!! SPAM]** o **[?? Probabile spam]**.

È possibile selezionare ulteriori azioni da eseguire in caso di spam o probabile spam. In MS Outlook, Outlook Express e The Bat! esistono plug-in specifici per questo scopo. Per altri client di posta è possibile configurare delle regole di filtraggio.

13.3.9. Configurazione dell'elaborazione di spam in MS Outlook

Osservare che non è disponibile un plug-in antispam per MS Outlook se il programma è installato in Windows 9x.

I messaggi classificati da Anti-Spam come *spam* o *probabile spam* vengono contrassegnati per impostazione predefinita da speciali annotazioni **[!! SPAM]** o **[?? Probabile Spam]** nella riga dell'**Oggetto**.

In Outlook è possibile trovare ulteriori azioni per lo spam e il probabile spam nell'apposita scheda **Anti-Spam** nel menu **Guida→ Impostazioni** (cfr. Figura 61).

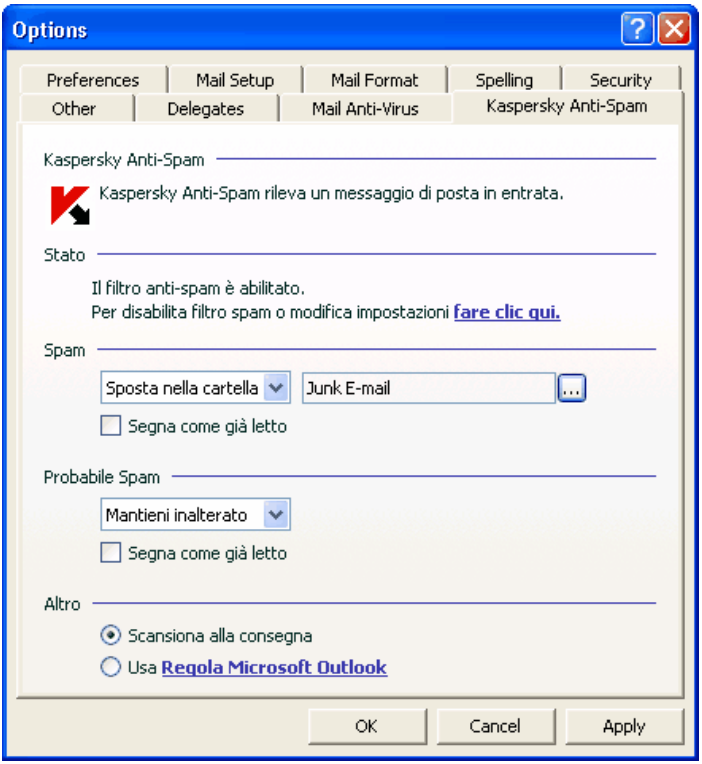


Figura 61. Configurazione dell'elaborazione di spam in Microsoft Office Outlook

Si apre automaticamente alla prima apertura del client di posta dopo l'installazione del programma e chiede se si desidera configurare l'elaborazione dello spam.

È possibile assegnare le seguenti regole sia ai messaggi di spam sia al probabile spam:

Sposta nella cartella – lo spam viene trasferito nella cartella specificata della casella di posta in arrivo.

Copia nella cartella – viene creata una copia del messaggio e trasferita nella cartella specificata. Il messaggio originale resta nella casella della posta in arrivo.

Elimina – elimina lo spam dalla casella della posta in arrivo dell'utente.

Ignora – lascia il messaggio nella casella della posta in arrivo.

A tal fine, selezionare il valore appropriato dall'elenco a discesa della sezione **Spam** o **Probabile spam**.

È possibile inoltre configurare Microsoft Office Outlook e Anti-Spam in modo da lavorare congiuntamente:

- **Scansiona alla consegna**. Tutti i messaggi che entrano nella casella della posta in arrivo dell'utente vengono elaborati secondo le regole di Outlook. Al termine dell'elaborazione, il plug-in di Anti-Spam elabora i messaggi rimanenti che non rientrano in alcuna regola. In altre parole, i messaggi vengono elaborati secondo la priorità delle regole. Talvolta la sequenza delle priorità può essere ignorata se, per esempio, viene consegnato nella casella della posta in arrivo un gran numero di messaggi contemporaneamente. In tal caso possono verificarsi situazioni in cui le informazioni relative a un messaggio elaborato in base a una regola di Outlook vengono registrate nel report di Anti-Spam come *spam*. Per evitare questo inconveniente si raccomanda di configurare il plug-in di Anti-Spam come una regola di Outlook.
- **Usa regola di Microsoft Outlook**. Questa opzione consente di elaborare i messaggi in arrivo in base alla gerarchia delle regole di Outlook create. Una delle regole deve essere relativa all'elaborazione dei messaggi da parte di Anti-Spam. Si tratta della configurazione ottimale che non provoca conflitti tra Outlook e il plug-in diAnti-Spam. L'unico svantaggio di questa configurazione consiste nel fatto che occorre creare ed eliminare le regole di elaborazione dello spam manualmente attraverso Outlook.

A causa di un errore di Outlook XP non è possibile utilizzare il plug-in di Anti-Spam come una regola di Outlook in Microsoft Office XP se si esegue 9x/ME/NT4.

Per creare una regola di elaborazione dello spam:

1. Aprire Microsoft Office Outlook e selezionare **Strumenti** → **Creazione guidata Regole** nel menu principale. Il comando di apertura della creazione guidata dipende dalla versione di Microsoft Office Outlook. Questo manuale d'uso descrive come creare una regola utilizzando Microsoft Office Outlook 2003.
2. Nella finestra **Creazione guidata regole**, selezionare la scheda **Regole posta elettronica** e fare clic su **Nuova**. The New Rule Wizard will then open. Essa guida l'utente attraverso le finestre e i passaggi che seguono:

Passaggio 1

È possibile scegliere di creare una regola *ex novo* o sulla base di un modello esistente. Selezionare **Crea nuova regola** e **Applica la regola dopo l'arrivo del messaggio**. Fare clic sul pulsante **Avanti**.

Passaggio 2

Nella finestra Condizioni delle regole, fare clic su **Avanti** senza selezionare alcuna casella. Confermare nella finestra di dialogo che si desidera applicare questa regola a tutti i messaggi ricevuti.

Passaggio 3

Nella finestra di selezione delle azioni da eseguire sui messaggi, selezionare la casella ☑ **Applica azione avanzata advanced action** dall'elenco delle azioni. Nella parte inferiore della finestra fare clic su azione avanzata. Nella finestra che si apre, selezionare **Kaspersky Anti-Spam** dal menu a discesa e fare clic su **OK**.

Passaggio 4

Nella finestra di selezione delle eccezioni alla regola, fare clic su **Avanti** senza selezionare alcuna casella.

Passaggio 5

Nella finestra finale della creazione guidata della regola è possibile modificarne il nome (il nome predefinito è **Kaspersky Anti-Spam**). Accertarsi che la casella ☑ **Applica regola** sia selezionata e fare clic su **Fine**.

3. Per impostazione predefinita alla nuova regola viene assegnata la prima posizione nell'elenco delle regole nella finestra **Regole messaggi**. Se lo si desidera, è possibile spostare questa regola in fondo all'elenco in modo da applicarla ai messaggi per ultima.

Tutti i messaggi in arrivo vengono elaborati in base a queste regole. L'ordine in cui il programma applica le regole dipende dalla priorità assegnata a ciascuna. Esse vengono applicate a partire dalla prima posizione dell'elenco. Ogni regola successiva occupa la posizione inferiore rispetto a quella che la precede. È possibile modificare la priorità di applicazione delle regole ai messaggi.

Se non si desidera continuare ad applicare ai messaggi una regola di Anti-Spam dopo averla usata una volta, occorre selezionare la casella ☑ **Interrompi l'elaborazione di ulteriori regole** tra le impostazioni delle regole (cfr. il passaggio 3 della creazione di una regola).

Se si possiede una certa esperienza nella creazione di regole di elaborazione dei messaggi in Outlook, si possono creare regole personalizzate per Anti-Spam sulla base della configurazione suggerita.

13.3.10. Configurazione dell'elaborazione dello spam in Outlook Express

I messaggi classificati da Anti-Spam come *spam* o *probabile spam* vengono contrassegnati per impostazione predefinita da speciali annotazioni **[!! SPAM]** o **[?? Probabile Spam]** nella riga dell'**Oggetto**.

Ulteriori azioni da eseguire sui messaggi di spam e probabile spam in Outlook Express sono disponibili in una speciale finestra che si apre (cfr. Figura 62) facendo clic sul pulsante **Impostazioni** accanto ai pulsanti di Anti-Spam sul pannello delle attività: **Spam** e **Accetta**.

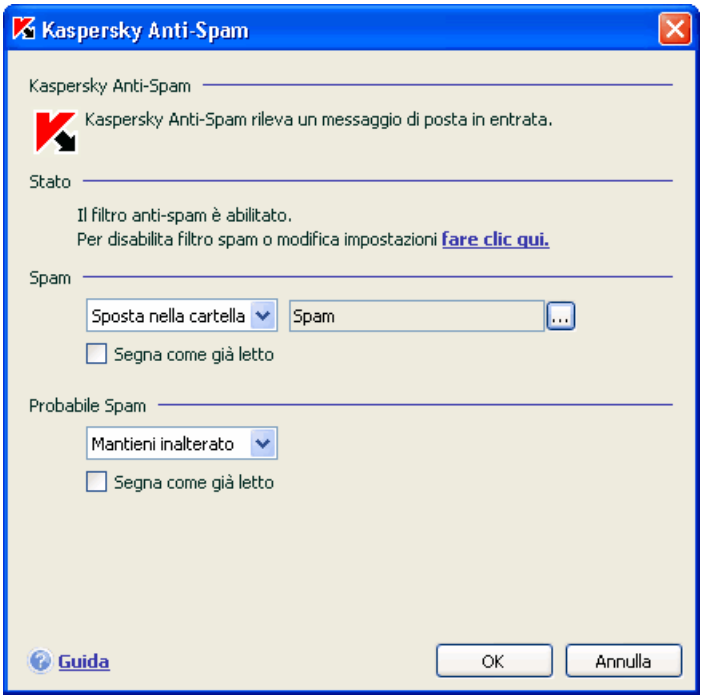


Figura 62. Configurazione dell'elaborazione dello spam in MS Outlook Express

Si apre automaticamente alla prima apertura del client di posta dopo l'installazione del programma e chiede se si desidera configurare l'elaborazione dello spam.

È possibile assegnare le seguenti regole sia ai messaggi di spam sia al probabile spam:

Sposta nella cartella – lo spam viene trasferito nella cartella specificata della casella di posta in arrivo.

Copia nella cartella – viene creata una copia del messaggio e trasferita nella cartella specificata. Il messaggio originale resta nella casella della posta in arrivo.

Elimina – elimina lo spam dalla casella della posta in arrivo dell'utente.

Ignora – lascia il messaggio nella casella della posta in arrivo.

A tal fine, selezionare il valore appropriato dall'elenco a discesa della sezione **Spam** o **Probabile spam**.

13.3.11. Configurazione dell'elaborazione dello spam in The Bat!

Le azioni per lo spam e il probabile spam in The Bat! sono definite mediante gli strumenti propri del client.

Per impostare le regole di protezione dello spam in The Bat!:

1. Selezionare **Impostazioni** dal menu **Proprietà** del programma di posta.
2. Selezionare **Protezione spam** dalla struttura ad albero delle impostazioni (cfr. Figura 63).

Le impostazioni di protezione antispam visualizzate valgono per tutti i moduli antispam installati nel computer che supportano The Bat!

È necessario impostare il livello di valutazione e specificare come reagire ai messaggio con un determinato punteggio (nel caso di Anti-Spam, la probabilità che il messaggio sia spam):

- Eliminare i messaggi con un puntaggio più elevato di un determinato valore.
- Trasferire i messaggi con un determinato punteggio in una cartella specifica per lo spam.
- Trasferire nella cartella dello spam i messaggi contrassegnati da apposite intestazioni.
- Lasciare lo spam nella casella della posta in arrivo.

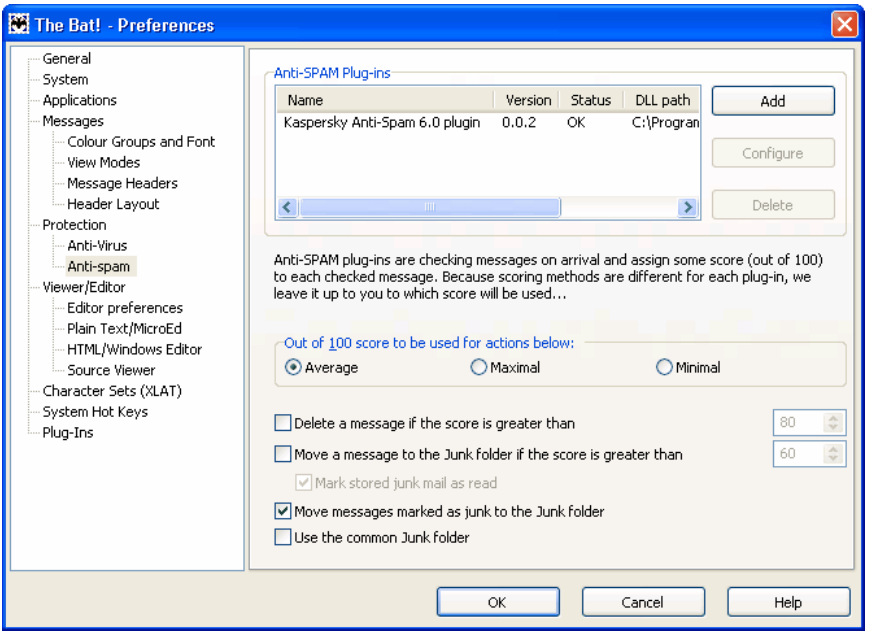


Figura 63. Configurazione del riconoscimento e dell'elaborazione dello spam in The Bat!

Attenzione!

Dopo aver elaborato un messaggio, Kaspersky Internet Security gli assegna uno status di spam o probabile spam in base a un fattore (cfr. 13.3.3 a pag. 185) con un valore regolabile dall'utente stesso. The Bat! possiede il proprio metodo di valutazione dello spam, basato anch'esso su un fattore di spam. Per garantire che non vi siano discrepanze tra il fattore di spam di Kaspersky Internet Security e quello di The Bat!, tutti i messaggi esaminati da Anti-Spam ottengono un punteggio conforme allo status del messaggio: *Non spam* – 0%; *probabile spam – 50 %*, spam – *100 %*.

In tal modo, il punteggio dello spam in The Bat! corrisponde al fattore di spam assegnato in Anti-Spam ma non al fattore dello status corrispondente.

Per ulteriori informazioni sulle regole di valutazione e di elaborazione dello spam, consultare la documentazione relativa a The Bat!

CAPITOLO 14. LA SCANSIONE ANTIVIRUS DEL COMPUTER

Un aspetto importante nella protezione di un computer dai virus è rappresentato dalla scansione anti-virus di aree definite dall'utente. Kaspersky Internet Security 6.0 può operare tale scansione su singoli oggetti (file, cartelle, unità disco, dispositivi plug-and-play), o sull'intero computer. La scansione anti-virus impedisce la diffusione di quei codici dannosi che non sono stati individuati dalle componenti di protezione.

Kaspersky Internet Security 6.0 comprende tre modalità di scansione predefinite:

Aree critiche

La scansione antivirus viene effettuata su tutte le aree critiche del computer, ovvero: la memoria del sistema, i programmi caricati all'avvio, i settori di boot del disco fisso e le directory di sistema *Windows* e *system32*. Tale funzione ha lo scopo di individuare rapidamente i virus presenti nel sistema senza operare la scansione completa dello stesso.

Risorse del computer

Esegue la scansione del computer, con una ispezione completa di tutte le unità disco, della memoria e dei file.

Oggetti all'avvio

Esegue la scansione anti-virus dei programmi caricati all'avvio del sistema operativo.

Le impostazioni raccomandate per queste modalità sono quelle predefinite. È possibile visualizzare tali impostazioni (cfr. 14.4.4 a pag. 210) o stabilire un programma (cfr. 6.5 on pg. 85) per l'esecuzione delle scansioni secondo dette modalità.

È inoltre possibile creare modalità di scansione personalizzate (vedere 14.4.3 a pagina 209) e pianificarne l'esecuzione. Ad esempio, è possibile pianificare la scansione anti-virus dell'archivio della posta elettronica una volta la settimana, o la scansione della sola cartella **Documenti**.

È comunque possibile eseguire la scansione anti-virus di singoli oggetti (come ad esempio il disco fisso contenente programmi e giochi, l'archivio di posta elettronica prelevato al lavoro, un archivio allegato ad una e-mail, ecc.) senza dover impostare una modalità di scansione specifica. È sufficiente selezionare l'oggetto sul quale eseguire la scansione dall'interfaccia di Kaspersky Internet

Security 6.0, o tramite i normali strumenti del sistema operativo Windows (ad esempio tramite **Explorer**, o direttamente dal **Desktop**, ecc.).

È possibile vedere la lista completa delle modalità di scansione del computer in **Scansione**

14.1. Gestione delle attività di scansione antivirus

La scansione antivirus può essere avviata manualmente, oppure in maniera automatica, a scadenze predefinite (cfr. 6.5 on pg. 85).

Per avviare manualmente un'attività di scansione:

Selezionare il nome dell'attività nella sezione **Scan** della finestra principale del programma, e fare clic sul pulsante nella barra di stato.

Per mettere in pausa un'attività:

Fare clic sul pulsante nella barra di stato. Lo status della scansione cambierà in *sospeso*. In tal modo la scansione risulterà sospesa, e rimarrà tale fino a che non sarà riavviata manualmente, o fino all'occorrenza della successiva scansione programmata.

Per terminare una scansione:

Fare clic sul pulsante nella barra di stato. Lo status della scansione cambierà in *terminato*. Ciò determinerà l'arresto della scansione, che potrà essere riavviata manualmente, o che sarà riavviata automaticamente alla successiva scansione programmata. Al successivo avvio di una scansione, il programma chiederà all'utente se desidera riprendere la scansione dal punto in cui era stata precedentemente interrotta, o ricominciarla dal principio.

14.2. Creazione di un elenco di oggetti su cui eseguire una scansione

Per visualizzare un elenco di oggetti su cui operare una scansione secondo una determinata modalità, selezionare il tipo di scansione (ad esempio, **Computer**) nella sezione **Scansione** della finestra del programma principale. L'elenco degli oggetti sarà visualizzato sul lato destro della finestra, sotto la barra di stato (vedere Figura 64).

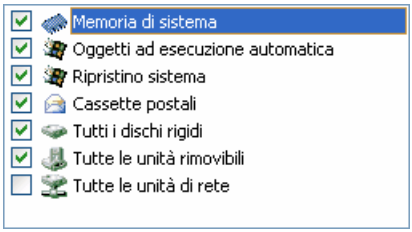


Figura 64. Elenco di oggetti su cui operare la scansione

Quando il programma viene installato, vengono già creati degli elenchi di oggetti su cui operare la scansione. Creando modalità di scansione personalizzate o selezionando un oggetto per la scansione, è possibile impostare un elenco di oggetti.

È possibile ampliare e visualizzare un elenco di oggetti utilizzando i pulsanti sulla destra dell'elenco. Per aggiungere un oggetto all'elenco, cliccare sul pulsante **Aggiungi**; si aprirà una finestra nella quale selezionare l'oggetto su cui eseguire la scansione. Per cancellare un oggetto, selezionarlo nell'elenco (così facendo, il nome dell'oggetto verrà evidenziato in grigio) e cliccare sul pulsante **Elimina**. È possibile disabilitare temporaneamente la scansione su determinati oggetti di un elenco, senza doverli cancellare. Per far ciò è sufficiente deselezionare gli oggetti in questione.

Per avviare una scansione, cliccare sul pulsante **Scansione**, e selezionare **Scansione** dal menu che appare cliccando sul pulsante **Azione**.

Oltre a questo, è possibile selezionare un oggetto su cui eseguire una scansione anche utilizzando gli strumenti del sistema operativo Windows (ad esempio tramite la finestra di Explorer, o direttamente dal Desktop, ecc.) (vedere Figura 65). Per far ciò, posizionare il cursore sul nome dell'oggetto in questione, aprire il menu contestuale di Windows facendo clic con il pulsante destro del mouse, e selezionare **Scansione anti-virus**.

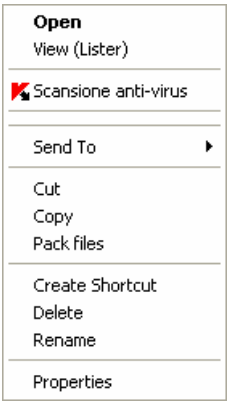


Figura 65. Scansione di oggetti attraverso il menu contestuale di Windows

14.3. Creazione di attività di scansione antivirus

Per eseguire la scansione antivirus di oggetti presenti sul computer, è possibile utilizzare le modalità di scansione predefinite offerte dal programma o crearne di nuove. Queste ultime vengono create a partire da attività di scansione preesistenti.

Per creare una nuova attività di scansione antivirus:

1. Selezionare, nella sezione **Scansione** della finestra del programma proncipale, la modalità di scansione le cui impostazioni si avvicinano maggiormante a quelle desiderate.
2. Aprire il menu contestuale facendo clic con il pulsante destro del mouse, o fare clic sul pulsante **Azioni** a destra dell'elenco degli oggetti, e selezionare **Salva con nome**.
3. Nella finestra che appare, inserire il nome della nuova modalità di scansione e premere **OK**. Nell'elenco delle modalità di scansione, nella sezione **Scansione** della finestra del programma principale, figurerà una nuova modalità col nome appena inserito.

Attenzione!

Un utente può creare un massimo di quattro modalità di scansione..

La nuova attività di scansione eredita tutte le proprieà di quella da cui è stata creata. Per mettere ulteriormente a punto la nuova attività è necessario creare l'elenco di oggetti su cui operare la scansione (cfr. 14.4.2 a pag. 207), impostare

le proprietà (cfr. 14.4.4 a pag. 210) della modalità stessa, e, se necessario, configurare le scadenze (cfr. 6.5 on pg. 85) per l'esecuzione automatica della scansione.

Per cambiare nome a un'attività di scansione:

> Selezionare l'attività da rinominare nella sezione **Scansione** della finestra del programma principale, fare clic col pulsante destro del mouse per aprire il menu contestuale, oppure fare clic sul pulsante **Azioni**, sulla destr dell'elenco degli oggetti, e selezionare **Rinomina**.

Digitare, nella finestra che appare, il nuovo nome, e cliccare su **OK**. Nella sezione **Scansione**, il nome della modalità di scansione risulterà modificato.

Per eliminare un'attività di scansione:

> Selezionare l'attività da eliminare nella sezione **Scansione** della finestra del programma principale, fare clic con il pulsante destro del mouse per aprire il selezionare, oppure fare clic sul pulsante **Azioni**, sulla destra dell'elenco degli oggetti, e selezionare **Elimina**.

Apparirà una finestra nella quale verrà chiesto all'utente di confermare l'operazione di cancellazione. A conferma avvenuta, l'attività di scansione eliminata non sarà più presente nell'elenco delle attività della sezione **Scansione**.

Attenzione!

È possibile rinominare o cancellare soltanto le modalità di scansione create dall'utente.

14.4. Configurazione delle attività di scansione antivirus

Il metodo impiegato per operare la scansione degli oggetti presenti nel computer dipende da un insieme di proprietà assegnate a ciascuna modalità.

Configurare le impostazioni delle modalità di scansione:

> Selezionare il nome dell'attività nella scheda **Scansione** della finestra principale e usare il link Impostazioni per aprire la finestra delle impostazioni.

Per ciascuna modalità di scansione, è possibile utilizzare tale finestra al fine di:

- Selezionare un livello di sicurezza per la modalità di scansione (vedere 14.4.1 a pagina 206)
- Modificare le impostazioni avanzate:

- Impostazioni che definiscono i tipi di file da sottoporre a scansione (vedere 14.4.2 a pagina 207)
- configurare l'avvio dell'attività utilizzando un profilo utente diverso (cfr. 6.4 a pag.. 84)
- configurare le impostazioni di scansione avanzate (cfr. 14.4.5 a pag. 212)

- ripristinare le impostazioni di scansione predefinite (vedere 14.4.3 a pagina 209)
- selezionare l'azione che il programma deve intraprendere non appena venga rilevato un oggetto infetto, o presunto tale (vedere 14.4.4 a pagina 210)
- creare un programma (vedere 6.5 a pagina 85) di avvio automaticoto delle scansioni.
- È inoltre possibile configurare delle impostazioni globali (vedere 14.4.6 a pagina 213) applicabili a tutte le modalità di scansione.

Questa sezione del manuale d'uso esaminerà in dettaglio tutte le impostazioni sopra citate.

14.4.1. Selezione del livello di sicurezza

Ogni operazione di scansione anti-virus, in qualsiasi modalità, può eseguire l'analisi degli oggetti del computer ad uno di questi livelli (vedere Figura 66):

Elevato – massima accuratezza nella scansione della macchina nel suo complesso, o di singoli dischi, cartelle o file. Se ne raccomanda l'impiego qualora si sospetti che un virus possa essere penetrato nel computer.

Raccomandato. È il livello consigliato dagli esperti Kaspersky Lab. La scansione funziona in maniera analoga al livello **Elevato**, fatta eccezione per i file di posta.

Basso – livello che permette all'utente un agevole impiego di applicazioni che utilizzino estensivamente le risorse della macchina, poiché la gamma dei file sottoposti a scansione è ridotta.

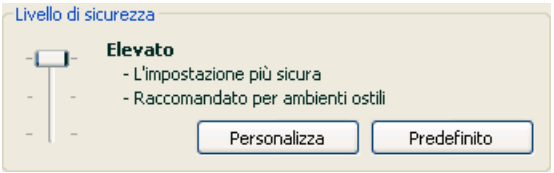


Figura 66. Selezione di un livello di sicurezza per la scansione antivirus

Per impostazione predefinita, File Anti-Virus è impostato su **Raccomandato**.

È possibile aumentare o diminuire la sicurezza della scansione anti-virus selezionando il livello desiderato, oppure cambiando le impostazioni del livello corrente.

Per modificare il livello di sicurezza:

Regolare i cursori. Regolando il livello di sicurezza, si definisce il rapporto tra la velocità di scansione e il numero totale di file esaminati: la rapidità della scansione è inversamente proporzionale alla quantità di file esaminati.

Se nessuno dei livelli di sicurezza è ritenuto soddisfacente, è possibile personalizzarne le impostazioni di protezione. Selezionare a tal fine il livello che più si approssima alle esigenze di sicurezza del computer e utilizzarlo come modello per modificare le impostazioni. In questo caso il livello diventa **Impostazioni personalizzate**.

Per modificare le impostazioni di un livello di sicurezza:

Fare clic sul pulsante **Personalizza** nella finestra delle impostazioni dell'attività. Nella finestra che appare, aggiustare i parametri di scansione e premere **OK**.

Viene quindi creato un quarto livello di sicurezza, **Impostazioni personalizzate**, che contiene le impostazioni di protezione configurate dall'utente.

14.4.2. Definizione del tipo di oggetti da sottoporre a scansione

Quando si specificano i tipi di oggetti da analizzare, si stabilisce il formato dei file, la dimensione e i dischi che saranno sottoposti a scansione anti virus in una specifica modalità.

I tipi di file esaminati vengono definiti nella sezione **Tipi di file** (cfr. Figura 67):

- **Tutti**. Con questa opzione, tutti gli oggetti vengono sottoposti a scansione, senza eccezioni.
- **Programmi e documenti (per contenuto)**. Selezionando questo gruppo di programmi, si sottopongono a scansione solo i file a rischio di infezione – quelli in cui si potrebbe nascondere un virus.

> Nota:
> Vi sono file nei quali non possono annidarsi virus, poiché il codice di tali file non contiene alcun elemento a cui il virus possa attaccarsi, Un esempio è costituito dai file .txt.

Prima di cercare un virus in un oggetto, la sua intestazione viene analizzata per rilevarne il formato (txt, doc, exe, ecc.).

Programmi e documenti (per estensione). In questo caso, il programma sottoporrà a scansione solamente i file potenzialmente infetti, determinandone il formato in base all'estensione. Utilizzando il link, è possibile accedere ad un elenco di estensioni file che, con questa opzione, vengono sottoposti a scansione (vedere A.1 a pagina 290).

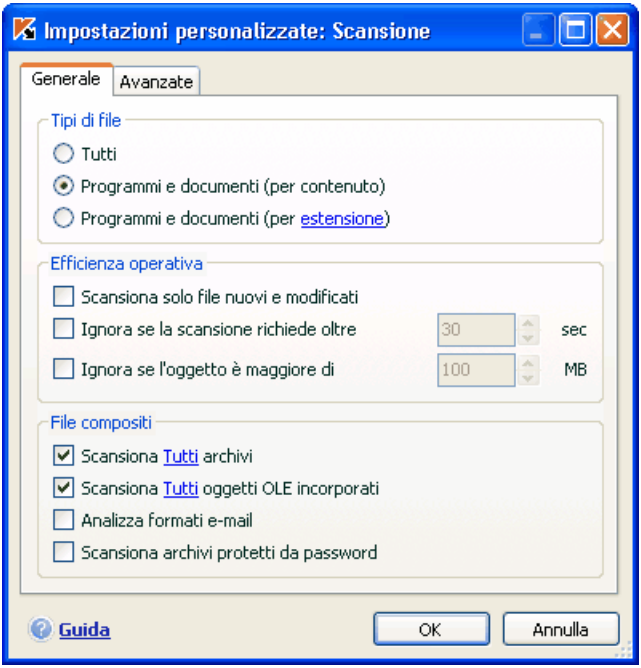


Figura 67. Configurazione delle impostazioni di scansione

Suggerimento:
Ricordare che è possibile inviare virus all'interno di file con estensione .txt che sono in realtà file eseguibili rinominati come file di testo. Selezionando l'opzione **Programmi e documenti (per estensioni)**, tale file sarebbe escluso dalla scansione. Invece, selezionando l'opzione **Programmi e documenti (per contenuto)**, il programma ignorerà l'estensione del file analizzandone invece l'intestazione, e detrminando così la sua vera natura di file eseguibile. Il file sarebbe quindi sottoposto a un'approfondita scansione antivirus.

Nella sezione **Efficienza operativa**, è possibile specificare se si vuole sottoporre a scansione solamente i nuovi file, oppure i nuovi file e quelli che sono stati modificati dopo la scansione precedente. Questa modalità riduce

considerevolmente la durata della scansione e aumenta la velocità del programma. Per attivare questa modalità, selezionare la casella **Scansiona solo file nuovi e modificati**. Questa modalità si applica sia ai file semplici sia a quelli complessi.

Nella sezione **Efficienza operativa** si possono inoltre stabilire limiti di tempo e di dimensione dei file per la scansione.

Ignora se la scansione richiede oltre ... sec. Selezionare quest'opzione ed inserire la durata massima per la scansione di un singolo oggetto. Se la scansione di un oggetto richiede un tempo superiore a quello specificato, l'oggetto viene rimosso dalla coda di scansione.

Ignora se l'oggetto и maggiore di … MB. Selezionare quest'opzione ed inserire la dimensione massima dell'oggetto. Se la dimensione di un oggetto supera quella specificata, l'oggetto viene rimosso dalla coda di scansione.

Nella sezione **File compositi**, specificare quali file composti debbano essere sottoposti a scansione anti-virus:

Scansiona Tutti/Solo nuovi archivi – analizza gli archivi con estensione .rar, .arj, .zip, .cab, .lha, .jar, e .ice.

Scansiona Tutti/Solo nuovi oggetti OLE incorporati – analizza gli oggetti incorporati nei file (per esempio fogli di calcolo di Excel o macro incorporati in un file di Microsoft Word, allegati di posta, ecc.).

Per ogni tipo di file complesso è possibile selezionare ed esaminare tutti i file o solo quelli nuovi usando il link a fianco del nome dell'oggetto. Facendovi clic sopra con il pulsante sinistro del mouse, il suo valore cambia. Se la sezione **Efficienza operativa** è stata impostata in modo da esaminare solo i file nuovi e modificati, non sarà possibile selezionare il tipo di file complesso da sottoporre a scansione.

Analizza formati e-mail – esegue la scansione dei file e dei database di posta elettronica. Se questo riquadro non è selezionato, il programma non opera la scansione di tali oggetti, e il loro stato, nel rapporto, sarà indicato come *ok*.

In merito alla scansione di database di posta elettronica protetti da password, si prega di notare quanto segue:

- Kaspersky Internet Security rileva i codici dannosi presenti nei database di Microsoft Office Outlook 2000, ma non interviene su di essi;
- Il programma non supporta la scansione anti-virus dei database protetti di Microsoft Office Outlook 2003.

Scansiona archivi protetti da password – esegue la scansione di archivi protetti da password. Se quest'opzione è attiva, una finestra richiederà

l'inseriento di una password prima che venga eseguita la scansione di un oggetto archiviato. Se il riquadro non è selezionato, la scansione salterà gli archivi protetti.

14.4.3. Ripristino delle impostazioni di scansione predefinite

Quando si configurano le impostazioni per una data modalità di scansione, è sempre possibile ripristinare le impostazioni raccomandate. Kaspersky Lab le considera ottimali e le ha riunite nel livello di sicurezza **Raccomandato**.

Per ripristinare le impostazioni predefinite di File Anti-Virus:

1. Selezionare il nome dell'attività nella scheda **Scansione** della finestra principale e usare il link Impostazioni per aprire la finestra delle impostazioni.
2. Fare clic sul pulsante **Predefinito** nella sezione **Livello di sicurezza**.

14.4.4. Selezione delle azioni da applicare agli oggetti

Se durante una scansione viene rilevato un file infetto, o presunto tale, il programma reagirà in base allo stato del file e all'azione selezionata.

All'oggetto in questione può venire classificato, dopo la scansione, con dei seguenti stati:

- Programma nocivo (per esempio, *virus, troiano*).
- *Probabilmente infetto*, quando la scansione non è in grado di determinare se l'oggetto è infetto. Ciò significa che il codice del file contiene una sezione che sembra essere la variante di un virus noto o ricorda la struttura di una sequenza virale.

Per impostazione predefinita, tutti i file infetti sono sottoposti a un tentativo di riparazione e se sono potenzialmente infetti vengono inviati in Quarantena.

Per modificare un'azione da applicare a un oggetto:

Dopo aver cliccato sul pulsante **Scansione** nella finestra principale del programma, selezionare il nome della modalità di scansione, ed usare il collegamento Impostazioni per aprire la finestra delle impostazioni. Tutte le azioni potenziali sono visualizzate nelle sezioni appropriate (cfr. Figura 68).

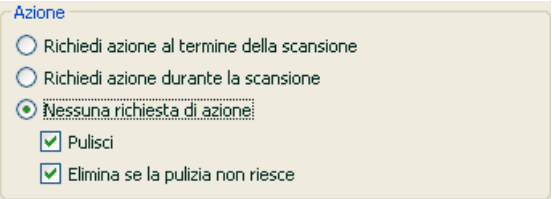


Figura 68. Selezione di un'azione per gli oggetti pericolosi

Se l'azione selezionata è	**Se viene rilevato un oggetto dannoso o potenzialmente infetto**
Richiedi azione al termine della scansione	Il programma non interviene sugli oggetti prima della fine della scansione. Al termine del processo, una finestra di statistiche relative alla scansione appena ultimata mostrerà l'elenco degli oggetti rilevati, chiedendo all'utente se intervenire su di essi o meno.
Richiedi azione durante la scansione	Il programma mostrerà un messaggio di allarme contenente informazioni sul codice dannoso che ha, o che potrebbe avere, infettato un file, e offrirà all'utente la possibilità di scegliere tra una delle seguenti azioni.
Nessuna richiesta di azione	Il programma registra nel rapporto le informazioni relative agli oggetti rilevati, senza intervenire su di essi e senza notificare la cosa all'utente. Si sconsiglia di avvalersi di quest'opzione, poiché gli oggetti dannosi permangono sul computer, ed è praticamente impossibile evitare l'infezione.
Nessuna richiesta di azione **Pulisci**	Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Qualora l'oggetto non possa essere disinfettato, il programma provvederà a porlo in quarantena (cfr. 17.1 a pag. 231). Le informazioni

	relative all'evento vengono registrate nel report (cfr. 17.3 a pag. 237). In un secondo momento sarà possibile tentare di riparare l'oggetto.
Nessuna richiesta di azione **Pulisci** **Elimina se la pulizia non riesce**	Il programma cerca di trattare l'oggetto rilevato senza chiedere conferma all'utente. Se la riparazione non riesce, l'oggetto viene eliminato.
Nessuna richiesta di azione **Pulisci** **Elimina**	Il programma cancella automaticamente l'oggetto rilevato.

A prescindere dallo stato dell'oggetto (infetto o potenzialmente tale), prima di tentarne la disinfezione o la cancellazione, Kaspersky Internet Security ne esegue una copia di backup e la invia a Backup (vedere 17.2 a pagina 234) cosicché l'oggetto rimane disponibile qualora risulti necessari ripristinarlo, o emerga l'opportunità di disinfettarlo.

14.4.5. Opzioni avanzate per la scansione anti-virus

Oltre alle impostazioni di base per la scansione anti-virus, è possibile configurare una serie di impostazioni avanzate (vedere Figura 69):

Abilita tecnologia iChecker – abilita l'impiego di una tecnologia che permette di incrementare la velocità di scansione saltando tutti gli oggetti che non siano stati modificati dalla scansione precedente, ammesso che le impostazioni di scansione (elenchi delle minacce e impostazioni) non siano state modificate. Tutte le informazioni in merito sono immagazzinate in un apposito database.

Ad esempio, se nel computer è presente un file archivio che è stato sottoposto a scansione e classificato come non infetto, alla successiva scansione il programma ignorerà questo file, a meno che non sia stato modificato nel frattempo, o che non siano state cambiate le impostazioni di scansione.. Se la struttura dell'archivio è stata modificata in seguito all'aggiunta di un oggetto, se sono state modificate le opzioni di scansione, o se gli elenchi delle minacce sono stati aggiornati, il programma eseguirà nuovamente la scansione dell'archivio.

L'applicazione della tecnologia iChecker™ è limitata agli oggetti la cui struttura viene riconosciuta da Kaspersky Internet Security (ad esempio, file con estensione .exe, .dll, .lnk, .ttf, .inf, .sys, .com, .chm, .zip, .rar).

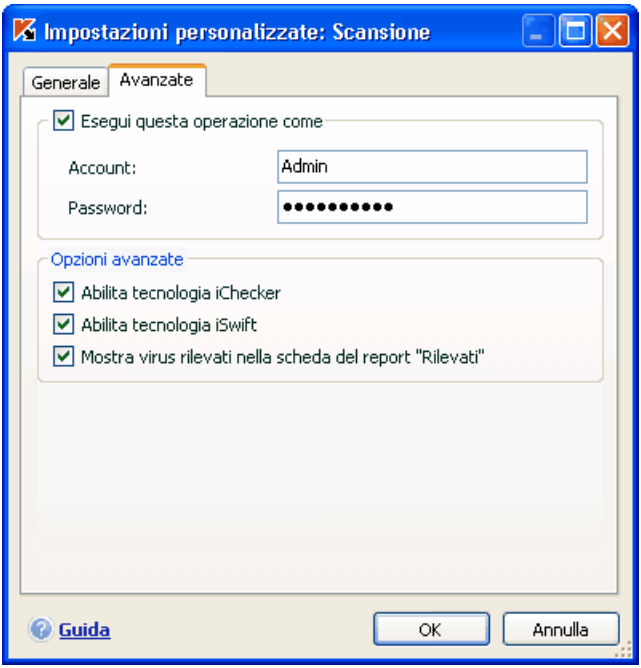


Figura 69. Impostazioni di scansione avanzate

Abilita tecnologia iSwift – abilita l'impiego di una tecnologia che può incrementare la velocità di scansione eseguendo solamente l'analisi degli oggetti nuovi o modificati.. L'applicazione della tecnologia iChecker™ è limitata agli oggetti del file system NTFS.

> La tecnologia iSwift non è disponibile su computer con sistema operativo Microsoft Windows 98SE/ME/XP64.

Mostra virus rilevati nella scheda del report "Rilevati" – mostra, nella scheda **Rilevati** della finestra del rapporto (vedere 17.3.2 a pag. 241), un elenco delle minacce individuate durante la scansione. Può risultare utile disabilitare questa funzione in casi speciali, come ad esempio collezioni di testi, per aumentare la velocità di scansione.

14.4.6. Configurazione di impostazioni di scansione globali per tutte le attività

Ogni operazione di scansione viene eseguita secondo una modalità definita da specifiche impostazioni. La modalità di scansione che si crea all'atto dell'installazione del programma utilizza le impostazioni predefinite raccomandate dagli esperti di Kaspersky Lab.

È possibile definire delle impostazioni globali valide per tutte le operazioni di scansione, in qualsiasi modalità. Come termine di riferimento si utilizza un gruppo di proprietà applicabili alla scansione anti-virus di un singolo oggetto.

Per assegnare impostazioni di scansione globali:

1. Selezionare la sezione **Scansione** nella parte sinistra della finestra del programma principale, e cliccare su Impostazioni.
2. Configurare, nella finestra che appare, le impostazioni di scansione: Selezionare il livello di sicurezza (cfr. 14.4.1 a pag.. 206), configurare le impostazioni di livello avanzato, e selezionare un'azione (cfr. 14.4.4 a pag. 210) per gli oggetti.
3. Per rendere queste impostazioni valide in qualunque modalità di scansione, cliccare sul pulsante **Applica** nella sezione **Altre operazioni di scansione**. Confermare le impostazioni globali selezionate nella successiva finestra di dialogo.

CAPITOLO 15. AGGIORNAMENTI DEL PROGRAMMA

Mantenere aggiornato il software antivirus costituisce un investimento in termini di sicurezza per il proprio computer. Poiché ogni giorno nascono nuovi virus, trojan e altri software dannosi, per proteggere costantemente le proprie informazioni è fondamentale aggiornare regolarmente l'applicazione di protezione.

L'aggiornamento dell'applicazione implica lo scaricamento e l'installazione, sul proprio computer, dei seguenti componenti:

- **Elenchi di minacce**

  Per proteggere le informazioni presenti sul computer l'applicazione fa uso di elenchi di minacce, che vengono utilizzati dai componenti del programma che forniscono la protezione per rilevare e disinfettare oggetti dannosi eventualmente presenti. Le firme vengono aggiunte di ora in ora con la registrazione di nuove minacce e dei metodi per debellarle, ed è pertanto consigliabile aggiornarle in maniera regolare.

  Le precedenti versioni di Kaspersky Lab supportavano il database sia in assetto *standard* che *esteso*, ciascuno dei quali implicato nella protezione del computer da diversi tipi di oggetti dannosi. Con Kaspersky Internet Security non è più necessario decidere quale sistema di elenchi di minacce adottare poiché quelle impiegate da questo prodotto garantiscono la protezione sia da diversi tipi di oggetti dannosi, o potenzialmente pericolosi, che dagli attacchi da parte di hacker.

- **Moduli del programma**

  Oltre alle segnatures, Kaspersky Internet Security consente anche l'aggiornamento dei moduli di programma. Nuovi aggiornamenti dell'applicazione vengono elaborati con regolarità.

La principale fonte di aggiornamenti per Kaspersky Internet Security è rappresentata dai server di Kaspersky Lab. Questi sono alcuni dei loro indirizzi:

http://downloads1.kaspersky-labs.com/updates/

http://downloads2.kaspersky-labs.com/updates/

ftp://downloads1.kaspersky-labs.com/updates/

Per scaricare dai server gli aggiornamenti disponibili è necessario disporre di una connessione Internet.

Qualora non si disponesse di un accesso ai server di Kaspersky Lab (ad esempio, se il computer non fosse connesso ad Internet), è possibile rivolgersi direttamente all'ufficio di Kaspersky Lab chiamando il +7 (495) 797-87-00, chiedendo di essere messi in contatto con partner di Kaspersky Lab che siano in grado di fornire gli aggiornamenti desiderati in formato compresso su floppy disk o CD.

Lo scaricamento degli aggiornamenti può essere effettuato secondo una delle seguenti modalità:

- *Automatico*. Con questa opzione, Kaspersky Internet Security scarica ed installa gli aggiornamenti automaticamente, non appena vengono resi disponibili sugli appositi server.
- *Programmazione*. L'aggiornamento è messo in programma in modo da cominciare ad un tempo prestabilito.
- *Manuale*. Con questa opzione, la procedura di aggiornamento viene avviata manualmente.

Durante l'aggiornamento, l'applicazione confronta gli elenchi delle minacce ed i moduli di programma presenti sul computer con le versioni disponibili sul server. Se il computer dispone delle versioni più recenti, la cosa verrà notificata in una apposita finestra, confermando che la macchina è aggiornata. Qualora le versioni presenti sul computer non corrispondano a quelle disponibili sul server, il programma eseguirà lo scaricamento delle sole parti mancanti. Non verranno invece scaricate le signatures e i moduli già presenti sulla macchina, permettendo in tal modo un significativo aumento nella velocità del processo ed una corrispondente riduzione del traffico in rete.

Prima di aggiornare gli elenchi delle minacce, Kaspersky Internet Security ne esegue una copia di backup, che può essere utilizzata qualora non si desiderasse impiegare le versioni più recenti delle firme stesse.

Può risultare necessario l'utilizzo delle opzioni di ripristino (vedere 15.2 a pag. 217), nel caso in cui, ad esempio, si tentasse di aggiornare gli elenchi delle minacce e questi risultassero danneggiati durante il processo. È possibile ripristinare le opzioni precedenti e ritentarne l'aggiornamento in un secondo momento.

15.1. Avvio della procedura di aggiornamento

È possibile iniziare l'aggiornamento in qualsiasi momento. Il processo opererà dall-origine dell-aggiornamento selezionata dall'utente (vedere 13.3.9 a pag. 194).

La procedura di aggiornamento può essere avviata da:

- il menu contestuale (vedere 4.2 a pag. 48).
- la finestra principale del programma (vedere 4.3 a pag. 49)

Per avviare la procedura di aggiornamento dal menu di scelta rapida:

1. Aprire il menu di scelta rapida cliccando col pulsante destro del mouse sull'icona dell'applicazione nella barra delle applicazioni.
2. Selezionare **Aggiornamento**.

Per avviare la procedura di aggiornamento dalla finestra principale del programma:

1. Selezionare **Aggiornamento** nella sezione **Servizi**.
2. Cliccare su **Aggiorna subito!** nel pannello di destra della finestra principale, o utilizzare il pulsante nella barra di stato.

Lo stato dell'aggiornamento verrà visualizzato in una speciale finestra. È possibile nascondere la finestra delle informazioni sulla scansione facendo clic su **Chiudi**. L-aggiornamento prosegue a finestra chiusa.

15.2. Ripristino dell'aggiornamento precedente

Ogni volta che si avvia la procedura di aggiornamento, Kaspersky Internet Security crea innanzitutto una copia degli elenchi delle minacce correnti, e solo successivamente inizia a scaricarne le nuove versioni. In tal modo, qualora l'aggiornamento non vada a buon fine, è possibile tornare ad utilizzare gli elenchi delle minacce precedenti.

L'opzione di ripristino potrebbe tornare utile nel caso in cui, ad esempio, la procedura di aggiornamento fallisse a causa di un errore di connessione. Basterebbe in tal caso ripristinare gli elenchi delle minacce precedenti, e ritentare l'aggiornamento in un secondo momento.

Per ripristinare la versione precedente degli elenchi delle minacce:

1. Selezionare il componente **Aggiornamento** nella sezione **Servizi** della finestra del programma principale.
2. Cliccare sul pulsante **Ripristina** nel pannello destro della finestra del programma principale.

15.3. Configurazione delle impostazioni di aggiornamento

La procedura di aggiornamento opera secondo impostazioni che definiscono i seguenti aspetti:

- La sorgente da cui l'aggiornamento viene scaricato e installato (vedere 13.3.9 a pag. 194)
- La modalità operativa della procedura di aggiornamento stessa (vedere 15.3.2 a pag. 221)
- Gli oggetti che devono essere aggiornati
- Le azioni da compiere al termine dell'aggiornamento (vedere 15.3.4 a pag. 225)

La presente sezione prende in esame gli aspetti sopra elencati.

15.3.1. Selezione di un'origine per l'aggiornamento

L'*origine degli aggiornamenti* è dove si scaricano gli aggiornamenti degli elenchi delle minacce e dei moduli delle applicazioni di Kaspersky Internet Security. Le origini degli aggiornamenti possono essere server HTTP e FTP, cartelle locali o cartelle di rete.

L'origine di aggiornamento principale è costituita dai *server degli aggiornamenti di Kaspersky Lab*. Si tratta di speciali siti web contenenti gli aggiornamenti disponibili per gli elenchi delle minacce e i moduli delle applicazioni per tutti i prodotti Kaspersky Lab.

Se non si è in grado di accedere ai server degli aggiornamenti di Kaspersky Lab (per esempio perché manca la connessione Internet), è possibile rivolgersi alla sede di Kaspersky Lab chiamando il numero +7 (495) 797-87-00 per richiedere i nominativi dei partner Kaspersky Lab in grado di fornire gli aggiornamenti in file compressi su dischetto o CD.

Attenzione!

Per richiedere gli aggiornamenti salvati su un supporto, è necessario specificare se si desiderano anche gli aggiornamenti dei moduli dell'applicazione.

È possibile copiare gli aggiornamenti da un disco e caricarli su un sito FTP o HTTP oppure salvarli in una cartella locale o di rete.

Selezionare l'origine degli aggiornamenti nella scheda **Aggiorna configurazione** (cfr. Figura 70).

L'elenco contiene solo i server degli aggiornamenti di Kaspersky Lab predefiniti. L'elenco dei server non può essere modificato. Durante l'aggiornamento, Kaspersky Internet Security consulta l'elenco, seleziona l'indirizzo del primo server e cerca di scaricare i file. Se lo scaricamento dei file dal primo server non va a buon fine, l'applicazione cerca di connettersi al server successivo e di scaricare i file da quello. L'indirizzo dal quale si riesce a scaricare gli aggiornamenti va automaticamente ad occupare la prima posizione dell'elenco. All'aggiornamento successivo, l'applicazione cercherà innanzitutto di connettersi al server da cui sono stati scaricati gli ultimi aggiornamenti.

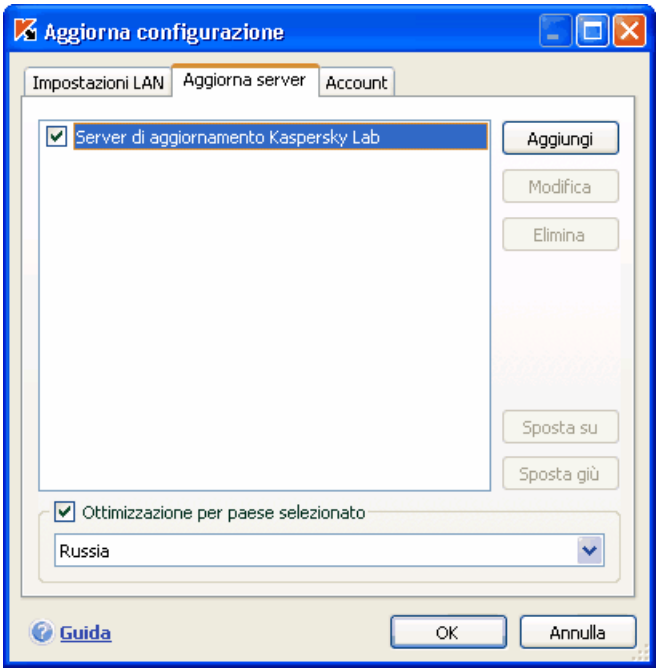


Figura 70. Selezione di un'origine per l'aggiornamento

Per scaricare gli aggiornamenti da un altro sito FTP o HTTP:

1. Fare clic su **Aggiungi**.
2. Nella finestra di dialogo **Seleziona una sorgente di aggiornamento**, selezionare il sito FTP o HTTP a cui si desidera connettersi, oppure specificare l'indirizzo IP, o l'URL del sito nel campo **Sorgente**.

Attenzione!

Se come origine degli aggiornamenti è stata selezionata una risorsa di rete, come i server degli aggiornamenti Kaspersky Lab o altri siti FTP/HTTP, è necessaria una connessione Internet per scaricare i file.

Per scaricare l'aggiornamento da una cartella locale:

1. Fare clic su **Aggiungi**.
2. Nella finestra di dialogo **Seleziona una sorgente di aggiornamento**, selezionare una cartella o specificare il percorso completo di questa cartella nel campo **Sorgente**.

Kaspersky Internet Security aggiunge la nuova origine all'inizio dell'elenco e la abilita automaticamente.

Se sono state selezionate più risorse, l'applicazione cerca di connettersi ad esse una dopo l'altra a partire da quella che occupa la prima posizione dell'elenco, e preleva gli aggiornamenti dalla prima disponibile. È possibile modificare l'ordine delle origini nell'elenco servendosi dei pulsanti **Sposta su** e **Sposta giù**.

Per modificare l'elenco, usare i pulsanti **Aggiungi**, **Modifica** ed **Elimina**. L'unico tipo di origine che non può essere modificato né eliminato sono i server degli aggiornamenti di Kaspersky Lab.

Un altro aspetto dell'aggiornamento degli elenchi delle minacce che può essere personalizzato è il formato. Gli elenchi delle minacce includono uno speciale file .xml che descrive la struttura delle directory che contengono gli aggiornamenti. Questa struttura è utilizzata durante l'aggiornamento delle firme sul computer. La struttura dell'elenco corrente delle minacce è diversa da quella del database antivirus utilizzato dalle versioni precedenti delle applicazioni Kaspersky Lab.

Se si aggiorna il programma da una cartella o file .zip che non supporta la struttura corrente degli elenchi delle minacce anziché da un server degli aggiornamenti di Kaspersky Lab, si raccomanda di selezionare la casella **Aggiornamento da cartella non strutturata o archivio-zip (rallenta l'aggiornamento)**. Questa impostazione ha la caratteristica di rallentare leggermente la procedura di aggiornamento ma potrebbe evitare errori nell'esecuzione.

Se si prelevano gli aggiornamenti dai server di Kaspersky Lab, è possibile selezionare la posizione ottimale del server da cui scaricare i file. Kaspersky Lab dispone di server in diversi paesi. La scelta del server di Kaspersky Lab più vicino aiuta a risparmiare tempo e ad accelerare il prelievo degli aggiornamenti.

Per scegliere il server più vicino, selezionare la casella **Ottimizzazione per paese selezionato** e selezionare quindi dall'elenco a discesa il paese più vicino al proprio paese di residenza.

Osservare che l'opzione di selezione del server più vicino non è disponibile con Windows 9X/NT 4.0.

15.3.2. Selezione di un metodo di aggiornamento e degli oggetti da aggiornare

Durante la configurazione delle impostazioni di aggiornamento è importante definire cosa sarà aggiornato e con quale metodo.

Gli oggetti dell-aggiornamento (cfr. Figura 71) sono i componenti che si desidera aggiornare: gli elenchi delle minacce, i moduli del programma e gli elenchi degli attacchi di rete usati da Anti-Hacker. Gli elenchi delle minacce vengono sempre aggiornati, mentre i moduli dell'applicazione e le informazioni sugli attacchi di rete vengono aggiornati solo se è stata selezionata la modalità corrispondente.

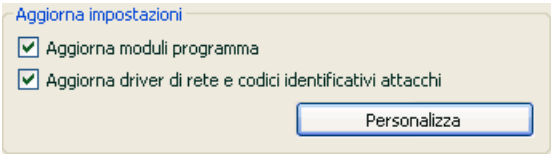


Figura 71. Selezione di un oggetto da aggiornare

Se si desidera scaricare e installare gli aggiornamenti dei moduli del programma:

Selezionare la casella **Aggiorna moduli programma** nella finestra di dialogo **Impostazioni** del componente **Aggiornamento**.

Se nell'origine prescelta sono disponibili aggiornamenti per i moduli del programma, il programma scarica quelli necessari e li applica al riavvio del computer. Gli aggiornamenti dei moduli scaricati saranno installati solo dopo che il computer sarà stato riavviato.

Se l'aggiornamento successivo viene reso disponibile prima che il computer sia stato riavviato e prima che gli aggiornamenti scaricati in precedenza siano stati installati, saranno aggiornati solo gli elenchi delle minacce.

Se si desidera scaricare e installare informazioni sui nuovi attacchi di rete e su come bloccarli:

Selezionare la casella **Aggiorna driver di rete e codici identificativi attacchi** nella finestra delle impostazioni del componente Updater.

Il metodo di aggiornamento (cfr. Figura 72) definisce le modalità di avvio di Updater. È possibile selezionare una delle seguenti opzioni:

Automatico. Selezionando questa opzione, Kaspersky Internet Security copia e installa gli aggiornamenti non appena vengono messi a disposizione sui server degli aggiornamenti o su altre origini (cfr. 13.3.9 a pag. 194). Questa modalità è selezionata per impostazione predefinita.

Se si dispone di una connessione Internet remota ed è specificata una risorsa di rete come origine di aggiornamento, Kaspersky Internet Security cerca di avviare Updater ogni volta che il computer si connette a quella risorsa o alla scatime the computer connects to that resource or after a certain amount of time has elapsed as specified in the previous update packet. Se come origine di aggiornamento è stata selezionata una cartella locale, l'applicazione cerca di scaricare gli aggiornamenti da quest'ultima con la frequenza specificata nell'ultimo pacchetto di aggiornamento scaricato. Questa opzione consente a Kaspersky Lab di regolare la frequenza di aggiornamento del programma in caso di epidemie o di altre situazioni potenzialmente pericolose. L'applicazione riceverà tempestivamente gli aggiornamenti più recenti degli elenchi delle minacce, del database degli attacchi di rete e dei moduli del software, impedendo ai programmi nocivi di penetrare nel computer.

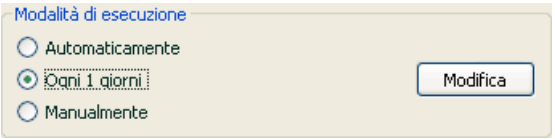


Figura 72. Selezione di una modalità di esecuzione degli aggiornamenti

Programmazione. Updater è programmato per avviarsi a un'ora specificata. La frequenza predefinita è una volta al giorno. Per modificare la programmazione predefinita, fare clic sul pulsante **Modifica** nel riquadro del metodo e apportare le modifiche desiderate nella finestra che si apre (per ulteriori informazioni, cfr. 6.5 a pag. 85).

Manuale. Questa opzione consente di avviare Updater manualmente. Kaspersky Internet Security informa l'utente quando è necessario provvedere all'aggiornamento:

- Sopra l'icona dell'applicazione nella barra delle applicazioni compare un messaggio che informa che sono necessari degli aggiornamenti (cfr. 17.11.1 a pag. 267)
- Il secondo indicatore nella finestra principale del programma informa che il computer non è aggiornato (cfr. 5.1.1 a pag. 55)
- Nella sezione messaggi dell finestra principale del programma viene visualizzata la raccomandazione di aggiornare l'applicazione (cfr. 4.3 a pag. 49)

15.3.2.1. Pianificazione degli aggiornamenti

Se il metodo di aggiornamento selezionato è la pianificazione, la frequenza di aggiornamento predefinita per le firme è ogni giorno. Se la frequenza predefinita non è quella desiderata, è possibile modificarla nella finestra di dialogo **Programmazione**.

È necessario innanzitutto definire il tipo di programmazione. È possibile selezionare una delle seguenti opzioni:

Una volta. L'attività sarà eseguita una volta nel giorno e nell'ora specificati.

Ogni minuto. Il programma sarà aggiornato con la frequenza in minuti indicata. Specificare il numero dei minuti tra gli aggiornamenti. Non deve essere superiore a 59 minuti.

Ogni ora. Updater viene eseguito con la frequenza indicata in ore. Se si sceglie questa opzione, selezionare tra le impostazioni **Ogni N ore** e specificare il valore di *N*. Per esempio, per scaricare gli aggiornamenti ogni ora, selezionare *Ogni 1 ora*.

Giornalmente – l'applicazione viene aggiornata con la frequenza indicata in giorni. Nelle impostazioni selezionare le seguenti opzioni:

- *Ogni giorno* – se si desidera eseguire aggiornamenti giornalieri **Ogni N giorno(i)**, specificando il valore di *N* se si desidera interporre un intervallo di giorni tra le sessioni di aggiornamento. Per eseguire Updater ogni due giorni, digitare *Ogni 2 giorni*.
- **Tutti i giorni feriali** se si desidera aggiornare il programma tutti i giorni dal lunedì al venerdì.
- **Tutti i giorni festivi** per eseguire Updater solo di sabato e di domenica.

  Oltre alla frequenza, specificare l'ora di inizio nel campo **Ora**.

Settimanalmente – l'applicazione viene aggiornata determinati giorni della settimana. Se si seleziona questa opzione, indicare i giorni della settimana in cui si desidera scaricare gli aggiornamenti. Indicare inoltre un'ora di inizio nel campo *Ora*.

Mensilmente – l'attività di scansione sarà eseguita una volta al mese all'ora specificata.

Se per qualsiasi motivo un aggiornamento viene saltato (per esempio all'ora prevista il computer era spento), è possibile configurare l'attività da recuperare in modo da iniziare automaticamente non appena possibile. A tal fine, selezionare la casella **Esegui operazione se ignorata** nella finestra delle pianificazioni.

15.3.3. Configurazione delle impostazioni di connessione

Se si imposta il programma in modo da scaricare gli aggiornamenti dai server di Kaspersky Lab o da altri siti FTP o HTTP, si raccomanda di selezionare prima le impostazioni di connessione.

Per impostazione predefinita, per stabilire una connessione Internet l'applicazione usa le impostazioni del browser (per esempio Microsoft Internet Explorer). Per modificare le impostazioni di connessione, è necessario sapere se viene utilizzato un server proxy e se ci si trova dietro un firewall. Se non si conosce questa informazione, rivolgersi all'amministratore di sistema o all'Internet provider.

Tutte le impostazioni sono raggruppate in un'apposita scheda, **Impostazioni LAN** (cfr. Figura 73).

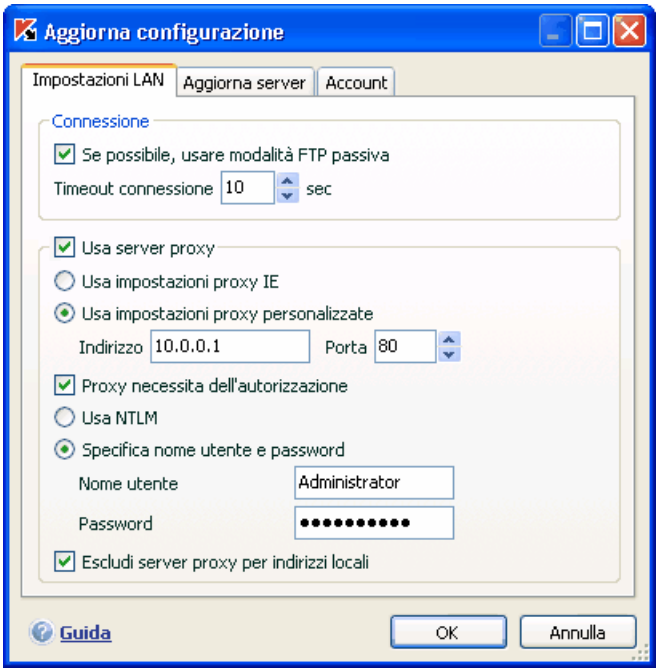


Figura 73. Configurazione delle impostazioni di aggiornamento

Selezionare la casella ☑ **Se possibile, usare modalità FTP passiva** se si scaricano gli aggiornamenti da un server FTP in modalità passiva (per esempio

attraverso un firewall). Se si lavora in modalità FTP attivo, deselezionare la casella.

Selezionare la casella **Usa server proxy** se si accede a Internet attraverso un server proxy e, se necessario, selezionare le seguenti impostazioni:

- Selezionare le impostazioni del server proxy da utilizzare durante l'aggiornamento:
  - **Usa impostazioni proxy IE** – per utilizzare le impostazioni di Internet Explorer per il collegamento attraverso un server proxy.
  - **Usa impostazioni proxy personalizzate** – per usare un proxy diverso da quello specificato nelle impostazioni di connessione del browser. Nel campo **Indirizzo**, digitare l'indirizzo IP o il nome simbolico del server proxy e specificare il numero della porta proxy utilizzata per aggiornare l'applicazione nel campo **Porta**.
- Specificare se si richiede l'autenticazione sul server proxy. Se è necessaria l'autenticazione per stabilire una connessione Internet, selezionare la casella **Proxy necessita dell'autorizzazione**.
- Selezionare le modalità di accesso al server proxy durante la connessione a Internet:
  - **Usa NTLM** – per connettersi a Internet utilizzando i dati del profilo utente.

    Nota:
    Non è possibile utilizzare le informazioni sull'account se l'applicazione è installata su un computer con Microsoft Windows 9X/NT che non è incluso come parte del dominio.
  - **Specifica nome utente e password.** La procedura di accesso richiede il nome utente e la password. Digitare il nome di connessione e la password nei campi **Nome utente** e **Password**.

Per proibire l'uso di un proxy quando l'origine degli aggiornamenti è una cartella locale, selezionare la casella **Escludi server proxy per indirizzi locali**.

Questa funzione non è disponibile in Windows 9X/NT 4.0. Tuttavia, per impostazione predefinita, il server proxy non è utilizzato per gli indirizzi locali.

15.3.4. Azioni successive all'aggiornamento del programma

Ogni aggiornamento degli elenchi delle minacce contiene nuovi elementi che proteggono il computer dalle minacce più recenti.

Kaspersky Lab raccomanda di esaminare ogni volta gli *oggetti in quarantena* e gli *oggetti all'avvio* dopo l'aggiornamento del database.

Perché è necessario esaminare questi oggetti?

La cartella Quarantena contiene oggetti che il programma ha catalogato come sospetti o probabilmente infetti (cfr. 17.1 a pag. 231). Utilizzando la versione più recente degli elenchi delle minacce, Kaspersky Internet Security potrebbe essere in grado di identificare la minaccia e di eliminarla.

Per impostazione predefinita, l'applicazione esamina gli oggetti in quarantena dopo ogni aggiornamento degli elenchi delle minacce. Si raccomanda inoltre di consultare periodicamente gli oggetti in quarantena poiché il loro status può cambiare in seguito alle scansioni. Alcuni oggetti possono quindi essere ripristinati nelle posizioni originarie per continuare a lavorare con loro.

Per disabilitare la scansione degli oggetti in Quarantena, deselezionare la casella ☑ **Ripeti scansione della cartella di Quarantena** nella sezione **Azioni successive all'aggiornamento**.

Gli oggetti all'avvio sono di importanza vitale per la sicurezza del computer. Se uno di essi è infetto da un'applicazione nociva, potrebbe verificarsi un errore di avvio del sistema operativo. Kaspersky Internet Security è dotato di un'attività di scansione degli oggetti all'avvio per quest'area (cfr. Capitolo 14 a pag. 201). Si raccomanda di pianificare un calendario di esecuzione per questa attività in modo da avviarlo automaticamente ad ogni aggiornamento degli elenchi delle minacce (cfr. 6.5 a pag. 85).

CAPITOLO 16. AGGIORNA DISTRIBUZIONE

Se i PC di casa sono collegati in una rete domestica, non è necessario scaricare ed installare gli aggiornamenti individualmente su ciascuno di essi, poiché ciò aumenterà notevolmente il traffico di rete. Il servizio aggiorna distribuzione consente di risparmiare larghezza di banda. A tal fine, impostare lo strumento aggiorna distribuzione come segue:

1. Uno dei computer della rete recupera un pacchetto di aggiornamento dell'applicazione e degli elenchi dei virus dai server Web di Kaspersky Lab, oppure da altre risorse di rete che ospitano un insieme di aggiornamenti. Gli aggiornamenti recuperati vengono salvati in una cartella ad accesso pubblico.
2. Gli altri computer della rete accedono alla cartella ad accesso pubblico per recuperare gli aggiornamenti all'applicazione.

I pacchetti di aggiornamento possono essere copiati dai server di Kaspersky Lab alla cartella ad accesso pubblico tramite uno dei seguenti metodi:

- *Come da programma*. Gli aggiornamenti vengono copiati all'ora specificata.
- *Manualmente*. Con questa opzione, gli aggiornamenti vengono copiati manualmente.

Se si desidera che altri computer nella rete si aggiornino dalla cartella contenente gli aggiornamenti copiati da Internet, attenersi alla seguente procedura:

1. Consentire l'accesso pubblico alla cartella.
2. Specificare la cartella ad accesso pubblico quale origine degli aggiornamenti nelle impostazioni dell'Updater degli altri computer di rete.

Kaspersky Internet Security è in grado di creare un elenco degli oggetti (cfr. 16.2 a pag. 228) da aggiornare sui computer di rete.

Si noti che Kaspersky Internet Security 6.0 recupera dai server di aggiornamento di Kaspersky Lab esclusivamente i pacchetti di aggiornamento relativi alle applicazioni v. 6.0.

16.1. Impostazioni dello strumento Aggiorna distribuzione

Le impostazioni dello strumento Aggiorna distribuzione sono visualizzate nella sezione **Aggiorna distribuzione** della finestra delle impostazioni dell'applicazione. Per configurarle:

1. Aprire la finestra principale di Kaspersky Internet Security e selezionare **Aggiorna distribuzione** nella sezione **Servizio**.
2. Fare clic ovunque nel riquadro **Impostazioni** o utilizzare il collegamento Impostazioni nella parte superiore della finestra principale dell'applicazione.

È possibile configurare le seguenti impostazioni per lo strumento Aggiorna distribuzione:

- Selezionare la *Modalità di avvio di Aggiorna distribuzione*: automatico o manuale. A tal fine, selezionare l'opzione desiderata nella finestra **Modalità esecuzione**. Se si seleziona la modalità automatica, assegnare le impostazioni di programmazione (cfr. 6.5 a pag. 85) nella finestra che si apre facendo clic su **Modifica**.
- Specificare il *percorso alla cartella ad accesso pubblico* nella quale saranno salvati i pacchetti di aggiornamento recuperati dai server Web di Kaspersky Lab quando si copiano gli aggiornamenti. Servirsi del pulsante **Sfoglia** per modificare il percorso.
- Creare un *insieme di aggiornamenti disponibili* (cfr. 16.2 a pag. 228): cosa deve essere specificatamente disponibile per aggiornare i computer in rete dal pacchetto recuperato dal server Web. A tal fine, fare clic sul pulsante **Componenti** ubicato nel riquadro **Impostazioni**.
- Configurare le impostazioni per il recupero dei pacchetti di aggiornamento da Internet: selezionare un'origine degli aggiornamenti (cfr. 15.3.1 a pag. 218), specificare le impostazioni della connessione di rete (cfr. 15.3.3 a pag. 224), e configurare l'avvio delle attività con un altro profilo (cfr. 6.4 a pag. 84) (se necessario). A tal fine, fare clic sul pulsante **Configura** ubicato nel riquadro **Impostazioni**.

16.2. Creazione di un insieme di aggiornamenti disponibili

Questa finestra visualizza un elenco degli elementi presenti nei pacchetti di aggiornamento recuperati dai server di aggiornamento di Kaspersky Lab quando vengono copiati (cfr. Figura 74). È necessario specificare cosa, all'interno del pacchetto recuperato, deve essere disponibile agli altri computer per l'aggiornamento.

Per creare un insieme di aggiornamenti disponibili, selezionare la casella relativa agli oggetti che si desidera aggiornare sui computer di rete. Si noti che per eseguire la procedura di aggiornamento, almeno un oggetto deve essere selezionato dall'elenco.

Figura 74. Selezione dei componenti da distribuire

CAPITOLO 17. OPZIONI AVANZATE

Kaspersky Internet Security è dotato di altre funzioni che ne espandono la funzionalità.

Il programma colloca alcuni oggetti in apposite aree di archiviazione al fine di garantire la massima protezione dei dati riducendo al minimo le perdite.

- La cartella Backup contiene copie degli oggetti modificati o eliminati da Kaspersky Internet Security (cfr. 17.2 a pag. 234). Se un oggetto conteneva informazioni importanti e non è stato possibile recuperarlo completamente durante l'elaborazione antivirus, è possibile ripristinare l'oggetto dalla copia di backup.

- La Quarantena contiene oggetti potenzialmente infetti che non è stato possibile elaborare con le firme correnti (cfr. 17.1 a pag. 231).

Si raccomanda di esaminare periodicamente l'elenco degli oggetti. Alcuni di essi infatti possono essere già obsoleti e altri possono essere stati ripristinati.

Alcune funzioni sono state ideate per aiutare l'utente durante l'uso del programma. Ad esempio:

- Il servizio di supporto tecnico offre un'assistenza completa per Kaspersky Internet Security (cfr. 17.5 a pag. 254). Kaspersky offre una scelta di canali di supporto più vasta possibile: assistenza on-line, un forum di domande e commenti per gli utenti del programma, ecc.

- La funzione di Notifica serve per configurare le notifiche agli utenti relative a eventi chiave di Kaspersky Internet Security (cfr. 17.11.1 a pag. 267). Può trattarsi di eventi di natura informativa o di errori da eliminare immediatamente, ed è estremamente importante esserne a conoscenza.

- Protezione automatica protegge i file del programma da qualsiasi modifica o danno perpetrati dagli hacker, blocca l'uso delle funzioni del programma da parte di amministrazioni remote e proibisce ad altri utenti del computer di eseguire determinate azioni in Kaspersky Internet Security (cfr. 17.11.2 a pag. 271). Per esempio, la modifica del livello di protezione può influire considerevolmente sulla sicurezza del computer.

- Gestione chiavi di licenza è in grado di ottenere informazioni dettagliate sulla licenza utilizzata, attivare la copia del programma, and manage license key files (cfr. 17.5 a pag. 254).

Il programma offre anche una sezione di Guida (cfr. 17.4 a pag. 253) e report dettagliati (cfr. 17.3 a pag. 237) sul funzionamento di tutti i componenti di protezione e le attività di scansione antivirus.

Le porte monitorate possono regolare quali moduli di Kaspersky Internet Security controllano i dati trasferiti sulle porte selezionate (cfr. 17.7 a pag. 258).

Il disco di emergenza può agevolare il ripristino della funzionalità del computer dopo un'infezione (cfr. 17.10 a pag. 263). Si tratta di una funzione particolarmente utile quando non si riesce a caricare il sistema operativo del computer in seguito al danneggiamento dei file di sistema da parte di un codice nocivo.

È possibile inoltre modificare l'aspetto di Kaspersky Internet Security e personalizzare l'interfaccia del programma (cfr. 17.9 a pag. 260).

Esaminiamo in dettaglio queste funzioni.

17.1. Quarantena per gli oggetti potenzialmente infetti

La **Quarantena** è una speciale area di archiviazione che contiene gli oggetti potenzialmente infetti.

Gli **oggetti potenzialmente infetti** sono oggetti sospettati di contenere un virus o la variante di un virus.

Perché *potenzialmente infetti*? Non sempre è possibile stabilire con certezza se un oggetto sia infetto oppure no. Questo è dovuto a diverse ragioni:

- Il codice dell'oggetto esaminato somiglia a una minaccia nota ma appare parzialmente modificato.

  Gli elenchi delle minacce contengono minacce già studiate da Kaspersky Lab. Se un programma nocivo è stato modificato e le variazioni non sono ancora state registrate tra le firme, Kaspersky Internet Security classifica l'oggetto contenente il programma nocivo modificato come potenzialmente infetto e indica la minaccia a cui il codice somiglia.

- Il codice dell'oggetto intercettato ricorda per struttura un programma nocivo. Tuttavia nessun oggetto simile è ancora registrato negli elenchi delle minacce.

  È possibile che si tratti di un nuovo tipo di minaccia, perciò Kaspersky Internet Security classifica l'oggetto come potenzialmente infetto.

L'analizzatore di *codice euristico* intercetta i virus potenziali e identifica fino al 92% dei nuovi virus. Si tratta di un meccanismo piuttosto efficace che raramente produce falsi positivi.

Un oggetto potenzialmente infetto può essere intercettato e trasferito in Quarantena da File Anti-Virus, Mail Anti-Virus , Difesa proattiva o nel corso di una scansione antivirus.

Per trasferire un oggetto in quarantena è sufficiente fare clic sul pulsante **Quarantena** nella notifica visualizzata al rilevamento di un oggetto potenzialmente infetto.

Quando un oggetto viene messo in Quarantena, esso non viene copiato ma trasferito. L'oggetto viene quindi eliminato dal disco o messaggio e salvato nella cartella Quarantena. I file in Quarantena vengono salvati in uno speciale formato e pertanto non sono pericolosi.

17.1.1. Azioni da eseguire sugli oggetti in Quarantena

Il numero totale degli oggetti presenti nella cartella Quarantena è visualizzato in **File dati** nella sezione **Servizi**. Nella parte destra dello schermo si trova uno speciale riquadro *Cartella Quarantena* che indica:

- Il numero dei file potenzialmente infetti intercettati da Kaspersky Internet Security.
- Le dimensioni correnti della cartella Quarantena.

Da qui è possibile eliminare tutti gli oggetti in Quarantena per mezzo del pulsante **Elimina**. Osservare che così facendo si eliminano anche i file presenti nella cartella Backup e i report.

Per accedere agli oggetti in Quarantena:

Fare clic con il pulsante sinistro del mouse su qualsiasi punto del riquadro *Cartella Quarantena*.

Nella scheda Cartella Quarantena (cfr. Figura 75) è possibile compiere le seguenti azioni:

- Trasferire in Quarantena un file sospettato di contenere un'infezione che il programma non ha rilevato facendo clic sul pulsante **Aggiungi** e selezionando il file desiderato nella finestra di selezione. Il file viene aggiunto all'elenco con lo status *Aggiunto dall'utente*.

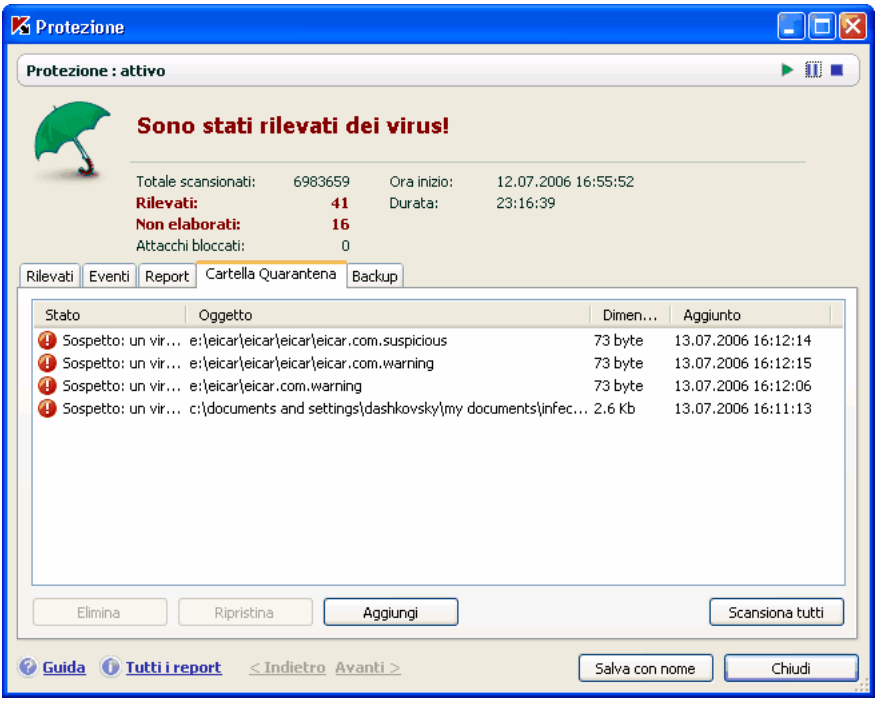


Figura 75. Elenco degli oggetti in Quarantena

- Esaminare e riparare tutti gli oggetti potenzialmente infetti in Quarantena per mezzo di elenchi delle minacce aggiornati facendo clic su **Scansiona tutti**.

  Dopo la scansione e l'eventuale riparazione di oggetti in Quarantena, lo status può diventare *infetto, potenzialmente infetto, falso positivo, OK,* ecc.

  Lo status *infetto* significa che l'oggetto è stato riconosciuto come infetto ma non è stato possibile ripararlo. Si raccomanda di eliminare gli oggetti appartenenti a questa categoria.

  Tutti gli oggetti classificati come *falso positivo* possono essere ripristinati poiché il precedente status di *potenzialmente infetto* non è stato confermato dal programma in seguito alla nuova scansione.

- Ripristinare i file in una cartella selezionata dall'utente o nella cartella in cui si trovavano prima della Quarantena (impostazione predefinita). Per ripristinare un oggetto, selezionarlo dall'elenco e fare clic su **Ripristina**. Durante il ripristino di oggetti da archivi, database di posta e file in

formato posta trasferiti in Quarantena, è necessario selezionare anche la directory in cui ripristinarli.

> Suggerimento:
> Si raccomanda di ripristinare solo gli oggetti classificati con lo di *falso positivo, OK* e *riparato* poiché il ripristino di altri oggetti può provocare l'infezione del computer.

- Eliminare oggetti o gruppi selezionati di oggetti in Quarantena. Eliminare solo gli oggetti che non possono essere riparati. Per eliminare questi oggetti, selezionarli nell'elenco e fare clic su **Elimina**.

17.1.2. Configurazione della Quarantena

È possibile configurare le impostazioni di layout e funzionamento della Quarantena, in particolare:

- Impostare scansioni automatiche di oggetti in Quarantena dopo ogni aggiornamento degli elenchi delle minacce (per ulteriori informazioni, cfr. 15.3.4 a pag. 225).

> Attenzione!
> Se si usa la Quarantena, il programma non è in grado di esaminare gli oggetti isolati subito dopo l'aggiornamento degli elenchi delle minacce.

- Impostare la durata massima della conservazione degli oggetti in Quarantena.

  La durata predefinita è di 30 giorni, allo scadere dei quali gli oggetti vengono eliminati. È possibile modificare la durata di conservazione nella Quarantena o disabilitare del tutto questa limitazione

  procedendo come segue:

  3. Aprire le impostazioni di Kaspersky Internet Security facendo clic su Impostazioni nella finestra principale del programma.
  4. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
  5. Nella sezione **Cartella di Quarantena & Backup** (cfr. Figura 76), digitare il tempo massimo allo scadere del quale gli oggetti isolati saranno automaticamente eliminati.

Figura 76. Configurazione del periodo di conservazione degli oggetti in Quarantena

17.2. Copie di Backup di oggetti pericolosi

A volte, in seguito alla riparazione, gli oggetti perdono la propria integrità. Se un file riparato contiene informazioni importanti e dopo la riparazione risulta parzialmente o completamente corrotto, si può tentare di ripristinare l'oggetto originario da una copia di backup.

Una **copia di backup** è una copia dell'oggetto pericoloso creata prima di riparare o eliminare l'originale. Le copie di backup vengono salvate nella cartella Backup.

La cartella **Backup** è una particolare area di archiviazione che contiene copie di oggetti pericolosi da riparare o eliminare. Il Backup consente di ripristinare l'oggetto originale in qualsiasi momento. I file in Backup vengono salvati in uno speciale formato e pertanto non sono pericolosi.

17.2.1. Azioni da eseguire sulle copie di backup

Il numero totale delle copie di backup è visualizzato in **File dati** nella sezione **Backup**. Nella parte destra dello schermo si trova uno speciale riquadro *Backup* che indica:

- Il numero di copie di backup degli oggetti create da Kaspersky Internet Security.
- Le dimensioni correnti della cartella Backup.

Da qui è possibile eliminare tutte le copie di backup per mezzo del pulsante **Elimina**. Osservare che così facendo si eliminano anche i file presenti nella cartella Quarantena e i report.

Per accedere alle copie di oggetti pericolosi:

Fare clic con il pulsante sinistro del mouse in qualsiasi punto del riquadro *Backup*.

Viene visualizzato un elenco di copie di backup al centro della scheda Backup (cfr. Figura 77). Per ogni copia sono fornite le seguenti informazioni: il nome completo dell'oggetto con il percorso della posizione originaria, lo status dell'oggetto assegnato dalla scansione e le sue dimensioni.

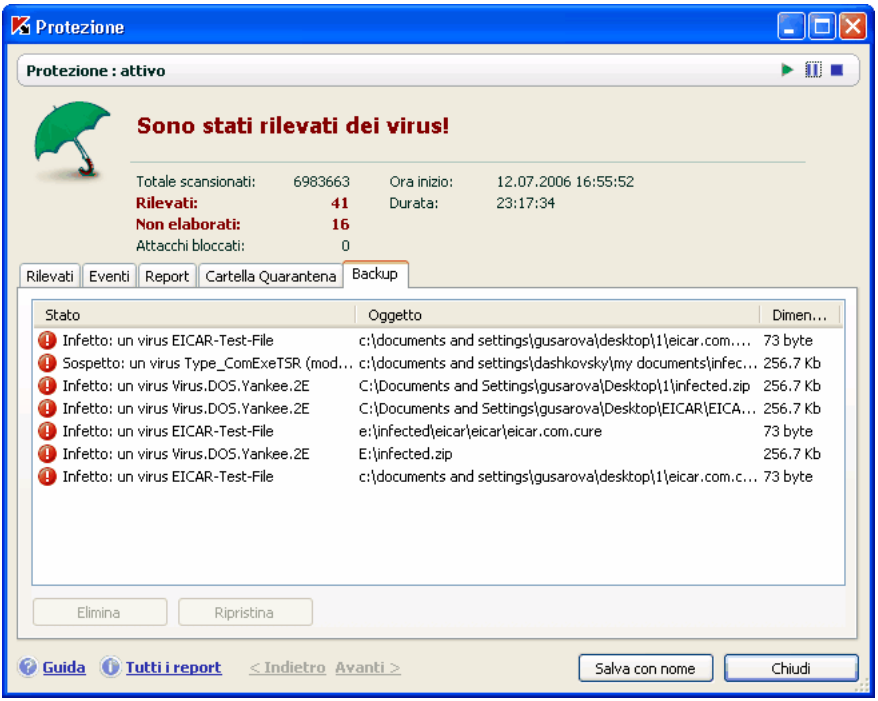


Figura 77. Copie di backup di oggetti eliminati o riparati

È possibile ripristinare le copie selezionate per mezzo del pulsante **Ripristina**. L'oggetto viene così ripristinato dalla cartella Backup con lo stesso nome dell'originale prima della riparazione.

Se esiste già un oggetto con quel nome nella posizione originaria (ciò è possibile se prima della riparazione è stata creata una copia dell'oggetto che si desidera ripristinare), viene visualizzato un apposito messaggio. È possibile quindi cambiare posizione all'oggetto da ripristinare oppure rinominarlo.

Si raccomanda di sottoporre l'oggetto a scansione antivirus subito dopo il ripristino. È possibile che le firme aggiornate consentano di ripulirlo senza perdere l'integrità del file.

Si sconsiglia di ripristinare le copie di backup degli oggetti se non strettamente necessario. Ciò potrebbe provocare l'infezione del computer.

Si raccomanda di esaminare periodicamente la cartella Backup e di vuotarla servendosi del pulsante **Elimina**. È possibile inoltre configurare il programma in modo da eliminare automaticamente dal Backup le copie di più vecchia data (cfr. 17.2.2 a pag. 236).

17.2.2. Configurazione delle impostazioni del Backup

È possibile definire la durata massima di conservazione nella cartella Backup.

La durata predefinita è di 30 giorni, allo scadere dei quali le copie vengono eliminate. È possibile inoltre modificare la durata di conservazione o disabilitare del tutto questa limitazione procedendo come segue:

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
3. Impostare la durata della conservazione delle copie di backup dalla sezione **Cartella di Quarantena e Backup** (cfr. Figura 76) nella parte destra della finestra.

17.3. Report

Le azioni dei componenti di Kaspersky Internet Security e le attività di scansione anvirus sono registrate in appositi report.

Il numero totale dei report creati dal programma e le loro dimensioni totali sono visualizzati in **File dati** nella sezione **Servizi** della finestra principale del programma. Queste informazioni sono indicate nel riquadro *Report*.

Per visualizzare i report:

Fare clic con il pulsante sinistro del mouse in qualsiasi punto del riquadro *Report*.

Si apre una finestra contenente, tra le altre, la scheda **Report** (cfr. Figura 78). Essa contiene i report più recenti su tutti i componenti e le attività di scansione antivirus eseguite durante la sessione corrente di Kaspersky Internet Security. Le informazioni sono visualizzate facendo clic sul nome di ciascun componente o attività. Per esempio, *disabilitato* o *completato*. Se si desidera visualizzare la cronologia completa della creazione dei report per la sessione corrente del programma, selezionare la casella ☑ **Mostra cronologia report**.

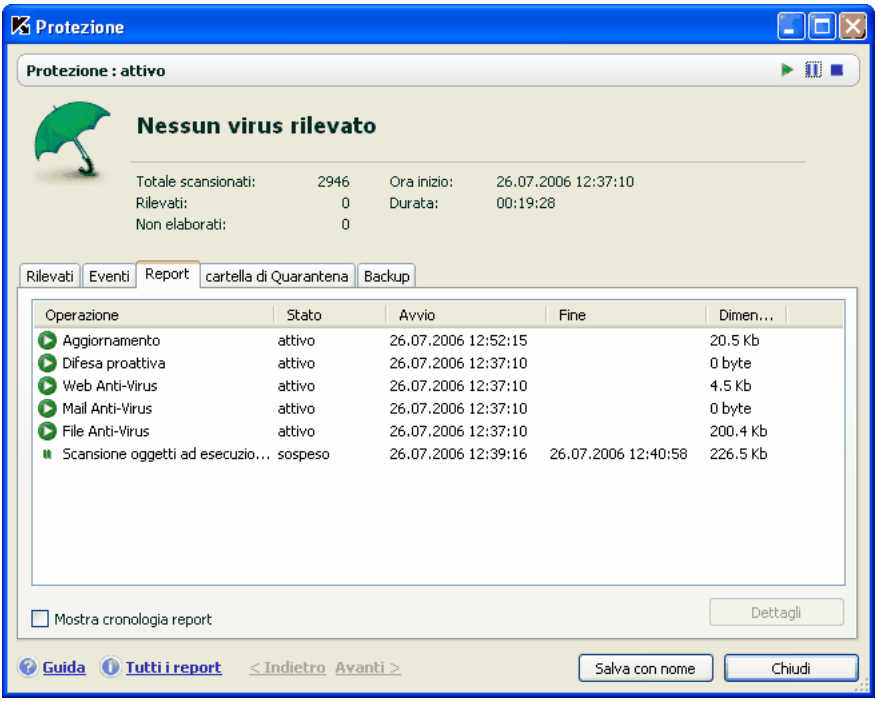


Figura 78. Report sul funzionamento dei componenti

Per consultare tutti gli eventi registrati nel report di un componente o attività:

Selezionare il nome del componente o attività nella scheda **Report** e fare clic sul pulsante **Dettagli**.

Si apre una finestra contenente informazioni dettagliate sulle prestazioni del componente o attività selezionati. Le statistiche sulle prestazioni sono visualizzate nella parte superiore della finestra, mentre le informazioni dettagliate sono riportate nelle schede. Le schede sono diverse a seconda del componente o attività:

- La scheda **Rilevati** contiene un elenco di oggetti pericolosi individuati da un componente o da un'attività di scansione antivirus.
- La scheda **Eventi** visualizza gli eventi relativi al componente o attività.
- La scheda **Statistiche** contiene le statistiche dettagliate su tutti gli oggetti esaminati.

- La scheda **Impostazioni** visualizza le impostazioni utilizzate da componenti di protezione, scansioni antivirus o aggiornamenti degli elenchi delle minacce.
- Le schede **Macro** e **Registro** sono presenti solo nel report di Difesa proattiva e contengono informazioni su tutte le macro di cui è stata tentata l'esecuzione sul computer e su tutti i tentativi di modificare il registro del sistema operativo.
- Le schede **Phishing**, **Popup**, **Banner** e **Connessioni dialer** sono presenti solo nel report di Anti-Spy. Esse contengono informazioni su tutti gli attacchi di phishing intercettati e su tutti i popup, i banner e i tentativi di connessione dialer bloccati durante la sessione.
- Le schede **Attacchi di rete**, **Host banditi**, **Attività dell'applicazione** e **Filtro pacchetti** sono presenti solo nel report di Anti-Hacker. Esse contengono informazioni su tutti i tentativi di attacco di rete al computer e sugli host banditi in seguito ad attacchi, e le descrizioni delle attività di rete delle applicazioni che corrispondono alle regole di attività create, e tutti i pacchetti dati che corrispondono alle regole per filtro pacchetti di Anti-Hacker.
- Le schede **Connessioni stabilite**, **Porte aperte** e **Traffico** coprono inoltre l'attività di rete del computer, visualizzando le connessioni correnti, le porte aperte e la quantità di traffico inviato e ricevuto dal computer.

I report possono essere interamente esportati in formato testo. Questa funzione è utile nei casi in cui in un componente o attività si è verificato un errore impossibile da eliminare autonomamente, per il quale si necessita di assistenza tecnica. In tali casi è necessario inviare il report in formato .txt al servizio di Assistenza tecnica per consentire ai nostri specialisti di studiare approfonditamente il problema e risolverlo nel più breve tempo possibile.

Per esportare un report in formato testo:

Fare clic su **Salva con nome** e specificare dove si desidera salvare il file del report.

Al termine del lavoro con il report, fare clic su **Chiudi**.

Esiste un pulsante **Azioni** su tutte le schede ad eccezione di **Impostazioni** e **Statistiche**, che può essere utilizzato per definire le reazioni agli oggetti presenti nell'elenco. Facendo clic su di esso, si apre un menu contestuale con i seguenti elementi di menu (il menu è diverso a seconda del componente; di seguito sono elencate tutte le opzioni possibili):

Neutralizza – il programma cerca di riparare l'oggetto pericoloso. Se la riparazione non va a buon fine, è possibile lasciare l'oggetto nell'elenco per esaminarlo in seguito con gli elenchi delle minacce aggiornati oppure eliminarlo.

Elimina – l'oggetto viene eliminato dall'elenco.

Aggiungi a zona attendibile – l'oggetto viene escluso dalla protezione. Si apre una finestra con una regola di esclusione per l'oggetto.

Vai a file – si apre la cartella in cui è stato salvato l'oggetto in Windows Explorer.

Neutralizza tutti – tutti gli oggetti presenti nell'elenco vengono neutralizzati. Kaspersky Internet Security cerca di elaborare gli oggetti per mezzo degli elenchi delle minacce.

Pulisci tutti – il report sugli oggetti rilevati viene azzerato. Con questa funzione, tutti gli oggetti pericolosi rilevati restano nel computer.

Cerca www.viruslist.ru – si apre una descrizione dell'oggetto nell'enciclopedia dei virus del sito web Kaspersky Lab.

Cerca www.google.com – vengono cercate informazioni sull'oggetto utilizzando questo motore di ricerca.

Cerca – consente di inserire parole chiave per la ricerca per nome o per status di oggetti presenti nell'elenco.

Inoltre è possibile organizzare le informazioni visualizzate in ordine crescente o decrescente per ciascuna colonna.

17.3.1. Configurazione delle impostazioni dei report

Per configurare le impostazioni di creazione e salvataggio dei reports:

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic su Impostazioni nella finestra principale del programma.
2. Selezionare **File dati** dalla struttura ad albero delle impostazioni.
3. Configurare il riquadro **Report** (cfr. Figura 79) come segue:
   - Consentire o disabilitare la registrazione di eventi informativi. Questi eventi di solito non sono rilevati ai fini della sicurezza. Per registrare gli eventi, selezionare la casella ☑ **Registra eventi non critici**.
   - Scegliere di salvare nel report solo gli eventi verificatisi successivamente all'ultima scansione. Questa impostazione consente di salvare spazio su disco riducendo le dimensioni del report. Se la casella ☑ **Salva solo eventi recenti** è selezionata, le informazioni contenute nel report saranno salvate ogni volta che si riavvia l'attività. Tuttavia saranno sovrascritte solo le informazioni non critiche.

- Impostare la durata della conservazione dei report. La durata predefinita è di 30 giorni, allo scadere dei quali i report vengono eliminati. È possibile modificare la durata massima di conservazione o disabilitare del tutto questa limitazione

Figura 79. Configurazione delle impostazioni dei report

17.3.2. La scheda *Rilevati*

Questa scheda (cfr. Figura 80) contiene un elenco di oggetti pericolosi rilevati da Kaspersky Internet Security. Per ogni oggetto è indicato il nome completo, accompagnato dallo status assegnatogli dal programma in seguito alla scansione o all'elaborazione.

Se si desidera che l'elenco contenga sia gli oggetti pericolosi sia quelli neutralizzati con successo, selezionare la casella **Mostra oggetti neutralizzati**.

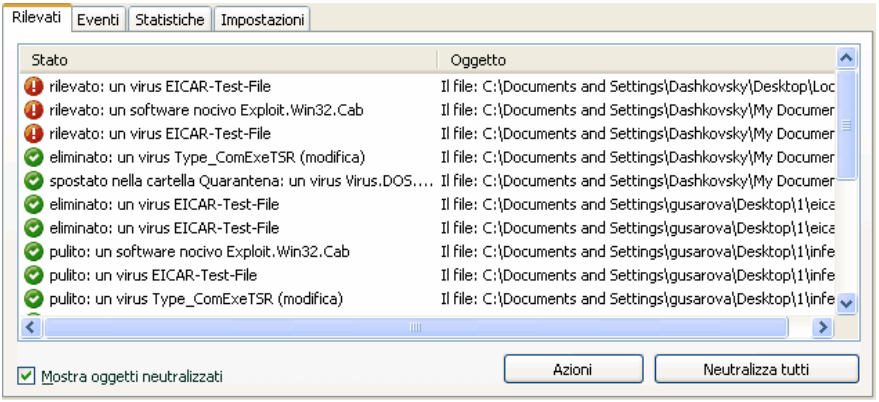


Figura 80. Elenco degli oggetti pericolosi rilevati

17.3.3. La scheda *Eventi*

Questa scheda (cfr. Figura 81) contiene un elenco completo degli eventi importanti verificatisi durante il funzionamento di un componente, la scansione

antivirus e gli aggiornamenti degli elenchi delle minacce non ignorati da una regola di controllo delle attività (cfr. 10.1.1 a pag. 127).

Questi eventi possono essere:

Eventi critici – eventi di importanza critica che segnalano problemi di funzionamento del programma o vulnerabilità del computer. Per esempio, *virus rilevato*, *errore di funzionamento*.

Eventi importanti – eventi da approfondire poiché riflettono situazioni importanti nel funzionamento del programma. Per esempio, *terminato.*

Messaggi informativi – messaggi di riferimento che di solito non contengono informazioni rilevanti. Per esempio, *OK, non elaborato*. Questi eventi sono riportati nel registro eventi solo se la casella ☑ **Mostra eventi non critici**.

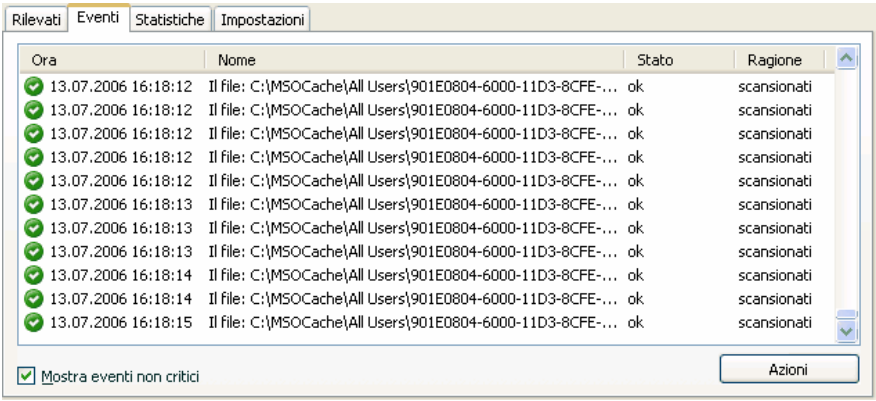


Figura 81. Eventi che si verificano durante il funzionamento di un componente

Il formato di visualizzazione degli eventi nel registro può variare in base al componente o all'attività. Per ogni attività di aggiornamento sono riportate le seguenti informazioni:

- Nome dell'evento
- Nome dell'oggetto interessato dall'evento
- L'ora in cui si è verificato l'evento
- Le dimensioni del file caricato

Per le attività di scansione antivirus, il registro degli eventi contiene il nome dell'oggetto esaminato e lo status assegnatogli in seguito alla scansione/elaborazione.

È possibile inoltre addestrare Anti-Spam durante la visualizzazione del report per mezzo dell'apposito menu contestuale. Per fare ciò, selezionare il nome del messaggio e aprire il menu contestuale facendo clic con il pulsante destro del mouse, quindi selezionare **Segna come spam** se il messaggio è indesiderato, o **Segna come non spam** se il messaggio selezionato rientra tra quelli accettati. Inoltre, in base alle informazioni ottenute analizzando il messaggio, è possibile aggiungerlo alle liste bianche o alle liste nere di Anti-Spam. Per fare questo servirsi degli elementi corrispondenti nel menu contestuale.

17.3.4. La scheda *Statistiche*

Questa scheda (cfr. Figura 82) contiene le statistiche dettagliate sui componenti e le attività di scansione antivirus. Da questa finestra risulta:

- Quanti oggetti sono stati esaminati in cerca di tratti pericolosi nella sessione corrente di un componente o dopo il completamento di un'attività. Il numero degli archivi, dei file compressi e degli oggetti protetti da password e corrotti esaminati.
- Quanti oggetti pericolosi sono stati rilevati, non riparati, eliminati e trasferiti in Quarantena.

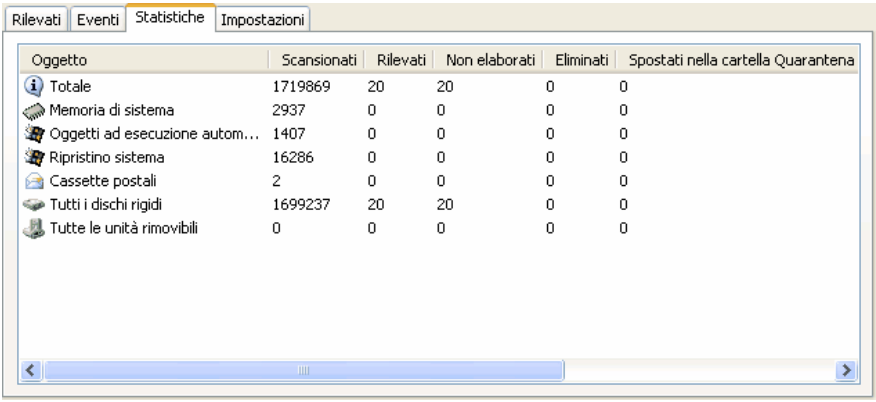


Figura 82. Statistiche dei componenti

17.3.5. La scheda Impostazioni

La scheda **Impostazioni** (cfr. Figura 83) visualizza l'elenco completo delle impostazioni dei componenti, delle scansioni antivirus e degli aggiornamenti del programma. È possibile vedere il livello di esecuzione di un componente o di una scansione antivirus, le azioni compiute sugli oggetti pericolosi o le impostazioni

in uso per gli aggiornamenti del programma. Usare il link Modifica impostazioni per configurare il componente.

È possibile configurare impostazioni avanzate per le scansioni antivirus:

- Stabilire la priorità delle attività di scansione in caso di sovraccarico sul processore. L'impostazione predefinita per **Sospendi scansione anti-virus quando la CPU è occupata da altre applicazioni** è deselezionata. Con questa funzione, il programma individua il carico sul processore e sui sottosistemi del disco per l'attività di altre applicazioni. Se il carico sul processore aumenta considerevolmente e impedisce alle applicazioni dell'utente di funzionare normalmente, il programma riduce l'attività di scansione. In tal modo si riduce il tempo di scansione e si liberano risorse per le applicazioni dell'utente.

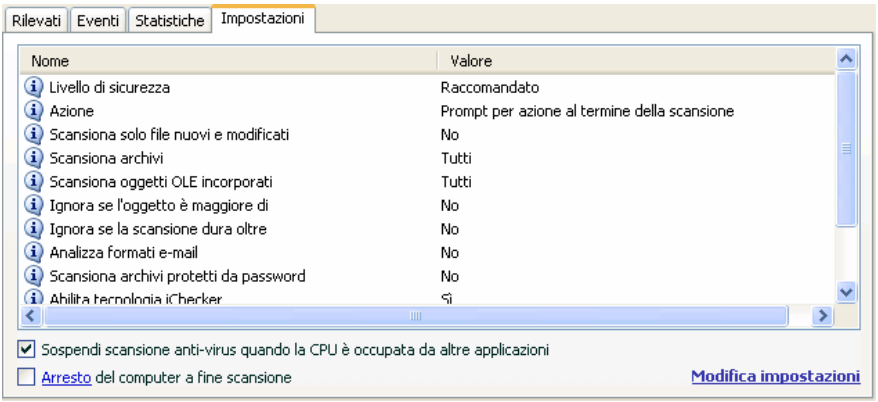


Figura 83. Impostazioni dei componenti

- Impostare la modalità operativa del computer per il periodo successivo al completamento della scansione antivirus. È possibile configurare il computer in modo da spegnersi, riavviarsi o funzionare in standby o in modalità di risparmio. Per selezionare un'opzione, fare clic con il pulsante sinistro del mouse sull'ipertesto fino a visualizzare l'opzione desiderata.

  Questa funzione può risultare utile se, per esempio, si avvia una scansione antivirus al termine della giornata lavorativa e non si desidera aspettarne la conclusione.

  Tuttavia, per poter utilizzare questa funzione è necessario eseguire i seguenti passaggi supplementari: prima di lanciare la scansione è necessario disabilitare le richieste di password per gli oggetti esaminati, se abilitata, e abilitare l'elaborazione automatica degli oggetti pericolosi. Le funzioni interattive del programma saranno quindi disabilitate e il

programma non richiederà più l'intervento dell'utente interrompendo il processo di scansione.

17.3.6. La scheda *Macro*

Tutte le macro che tentano di aprirsi durante la sessione corrente di Kaspersky Internet Security sono elencate nella scheda **Macro** (cfr. Figura 84). Essa contiene il nome completo di ogni macro, l'ora in cui è stata eseguita e lo status ottenuto dopo l'elaborazione.

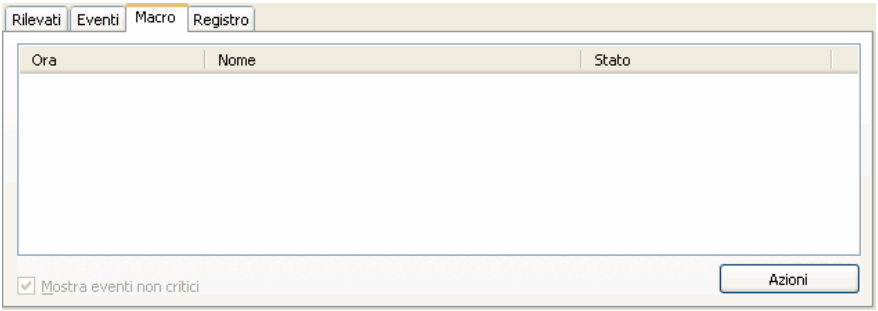


Figura 84. List of dangerous macros detected

17.3.7. La scheda *Registro*

Il programma registra nella scheda **Registro** le operazioni con le chiavi di registro che sono state tentate dall'avvio del programma, a meno che non fossero proibite da una regola (cfr. Figura 85).

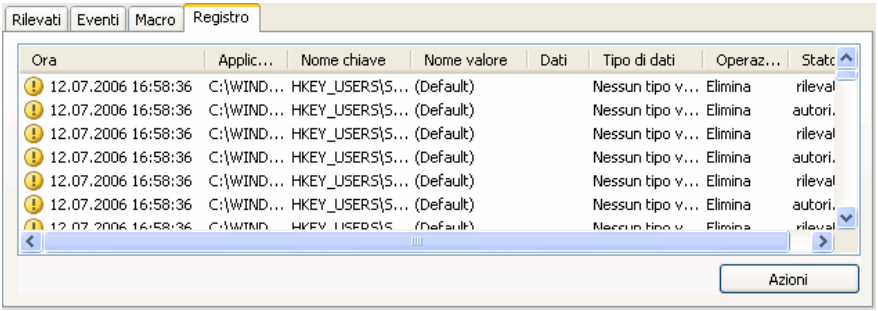


Figura 85. Lettura e modifica degli eventi del registro di sistema

La scheda riporta il nome completo della chiave, il suo valore, il tipo di dati e le informazioni relative all'operazione che ha avuto luogo: l'azione tentata, l'ora e l'eventuale autorizzazione.

17.3.8. La scheda *Phishing*

Questa scheda di report (cfr. Figura 86) visualizza tutti i tentativi di phishing eseguiti durante la sessione corrente di Kaspersky Internet Security. Il report contiene un link al sito di phishing rilevato nel messaggio, la data e l'ora di intercettazione dell'attacco e lo status dell'attacco (se è stato bloccato oppure no).

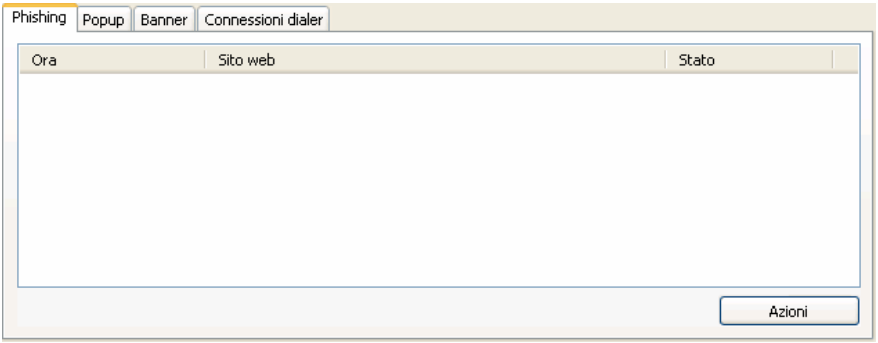


Figura 86. Attacchi di phishing bloccati

17.3.9. La scheda *Popup*

Questa scheda di report (cfr. Figura 87) elenca gli indirizzi di tutti i popup bloccati da Anti-Spy. Si tratta generalmente di finestre che si aprono dai siti web.

Per ognuno di essi sono registrati l'indirizzo e la data in cui Popup Blocker ha bloccato la finestra.

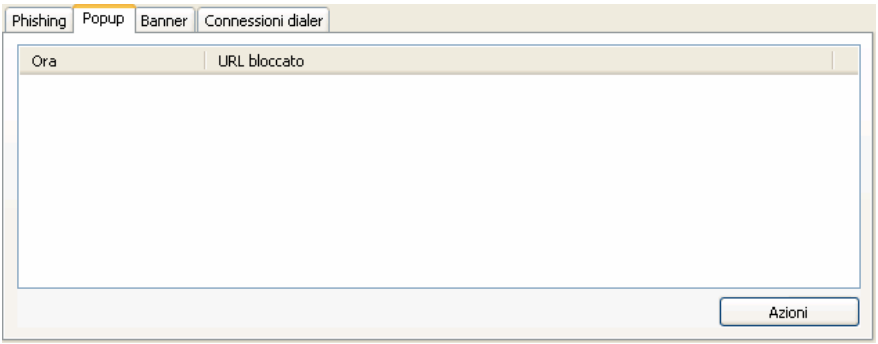


Figura 87. Elenco dei popup bloccati

17.3.10. La scheda *Banner*

Questa scheda di report (cfr. Figura 88) contiene gli indirizzi dei banner rilevati da Kaspersky Internet Security nella sessione corrente. Per ogni banner è riportato l'indirizzo web accompagnato dallo status di elaborazione (banner bloccato o visualizzato).

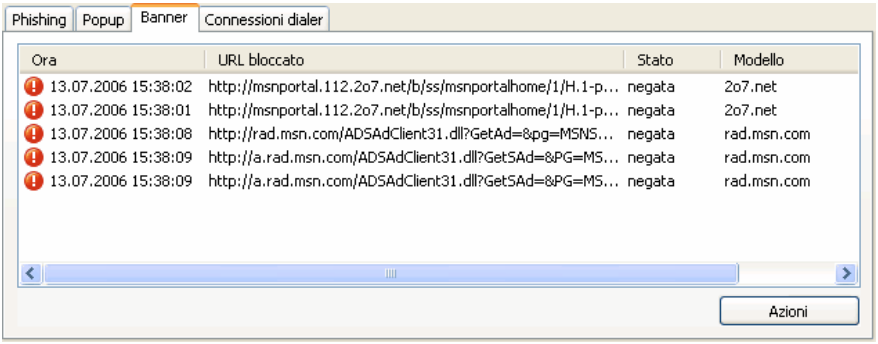


Figura 88. Elenco dei banner bloccati

È possibile consentire la visualizzazione dei banner bloccati selezionando l'oggetto desiderato dall'elenco e facendo clic su **Azioni** → **Autorizza**.

17.3.11. La scheda Connessioni dialer

Questa scheda (cfr. Figura 89) visualizza tutti i tentativi dei dialer di connettersi a siti web a pagamento. Tali tentativi vengono generalmente eseguiti da programmi nocivi installati sul computer.

Il report indica il programma che ha tentato di formulare il numero per connettersi a Internet e lo status del tentativo: bloccato o autorizzato.

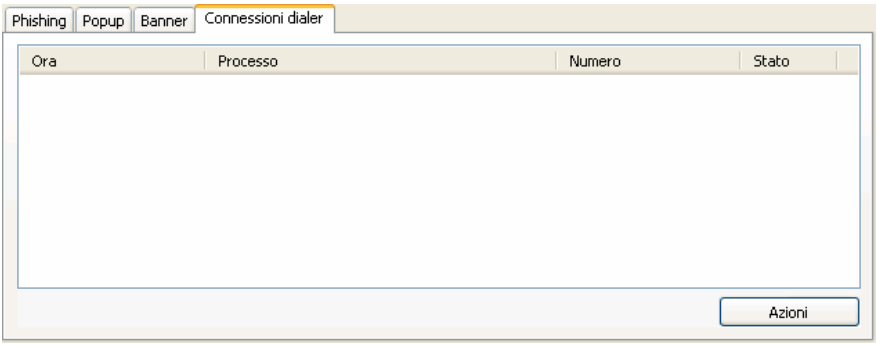


Figura 89. Elenco dei tentativi di connessioni dialer

17.3.12. La scheda Attacchi di rete

Questa scheda (cfr. Figura 90) visualizza una breve sintesi degli attacchi di rete al computer. Questa informazione viene registrata se è stato abilitato Intrusion Detector, che monitora tutti i tentativi di attacco perpetrati al computer.

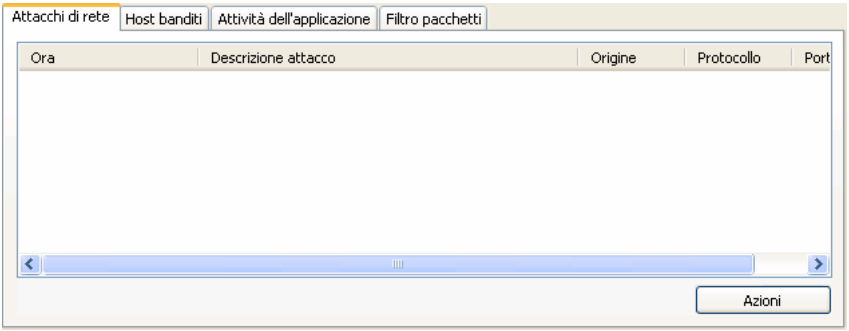


Figura 90. Elenco degli attacchi di rete bloccati

La scheda *Attacchi di rete* elenca le seguenti informazioni sugli attacchi:

- Provenienza dell'attacco. Può essere un indirizzo IP, un host, ecc.
- La porta locale sulla quale è stato tentato l'attacco al computer.
- Una breve descrizione dell'attacco.
- L'ora in cui l'attacco è stato tentato.

17.3.13. La scheda Host banditi

Tutti gli host bloccati dopo l'intercettazione di un attacco da parte di Intrusion Detector sono elencati in questa scheda di report (cfr. Figura 91).

Sono visualizzati anche il nome di ogni host e l'ora in cui sono stati banditi. Da questa scheda è possibile sbloccare gli host selezionando l'host dall'elenco e facendo clic sul pulsante **Azioni** → **Blocca**.

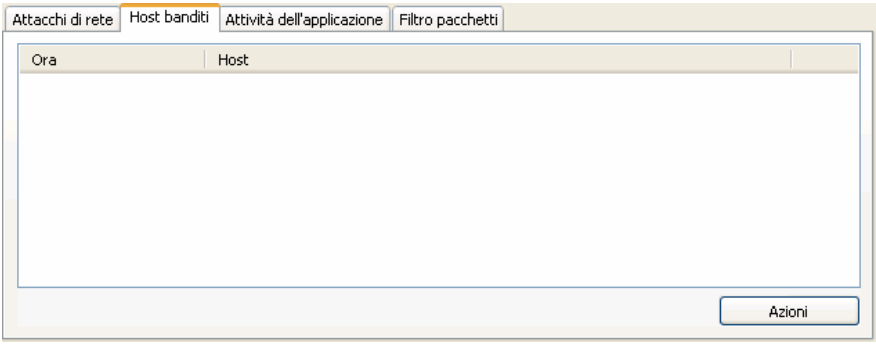


Figura 91. Elenco degli host bloccati

17.3.14. La scheda Attività dell'applicazione

Se Kaspersky Internet Security usa un firewall, tutte le applicazioni con azioni che corrispondono alle regole per le applicazioni e che sono state registrate durante la sessione corrente del programma sono elencate nella scheda **Attività dell'applicazione** (cfr. Figura 92).

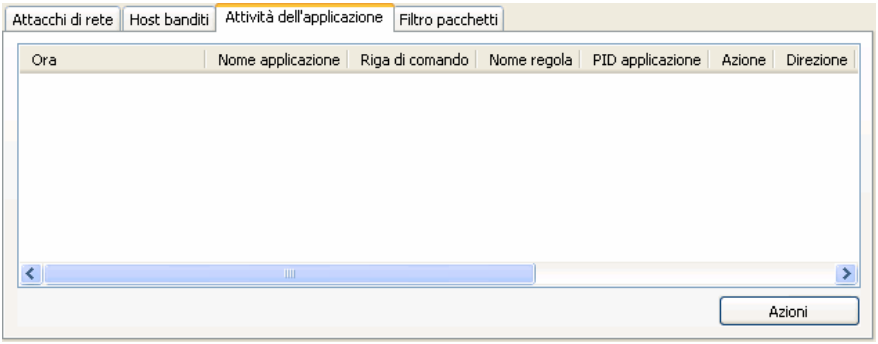


Figura 92. Attività dell'applicazione monitorata

L'attività è registrata solo se nella regola è stata selezionata l'opzione **Registro**. Essa è selezionata nelle regole per applicazioni incluse in Kaspersky Internet Security.

Questa scheda visualizza le proprietà di base di ogni applicazione (nome, PID, nome della regola) e una breve sintesi della relativa attività (protocollo, direzione dei pacchetti, ecc.). Inoltre sono visualizzate informazioni relative all'eventuale blocco dell'attività dell'applicazione.

17.3.15. La scheda Filtro pacchetti

Tutti i pacchetti inviati e ricevuti che corrispondono a una regola per filtro pacchetti e sono stati registrati durante la sessione corrente di Kaspersky Internet Security sono elencati nella scheda **Filtro pacchetti** (cfr. Figura 93).

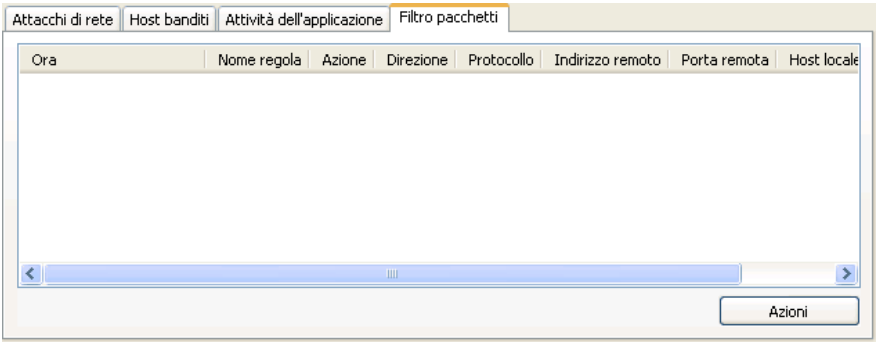


Figura 93. Pacchetti dati monitorati

L'attività è registrata solo se nella regola è stata selezionata l'opzione **Registro**. Essa è deselezionata nelle regole per filtro pacchetti incluse in Kaspersky Internet Security.

Per ogni pacchetto sono indicati inoltre il nome dell'applicazione che ha iniziato l'invio o la ricezione, il risultato del filtraggio (l'eventuale blocco del pacchetto), la direzione del pacchetto, il protocollo e altre impostazioni della connessione di rete per l'invio e la ricezione di pacchetti.

17.3.16. La scheda Connessioni stabilite

Tutte le connessioni di rete attive correnti stabilite dal computer sono elencate nella scheda **Connessioni stabilite** (cfr. Figura 94). Questa scheda riporta il nome dell'applicazione che ha iniziato la connessione, il protocollo usato, la direzione della connessione (in entrata o in uscita) e le impostazioni di connessione (porte locali e remote e indirizzi IP). Inoltre è possibile vedere per quanto tempo una connessione è stata attiva e il volume dei dati inviati e ricevuti. È possibile creare una regola di connessione o eliminarla utilizzando le apposite opzioni nel menu contestuale, accessibile facendo clic con il pulsante destro del mouse sull'elenco delle connessioni.

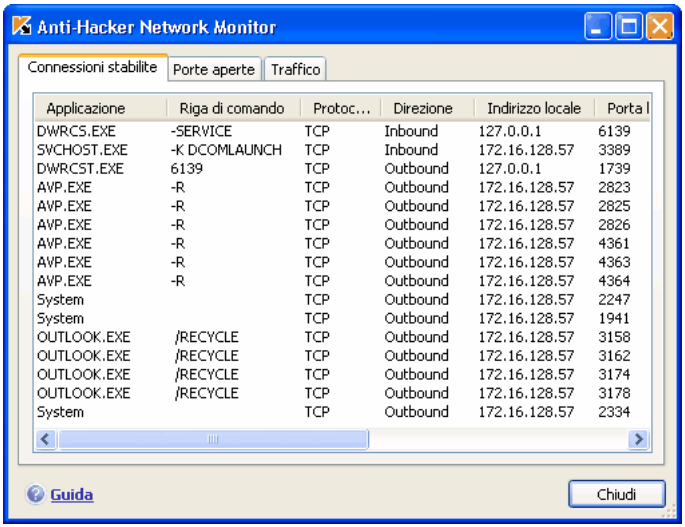


Figura 94. Elenco delle connessioni stabilite

17.3.17. La scheda Porte aperte

Tutte le porte correntemente aperte sul computer per le connessioni di rete sono elencate nella scheda *Porte aperte* (cfr. Figura 95). Essa elenca per ciascuna porta il numero, il protocollo di trasferimento dati, il nome dell'applicazione che la usa e per quanto tempo la porta è rimasta aperta.

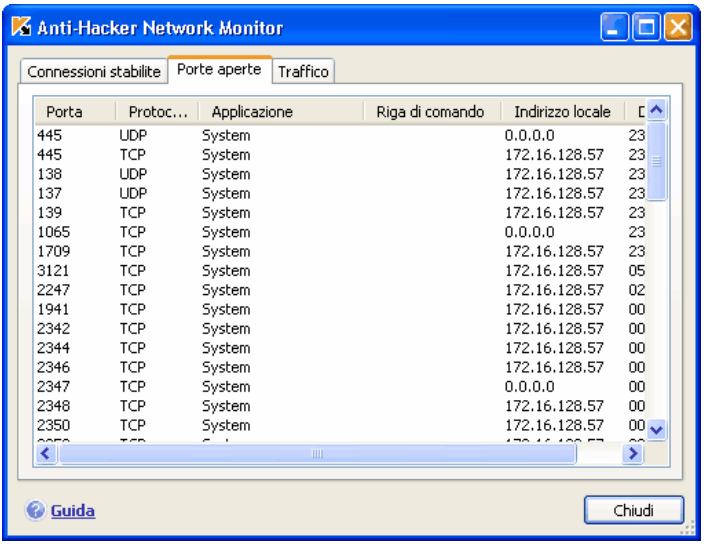


Figura 95. Elenco delle porte aperte del computer

Questo tipo di informazione può essere utile durante le epidemie virali e gli attacchi di rete, per conoscere esattamente quali porte sono vulnerabili. In tal modo è possibile sapere quale porta è aperta e adottare le misure necessarie alla protezione del computer (per esempio abilitando Intrusion Detector, chiudendo la porta vulnerabile o creando una regola per quest'ultima).

17.3.18. La scheda *Traffico*

Questa scheda (cfr. Figura 96) contiene informazioni su tutte le connessioni in entrata e in uscita stabilite tra il computer dell'utente e altri computers, compresi server web, server di posta, ecc. Per ciascuna connessione sono indicate le seguenti informazioni: nome e indirizzo IP dell'host con cui si è connessi, e la quantità di traffico inviato e ricevuto.

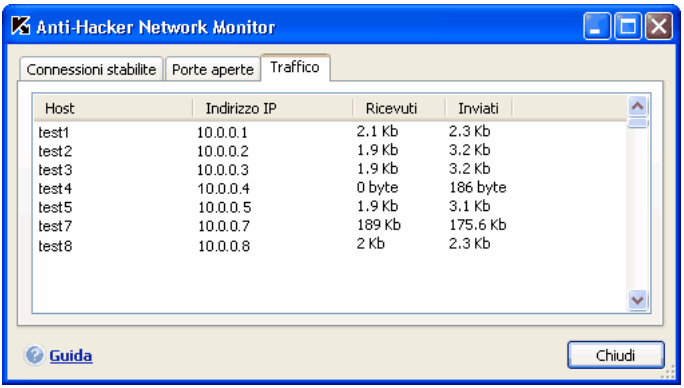


Figura 96. Traffico sulle connessione di rete stabilite

17.4. Informazioni generali sul programma

È possibile visualizzare informazioni di carattere generale sul programma nella sezione **Servizi** della finestra principale (cfr. Figura 97).

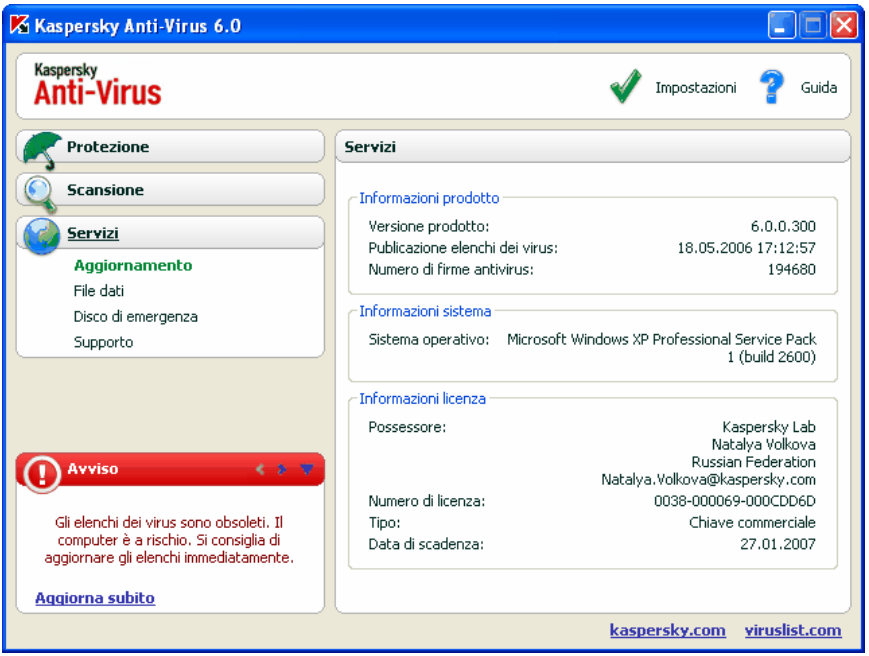


Figura 97. Informazioni sul programma, la licenza e il sistema

Tutte le informazioni sono suddivise in tre sezioni:

- La versione del programma, la data dell'ultimo aggiornamento e il numero delle minacce note sono visualizzati nel riquadro **Informazioni prodotto**.
- Le informazioni di base sulla licenza acquistata per Kaspersky Internet Security sono visualizzate nel riquadro **Informazioni licenza**.
- Le informazioni di base sul sistema operativo installato sul computer sono visualizzate nel riquadro **Informazioni sistema**.

Tutte queste informazioni sono necessarie qualora ci si rivolga al servizio di assistenza tecnica di Kaspersky Lab (cfr. 17.5 a pag. 254).

17.5. Estensione della licenza

Per funzionare, Kaspersky Internet Security necessita di una *chiave di licenza*. La chiave, fornita sulla base di un codice di attivazione, dà diritto all'uso del programma dal giorno dell'acquisto e dell'installazione della chiave stessa.

Alla scadenza della chiave di licenza, il programma continua a funzionare ma non è in grado di scaricare gli aggiornamenti degli elenchi delle minacce. Come in precedenza, è possibile continuare a scansionare il computer e a usare i componenti di protezione, ma utilizzando solo gli elenchi delle minacce installati al momento della scadenza della chiave. Pertanto non siamo in grado di garantire la protezione del computer dai virus diffusi successivamente alla scadenza della licenza d'uso del programma.

Per evitare di infettare il computer con nuovi virus, si raccomanda di estendere la licenza di Kaspersky Internet Security. Due settimane prima della scadenza, il programma visualizza un apposito messaggio e continuerà a visualizzarlo per due settimane ogni volta che lo si avvia.

Per estendere la licenza è necessario ottenere un nuovo codice di attivazione procedendo come segue:

1. Rivolgersi al rivenditore presso il quale si è acquistato il prodotto e acquistare un codice di attivazione.

oppure

Acquistare un codice di attivazione direttamente da Kaspersky Lab facendo clic sul link Acquista licenza nella finestra della chiave di licenza (cfr. Figura 98). Compilare quindi il modulo sul nostro sito web. Dopo aver effettuato il pagamento, invieremo un codice di attivazione all'indirizzo e-mail indicato nel modulo d'ordine.

Figura 98. Informazioni sulla licenza

Kaspersky Lab offre regolarmente speciali tariffe per il rinnovo delle licenze sui nostri prodotti. Cercate le offerte speciali sul sito web Kaspersky Lab nelle sezioni **Products → Sales and special offers**.

2. Attivare il programma per mezzo del codice di attivazione procedendo come segue:

   a. Selezionare la sezione **Servizi** della finestra principale del programma e fare clic con il pulsante sinistro su un punto qualsiasi del riquadro **Informazioni licenza**.

   b. Se si desidera estendere la licenza con una chiave di licenza, fare clic sul pulsante **Aggiungi** nella finestra **Informazioni licenza** e selezionare la nuova chiave di licenza nella finestra di selezione standard.

   c. Se si dispone di un codice di attivazione del programma, fare clic sul pulsante **Attiva** nella finestra di gestione delle licenze e attivare il programma per mezzo della procedura guidata.

17.6. Supporto tecnico

Kaspersky Internet Security offre una vasta serie di opzioni per porgere domande e risolvere problemi relativi al funzionamento del programma. Esse sono disponibili in **Supporto** (cfr. Figura 99) nella sezione **Servizi**.

Figura 99. Informazioni sul servizio di assistenza tecnica

A seconda del problema riscontrato, siamo in grado di offrire diversi servizi di assistenza tecnica:

Forum utenti. A questa risorsa è dedicata un'apposita sezione del sito web Kaspersky Lab con domande, commenti e suggerimenti da parte degli utenti del programma. È possibile consultare i principali argomenti del forum ed eventualmente lasciare un commento. Il sito potrebbe contenere anche la soluzione del problema dell'utente.

Per accedere a questa risorsa seguire il link Forum utenti.

Assistenza tecnica online. Anche a questa risorsa è dedicata una sezione apposita del sito web Kaspersky Lab; essa contiene i consigli dei tecnici dell'assistenza sull'uso del software Kaspersky Lab e le risposte alle

domande più comuni. È una valida risorsa per trovare la risposta a una domanda o la soluzione a un problema.

Per ottenere assistenza tecnica online, seguire il link Domande frequenti (FAQ).

Commenti sul funzionamento del programma. Questo servizio è concepito per l'invio di commenti o la descrizione di problemi presentatisi durante l'uso del programma. Per avvalersi di questo servizio è necessario compilare un apposito modulo sul sito web dell'azienda e descrivere in dettaglio la situazione. Per affrontare il problema in maniera efficiente, Kaspersky Lab necessita di alcune informazioni sul computer. A tal fine è possibile descrivere il sistema o usare l'applicazione del computer studiata per raccogliere le informazioni richieste.

Per aprire il modulo dei commenti seguire il link Inviare un report sugli errori o un suggerimento.

Assistenza tecnica. Se si necessita di assistenza immediata con Kaspersky Anti-Virus, chiamare il numero indicato per l'assistenza tecnica internazionale.

17.7. Creazione di un elenco delle porte monitorate

Durante l'uso di component come Mail Anti-Virus, Web Anti-Virus, Anti-Spy e Anti-Spam, vengono monitorati i flussi di dati trasmessi mediante protocolli specifici attraverso determinate porte aperte del computer. Così, per esempio, Mail Anti-Virus analizza le informazioni trasmesse per mezzo del protocollo SMTP mentre Web Anti-Virus analizza quelle trasmesse mediante HTTP.

Il pacchetto del programma include un elenco delle porte più utilizzate per la trasmissione della posta e del traffico HTTP. È possibile aggiungere una nuova porta o disabilitare il monitoraggio di una esistente disabilitando in tal modo il rilevamento di oggetti pericolosi del traffico che passa attraverso la porta in questione.

Per modificare l'elenco delle porte monitorate procedere come segue:

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic sul link Impostazioni nella finestra principale del programma.
2. Selezionare **Impostazioni di rete** nella sezione **Servizi** della struttura ad albero delle impostazioni del programma.

3. Nella parte destra della finestra delle impostazioni, fare clic su **Impostazioni delle porte**.

4. Modificare l'elenco delle porte monitorate nella finestra che si apre (cfr. Figura 100).

Figura 100. Elenco delle porte monitorate

Per aggiungere una nuova porta all'elenco delle porte monitorate:

1. Fare clic sul pulsante **Aggiungi** nella finestra **Impostazioni delle porte**.

2. Digitare il numero della porta e una descrizione della stessa negli appositi campi della finestra **Nuova porta**.

Per esempio, il computer possiede una porta non standard attraverso la quale vengono scambiati dati con un computer remoto per mezzo del protocollo HTTP. Web Anti-Virus monitora il traffico HTTP. Per analizzare questo traffico in cerca di codici nocivi, è possibile aggiungere la porta a un elenco di porte controllate.

All'avvio di uno qualsiasi dei suoi componenti, Kaspersky Internet Security apre la porta 1110 come porta di ascolto per tutte le connessioni in entrata. Se in quel momento la porta è occupata, seleziona le porte 1111, 1112, ecc.

Se si utilizzano simultaneamente Kaspersky Internet Security e il firewall di un altro fabbricante, è necessario configurare il firewall in modo da autorizzare il processo *avp.exe* (processo interno di Kaspersky Internet Security) su tutte le porte sopra elencate.

Poniamo ad esempio che il firewall contenga una regola per *iexplorer.exe* che autorizza quel processo a stabilire connessioni sulla porta 80.

Quando Kaspersky Internet Security intercetta la richiesta di connessione iniziata da *iexplorer.exe* sulla porta 80, la trasferisce su *avp.exe* che, a sua volta, cerca di stabilire indipendentemente una connessione con la pagina web. In assenza di regole di autorizzazione per *avp.exe*, il firewall blocca la richiesta e l'utente quindi non è in grado di accedere alla pagina web.

17.8. Controllo della connessione SSL

Le connessioni effettuate con il protocollo SSL proteggono lo scambio di dati tramite Internet. Il protocollo SSL è in grado di identificare le parti che si scambiano dati tramite certificati elettronici, crittografare i dati trasferiti e garantirne l'integrità durante il trasferimento.

Queste funzioni del protocollo vengono utilizzate dai pirati informatici per diffondere programmi nocivi, poiché quasi tutti i programmi antivirus non esaminano il traffico SSL.

Kaspersky Internet Security 6.0 offre l'opzione di esaminare il traffico SSL alla ricerca di virus. In caso di tentativo di connessione protetta ad una risorsa Web, verrà visualizzata una notifica sullo schermo (cfr. fig.) che richiede l'intervento dell'utente.

Essa contiene informazioni sul programma che ha avviato la connessione protetta, unitamente all'indirizzo remoto ed alla porta remota. Il programma chiede di decidere se la connessione debba essere esaminata alla ricerca di virus:

- **Elabora** – esamina il traffico alla ricerca di virus in caso di connessione protetta ad un sito Web.

  Si consiglia di esaminare sempre il traffico SSL se ci si sta collegando ad sito Web sospetto o se parte un trasferimento SSL quando si passa alla pagina successiva. È assai probabile che ciò segnali il trasferimento di un programma nocivo sul protocollo protetto.

- **Salta** – continua la connessione protetta senza esaminare il traffico alla ricerca di virus.

Per applicare l'azione selezionata a tutti i futuri tentativi di stabilire una connessione SSL, selezionare **Applica a tutti**.

Figura 101. Notifica su rilevamento di una connessione SSL

Per esaminare le connessioni crittografate, Kaspersky Internet Security sostituisce il certificato di sicurezza richiesto con un certificato firmato dall'applicazione stessa. In alcuni casi, i programmi che stabiliscono la connessione non accetteranno questo certificato e la connessione non può essere stabilita. Si consiglia di disattivare la scansione del traffico SSL nei seguenti casi:

- Durante il collegamento ad una risorsa Web attendibile, ad esempio la pagina Web della propria banca, dal quale gestire il proprio conto corrente. In questo caso, è importante che l'autenticità del certificato della banca venga confermata.
- Se il programma che stabilisce la connessione verifica il certificato del sito web al quale si accede. Ad esempio, MSN Messenger verifica l'autenticità della firma digitale di Microsoft Corporation quando stabilisce una connessione al server.

È possibile configurare le impostazioni della scansione SSL dalla scheda **Impostazioni di rete** del riquadro del programma relativo alle impostazioni:

Controlla tutte le connessioni crittografate – esamina tutto il traffico in entrata tramite protocollo SSL alla ricerca di virus.

Richiedi all'utente quando viene rilevata una nuova connessione crittografata – visualizza un messaggio che richiede l'intervento dell'utente ogniqualvolta viene stabilita una connessione SSL.

Non controllare connessioni crittografate – non esamina il traffico in entrata tramite protocollo SSL alla ricerca di virus.

17.9. Configurazione dell'interfaccia di Kaspersky Internet Security

Kaspersky Internet Security offre la possibilità di modificare l'aspetto del programma creando e utilizzando nuovi stili. È possibile inoltre configurare l'uso degli elementi di interfaccia attiva come l'icona della barra delle applicazioni e i messaggi a comparsa.

Per configurare l'interfaccia del programma procedere come segue:

1. Aprire le impostazioni di Kaspersky Internet Security facendo clic sul link Impostazioni nella finestra principale del programma.
2. Selezionare **Aspetto** nella sezione **Servizi** della struttura ad albero delle impostazioni del programma (cfr. Figura 102).

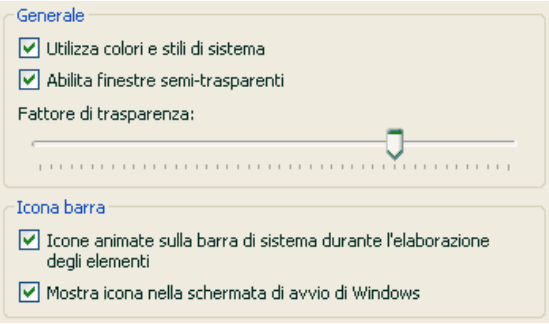


Figura 102. Configurazione delle impostazioni dell'interfaccia del programma

Nella parte destra della finestra delle impostazioni, è possibile determinare i seguenti elementi.

- Se visualizzare l'indicatore di protezione di Kaspersky Internet Security all'avvio del sistema operativo.

  Per impostazione predefinita, questo indicatore è visualizzato nell'angolo superiore destro dello schermo al caricamento del programma. Esso informa che il computer è protetto da tutti i tipi di minaccia. Se non si desidera usare l'indicatore di protezione, deselezionare la casella **Mostra icona nella schermata di avvio di Windows**.

- Se abilitare l'animazione nell'icona della barra delle applicazioni.

  A seconda dell'operazione eseguita dal programma, l'icona della barra delle applicazioni cambia. Per esempio, durante la scansione di uno script compare sullo sfondo dell'icona l'immagine miniaturizzata di uno script,

mentre durante la scansione di un messaggio e-mail compare una busta. L'animazione delle icone è abilitata per impostazione predefinita. Se si desidera disabilitare l'animazione, deselezionare la casella **Icone animate sulla barra di sistema durante l'elaborazione degli elementi**. Da quel momento in poi l'icona rappresenta solo lo status di protezione del computer: se la protezione è abilitata l'icona è a colori, mentre se la protezione è sospesa o disabilitata l'icona diventa grigia.

- Grado di trasparenza dei messaggi a comparsa.

  Tutte le operazioni di Kaspersky Internet Security che richiedono l'informazione dell'utente o il suo intervento immediato sono comunicate in un messaggio a comparsa sopra l'icona della barra delle applicazioni. Le finestre del messaggio sono trasparenti in modo da non interferire con il lavoro. Se si muove il cursore sul messaggio, la trasparenza svanisce. Il grado di trasparenza di questi messaggi può essere modificato regolando il cursore del **Fattore di trasparenza** sulla posizione desiderata. Per eliminare la trasparenza del messaggio, deselezionare la casella **Abilita finestre semi-trasparenti**.

- Applicare stili personalizzati all'interfaccia del programma.

  Tutti i colori, i font, le icone e i testi utilizzati nell'interfaccia di Kaspersky Internet Security possono essere modificati. È possibile creare elementi grafici personalizzati per il programma o localizzarli in un'altra lingua. Per usare uno stile, specificare la directory con le relative impostazioni nel campo **Directory con descrizioni degli stili**. Servirsi del pulsante **Sfoglia** per selezionare la directory.

  Per impostazione predefinita, lo stile del programma applica i colori e gli stili del sistema. Per eliminarli deselezionare la casella **Utilizza colori e stili di sistema**. Saranno quindi applicati gli stili specificati nelle impostazioni del tema dello schermo.

Osservare che le impostazioni dell'interfaccia di Kaspersky Internet Security definite dall'utente non vengono salvate in caso di ripristino delle impostazioni predefinite o di disinstallazione del programma.

17.10. Disco di emergenza

Kaspersky Internet Security dispone di uno strumento per creare un disco di emergenza.

Il disco di emergenza è progettato per consentire il ripristino della funzionalità del sistema dopo un attacco virale che ha danneggiato i file di sistema rendendo impossibile l'avvio del sistema operativo. Il disco include:

- File di sistema di Microsoft Windows XP Service Pack 2
- Una serie di utilità diagnostiche per il sistema operativo
- I file del programma Kaspersky Internet Security
- I file contenenti gli elenchi delle minacce

Per creare un disco di emergenza:

1. Aprire la finestra principale del programma e selezionare **Disco di emergenza** nella sezione **Servizi**.
2. Fare clic sul pulsante **Lancia procedura guidata** per avviare il processo di creazione del disco di emergenza.

Il disco di emergenza viene creato per il computer sul quale è stato creato. L'utilizzo del disco su altri computer può determinare conseguenze imprevedibili, poiché contiene informazioni sui parametri relativi ad un computer specifico (le informazioni sui settori di boot, ad esempio).

La creazione di un disco di emergenza è possibile solo con Windows XP. Non è possibile creare dischi di emergenza sui computer che eseguono Microsoft Windows XP Professional x64 Edition.

17.10.1. Creazione di un disco di emergenza

Attenzione! Per creare un disco di emergenza è necessario disporre del disco di installazione di Microsoft Windows XP Service Pack 2.

Per creare il Disco di emergenza è necessario il programma **PE Builder**.

Prima di creare un disco di emergenza è necessario installare PE Builder sul computer.

Inoltre, durante l'uso di PE Builder, è necessario eseguire una volta il programma dal menu (**Start → Programmi → PE Builder**) dopo averlo installato.

La creazione del disco di emergenza è agevolata da un'apposita procedura guidata che consiste di una serie di finestre/passaggi fra i quali navigare servendosi dei pulsanti **Indietro** e **Avanti**. Per completare la procedura guidata fare clic su **Fine**. Il pulsante **Annulla** serve per interrompere in qualsiasi momento la procedura.

17.10.1.1. La scrittura del disco

Se nel passaggio precedente si è scelto di creare un disco per mezzo di un programma apposito, indicare i percorsi alle seguenti cartelle:

- Cartella del programma PE Builder
- Cartella in cui sono stati salvati i file del disco di emergenza prima di masterizzare il CD

  Se non è la prima volta che si crea un disco di emergenza, questa cartella contiene già una serie di file creati la volta precedente. Per usare i file salvati in precedenza, selezionare la cartella corrispondente.

  > Osservare che i file del disco di emergenza creati precedentemente contengono elenchi delle minacce obsoleti. Per eseguire la scansione antivirus del computer e ripristinare il sistema in maniera ottimale, si raccomanda di aggiornare gli elenchi delle minacce e di creare una nuova versione del disco di emergenza.

- Il CD di installazione di Microsoft Windows XP Service Pack 2

Dopo aver indicato i percorsi alle cartelle richieste, fare clic su **Avanti**. PE Builder si avvia e ha inizio il processo di creazione del disco di emergenza. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.

17.10.1.2. Creazione di un file .iso

Dopo che PE Builder ha completato la creazione dei file del disco di emergenza, si apre la finestra **Crea file .iso**.

Il file .iso è un'immagine su CD del disco di emergenza salvata come archivio. La maggior parte dei programmi di masterizzazione CD è in grado di riconoscere correttamente i file .iso (Nero, per esempio).

Se non è la prima volta che si crea un disco di emergenza, è possibile selezionare il file .iso dal disco precedente selezionando **File .iso esistente**.

17.10.1.3. Masterizzazione del disco

Durante la procedura guidata viene chiesto di scegliere quando masterizzare il disco di emergenza su CD: adesso o più tardi.

Se si decide di masterizzare immediatamente il disco, specificare se si desidera formattare il disco prima di procedere, selezionando la casella corrispondente. Questa opzione è disponibile solo se si usano dischi CD-RW.

Per avviare la masterizzazione del CD fare clic sul pulsante **Avanti**. Attendere il completamento del processo. L'operazione potrebbe richiedere diversi minuti.

17.10.1.4. Completamento del disco di emergenza

Questa finestra della procedura guidata informa che il disco di emergenza è stato creato correttamente.

17.10.2. Uso del disco di emergenza

Se in seguito a un attacco di virus è impossibile caricare il sistema operativo, procedere come segue:

1. Creare un disco di boot di emergenza utilizzando Kaspersky Internet Security su un computer non infetto.
2. Inserire il disco di emergenza nell'unità CD del computer infetto e riavviare. Microsoft Windows XP SP2 si avvia con l'interfaccia di Bart PE.
   Bart PE è dotato di assistenza di rete incorporata per usare la LAN. All'avvio del programma, viene richiesto se si desidera abilitarlo. Agree to enable network support if you plan to update threat signatures from the LAN before scanning your computer. Se non è necessario aggiornare i file, disabilitare il supporto di rete.
3. Per aprire Kaspersky Intenet Security, fare clic su **Start→Programmi→Kaspersky Kaspersky Internet Security 6→Start**.

   Si apre la finestra principale di Kaspersky Internet Security. In modalità provvisoria è possibile accedere solo alle scansioni antivirus e agli aggiornamenti degli elenchi delle minacce dalla LAN (se era stato abilitato il supporto di rete in Bart PE).
4. Avviare la scansione antivirus. Le statistiche registrate nella scansione, così come gli oggetti trasferiti in Quarantena o in Backup, si troveranno in *C:\AVP6_TEMP*.

Osservare che Kaspersky Internet Security funziona in modalità provvisoria solo se la finestra principale è aperta. Chiudendo la finestra principale si chiude anche il programma.

Bart PE, il programma predefinito, non supporta i file .chm o i browser di Internet, pertanto in modalità provvisoria non è possibile visualizzare la Guida di Kaspersky Internet Security o i link dell'interfaccia del programma.

17.11. Uso delle opzioni avanzate

Kaspersky Internet Security offre le seguenti funzioni avanzate:

- Avvisi di determinati eventi che si verificano nel programma.
- Protezione automatica di Kaspersky Internet Security dalla disattivazione, eliminazione o modifica dei moduli, oltre alla protezione password del programma.
- Modalità di risparmio batterie in caso di utilizzo di un portatile.

Per configurare queste funzioni:

1. Aprire la finestra di configurazione del programma dal link Impostazioni nella finestra principale.
2. Selezionare **Servizi** dalla struttura ad albero delle impostazioni.

Nella parte destra dello schermo è possibile specificare se abilitare le funzioni supplementari durante l'uso del programma.

17.11.1. Notifica di eventi di Kaspersky Internet Security

Durante l'uso di Kaspersky Internet Security si verificano diversi tipi di evento. Le notifiche corrispondenti possono essere informative o contenere dati importanti. Per esempio, un messaggio può informare dell'avvenuto aggiornamento del programma oppure registrare l'errore di un componente da risolvere immediatamente.

Per ricevere gli aggiornamenti sul funzionamento di Kaspersky Internet Security è possibile utilizzare la funzione di notifica, progettata per informare l'utente degli eventi che si verificano.

Le notifiche possono essere trasmesse in vari modi:

- In forma di messaggi a comparsa sopra l'icona del programma nella barra delle applicazioni.
- Con segnali acustici.
- Per e-mail.

Per usare questa funzione procedere come segue:

1. Selezionare la casella **Abilita avvisi** nel riquadro **Avvisi** (cfr. Figura 103).

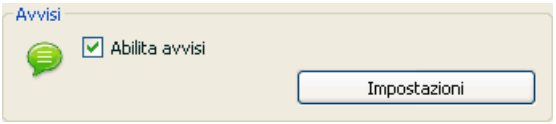


Figura 103. Abilitazione delle notifiche

2. Definire i tipi di eventi di Kaspersky Internet Security dei quali si desidera essere informati e il metodo di trasmissione della notifica (cfr. 17.11.1.1 a pag. 268).
3. Configurare le impostazioni di consegna delle notifiche via e-mail, se questo è il metodo in uso (cfr. 17.11.1.2 a pag. 269).

17.11.1.1. Tipi di eventi e metodo di notifica

Durante l'uso di Kaspersky Internet Security, possono verificarsi i seguenti tipi di eventi:

Eventi critici – eventi di importanza cruciale. Si raccomanda di abilitare gli avvisi, poiché questo tipo di eventi segnala la presenza di problemi di funzionamento del programma o di vulnerabilità della protezione del computer. Per esempio, *elenchi delle minacce corrotti* o *licenza scaduta*.

Eventi importanti – eventi da approfondire poiché riflettono situazioni importanti nel funzionamento del programma. Per esempio, *protezione disabilitata* o *la scansione antivirus del computer non viene eseguita da molto tempo.*

Messaggi informativi – messaggi di riferimento che di solito non contengono informazioni rilevanti. Per esempio, *all dangerous objects disinfected*.

Per specificare gli eventi da comunicare e le modalità di notifica:

1. Fare clic sul link Impostazioni nella finestra principale del programma.
2. Nella finestra delle impostazioni del programma, selezionare **Servizi**, selezionare la casella **Abilita avvisi**, e modificare le impostazioni dettagliate facendo clic sul pulsante **Impostazioni**.

È possibile configurare i seguenti metodi di notifica per gli eventi sopra elencati nella scheda **Eventi** della finestra che si apre (cfr. Figura 104):

- *Messaggi a comparsa* sopra l'icona del programma nella barra delle applicazioni, contenenti informazioni sull'evento verificatosi.

  Per usare questo tipo di notifica, selezionare la casella ☑ nella sezione **Fumetto** dall'evento del quale si desidera essere informati.

- Segnale acustico

  Se si desideri che l'avviso sia accompagnato da un segnale acustico, selezionare la casella ☑ **Suono** dall'evento.

- E-mail

  Per utilizzare questo tipo di notifica, selezionare la casella ☑ **E-mail** dall'evento del quale si desidera essere informati, e configurare le impostazioni di invio degli avvisi (cfr. 17.11.1.2 a pag. 269).

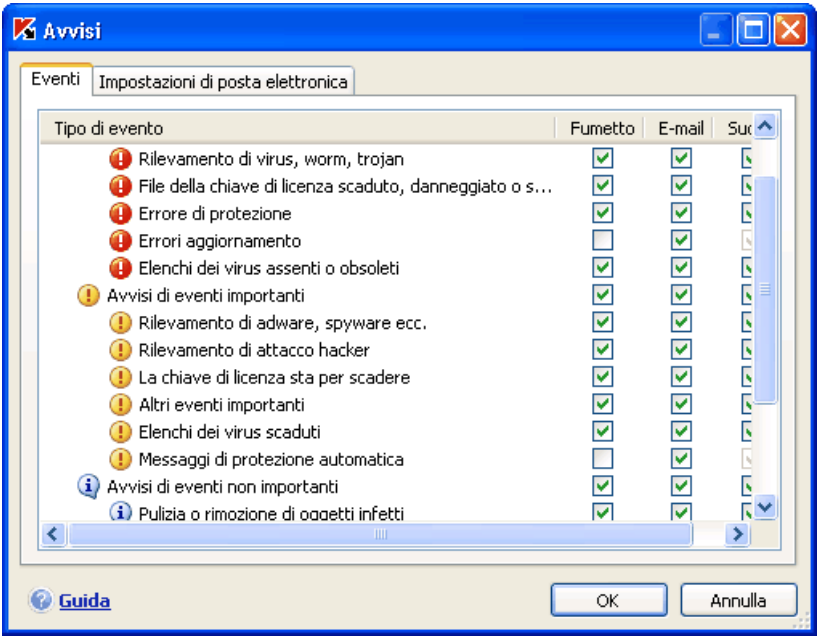


Figura 104. Eventi del programma e metodi di avviso

17.11.1.2. Configurazione delle notifiche via e-mail

Dopo aver selezionato gli eventi (cfr. 17.11.1.1 a pag.. 268) dei quali si desidera essere informati per e-mail, è necessario configurare la consegna dell'avviso procedendo come segue:

1. Aprire la finestra di configurazione del programma dal link Impostazioni nella finestra principale.
2. Selezionare **Servizi** dalla struttura ad albero delle impostazioni.
3. Fare clic su **Impostazioni** nel riquadro **Avvisi** (cfr. Figura 105) nella parte destra dello schermo.
4. Definire le seguenti impostazioni di invio dei messaggi nella scheda **Impostazioni di posta elettronica**:
   - Impostare la notifica di invio in **Da: Indirizzo**.
   - Specificare l'indirizzo e-mail a cui inviare gli avvisi in **A: Indirizzo**.
   - Impostare il metodo di avviso per e-mail in **Modalità invio**. Se si desidera che il programma invii il messaggio non appena l'evento si verifica, selezionare **Immediatamente al verificarsi dell'evento**. Per la notifica di eventi entro un determinato periodo di tempo, impostare il calendario di invio dei messaggi informativi facendo clic su **Modifica**. Gli invii quotidiani sono l'impostazione predefinita.

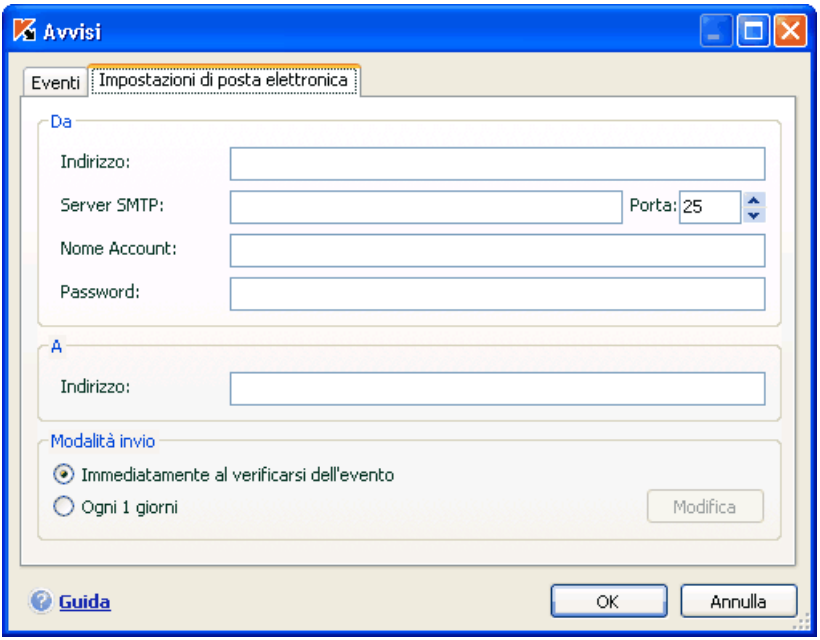


Figura 105. Configurazione delle notifiche via e-mail

17.11.2. Protezione automatica e limitazioni d'accesso

Kaspersky Internet Security garantisce la protezione del computer dai programmi nocivi e, proprio per questo, è spesso oggetto di attacchi da parte di programmi nocivi che cercano di bloccarne l'attività o perfino di eliminarlo dal computer.

Inoltre è possibile che più utenti si servano di un unico computer, non tutti ugualmente esperti nell'uso. Lasciare libero accesso al programma e alle sue impostazioni, pertanto, riduce considerevolmente la sicurezza del computer.

Per garantire la stabilità del sistema operativo, il programma è stato dotato di meccanismi di protezione automatica, protezione dall'accesso remoto e protezione mediante password.

Per abilitare la protezione automatica:

1. Aprire la finestra di configurazione del programma dal link Impostazioni nella finestra principale.
2. Selezionare **Servizi** dalla struttura ad albero delle impostazioni.

3. Effettuare le seguenti configurazioni nel riquadro **Protezione** (cfr. Figura 106):

Abilita protezione automatica. Se questa casella è selezionata, il programma protegge i propri file, processi di memoria e voci del registro di sistema dalla cancellazione o dalla modifica.

Disabilita controllo del servizio esterno. Se questa casella è selezionata, qualsiasi tentativo di uso del programma da parte di amministrazioni remote viene bloccato.

In presenza di qualsiasi azione tra quelle sopra elencate, viene visualizzato un messaggio sopra l'icona del programma nella barra delle applicazioni.

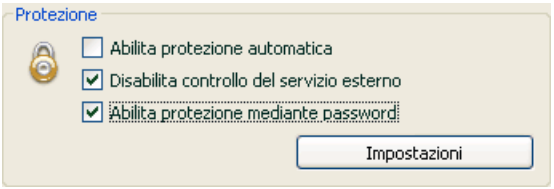


Figura 106. Configurazione della protezione automatica

Per proteggere il programma mediante password, selezionare la casella **Abilita protezione mediante password**. Digitare la password e l'area a cui limitare l'accesso nella finestra che si apre facendo clic su **Impostazioni** (cfr. Figura 107). È possibile bloccare qualsiasi operazione del programma, ad eccezione della notifica di rilevamento di oggetti pericolosi, o impedire l'esecuzione di qualsiasi tra le seguenti azioni:

- Modifica delle impostazioni del programma.
- Chiusura di Kaspersky Internet Security.
- Disattivazione o sospensione della protezione del computer.

Ciascuna delle azioni sopra elencate riduce la sicurezza del computer ed è quindi necessario stabilire quali tra gli utenti del computer sono sufficientemente attendibili da poter compiere tali azioni.

Selezionando questa opzione, ogni volta che un utente del computer cerca di eseguire le azioni selezionate, il programma richiede una password.

Figura 107. Impostazioni di protezione del programma mediante password

17.11.3. Opzioni di alimentazione

Per preservare la batteria del laptop e ridurre il carico sul processore e sui sottosistemi del disco è possibile posticipare le scansioni antivirus:

- Poiché le scansioni antivirus a gli aggiornamenti del programma richiedono talvolta una discreta quantità di risorse e possono durare diverso tempo, si raccomanda di disabilitare le pianificazioni di queste attività. Questo accorgimento consente di prolungare la durata della batteria. Se necessario, è possibile aggiornare manualmente il programma (cfr. 5.8 a pag. 65) oppure avviare una scansione antivirus. Per usare la funzione di risparmio energetico, selezionare la casella appropriata nel riquadro **Alimentazione e produttività** (cfr. Figura 108).

- Le scansioni antivirus aumentano il carico sul processore centrale e sui sottosistemi del disco, rallentando di conseguenza altri programmi. Per impostazione predefinita, in tali circostanze il programma sospende temporaneamente la scansione antivirus e libera risorse di sistema per le applicazioni dell'utente.

  Esistono tuttavia numerosi programmi che possono essere avviati non appena si liberano risorse di sistema e funzionano in modalità secondaria. Affinché le scansioni antivirus non dipendano dal funzionamento di tali programmi, deselezionare la casella ☑ **Sospendi scansione antivirus quando la CPU è occupata da altre applicazioni**.

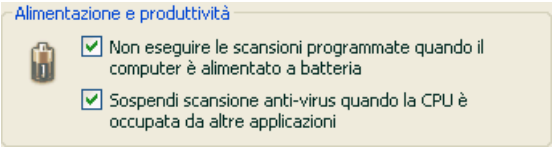


Figura 108. Configurazione delle impostazioni di alimentazione

17.11.4. Risoluzione dei conflitti con altre applicazioni

Ci sono casi in cui Kaspersky Internet Security può determinare conflitti con altre applicazioni installate sul computer. Ciò succede perché quei programmi hanno meccanismi di autodifesa interni, che si attivano quando Kaspersky Internet Security cerca di ispezionarli. Queste applicazioni comprendono il plug-in Authentica per Acrobat Reader, che verifica l'accesso ai file .pdf, Oxygen Phone Manager II, ed alcuni giochi per PC dotati di strumenti per la gestione dei diritti in digitale.

PEr risoolvere il problema, selezionare la casella **Modalità compatibilità con programmi che utilizzano metodi di auto-protezione** nella sezione **Servizio** del riquadro delle impostazioni dell'applicazione. Tuttavia, si tenga presente che abilitando questa opzione vengono disattivate alcune funzioni di Kaspersky Internet Security (ad esempio, Registry Guard, il rilevamento delle attività delle applicazioni, la scansione degli script, ecc.).

È necessario riavviare il sistema operativo perché tale modifica abbia effetto.

CAPITOLO 18. USO DEL PROGRAMMA DAI PROMPT DI COMANDO

Kaspersky Internet Security può essere utilizzato anche dai prompt di comando eseguendo le seguenti operazioni:

- Avvio, arresto, pausa e ripristino dell'attività dei componenti dell'applicazione
- Avvio, arresto, pausa e ripristino delle scansioni antivirus
- Ottenimento di informazioni sullo status corrente di componenti, attività e statistiche
- Scansione di oggetti selezionati
- Aggiornamento degli elenchi delle minacce e dei moduli del programma
- Accesso alla Guida per consultare la sintassi dei prompt di comando
- Accesso alla Guida per consultare la sintassi dei comandi

La sintassi dei prompt di comandi è la seguente:

```
avp.com <command> [Impostazioni]
```

Possono essere usati come **<comandi>** i seguenti:

START	Avvia un componente o attività
PAUSE	Sospende temporaneamente un componente o attività
RESUME	Ripristina l'uso di un componente o attività
STOP	Termina un componente o attività
STATUS	Visualizza lo status del componente o attività correnti
STATISTICS	Visualizza le statistiche del componente o attività
HELP	Fornisce indicazioni sulla sintassi dei comandi e

	sull'elenco dei comandi
SCAN	Esegue la scansione antivirus di oggetti
UPDATE	Avvia l'aggiornamento del programma
EXIT	Chiude il programma (è possibile eseguire questo comando solo con la password impostata nell'interfaccia del programma)
IMPORT	Importa le impostazioni di Kaspersky Internet Security
EXPORT	Esporta le impostazioni di Kaspersky Internet Security

Ogni comando corrisponde alle impostazioni specifiche del componente di Kaspersky Internet Security.

18.1. Gestione di componenti del programma e attività

È possibile gestire i componenti e le attività di Kaspersky Internet Security dal prompt di comando con i seguenti comandi:

- START
- PAUSE
- RESUME
- STOP
- STATUS
- STATISTICS

L'attività o componente a cui si applica il comando sono determinati dai relativi parametri.

STOP e PAUSE possono essere eseguiti solo con la password di Kaspersky Internet Security impostata nell'interfaccia del programma.

Sintassi dei comandi:

```
avp.com <command> <profile|taskid>
avp.com STOP
        PAUSE <profile|taskid> /password=<password>
```

Al parametro **<profile|taskid>** è assegnato uno dei seguenti valori:

RTP	Tutti i componenti della protezione
FM	File Anti-Virus
EM	Mail Anti-Virus
WM	Web Anti-Virus
BM	Difesa proattiva
ASPY	Anti-Spy
AH	Anti-Hacker
AS	Anti-Spam
UPDATER	Updater
SCAN_OBJECTS	Attività di scansione antivirus
SCAN_MY_COMPUTER	Attività Risorse del computer
SCAN_CRITICAL_AREAS	Attività aree critiche
SCAN_STARTUP	Attività oggetti ad esecuzione automatica
<task name>	Attività definita dall'utente

I componenti e le attività avviati dal prompt di comando vengono eseguiti con le impostazioni configurate dall'interfaccia del programma.

Esempi:

Per abilitare File Anti-Virus, digitare la seguente stringa nel prompt di comando:

```
avp.com START FM
```

Per visualizzare lo status corrente di Difesa proattiva sul computer, digitare il testo seguente nel prompt di comando:

```
avp.com STATUS BM
```

Per terminare un'attività di scansione di Risorse del computer dal prompt di comando, digitare:

```
avp.com STOP SCAN_MY_COMPUTER
/password=<your_password>
```

18.2. Scansioni antivirus

L'avvio della scansione antivirus di una determinata area e l'elaborazione degli oggetti nocivi dal prompt di comando generalmente appare così:

```
avp.com SCAN [<object scanned>] [<action>] [<action
query>] [<file types>] [<exclusions>] [<configuration
file>] [<report Impostazioni>]
```

Per eseguire la scansione di oggetti è possibile utilizzare anche le attività create in Kaspersky Internet Security avviando quella desiderata dal prompt di comando (cfr. 18.1 a pag. 276). L'attività viene eseguita con le impostazioni configurate nell'interfaccia del programma.

Descrizione dei parametri.

<object scanned> - questo parametro produce un elenco degli oggetti che saranno sottoposti alla scansione in cerca di codici nocivi. Può includere diversi valori dall'elenco fornito, separati da uno spazio.	
<files>	Elenco dei percorsi ai file e/o cartelle da sottoporre a scansione antivirus. È possibile inserire percorsi assoluti o relativi. Gli elementi dell'elenco devono essere separati da uno spazio. Note: • Se il nome dell'oggetto contiene uno spazio, esso deve essere incluso tra virgolette. • Se si seleziona una cartella specifica, saranno sottoposti a scansione antivirus tutti i file in essa contenuti.
/MEMORY	Oggetti della memoria di sistema.

/STARTUP	Oggetti ad esecuzione automatica.
/MAIL	Database di posta.
/REMDRIVES	Tutte le unità estraibili.
/FIXDRIVES	Tutte le unità interne.
/NETDRIVES	Tutte le unità di rete.
/QUARANTINE	Oggetti in quarantena
/ALL	Scansione completa.
/@:<filelist.lst>	Percorso al file con un elenco di oggetti e cartelle inclusi nella scansione. Il file deve essere in formato testo e ogni oggetto della scansione deve iniziare una nuova riga. È possibile indicare un percorso assoluto o relativo. Il percorso deve essere inserito tra virgolette se contiene spazi.
<action> - questo parametro imposta le reazioni agli oggetti nocivi rilevati durante la scansione. Se questo parametro non è definito, l'azione predefinita è quella con il valore per **/i2**.	
/i0	Nessuna azione sull'oggetto; solo registrazione delle informazioni nel report.
/i1	Trattare gli oggetti infetti e, se la riparazione non riesce, ignorare.
/i2	Trattare gli oggetti infetti e, se la disinfezione non riesce, eliminare, ma non eliminare gli oggetti appartenenti ad oggetti composti, ed eliminare gli oggetti composti con intestazione eseguibile (archivi sfx) (impostazione predefinita).
/i3	Trattare gli oggetti infetti e, se la riparazione non riesce, eliminare, ed eliminare completamente tutti gli oggetti composti se non si riesce ad eliminare l'allegato infetto.

/i4	Eliminare gli oggetti infetti e, se la riparazione non riesce, eliminare, ed eliminare completamente tutti gli oggetti composti se non si riesce ad eliminare l'allegato infetto.
<action query> - questo parametro definisce quali azioni richiederanno l'intervento dell'utente durante la scansione. Se il parametro non è definito, l'azione viene richiesta per impostazione predefinita al termine della scansione.	
/a0	Non richiedere.
/a1	Richiedi azione in caso di rilevamento di oggetto infetto.
/a2	Richiedi azione al termine della scansione.
<file types> - questo parametro definisce i tipi di file che saranno sottoposti alla scansione antivirus. Per impostazione predefinita questo parametro non è definito; solo i file potenzialmente infetti saranno esaminati in base ai contenuti.	
/fe	Esaminare solo i file potenzialmente infetti in base all'estensione.
/fi	Esaminare solo i file potenzialmente infetti in base ai contenuti.
/fa	Esaminare tutti i file.
<exclusions> - questo parametro definisce gli oggetti da escludere dalla scansione. Può includere diversi valori dall'elenco fornito, separati da uno spazio.	
/e:a	Non esaminare archivi
/e:b	Non esaminare i database di posta.
/e:m	Non esaminare i messaggi di testo semplice
/e:<mask>	Non esaminare oggetti in base alle maschere.
/e:<seconds>	Ignorare oggetti esaminati più a lungo del tempo specificato dal parametro <seconds>.

<configuration file> - questo parametro definisce il percorso al file di configurazione che contiene le impostazioni del programma per la scansione. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono applicati i valori impostati dall'interfaccia di Kaspersky Internet Security.	
/C:<Impostazioni_file>	Usare i valori delle impostazioni assegnati nel file **<Impostazioni_file>**
<report Impostazioni> - questo parametro definisce il formato del report sui risultati della scansione. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, vengono visualizzati i risultati della scansione e tutti gli eventi.	
/R:<report_file>	Registrare in questo file solo gli eventi importanti.
/RA:<report_file>	Registrare tutti gli eventi in questo file.

Esempi:

*avvio di una scansione della RAM, programmi ad esecuzione automatica, database di posta, le directory **Documenti** e **Programmi**, e il file **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Impostazioni\All Users\My Documents" "C:\Program
Files" "C:\Downloads\test.exe"
```

Sospensione temporanea della scansione di oggetti selezionati e avvio di una scansione completa del computer, quindi proseguimento della scansione antivirus degli oggetti selezionati:

```
avp.com PAUSE SCAN_OBJECTS /password=<your_password>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Scansione degli oggetti elencati nel file **object2scan.txt**. Uso del file di configurazione **scan_setting.txt**. Dopo la scansione, creazione di un report con registrazione di tutti gli eventi:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_Impostazioni.txt /RA:scan.log
```

18.3. Aggiornamenti del programma

La sintassi per l'aggiornamento dei moduli di Kaspersky Internet Security e degli elenchi delle minacce dal prompt di comando è la seguente:

```
avp.com UPDATE [<path/URL>] [/R[A]:<report_file>]
[/C:<Impostazioni_file>] [/APP]
```

Descrizione dei parametri:

[<path/URL>]	Server HTTP o FTP o cartella di rete per il prelievo degli aggiornamenti. In assenza di percorso selezionato, l'origine degli aggiornamenti sarà quella delle impostazioni di Updater.
/R[A]:<report_file>	**/R:<report_file>** – registrare solo gli eventi importanti nel report. **/R[A]:<report_file>** – registrare tutti gli eventi nel report. È possibile indicare un percorso assoluto o relativo. Se il parametro non è definito, vengono visualizzati i risultati della scansione e tutti gli eventi.
/C:<Impostazioni_file>	Percorso al file di configurazione con le impostazioni degli aggiornamenti del programma. È possibile indicare un percorso assoluto o relativo. Se questo parametro non è definito, vengono applicati i valori impostati dall'interfaccia di Kaspersky Internet Security.
/APP	Aggiorna moduli programma

Esempi:

Aggiornamento degli elenchi delle minacce dopo la registrazione di tutti gli eventi nel report:

```
avp.com UPDATE /RA:avbases_upd.txt
```

Aggiornamento dei moduli di Kaspersky Internet Security applicando le impostazioni nel file di configurazione ***updateapp.ini****:*

```
avp.com UPDATE /APP /C:updateapp.ini
```

18.4. Esportazione delle impostazioni

Sintassi dei comandi:

```
avp.com EXPORT <profile|taskid> <Impostazioni_file>
```

Descrizione dei parametri:

<profile>	Componente o attività le cui impostazioni vengono esportate. Può essere usato uno dei seguenti valori: **RTP** – tutti i componenti di protezione. **FM** – File Anti-Virus **EM** – Mail Anti-Virus **WM** – Web Anti-Virus **BM** - Difesa proattiva **ASPY** – Anti-Spy **AH** – Anti-Hacker **AS** – Anti-Spam
<Impostazioni_file>	Percorso al file su cui sono esportate le impostazioni di Kaspersky Internet Security. È possibile inserire percorsi assoluti o relativi. È possibile usare solo file binari (*cfg*).

Esempi:

```
avp.com EXPORT c:\kis60settings.cfg
```

18.5. Importazione delle impostazioni

Sintassi dei comandi:

```
avp.com IMPORT <Impostazioni_file>
```

<Impostazioni_file>	Percorso al file da cui sono importate le impostazioni di Kaspersky Internet Security. È possibile inserire percorsi assoluti o relativi. È possibile usare solo file binari (*cfg*).

Esempi:

```
avp.com IMPORT c:\kis60settings.cfg
```

18.6. Avvio del programma

Sintassi dei comandi:

```
avp.com
```

18.7. Arresto del programma

Sintassi dei comandi:

```
EXIT /password=<password>
```

<password>	La password di Kaspersky Internet Security impostata dall'interfaccia del programma.

Osservare che non è possibile eseguire questo comando senza digitare la password.

18.8. Visualizzazione della Guida

Questo comando è disponibile per visualizzare la Guida con la sintassi del prompt di comando:

```
avp.com [ /? | HELP ]
```

Per ricevere aiuto sulla sintassi di un comando specifico, è possibile usare uno dei seguenti comandi:

```
avp.com <command> /?
avp.com HELP <command>
```

CAPITOLO 19. MODIFICA, RIPARAZIONE E DISINSTALLAZIONE DEL PROGRAMMA

In caso di errori di funzionamento dovuto a un'errata configurazione o alla corruzione dei file può rendersi necessario riparare il programma.

La modifica del programma consente di installare componenti di Kaspersky Internet Security assenti o di eliminare quelli che non si desiderano.

Per riparare o modificare i componenti assenti di Kaspersky Internet Security o disinstallare il programma:

1. Chiudere il programma facendo clic con il pulsante sinistro del mouse sull'icona del programma nella barra delle applicazioni e selezionare**Esci** dal menu contestuale.
2. Inserire l'eventuale CD di installazione nell'unità CD-ROM (se utilizzato per installare il programma). Se Kaspersky Internet Security è stato installato da una diversa origine (cartella ad accesso pubblico, cartella nel disco fisso, ecc.), verificare che la cartella contenga il pacchetto di installazione e di potervi accedere.
3. Selezionare **Start → Programmi → Kaspersky Internet Security 6.0 → Modifica, ripara o rimuovi**.

Si apre una procedura di installazione guidata del programma. Osserviamo in dettaglio i passaggi necessari per riparare, modificare o eliminare il programma.

Passaggio 1. Finestra di avvio dell'installazione

Dopo aver eseguito tutti i passaggi sopra descritti, necessari per riparare o modificare il programma, si apre la finestra iniziale di installazione di Kaspersky Internet Security. Fare clic sul pulsante **Avanti** per continuare.

Passaggio 2. Selezione di un'operazione

In questa fase è richiesto di selezionare l'operazione che si desidera eseguire. È possibile modificare i componenti del programma, riparare i componenti già installati o rimuovere dei componenti o l'intero programma. Per eseguire l'operazione desiderata, fare clic sul pulsante appropriato. La reazione del programma dipende dall'operazione selezionata.

La modifica del programma è analoga all'installazione in cui è possibile specificare quali componenti si desidera installare e quali eliminare.

La riparazione del programma dipende dai componenti installati. Saranno riparati i file di tutti i componenti installati e per ciascuno di essi sarà impostato il livello di sicurezza Raccomandato.

Se si rimuove il programma, è possibile selezionare quali dati creati e usati dal programma si desidera salvare sul computer. Per eliminare tutti i dati di Kaspersky Internet Security, selezionare **Disinstallazione completa**. Per salvare i dati, selezionare **Salva oggetti dell'applicazione** e specificare quali oggetti non eliminare:

- *Dati di attivazione* – la chiave di licenza o il codice di attivazione del programma.
- *Elenchi delle minacce* – serie completa delle firme di programmi pericolosi, virus e altre minacce correnti all'ultimo aggiornamento.
- *Database di Anti-Spam* – database utilizzato per individuare la posta indesiderata. Questo database contiene informazioni dettagliate su quali messaggi costituiscono spam e quali no.
- *File di backup* – copie di backup di oggetti eliminati o riparati Si raccomanda di salvarli per poterli eventualmente ripristinare in un secondo momento.
- *File in Quarantena* – file potenzialmente infetti da virus o varianti di essi. Questi file contengono codici simili a quelli di virus noti ma è difficile stabilire se siano nocivi. Si raccomanda di salvare questi file poiché potrebbero essere normali o riparati dopo l'aggiornamento degli elenchi delle minacce.
- *Impostazioni dell'applicazione* – configurazioni per tutti i componenti del programma.
- *Dati iSwift* – database con informazioni sugli oggetti esaminati nel file system NTFS. Può accelerare la scansione. Quando usa questo database, Kaspersky Internet Security esamina solo i file che hanno subito modifiche in seguito all'ultima scansione.

Attenzione!

Se trascorre un lungo periodo tra la disinstallazione di una versione di Kaspersky Internet Security e l'installazione di un'altra, si sconsiglia di utilizzare il database *iSwift* di una versione precedente. Un programma pericoloso potrebbe essere penetrato nel computer nel frattempo e i suoi effetti non sarebbero rilevati dal database, con conseguente rischio di infezione.

Per avviare l'operazione selezionata fare clic sul pulsante **Avanti**. Il programma inizia a copiare i file necessari sul computer o a eliminare i componenti e i dati selezionati.

Passaggio 3. Elenco dei programmi che interferiscono con la corretta modifica, riparazione o rimozione

Se durante il processo di modifica, riparazione o rimozione il programma rileva l'uso dei propri file da parte di altre applicazioni, viene visualizzato un elenco di tali file. Questo elenco contiene di solito applicazioni che usano plug-in di Kaspersky Internet Security. Il programma chiede di chiudere tali applicazioni.

Per continuare l'operazione fare clic sul pulsante **Ignora**. Per proseguire dopo la chiusura delle applicazioni elencate, fare clic sul pulsante **Riprova**.

Passaggio 4. Completamento della modifica, riparazione o rimozione del programma

L'avanzamento del processo di modifica, riparazione o rimozione del programma viene seguito sullo schermo. Al termine l'utente viene informato del completamento dell'operazione.

La rimozione del programma richiede solitamente il riavvio del computer, necessario per applicare le modifiche al sistema. Il programma chiede quindi se si desidera riavviare il computer. Fare clic su **Sì** per riavviarlo subito. Per riavviarlo in un secondo momento, scegliere invece **No**.

CAPITOLO 20. DOMANDE FREQUENTI

Questo capitolo è dedicato alle domande più frequenti poste dai nostri utenti sull'installazione, la configurazione e il funzionamento di Kaspersky Internet Security; faremo il possibile per fornire risposte più esaurienti possibile.

Domanda: È possibile usare Kaspersky Internet Security 6.0 con prodotti antivirus di altri fabbricanti?

No. Si raccomanda di disinstallare altri prodotti antivirus eventualmente presenti sul computer prima di installare Kaspersky Internet Security per evitare conflitti di software.

Domanda: Kaspersky Internet Security non riesamina i file precedentemente sottoposti alla scansione? Perché?

È vero. Kaspersky Internet Security non riesamina i file che non hanno subito variazioni dalla scansione precedente.

Ciò è possibile grazie alle nuove tecnologie iChecker e iStreams. La tecnologia viene implementata nel programma utilizzando un database di checksum dei file e un archivio di checksum dei file in flussi NTFS alternati.

Domanda: Perché mi occorre una chiave di licenza? Kaspersky Internet Security non funziona senza?

Kaspersky Internet Security funziona anche senza chiave di licenza ma il programma non è in grado di accedere ad Updater e all'assistenza tecnica.

Se non si è ancora deciso se acquistare Kaspersky Internet Security, possiamo fornire una chiave di licenza in prova per due settimane o un mese. Trascorso questo periodo, la chiave scade.

Domanda: Dopo l'installazione di Kaspersky Internet Security il sistema operativo ha iniziato a "comportarsi" in maniera strana (schermo blu, riavvi frequenti, ecc.). Cosa devo fare?

Sebbene si tratti di una circostanza rara, è possibile che Kaspersky Internet Security e altri software presenti sul computer siano in conflitto.

Per ripristinare la funzionalità del sistema operativo procedere come segue:

1. Premere il tasto **F8** non appena il computer inizia a caricarsi fino a visualizzare il menu di boot.
2. Selezionare la **Modalità provvisoria** e caricare il sistema operativo.
3. Aprire Kaspersky Internet Security.
4. Usare il link Impostazioni nella finestra principale e selezionare la sezione **Protezione** nella finestra delle impostazioni del programma.
5. deselezionare **Run Kaspersky Internet Security 6.0 on system startup** and click **OK**.
6. Ricaricare il sistema operativo in modalità regolare.

Quindi rivolgersi al servizio di assistenza tecnica attraverso il sito web aziendale di Kaspersky Lab (**Services→Technical Support)**. Descrivere dettagliatamente il problema e le circostanze in cui esso si è verificto.

Ricordare di allegare alla domanda un file contenente un'immagine completa della memoria del sistema operativo Microsoft Windows. Per creare questo file procedere come segue:

1. Fare clic con il pulsante destro del mouse su **Risorse del computer** e selezionare l'elemento **Proprietà** del menu di scelta rapida che si apre.
2. Selezionare la scheda **Avanzate** nella finestra **Proprietà del sistema**, quindi premere il pulsante **Impostazioni** nella sezione **Avvio e ripristino**.
3. Selezionare l'opzione **Immagine della memoria completa** dal menu a discesa della sezione **Scrivi informazioni di debug** nella finestra **Avvio e ripristino**.

   Per impostazione predefinita, il file dell'immagine della memoria viene salvato nella cartella di sistema come *memory.dmp*. È possibile modificare la cartella di salvataggio dell'immagine rinominando la cartella nel campo corrispondente.
4. Riprodurre il problema relativo al funzionamento di Kaspersky Internet Security.
5. Accertarsi che l'immagine completa della memoria sia stata salvata correttamente.

APPENDICE A. RIFERIMENTI

Questa appendice contiene materiale di riferimento sui formati dei file e le maschere delle estensioni utilizzate nelle impostazioni di Kaspersky Internet Security.

A.1. Elenco dei file esaminati in base all'estensione

Se si seleziona **Programmi e documenti (per estensione)**, File Anti-Virus sottopone a un'approfondita scansione antivirus i file con le estensioni sotto elencate. Se si abilita il filtro degli allegati, anche Mail Anti-Virus esaminerà questi file.

com – file eseguibile di un programma di dimensioni non superiori a 64 KB

exe – file eseguibile o archivio autoestraente

sys – file di sistema

prg – testo di programma per dBase, Clipper o Microsoft Visual FoxPro, o programma di WAVmaker

bin – file binario

bat – file batch

cmd – file di comando per Microsoft Windows NT (simile a un file .bat per DOS), OS/2

dpl – libreria compressa Borland Delphi

dll – libreria di caricamento dinamico

scr – splash screen di Microsoft Windows

cpl – modulo del pannello di controllo di Microsoft Windows

ocx – oggetto Microsoft OLE (Object Linking and Embedding)

tsp – programma eseguito in modalità split-time

drv – driver di periferica

vxd – Microsoft Windows virtual device driver

pif – program information file

lnk – file link di Microsoft Windows

reg – file della chiave di registro del sistema di Microsoft Windows

ini – file di inizializzazione

cla – classe Java

vbs – Visual Basic script

vbe – estensione video BIOS

js, jse – testo origine JavaScript

htm – documento ipertestuale

htt – intestazione ipertesto di Microsoft Windows

hta – file di ipertesto usato per aggiornare il registro del sistema operativo

asp – script Active Server Pages

chm – file HTML compilato

pht – HTML con script PHP incorporati

php – script incorporato in file HTML

wsh – file di configurazione Windows Script Host

wsf – script Microsoft Windows

the – wallpaper di Microsoft Windows 95

hlp – file Win Help

eml – file di posta di Microsoft Outlook Express

nws – nuovo file di posta di Microsoft Outlook Express

msg – file di posta Microsoft Mail

plg – e-mail

mbx – estensione dei messaggi di Microsoft Office Outlook salvati

doc – documento di Microsoft Office Word

dot – modello di documento di Microsoft Office Word

fpm – programma di database, file di avvio di Microsoft Visual FoxPro

rtf – documento Rich Text Format

shs – frammento Shell Scrap Object Handler

dwg – database blueprint AutoCAD

msi – pacchetto Microsoft Windows Installer

otm – progetto VBA per Microsoft Office Outlook

pdf – documento di Adobe Acrobat

swf – file Shockwave Flash

jpg, jpeg – formato immagini compresso

emf – formato Enhanced Metafile, la prossima generazione di metafile per Microsoft Windows OS. I file EMF non sono supportati da Microsoft Windows a 16 bit.

ico – icona di un programma (Windows, Unix, Gimp)

ov? – file eseguibili MS DOC

*xl** – documenti e file di Microsoft Office Excel, come: *xla* – estensione Microsoft Office Excel, *xlc* – diagramma, *xlt* – modelli di documento, ecc.

*pp** – documenti e file di Microsoft Office PowerPoint, come: *pps* – diapositiva Microsoft Office PowerPoint, *ppt* – presentazione, ecc.

*md** – documenti e file di Microsoft Office Access, come: *mda* – gruppo di lavoro di Microsoft Office Access, mdb – database, ecc.

Ricordare che il formato effettivo di un file può non corrispondere al formato indicato dall'estensione.

A.2. Maschere di esclusione file possibili

Osserviamo alcuni esempi delle maschere possibili per la creazione di elenchi di esclusione di file:

- Maschere senza percorso file:
  - ***.exe** – tutti i file con estensione exe
  - ***.ex?** – tutti i file con estensione *.ex?,* dove ? può rappresentare qualsiasi carattere singolo
  - **test** – tutti i file di nome *test*
- Maschere con percorso file assoluto:
  - **C:\dir*.*** o **C:\dir*** o **C:\dir** – tutti i file nella cartella *C:\dir*
  - **C:\dir*.exe** – tutti i file con estensione *.exe* contenuti nella cartella C:\dir\
  - **C:\dir*.ex?** – tutti i file con estensione *.ex?* nella cartella *C:\dir*, in cui ? è utilizzato in sostituzione di un carattere
  - **C:\dir\test** – solo il file *C:\dir\test*

  Se non si desidera che il programma esamini i file nelle sottocartelle di questa cartella, selezionare **Includi sottocartelle** durante la creazione della maschera.
- Maschere con percorso file relativo:
  - **dir*.*** o **dir*** o **dir** – tutti i file in tutte le cartelle *dir*
  - **dir\test** – tutti i file *test* nelle cartelle *dir*
  - **dir*.exe** – tutti i file con estensione *.exe* in tutte le cartelle in *dir*

- **dir*.ex?** – tutti i file con estensione *.ex?* in tutte le cartelle di *C:\dir*, in cui ? è utilizzato in sostituzione di un carattere

Se non si desidera che il programma esamini i file nelle sottocartelle di questa cartella, selezionare **Includi sottocartelle** durante la creazione della maschera.

Suggerimento:
Le maschere di esclusione *.* e * possono essere usate esclusivamente se si assegna un verdetto di minaccia esclusa. In caso contrario, la minaccia specificata non sarà rilevata in alcun oggetto. L'uso di queste maschere senza selezionare un verdetto disabilita il monitoraggio.
Si sconsiglia inoltre di selezionare un'unità virtuale creata sulla base di una directory di file system usando il comando *subst* come esclusione. Non avrebbe alcun senso farlo poiché, durante la scansione, il programma percepisce questa unità virtuale come cartella e di conseguenza la esamina.

A.3. Maschere di esclusione minacce possibili

Durante l'aggiunta di minacce con un determinato verdetto dalla classificazione dell'enciclopedia dei virus come esclusioni, è possibile specificare:

- Il nome completo della minaccia come indicato nell'enciclopedia dei virus all'indirizzo www.viruslist.com (per esempio, **not-a-virus:RiskWare.RemoteAdmin.RA.311** or **Flooder.Win32.Fuxx);**
- Il nome della minaccia mediante maschera. Ad esempio:
  - **not-a-virus*** – esclude dalla scansione potenziali programmi pericolosi e programmi scherzo.
  - ***Riskware.*** – esclude dalla scansione i riskware.
  - ***RemoteAdmin.*** – esclude dalla scansione tutti i programmi di amministrazione remota.

APPENDICE B. KASPERSKY LAB

Fondata nel 1997, Kaspersky Lab è diventata un leader indiscusso nel settore delle tecnologie per la sicurezza informatica. Produce una vasta gamma di applicazioni per la sicurezza dei dati e offre soluzioni complete di alto livello per garantire la sicurezza di computer e reti contro ogni tipo di programma dannoso, messaggi di posta elettronica non sollecitati e indesiderati e attacchi di pirateria informatica.

Kaspersky Lab è un'azienda internazionale con sede nella Federazione Russia e rappresentanti nel Regno Unito, Francia, Germania, Giappone, USA (CA), Benelux, Cina, Polonia e Romania. Recentemente è stato inaugurato un nuovo reparto, l'European Anti-Virus Research Centre, in Francia. Kaspersky Lab conta su una rete di partner costituita da oltre 500 aziende in tutto il mondo.

Oggi Kaspersky Lab si avvale di oltre 450 esperti, tutti specializzati in tecnologie antivirus, 10 dei quali in possesso di laurea in amministrazione aziendale, 16 di specializzazione postlaurea, e vari membri della Computer Anti-Virus Researcher's Organization (CARO).

Kaspersky Lab offre soluzioni di sicurezza di alto livello, elaborate grazie a un'esperienza esclusiva accumulata in più di 14 anni di attività nel settore dei virus informatici. La scrupolosa analisi delle attività dei virus consente all'azienda di offrire una protezione completa contro minacce presenti e future. La resistenza agli attacchi futuri è la strategia di base implementata in tutti i prodotti Kaspersky Lab. L'azienda si trova costantemente all'avanguardia rispetto a numerosi altri produttori offrendo una protezione antivirus completa per utenti domestici e commerciali.

Anni di duro lavoro ne hanno fatto un'azienda leader tra i principali produttori di software per la sicurezza informatica. Kaspersky Lab è stata una delle prime aziende di questo tipo a sviluppare i più severi standard della protezione antivirus. Il prodotto di punta dell'azienda, Kaspersky Anti-Virus, offre una protezione completa a tutti i livelli di una rete, inclusi workstation, server di file, sistemi di posta elettronica, firewall e gateway di Internet e computer portatili. I suoi strumenti di gestione, pratici e di facile utilizzo, garantiscono l'automazione avanzata per una sollecita protezione antivirus ad ogni livello dell'impresa. Numerose imprese di grande notorietà si affidano a Kaspersky Anti-Virus, per esempio Nokia ICG (USA), F-Secure (Finlandia), Aladdin (Israele), Sybari (USA), G Data (Germania), Deerfield (USA), Alt-N (USA), Microworld (India) e BorderWare (Canada).

Gli utenti Kaspersky Lab possono usufruire di una vasta serie di servizi supplementari volti a garantire sia un funzionamento stabile dei prodotti dell'azienda, sia la conformità a qualsiasi esigenza aziendale specifica. Il database antivirus di Kaspersky Lab viene aggiornato ogni ora. L'azienda offre ai

propri clienti un servizio di assistenza tecnica 24 ore su 24, disponibile in diverse lingue per soddisfare le esigenze di una clientela internazionale.

B.1. Altri prodotti Kaspersky Lab

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 è progettato per proteggere i personal computer dal software nocivo grazie a una combinazione ottimale di metodi di protezione antivirus convenzionali e nuove tecnologie proattive.

Il programma offre complesse verifiche antivirus fra cui:

- Scansione antivirus del traffico e-mail al livello del protocollo di trasmissione dati (POP3, IMAP e NNTP per la posta in arrivo, e SMTP per quella in uscita) indipendentemente dal client di posta usato, nonché riparazione dei database di posta.
- Scansione antivirus in tempo reale del traffico Internet trasferito mediante HTTP.
- Scansione antivirus di singoli file, directory o unità. Inoltre è possibile usare un'attività di scansione preimpostata per iniziare l'analisi antivirus esclusivamente delle aree critiche del sistema operativo e degli oggetti ad esecuzione automatica di Microsoft Windows.

La protezione proattiva offre le seguenti funzioni:

- **Controllo delle modifiche del file system**. Il programma consente agli utenti di creare un elenco di applicazioni che controllerà in base ai componenti. Aiuta a proteggere l'integrità delle applicazioni dall'influsso del software nocivo.
- **Monitoraggio dei processi nella RAM**. Kaspersky Anti-Virus 6.0 avvisa tempestivamente gli utenti ogni volta che rileva processi pericolosi, sospetti o nascosti, o nei casi in cui si siano verificate variazioni non autorizzate dei processi standard.
- **Monitoraggio delle variazioni del registro del SO** dovute al controllo del registro interno del sistema.
- **Blocco di macro VBA pericolose** nei documenti di Microsoft Office.
- **Ripristino del sistema** in seguito ai danni provocati da spyware nocivo a causa della registrazione di tutte le variazioni del registro e del file system del computer, e un'opportunità di eseguire il roll-back a discrezione dell'utente.

Kaspersky Lab News Agent

News Agent и progettato per comunicare tempestivamente le notizie pubblicate da Kaspersky Lab, per le notifiche relative allo status corrente dell'attivita dei virus e per notizie fresche. Il programma legge l'elenco dei canali news disponibili e il loro contenuto dai server di notizie di Kaspersky Lab con la frequenza specificata.

Il programma esegue le seguenti funzioni:

- Visualizza nella barra delle applicazioni lo status corrente dell'attività dei virus.
- Il prodotto consente di iscriversi e cancellarsi dai canali news.
- Recupera le notizie da ogni canale a cui è iscritto con la frequenza specificata e informa sulle ultime notizie.
- Consente di consultare le notizie sui canali a cui è iscritto.
- Consente di consultare l'elenco dei canali e il loro status.
- Consente di aprire nel browser pagine con particolari di notizie.

News Agent è un'applicazione Microsoft Windows stand-alone che puт essere utilizzata da sola o con varie soluzioni integrate offerte da Kaspersky Lab Ltd.

Kaspersky® OnLine Scanner

Questo programma è un servizio gratuito offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer. Kaspersky OnLine Scanner funziona direttamente dal browser web avvalendosi della tecnologia Microsoft ActiveX®. Gli utenti hanno così la possibilità di esaminare il computer in caso di sospetto di infezione virale. Con questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta.
- Selezionare per la scansione database antivirus standard/estesi.
- Salvare un report dei risultati di scansione in formato txt o html.

Kaspersky® OnLine Scanner Pro

Questo programma è un servizio a pagamento offerto ai visitatori del sito web Kaspersky Lab. Esso consente di effettuare un'efficace scansione antivirus online del computer e di riparare i file pericolosi. Kaspersky OnLine Scanner Pro funziona direttamente dal browser web avvalendosi della tecnologia Microsoft ActiveX®. Grazie a questo servizio, è possibile:

- Escludere dalla scansione archivi e database di posta.
- Selezionare per la scansione database antivirus standard/estesi.

- Salvare un report dei risultati di scansione in formato txt o html.

Kaspersky® Security for PDA

Kaspersky® Security for PDA offre un'affidabile protezione antivirus dei dati salvati su vari tipi di computer palmari e smartphone. Il programma contiene una serie ottimale di strumenti di protezione antivirus:

- **anti-virus scanner** per esaminare le informazioni (salvate sia nella memoria interna del PDA o smartphone oppure in schede di memoria di qualsiasi tipo) su richiesta;
- **un monitor antivirus** che intercetta i virus durante il trasferimento di dati con l'utility HotSync™ o prelevati da dispositivi portatili.

Esso offre l'accesso criptato al dispositivo e codifica tutti i dati memorizzati nel dispositivo e nelle schede di memoria.

Kaspersky Anti-Virus® Business Optimal

Il pacchetto offre una protezione completa esclusiva e configurabile dei dati per reti aziendali di piccole e medie dimensioni.

Kaspersky Anti-Virus® Business Optimal garantisce la protezione antivirus completa [3] per:

- *Workstation* con Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation e Linux;
- *File server* con Microsoft Windows NT 4.0 Server, Microsoft Windows 2000/2003 Server/Advanced Server, Microsoft Windows 2003 Server, Novell NetWare, FreeBSD e OpenBSD, Linux e Samba Servers;
- *Client di posta*, tra cui Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition.

Il kit di distribuzione di Kaspersky Anti-Virus® Business Optimal comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

La vasta gamma di applicazioni antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

[3] In base al tipo di kit di distribuzione.

Kaspersky® Corporate Suite

Questo pacchetto è stato sviluppato al fine di offrire una protezione totale dei dati di reti aziendali di qualsiasi dimensione e complessità. I componenti del pacchetto garantiscono la protezione di tutti i nodi di una rete aziendale, anche in ambienti informatici misti. Kaspersky® Corporate Suite supporta la maggior parte dei sistemi operativi e delle applicazioni in uso nelle aziende. Tutti i componenti del pacchetto sono gestiti da una console mediante un'unica interfaccia utente. Kaspersky® Corporate Suite è un affidabile sistema di protezione di alto livello totalmente compatibile con le esigenze specifiche di ogni configurazione di rete.

Kaspersky® Corporate Suite include la protezione antivirus completa per:

- *Workstation* con Microsoft Windows 98/ME, Microsoft Windows NT/2000/XP Workstation e Linux;
- File server con Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell NetWare, FreeBSD, OpenBSD, Linux e Samba Servers;
- *Client di posta*, inclusi Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim e Qmail;
- *Gateway di Internet*: CheckPoint Firewall –1; Microsoft ISA Server 2004 Enterprise Edition;
- *Computer palmari* (PDA) con Microsoft Windows CE e Palm OS, oltre a smartphone con Microsoft Windows Mobile 2003 for Smartphone e Microsoft Smartphone 2002.

Il kit di distribuzione di Kaspersky® Corporate Suite comprende Kaspersky® Administration Kit, uno *strumento esclusivo per la gestione e l'amministrazione automatizzate*.

La vasta gamma di applicazioni antivirus disponibili offre la massima libertà di scelta in base al sistema operativo e alle applicazioni in uso.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam è un'innovativa suite di software progettata per assistere le aziende con reti di piccole e medie dimensioni nella difesa contro i sempre più numerosi messaggi di posta elettronica non desiderati (spam). Il prodotto combina una tecnologia all'avanguardia in cui il programma analizza dal punto di vista linguistico il testo dei messaggi, i moderni metodi di filtraggio della posta elettronica (incluse le liste nere DNS e le caratteristiche della posta formale) e una raccolta esclusiva di servizi che consentono agli utenti di individuare ed eliminare fino al 95% del traffico indesiderato.

Installato all'ingresso di una rete, Kaspersky® Anti-Spam funziona come filtro controllando tutta la posta in entrata alla ricerca di spam. Il software è

compatibile con qualsiasi sistema di posta già in uso presso il cliente, e può essere installato sia su server mail esistenti sia su server dedicati.

L'elevato grado di efficacia di Kaspersky Anti-Spam è consentito dall'aggiornamento quotidiano del database di filtraggio dei contenuti con i campioni forniti dagli specialisti del laboratorio linguistico. I database vengono aggiornati ogni 20 minuti.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix è una soluzione studiata per la scansione antivirus della posta trasmessa mediante SMTP. L'applicazione contiene una serie di strumenti supplementari per il filtraggio del traffico e-mail per nome e per tipo di allegati MIME, oltre a una serie di strumenti volti a ridurre il carico sul sistema di posta e a prevenire gli attacchi informatici. La DNS Black List protegge dai messaggi di posta elettronica provenienti da server noti come origine di spam.

Kaspersky Security® for Microsoft Exchange 2003

Kaspersky Security for Microsoft Exchange esegue la scansione antivirus di messaggi inviati e ricevuti e di messaggi conservati sul server, compresi quelli conservati in cartelle pubbliche, e blocca la corrispondenza non desiderata per mezzo di tecnologie antispam "intelligenti" in combinazione con tecnologie Microsoft. L'applicazione esamina tutti i messaggi in arrivo su un Exchange Server attraverso il protocollo SMTP, controllando che non contengano virus per mezzo delle tecnologie antivirus Kaspersky Lab, e che non vi siano attributi di SPAM. L'applicazione blocca lo spam sulla base di attributi formali (indirizzo di posta, indirizzo IP, formato della lettera, intestazione) e analizza i contenuti dei messaggi e dei loro allegati per mezzo di tecnologie intelligenti, comprese esclusive firme grafiche per l'individuazione dello spam grafico. L'applicazione esamina sia il corpo del messaggio sia i file allegati.

Kaspersky® Mail Gateway

Kaspersky Mail Gateway è una soluzione completa per la protezione antivirus degli utenti dei sistemi di posta. Questa applicazione, installata tra la rete aziendale e Internet, esamina tutti i componenti dei messaggi e-mail per escludere la presenza di virus e altro malware (Spyware, Adware, ecc.) ed esegue il filtraggio antispam centralizzato del flusso dei messaggi. Questa soluzione offre anche alcune funzioni supplementari di filtraggio del traffico di posta.

B.2. Recapiti

Per qualsiasi domanda, commento o suggerimento, l'utente può rivolgersi ai distributori o direttamente a Kaspersky Lab. che sarà lieta di offrire assistenza per qualsiasi problematica relativa ai suoi prodotti, sia per telefono che per e-mail. Tutte le raccomandazioni e i suggerimenti pervenuti saranno presi in considerazione e valutati con attenzione..

Assistenza tecnica	Per qualsiasi informazione relativa al supporto tecnico, visitare la pagina http://www.kaspersky.com/supportinter.html Helpdesk: http://www.kaspersky.com/helpdesk.html
Informazioni generali	WWW: http://www.kaspersky.com http://www.viruslist.com Messaggio: info@kaspersky.com

APPENDICE C. CONTRATTO DI LICENZA

Contratto di licenza standard con l'utente finale

AVVERTENZA PER TUTTI GLI UTENTI: SI RACCOMANDA DI LEGGERE ATTENTAMENTE IL SEGUENTE CONTRATTO DI LICENZA ("CONTRATTO"), PER LA LICENZA DEL SOFTWARE KASPERSKY INTERNET SECURITY ("SOFTWARE") PRODOTTO DA KASPERSKY LAB.

QUANDO ACQUISTA IL PRESENTE SOFTWARE VIA INTERNET, FACENDO CLIC SUL PULSANTE DI ACCETTAZIONE, L'UTENTE ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO E A DIVENTARNE UNA DELLE PARTI. IN CASO CONTRARIO, FACENDO CLIC SUL PULSANTE CHE INDICA LA MANCATA ACCETTAZIONE DI TUTTE LE CONDIZIONI DEL PRESENTE, L'UTENTE RINUNCIA A INSTALLARE IL SOFTWARE.

SE IL SOFTWARE È STATO ACQUISTATO SU SUPPORTO FISICO E L'UTENTE HA ROTTO IL SIGILLO DELLA BUSTA DEL CD, ACCONSENTE (IN QUALITÀ DI PRIVATO O PERSONA GIURIDICA) AD ESSERE VINCOLATO DAL PRESENTE CONTRATTO. SE L'UTENTE NON ACCETTA TUTTE LE CONDIZIONI DEL PRESENTE CONTRATTO, EGLI DOVRÀ ASTENERSI DAL ROMPERE IL SIGILLO DELLA BUSTA DEL CD, SCARICARE, INSTALLARE O UTILIZZARE QUESTO SOFTWARE.

AI SENSI DELLA LEGISLAZIONE VIGENTE, PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI, ACQUISTATO ONLINE DAL SITO WEB DI KASPERSKY LAB O DEI SUOI PARTNER, IL CLIENTE HA QUATTORDICI (14) GIORNI LAVORATIVI DI TEMPO DALLA CONSEGNA DEL PRODOTTO PER RESTITUIRLO AL RIVENDITORE A FINI DI SOSTITUZIONE O DI RIMBORSO, A CONDIZIONE CHE IL SOFTWARE NON SIA STATO DISSIGILLATO.

PER QUANTO RIGUARDA IL SOFTWARE KASPERSKY PREVISTO PER SINGOLI UTENTI NON ACQUISTATO ONLINE VIA INTERNET, QUESTO SOFTWARE NON POTRÀ ESSERE RESTITUITO NÉ SOSTITUITO, ECCEZION FATTA PER LE CLAUSOLE CONTRARIE DEL PARTNER CHE VENDE IL PRODOTTO. IN QUESTO CASO, KASPERSKY LAB NON SARÀ RITENUTO RESPONSABILE DELLE CLAUSOLE DEL PARTNER.

IL DIRITTO ALLA RESTITUZIONE E AL RIMBORSO SI RIFERISCE SOLO ALL'ACQUIRENTE ORIGINARIO.

Qualsiasi riferimento al "Software" nel presente documento sarà da intendersi comprensivo di codice di attivazione fornito da Kaspersky Lab come parte integrante di Kaspersky Internet Security 6.0.

1. *Concessione della licenza.* Previo pagamento delle tasse di licenza applicabili e nel rispetto dei termini e delle condizioni del presente Contratto, con il presente Kaspersky Lab concede all'utente il diritto non esclusivo e non trasferibile di utilizzare una copia della versione specificata del Software e la documentazione in accompagnamento (la "Documentazione") per la durata del presente Contratto e unicamente a uso aziendale interno. È possibile installare una copia del Software su un computer.

1.1 *Uso.* Il Software è concesso in licenza in qualità di singolo prodotto; non può essere utilizzato su più di un computer o da più di un utente per volta, salvo diversamente specificato nella presente Sezione.

1.1.1 Il Software è "in uso" su un computer quando è caricato nella memoria temporanea (per esempio random access memory o RAM) oppure installato nella memoria permanente (per esempio disco fisso, CD-ROM o altro dispositivo di memorizzazione) di quel computer. La presente licenza autorizza l'utente a creare il numero di copie di backup del Software necessarie per il suo utilizzo legale e unicamente a scopi di archivio, a condizione che tutte le copie contengano le informazioni di proprietà del software. L'utente è tenuto a mantenere traccia del numero e dell'ubicazione di tutte le copie del Software e della Documentazione e a prendere tutte le ragionevoli precauzioni per proteggere il Software da copia o utilizzo non autorizzati.

1.1.2 Qualora l'utente metta in vendita il computer su cui è installato il Software, egli dovrà accertarsi che tutte le copie del Software siano state precedentemente cancellate.

1.1.3 È fatto divieto all'utente di decompilare, decodificare, disassemblare o altrimenti ridurre qualsiasi parte di questo Software in forma leggibile o consentire a terzi di farlo. Le informazioni di interfaccia necessarie per ottenere l'interoperatività del software con programmi per computer creati indipendentemente sarà fornita da Kaspersky Lab dietro richiesta e dietro pagamento dei ragionevoli costi e delle spese sostenute per procurarsi e fornire tali informazioni. Qualora Kaspersky Lab notificasse al cliente che, per qualsiasi ragione, inclusa senza tuttavia ad essa limitarsi quella dei costi, non intende fornire tali informazioni, l'utente sarà autorizzato a intraprendere le azioni necessarie per ottenere l'interoperatività a condizione di eseguire le operazioni di decompilazione o reverse engineering entro i limiti previsti dalla legge.

1.1.4 L'utente non deve né deve permettere ad altri (in modo diverso da quanto espressamente permesso nel presente) di effettuare la correzione di errori o altrimenti modificare, adattare o tradurre il Software né creare opere derivate dal Software.

1.1.5 È fatto divieto all'utente di concedere in locazione, in leasing o in prestito a terzi il Software o trasferire o cedere in sublicenza a terzi i diritti a lui conferiti dalla licenza.

1.1.6 All'utente è fatto divieto di utilizzare il Software con strumenti automatici, semi-automatici o manuali progettati per creare firme virus, routine di rilevazione virus, qualsiasi altro dato o codice per la rilevazione di codici o dati maligni.

2. *Assistenza.*

(i) Kaspersky Lab metterà a disposizione dell'utente i servizi di assistenza ("Servizi di assistenza") specificati di seguito, per la durata di un anno dal momento dell'attivazione, previo:

(a) pagamento della tariffa di assistenza corrente; e

(b) compilazione del Modulo di richiesta dei Servizi di assistenza fornito in allegato al presente Contratto o disponibile nel sito web di Kaspersky Lab, nel quale si richiede all'utente di fornire il proprio codice di attivazione fornito all'utente da Kaspersky Lab con il presente Contratto. Kaspersky Lab ha il diritto di stabilire, a propria discrezione, se l'utente abbia soddisfatto o meno questa condizione per la fornitura dei Servizi di Assistenza.

Il servizio di assistenza diventerà disponibile in seguito all'attivazione del Software. Il servizio di assistenza tecnica di Kaspersky Lab ha facoltà di richiedere all'utente finale un'ulteriore registrazione per poter usufruire dei servizi di assistenza.

Fino all'attivazione del Software e/o all'ottenimento dell'identificativo dell'utente finale (ID cliente) il servizio di assistenza tecnica offre assistenza esclusivamente per l'attivazione del Software e la registrazione dell'utente finale.

(ii) Con la compilazione del Modulo di sottoscrizione ai servizi di assistenza, l'utente accetta i termini della politica di tutela della riservatezza adottata da Kaspersky Lab e consultabile su www.kaspersky.com/privacy, e acconsente esplicitamente al trasferimento dei propri dati in paesi esterni a quello di residenza, come specificato nella politica di tutela della riservatezza.

(iii) I Servizi di Assistenza termineranno alla scadenza, salvo rinnovo annuo dietro il pagamento della tariffa annuale corrente e dietro soddisfacente nuova compilazione del Modulo di sottoscrizione ai servizi di assistenza .

(iv) Per "Servizi di assistenza" si intendono

(a) Aggiornamento del database antivirus ogni ora

(b) Aggiornamenti del database degli attacchi di rete

(c) Aggiornamenti del database antispam

(d) Aggiornamenti gratuiti del software, inclusi gli aggiornamenti della versione;

(e) Assistenza tecnica via Internet e numero verde fornita dal distributore e/o dal rivenditore;

(f) Aggiornamenti per il rilevamento e l'eliminazione di virus entro 24 ore.

(v) I servizi di assistenza sono forniti solo se e quando l'utente dispone della versione del Software più recente disponibile sul sito web ufficiale Kaspersky Lab (www.kaspersky.com) installata sul computer.

3. *Diritti di proprietà.* Il Software è protetto dalle leggi sul copyright. Kaspersky Lab e i relativi fornitori possiedono e mantengono tutti i diritti, l'autorità e gli interessi del Software e ad esso correlati, inclusi tutti i diritti di proprietà, i brevetti, i marchi commerciali e gli altri diritti di proprietà intellettuale ad esso connessi. Il possesso, l'installazione o l'utilizzo del Software non trasferiscono all'utente alcun diritto relativo alla proprietà intellettuale del Software e non determinano l'acquisizione di diritti sul Software salvo quelli espressamente indicati nel presente Contratto.

4. *Riservatezza.* L'utente riconosce che il Software e la Documentazione, inclusa la specifica configurazione e la struttura dei singoli programmi costituiscono informazioni proprietarie riservate di Kaspersky Lab. L'utente non dovrà divulgare, fornire o altrimenti rendere disponibili tali informazioni riservate in qualsivoglia forma a terzi senza previo consenso scritto di Kaspersky Lab. Dovrà inoltre applicare ragionevoli misure di sicurezza volte a proteggere tali informazioni riservate ma, senza tuttavia limitarsi a quanto sopra espresso dovrà fare quanto in suo potere per tutelare la sicurezza del codice di attivazione.

5. *Garanzia limitata.*

(i) Kaspersky Lab garantisce che per un periodo di [6] mesi a decorrere dal primo caricamento o installazione il Software acquistato su supporto fisico opererà sostanzialmente in conformità alle funzioni descritte nella Documentazione, a condizione che sia utilizzato in modo corretto e nella maniera specificata nella Documentazione.

(ii) L'utente si assume ogni responsabilità relativamente al fatto che il presente Software soddisfi i propri requisiti. Kaspersky Lab non garantisce che il Software e/o la Documentazione siano idonei a soddisfare le esigenze dell'utente né che il suo utilizzo sia esente da interruzioni o privo di errori.

(iii) Kaspersky Lab non garantisce che il Software identifichi tutti i virus noti né esclude che possa occasionalmente eseguire il report erroneo di un virus in un titolo non infettato da quel virus.

(iv) L'indennizzo dell'utente e la completa responsabilità di Kaspersky Lab per la violazione della garanzia di cui al paragrafo (i) saranno a discrezione di Kaspersky Lab, che deciderà se riparare, sostituire o rimborsare il Software in caso di reclamo a Kaspersky Lab o suoi fornitori durante il periodo di garanzia.

L'utente dovrà fornire tutte le informazioni ragionevolmente necessarie per agevolare il Fornitore nel ripristino dell'articolo difettoso.

(v) La garanzia di cui al punto (i) non è applicabile qualora l'utente (a) apporti modifiche al presente Software o determini la necessità di modificarlo senza il consenso di Kaspersky Lab, (b) utilizzi il Software in modo difforme dall'uso previsto o (c) impieghi il Software per usi diversi da quelli permessi ai sensi del presente Contratto.

(vi) Le garanzie e le condizioni stabilite dal presente Contratto sostituiscono eventuali altre condizioni, garanzie o termini relativi alla fornitura o fornitura presunta dello stesso; la mancata fornitura o eventuali ritardi nella fornitura del Software o della Documentazione che, salvo per il presente paragrafo (vi) potrebbero avere effetto tra Kaspersky Lab e l'utente o potrebbero essere diversamente impliciti o integrati nel presente Contratto o in un eventuale accordo collaterale mediante statuto, diritto consuetudinario o altrimenti, sono esclusi mediante il presente (inclusi, senza tuttavia ad essi limitarsi, le condizioni implicite, le garanzie o altri termini relativi a qualità soddisfacente, idoneità per l'uso previsto o esercizio di ragionevoli competenze e cautele).

6. *Responsabilità limitata.*

(i) Nessun elemento del presente Contratto escluderà o limiterà la responsabilità di Kaspersky Lab in merito a (a) responsabilità civile per frode, (b) decesso o lesioni personali causate da un suo mancato esercizio di cautela ai sensi del diritto consuetudinario o dalla violazione negligente di una delle condizioni del presente Contratto, (c) eventuali altre responsabilità che non possano essere escluse per legge.

(ii) Ai sensi del paragrafo (i) di cui sopra, Kaspersky Lab non deve essere ritenuto responsabile (relativamente al contratto, per responsabilità civile, restituzione o altro) per i seguenti danni o perdite (siano questi danni o perdite previsti, prevedibili, noti o altro):

(a) perdita di reddito;

(b) perdita di utili effettivi o presunti (inclusa la perdita di utili sui contratti);

(c) perdita di liquidità;

(d) perdita di risparmi presunti;

(e) perdita di affari;

(f) perdita di opportunità;

(g) perdita di avviamento;

(h) danni alla reputazione;

(i) perdita, danni o corruzione di dati; o

(j) eventuali perdite indirette o conseguenti o danni arrecati in qualsiasi modo (inclusi, a scanso di dubbi, i danni o le perdite del tipo specificato nei paragrafi (ii), da (a) a (ii), (i).

(iii) Ai sensi del paragrafo (i), la responsabilità di Kaspersky Lab (né a fini del contratto, frode, restituzione o in nessun'altra maniera) derivante da o in relazione alla fornitura del Software non supererà in nessun caso l'importo corrispondente all'onere ugualmente sostenuto dall'utente per il Software.

7. Il presente Contratto contiene per intero tutti gli intendimenti delle parti relativamente all'oggetto del presente e sostituisce tutti gli eventuali accordi, impegni e promesse precedenti tra l'utente e Kaspersky Lab, sia orali che per iscritto, che possano scaturire o essere impliciti da qualsiasi cosa scritta o pronunciata oralmente in fase di negoziazione tra Kaspersky Lab o suoi rappresentanti e l'utente precedentemente al presente Contratto; tutti gli accordi precedenti tra le parti relativamente all'oggetto di cui sopra decadranno a partire dalla Data di entrata in vigore del presente Contratto.