ESET NOD32 ANTIVIRUS 7

Guida dell'utente

(destinata alla versione del prodotto 7.0 e a versioni successive)

Microsoft® Windows® 8.1 / 8 / 7 / Vista / XP / Home Server 2003 / Home Server 2011

Fare clic qui per scaricare la versione più recente di questo documento

ESET NOD32 ANTIVIRUS

Assistenza clienti nel mondo: www.eset.it/supporto

REV. 5/13/2014

Contenuti

1. ESET NOD32 Antivirus

ESET NOD32 Antivirus rappresenta un nuovo approccio alla protezione effettivamente integrata del computer. La versione più recente del motore di controllo ThreatSense® sfrutta la velocità e la precisione per proteggere il computer. Il risultato è un sistema intelligente che rileva continuamente attacchi e software dannoso che potrebbero minacciare il computer.

ESET NOD32 Antivirus è una soluzione di protezione completa che associa massime prestazioni a un impatto minimo sul sistema. Le tecnologie avanzate utilizzano l'intelligenza artificiale per prevenire l'infiltrazione da parte di virus, spyware, trojan horse, worm, adware, rootkit e altre minacce senza ripercussioni sulle prestazioni del sistema o interruzioni del computer.

Funzioni e vantaggi

Antivirus e antispyware	Rileva e pulisce in modo proattivo virus, worm, trojan e rootkit noti e sconosciuti. La tecnologia dell'**Euristica avanzata** rileva persino malware mai rilevati precedenza, proteggendo l'utente da minacce sconosciute e neutralizzandole prima che possano arrecare danni al sistema. La **Protezione accesso Web** e **Anti-Phishing** monitora la comunicazione tra i browser Web e i server remoti (compreso il protocollo SSL). La **Protezione client di posta** garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3(S) e IMAP(S).
Aggiornamenti periodici	L'aggiornamento periodico del database delle firme antivirali e dei moduli del programma rappresenta il metodo migliore per ottenere il livello massimo di protezione del computer.
ESET Live Grid (Reputazione basata sul cloud)	È possibile controllare la reputazione dei processi e dei file in esecuzione direttamente da ESET NOD32 Antivirus.
Controllo dispositivi	Controlla automaticamente tutte le memorie USB, le schede di memoria e i CD/DVD. Blocca i supporti rimovibili in base al tipo di supporto, al produttore, alle dimensioni e ad altri attributi.
Funzionalità HIPS	È possibile personalizzare il comportamento del sistema in maggiori dettagli, specificando le regole per il registro di sistema, i processi e i programmi attivi e ottimizzando il livello di protezione.
Modalità giocatore	Rimanda tutte le finestre popup, gli aggiornamenti o altre attività di sistema intensive allo scopo di preservare le risorse di sistema per le attività di gioco o altre attività a schermo intero.

Affinché le funzioni di ESET NOD32 Antivirus siano attive, è necessario attivare una licenza. Si consiglia di rinnovare la licenza di ESET NOD32 Antivirus alcune settimane prima della scadenza.

1.1 Novità della versione 7

La versione 7 di ESET NOD32 Antivirus presenta numerosi piccoli miglioramenti:

- **Controllo dispositivi** - Sostituzione della funzione Controllo supporti rimovibili utilizzata nella versione 5 e 6. Questo modulo consente di controllare, bloccare o regolare le estensioni dei filtri o delle autorizzazioni e di definire la capacità dell'utente di accedere e di utilizzare un determinato dispositivo.
- **Exploit Blocker** - Progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office.
- **Scanner memoria avanzato** - Lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscazione e/o crittografia.
- **Miglioramenti Anti-phishing** - ESET NOD32 Antivirus è oggi in grado di bloccare siti scam e phishing. Invio potenziato di siti sospetti e falsi positivi da parte degli utenti.

- **Strumento di pulizia specializzato** - Fusione delle prime 3-5 minacce di malware critici con maggiore prevalenza.
- **Installazione più rapida e affidabile** - Comprende l'avvio di un primo controllo automatico 20 minuti dopo l'installazione o il riavvio.
- **Compatibilità plugin e-mail** - Il plugin è ora integrato in Office 2013 e Windows Live Mail.
- **Compatibilità potenziata in Windows 8/8.1** - Oggi, ESET SysRescue funziona perfettamente su Windows 8. Le notifiche di avviso di tipo popup, da oggi visualizzabili in ambiente Windows 8, inviano informazioni sui rilevamenti HIPS o di file che richiedono l'interazione dell'utente o il download di applicazioni potenzialmente indesiderate.

Per ulteriori informazioni sulle nuove funzionalità di ESET NOD32 Antivirus, consultare il seguente articolo della Knowledge base ESET:
Novità in ESET Smart Security 7 ed ESET NOD32 Antivirus 7

1.2 Requisiti di sistema

Per il corretto funzionamento di ESET NOD32 Antivirus, il sistema deve soddisfare i seguenti requisiti hardware e software:

Microsoft® Windows® XP

600 MHz 32 bit (x86)/64 bit (x64)
128 MB di memoria di sistema (RAM)
320 MB di spazio disponibile
Super VGA (800 x 600)

Microsoft® Windows® 8.1, 8, 7, Vista, Home Server

1 GHz 32 bit (x86)/64 bit (x64)
512 MB di memoria di sistema (RAM)
320 MB di spazio disponibile
Super VGA (800 x 600)

1.3 Prevenzione

Quando si utilizza il computer, e in particolare quando si naviga in Internet, occorre tenere presente che nessun sistema antivirus al mondo può eliminare completamente il rischio di infiltrazioni e attacchi. Per garantire la massima protezione e comodità, è essenziale utilizzare correttamente la soluzione antivirus e attenersi ad alcune regole utili:

Eseguire regolarmente l'aggiornamento

In base alle statistiche ottenute da ESET Live Grid, ogni giorno vengono create migliaia di infiltrazioni nuove e uniche per aggirare le misure di sicurezza esistenti e generare profitti per i rispettivi autori, a spese e discapito di altri utenti. Gli specialisti del laboratorio antivirus ESET analizzano queste minacce su base giornaliera, preparando e rilasciando gli aggiornamenti per migliorare costantemente il livello di protezione degli utenti. Per garantire l'efficacia massima di questi aggiornamenti, è importante che questi vengano configurati correttamente sul sistema. Per ulteriori informazioni su come configurare gli aggiornamenti, consultare il capitolo Impostazione dell'aggiornamento.

Scaricare le patch di protezione

Gli autori di software dannoso sfruttano spesso le varie vulnerabilità dei sistemi per aumentare l'efficacia della diffusione di codice dannoso. In considerazione di ciò, le società di software esaminano attentamente eventuali vulnerabilità nelle applicazioni create e rilasciano regolarmente gli aggiornamenti di protezione allo scopo di eliminare le potenziali minacce. È importante scaricare questi aggiornamenti della protezione non appena vengono rilasciati. Microsoft Windows e i Web browser quali Internet Explorer sono due esempi di programmi per cui gli aggiornamenti di protezione vengono rilasciati periodicamente.

Eseguire il backup dei dati importanti

Di norma, gli autori di malware non sono interessati alle esigenze degli utenti e l'attività dei programmi dannosi comporta spesso un malfunzionamento generale del sistema operativo e la perdita di dati importanti. È importante eseguire un backup periodico dei dati importanti e sensibili su un supporto esterno, ad esempio un DVD o un'unità hard disk esterna. Ciò consente di recuperare i dati in modo semplice e veloce in caso di errore del sistema.

Eseguire regolarmente la scansione antivirus

Il rilevamento di virus, worm, trojan e rootkit più noti e sconosciuti è gestito dal modulo della protezione file system in tempo reale. Ciò significa che ad ogni accesso ad un file o apertura dello stesso da parte dell'utente, questo viene controllato per la ricerca di attività malware. Si consiglia di eseguire un Controllo del computer completo almeno una volta al mese, in quanto le firme dei malware cambiano continuamente e il database delle firme antivirali si aggiorna con frequenza giornaliera.

Seguire le regole di protezione di base

Questa è la regola più utile e più efficace di tutte: essere sempre prudenti. Oggi, molte infiltrazioni richiedono l'intervento dell'utente affinché possano essere eseguite e distribuite. Adottando un comportamento prudente all'apertura di nuovi file, non sarà più necessario perdere tempo ed energie per pulire le infiltrazioni. Seguono alcune linee guida utili:

- Non visitare siti Web sospetti, con molte finestre popup e pubblicità che attirano l'attenzione.
- Prestare attenzione durante l'installazione di programmi freeware, pacchetti codec e così via. Utilizzare solo programmi sicuri e visitare solo siti Web Internet sicuri.
- Essere prudenti quando si aprono gli allegati e-mail, in particolare quelli inviati da programmi massmailer a destinatari multipli e quelli inviati da mittenti sconosciuti.
- Non utilizzare un account Amministratore per eseguire le attività quotidiane sul computer.

2. Installazione

Esistono vari metodi di installazione di ESET NOD32 Antivirus sul computer. I metodi di installazione possono variare in base al Paese e ai mezzi di distribuzione:

- Live installer può essere scaricato dal sito Web ESET. Il pacchetto di installazione è universale per tutte le lingue (scegliere la lingua desiderata). Di per sé, il Live installer è un file di piccole dimensioni; i file aggiuntivi necessari per l'installazione di ESET NOD32 Antivirus verranno scaricati automaticamente.

- Installazione off-line - Questo tipo di installazione viene utilizzato per le installazioni mediante il CD/DVD di un prodotto. Questa installazione utilizza un file *.msi* più grande rispetto al file Live installer e non richiede una connessione a Internet o file aggiuntivi per il completamento del processo.

Importante: Verificare che nel computer non siano installati altri programmi antivirus prima dell'installazione di ESET NOD32 Antivirus. Se su un singolo computer sono installate due o più soluzioni antivirus, potrebbero entrare in conflitto tra loro. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema. Per un elenco degli strumenti di disinstallazione dei software antivirus comuni, consultare l'articolo della Knowledge Base ESET (disponibile in inglese e in altre lingue).

2.1 Live installer

Dopo aver scaricato il pacchetto di installazione *Live installer*, fare doppio clic sul file di installazione e seguire le istruzioni dettagliate nella finestra del programma di installazione.

Importante: per questo tipo di installazione, è necessario effettuare la connessione a Internet.

Selezionare la lingua desiderata dal menu a discesa **Seleziona la lingua del prodotto** e fare clic su **Installa**. Attendere alcuni istanti per il download dei file di installazione.

Dopo aver accettato l'**Accordo di licenza per l'utente finale**, verrà richiesto di configurare **ESET Live Grid**. ESET Live Grid garantisce un aggiornamento tempestivo e ininterrotto di ESET sulle nuove minacce al fine di garantire la protezione di tutti gli utenti. Il sistema consente l'invio di nuove minacce al laboratorio antivirus ESET, dove i virus verranno analizzati, elaborati e aggiunti al database delle firme antivirali.

Per impostazione predefinita, viene selezionata l'opzione **Sì, desidero partecipare**, che attiverà questa funzione.

Il passaggio successivo del processo di installazione consiste nella configurazione dell'opzione di rilevamento delle applicazioni potenzialmente indesiderate. Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sul comportamento del sistema operativo. Per ulteriori informazioni, consultare il capitolo Applicazioni potenzialmente indesiderate.

Fare clic su **Avanti** per avviare il processo di installazione.

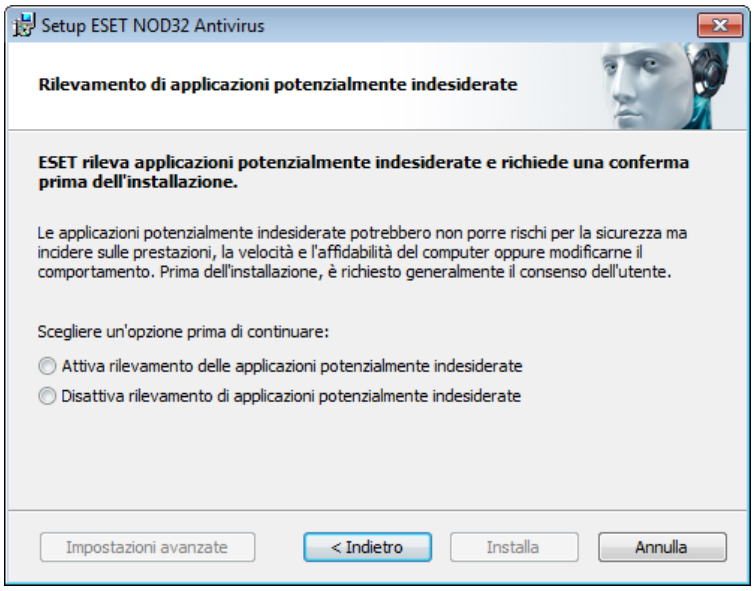
2.2 Installazione off-line

Dopo aver avviato il pacchetto di installazione off-line (.msi), la procedura di installazione guidata condurrà l'utente attraverso il processo di configurazione.

Il programma controlla innanzitutto se è disponibile una versione più recente di ESET NOD32 Antivirus. Se è disponibile una versione più recente, ciò verrà segnalato all'utente durante il primo passaggio del processo di installazione. Se si seleziona **Scarica e installa la nuova versione**, verrà scaricata la nuova versione e sarà possibile proseguire con l'installazione. La casella di controllo è visibile solo in caso di disponibilità di una versione più recente rispetto a quella installata dall'utente.

Successivamente, verrà visualizzato l'Accordo di licenza per l'utente finale. Si prega di leggere l'accordo e di fare clic su **Accetto** per confermare l'accettazione dei termini dell'Accordo di licenza per l'utente finale. Dopo aver accettato, l'installazione procederà.

Per ulteriori informazioni sui passaggi di installazione, **ESET Live Grid** e **Rilevamento di applicazioni potenzialmente indesiderate**, seguire le istruzioni nella sezione precedente (vedere "Live installer").



La modalità di installazione offre opzioni di configurazione adatte alla maggior parte degli utenti. Tali impostazioni garantiscono un livello di protezione ottimale, un'elevata facilità di configurazione e prestazioni del sistema potenziate. Le **Impostazioni avanzate** sono pensate per gli utenti che hanno esperienza nell'ottimizzazione dei programmi e che desiderano modificare le impostazioni avanzate durante l'installazione. Fare clic su **Installa** per avviare il processo di installazione e saltare le Impostazioni avanzate.

2.2.1 Impostazioni avanzate

Dopo aver selezionato **Impostazioni avanzate**, all'utente verrà richiesto di selezionare un percorso per l'installazione. Per impostazione predefinita, il programma viene installato nella directory seguente:

C:\Programmi\ESET\ESET NOD32 Antivirus

Scegliere **Sfoglia...** per selezionare un percorso diverso (scelta non consigliata).

Fare clic su **Avanti** per configurare la connessione a Internet. Se si utilizza un server proxy, è necessario configurarlo correttamente per l'esecuzione degli aggiornamenti delle firme antivirali. Se non si è sicuri se si sta utilizzando un server proxy per la connessione a Internet, selezionare **Utilizzo le stesse impostazioni di Internet Explorer (scelta consigliata)** e fare clic su **Avanti**. Se non si utilizza un server proxy, selezionare **Non utilizzo un server proxy**.

Per configurare le impostazioni del server proxy, selezionare **Viene utilizzato un server proxy**, quindi fare clic su **Avanti**. Immettere l'indirizzo IP o l'URL del server proxy nel campo **Indirizzo**. Nel campo **Porta** specificare la porta sulla quale il server proxy accetta le connessioni (per impostazione predefinita, la porta 3128). Nel caso in cui il server proxy richieda l'autenticazione, sarà necessario immettere un **Nome utente** e **Password** validi per consentire l'accesso al server proxy. Se si desidera è anche possibile copiare le impostazioni del server proxy da Internet Explorer.. A tale scopo, fare clic su **Applica** e confermare la selezione.

L'installazione personalizzata consente all'utente di definire le modalità di gestione degli aggiornamenti automatici del programma sul sistema. Fare clic su **Modifica...** per accedere alle Impostazioni avanzate.

Se non si desidera aggiornare i componenti di programma, selezionare **Non aggiornare mai i componenti di programma**. Selezionare **Chiedi prima di scaricare i componenti di programma** per visualizzare una finestra di conferma ogni volta che il sistema tenta di scaricare i componenti di programma. Per scaricare automaticamente gli upgrade dei componenti di programma, selezionare **Aggiorna sempre i componenti di programma**.

NOTA: in genere, dopo aver aggiornato un componente di programma, è necessario riavviare il sistema. Si consiglia di selezionare **Se necessario, riavvia il computer senza notifica**.

Nella finestra di installazione successiva è disponibile l'opzione per impostare una password per proteggere le impostazioni del programma. Selezionare **Proteggi le impostazioni di configurazione con password** e inserire la password nei campi **Nuova password** e **Conferma nuova password**. Questa password verrà richiesta per modificare o accedere alle impostazioni di ESET NOD32 Antivirus. Se i campi delle password corrispondono, fare clic su **Avanti** per continuare.

Per completare i successivi passaggi di installazione, **ESET Live Grid** e **Rilevamento di applicazioni potenzialmente indesiderate**, seguire le istruzioni nella sezione Live installer (vedere "Live installer").

Per disattivare il primo controllo dopo l'installazione, eseguito normalmente al termine dell'installazione ai fini della ricerca di codice dannoso, deselezionare la casella di controllo accanto a **Attiva controllo dopo l'installazione**. Fare clic su **Installa** nella finestra **Pronto all'installazione** per completare l'installazione.

2.3 Attivazione prodotto

Al termine dell'installazione, all'utente verrà richiesto di attivare il prodotto.

Esistono vari metodi per attivare il prodotto. La disponibilità di uno scenario di attivazione specifico nella finestra di attivazione potrebbe variare in base al paese e ai mezzi di distribuzione (CD/DVD, pagina Web ESET, ecc.).

Se è stata acquistata una versione presso un rivenditore al dettaglio del prodotto, selezionare **Attivazione tramite chiave**. La chiave di attivazione si trova generalmente all'interno o sul retro della confezione del prodotto. Per eseguire correttamente l'attivazione, è necessario inserire la chiave di attivazione così come fornita.

Se sono stati ricevuti un nome utente e una password, selezionare **Attivazione tramite nome utente e password** e inserire le credenziali negli appositi campi.

Se si desidera provare ESET NOD32 Antivirus prima di acquistarlo, selezionare **Attiva licenza di valutazione**. Inserire l' indirizzo e-mail e il paese per attivare ESET NOD32 Antivirus per un periodo di tempo limitato. La licenza di prova verrà inviata all'indirizzo indicato dall'utente. È possibile attivare una sola licenza di prova per cliente.

Qualora non si disponga di una licenza e si desideri acquistarne una, fare clic su **Acquista licenza**. In tal modo si verrà reindirizzati al sito Web o al distributore locale ESET.

Selezionare **Attiva in seguito** se si desidera valutare rapidamente il prodotto e non attivarlo immediatamente o se si desidera attivarlo in seguito.

È inoltre possibile attivare una copia di ESET NOD32 Antivirus direttamente dal programma. Fare clic sull'icona Menu del programma nell'angolo in alto a destra oppure fare clic con il pulsante destro del mouse sull'icona ESET NOD32 Antivirus sulla barra delle applicazioni e selezionare **Attivazione del prodotto...** nel menu.

2.4 Inserimento di nome utente e password

Per garantire una funzionalità ottimale è fondamentale che il programma venga aggiornato automaticamente. Ciò è possibile solo inserendo un Nome utente e una Password validi in **Configurazione aggiornamento**.

In caso di mancato inserimento di un Nome utente e di una Password durante l'installazione, è possibile inserirli in questa fase. Nella finestra principale del programma, fare clic su **Guida e supporto tecnico**, quindi selezionare **Attiva licenza** e inserire i dati di licenza ricevuti insieme al prodotto di protezione ESET nella finestra Attivazione prodotto.

Quando si immette il **Nome utente** e **Password**, è importante immetterli esattamente come sono scritti:

- Il nome utente e la password fanno distinzione tra maiuscole e minuscole e nel nome utente è necessaria la lineetta.
- La password è composta da dieci caratteri scritti tutti in lettere minuscole.
- La lettera L non viene utilizzata nelle password (al suo posto viene usato il numero uno (1)).
- Un grande "0" corrisponde al numero zero (0), mentre una piccola "o" corrisponde alla lettera o scritta in minuscolo.

Per evitare errori, si consiglia di copiare e incollare i dati dal messaggio e-mail di registrazione.

2.5 Aggiornamento a una versione più recente

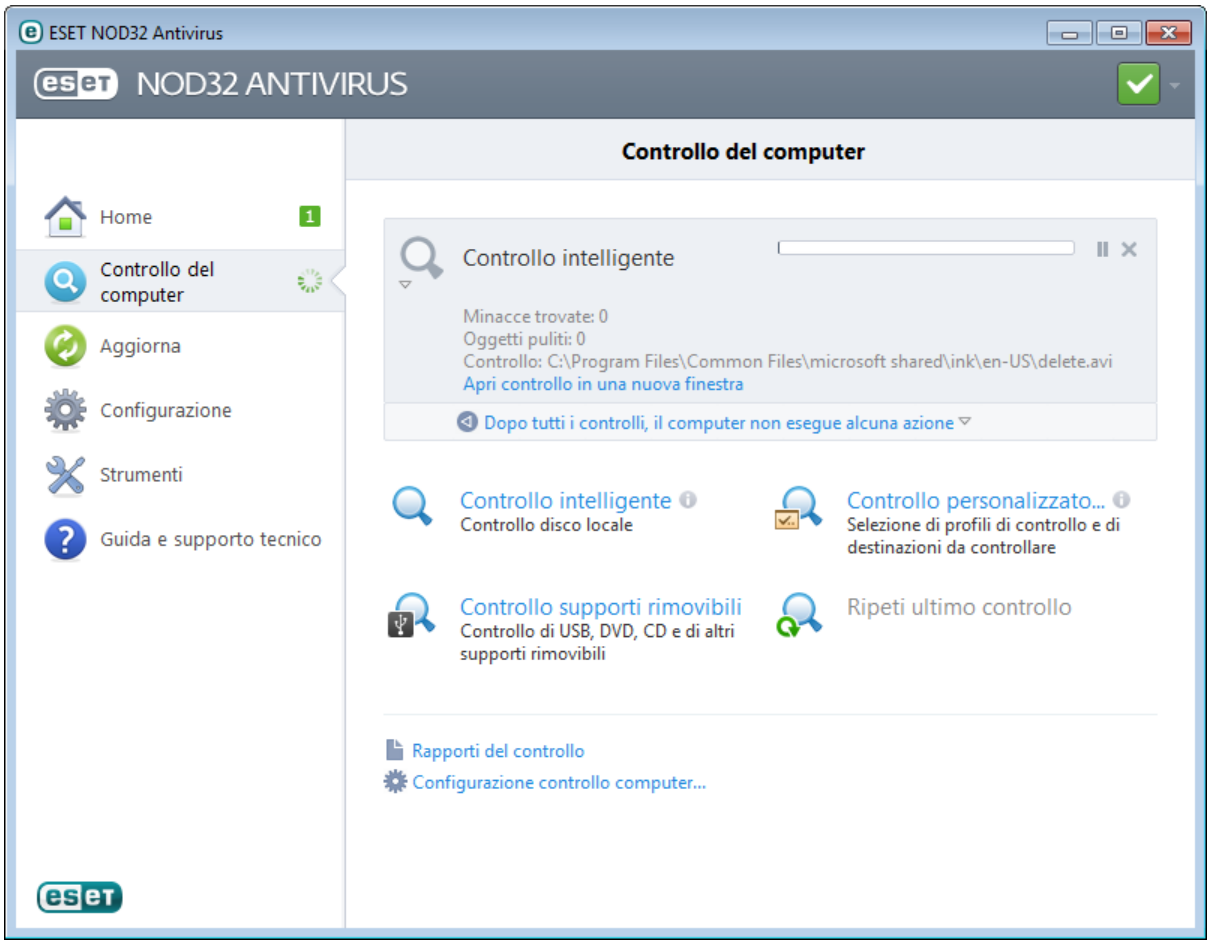
Le nuove versioni di ESET NOD32 Antivirus vengono rilasciate ai fini dell'implementazione di miglioramenti o della correzione di errori che non è possibile risolvere mediante aggiornamenti automatici dei moduli del programma. L'aggiornamento a una versione più recente può essere eseguito in diversi modi:

1. Automaticamente tramite un aggiornamento del programma.
   L'upgrade del programma, che viene distribuito a tutti gli utenti e che potrebbe incidere su alcune configurazioni di sistema, viene rilasciato dopo un lungo periodo di prova per garantire un livello di compatibilità massimo. Se è necessario eseguire l'aggiornamento a una versione più recente nel momento in cui viene rilasciato, usare uno dei metodi seguenti.
2. Manualmente, nella finestra principale del programma, facendo clic su **Installa/Ricerca aggiornamenti** nella sezione **Aggiorna**.
3. Manualmente scaricando e installando una versione più recente su quella precedente.

2.6 Primo controllo dopo l'installazione

Dopo aver installato ESET NOD32 Antivirus, verrà avviato un controllo del computer 20 minuti dopo l'installazione o il riavvio del computer ai fini della ricerca di codice dannoso.

È inoltre possibile avviare manualmente un controllo del computer dalla finestra principale del programma facendo clic su **Controllo del computer** > **Controllo intelligente**. Per ulteriori informazioni sui controlli del computer, consultare la sezione Controllo del computer.



3. Guida introduttiva

In questo capitolo viene fornita una panoramica su ESET NOD32 Antivirus e sulle configurazioni di base.

3.1 La finestra principale del programma

La finestra principale di ESET NOD32 Antivirus è suddivisa in due sezioni principali. La finestra principale sulla destra contiene informazioni corrispondenti all'opzione selezionata dal menu principale sulla sinistra.

Di seguito è riportata una descrizione delle opzioni del menu principale:

Stato protezione - Fornisce informazioni relative allo stato di protezione di ESET NOD32 Antivirus.

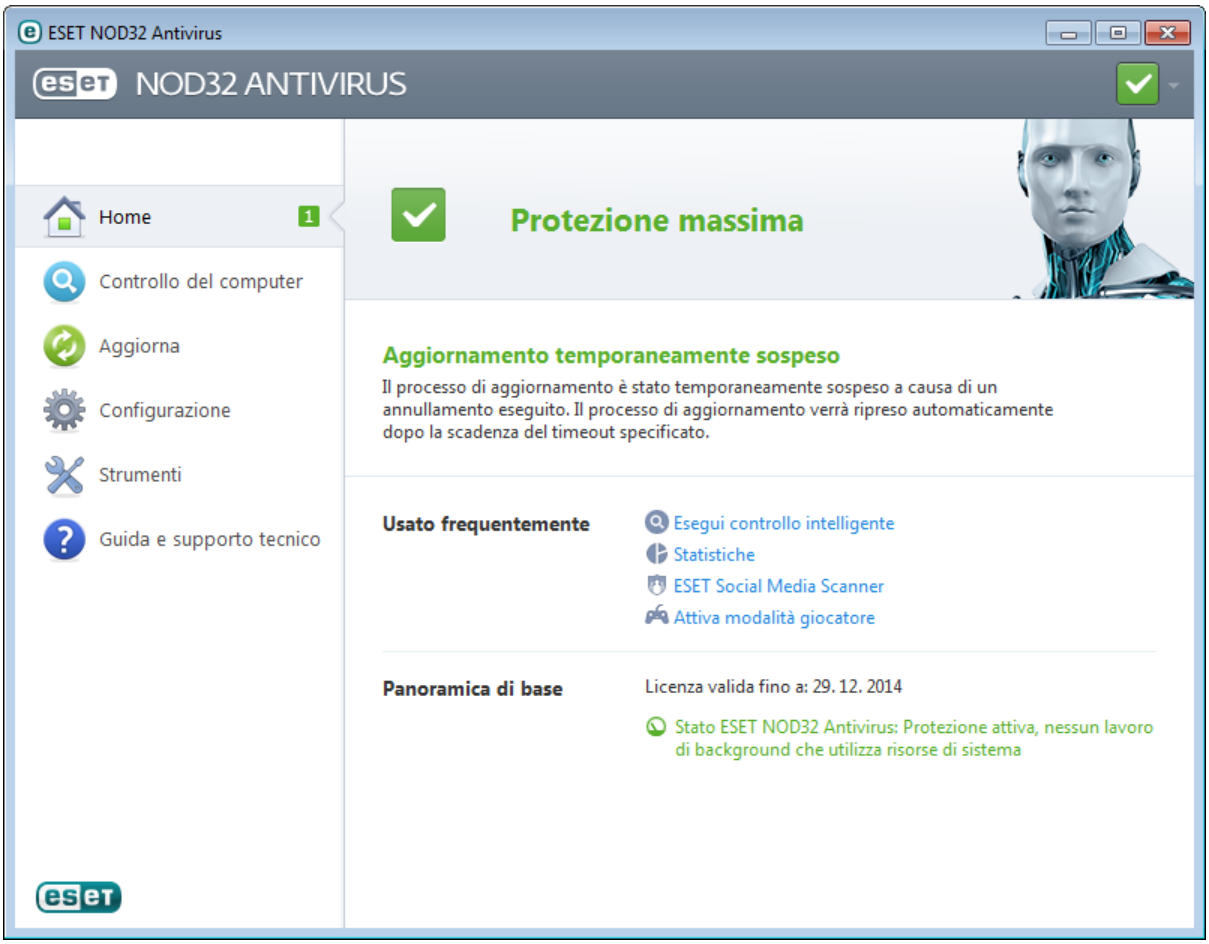
Controllo computer - Questa opzione consente di configurare e avviare un Controllo intelligente o un Controllo personalizzato.

Aggiorna - Consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.

Configurazione - Selezionare questa opzione per regolare il livello di protezione per Computer, Web ed e-mail.

Strumenti - Consente di accedere ai File di rapporto, Statistiche di protezione, Attività di verifica, Processi in esecuzione, Pianificazione attività, Quarantena, ESET SysInspector e ESET SysRescue.

Guida e supporto tecnico - Consente di accedere ai file della Guida, alla Knowledge Base ESET, al sito Web ESET e ai collegamenti per aprire una richiesta di assistenza al Supporto tecnico.



Nella schermata **Stato protezione** sono visualizzate informazioni sulla sicurezza e sul livello di protezione corrente del computer. Nella finestra di stato sono inoltre visualizzate le Funzionalità usate frequentemente di ESET NOD32 Antivirus. Nella finestra **Panoramica di base** sono inoltre disponibili informazioni sulla data di scadenza del programma.

L'icona verde e il colore verde dello stato **Protezione massima** indicano un livello di protezione massimo.

Cosa fare se il programma non funziona correttamente?

Se i moduli attivati funzionano correttamente, l'icona dello Stato di protezione sarà verde. Un punto esclamativo rosso o un'icona di notifica arancione indica che non è garantito il livello massimo di protezione. In **Home** verranno visualizzate informazioni aggiuntive sullo stato di protezione di ciascun modulo, nonché le soluzioni consigliate per il ripristino della protezione completa. Per modificare lo stato dei singoli moduli, fare clic su **Configurazione** e selezionare il modulo desiderato.

L'icona rossa e il colore rosso dello stato Protezione massima non garantiscono la segnalazione di problemi critici da parte dello stato.
Esistono vari motivi alla base della visualizzazione di questo stato, tra cui:

- **Prodotto non attivato** - È possibile attivare ESET NOD32 Antivirus da **Stato protezione** facendo clic su **Attiva versione completa** o **Acquista ora** in stato di protezione.
- **Il database delle firme antivirali è obsoleto** - Questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornamento del database delle firme antivirali. Si consiglia di controllare le impostazioni di aggiornamento. I motivi più comuni alla base di questo errore consistono in un inserimento errato dei dati di autenticazione o in una configurazione non corretta delle impostazioni di connessione.
- **Protezione antivirus e antispyware disattivata** - È possibile riattivare la protezione antivirus e antispyware facendo clic su **Avvia tutti i moduli di protezione antivirus e antispyware**.
- **Licenza scaduta** - Questa condizione è indicata dalla presenza di un'icona rossa dello stato di protezione. Allo scadere della licenza, non sarà possibile aggiornare il programma. Si consiglia di seguire le istruzioni nella finestra di avviso per rinnovare la licenza.

L'icona arancione indica che la protezione del computer è limitata. Ad esempio, si è verificato un problema nell'aggiornamento del programma o la licenza sta per scadere.
Esistono vari motivi alla base della visualizzazione di questo stato, tra cui:

- **Avviso ottimizzazione Anti-Furto** - Questo dispositivo non è ottimizzato per ESET Anti-Furto. Ad esempio, un Account fantasma, inizialmente inesistente, rappresenta una funzione di protezione che viene attivata

automaticamente nel momento in cui un dispositivo viene contrassegnato come mancante. Potrebbe essere necessario creare un Account fantasma utilizzando la funzione Ottimizzazione nell'interfaccia Web di ESET Anti-Furto.

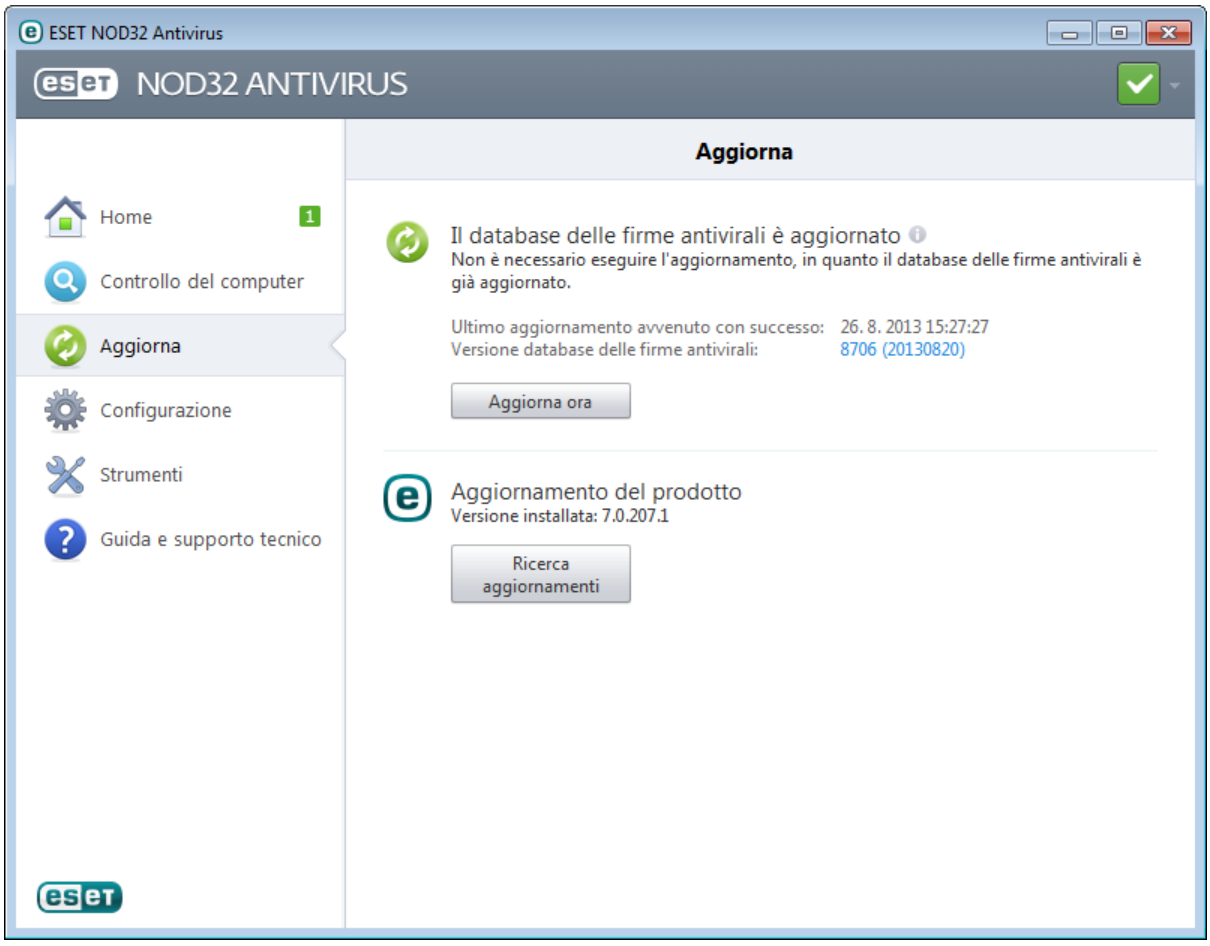
- **Modalità giocatore attivata** - L'attivazione della Modalità giocatore è un potenziale rischio di protezione. Attivando questa funzionalità, tutte le finestre popup vengono disattivate e l'attività di Pianificazione attività verrà completamente interrotta.
- **La licenza scadrà a breve** - Questa condizione è indicata dalla presenza di un'icona dello stato di protezione contenente un punto esclamativo vicino all'orologio di sistema. Allo scadere della licenza, non sarà possibile aggiornare il programma e l'icona dello stato di protezione diventerà rossa.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su **Guida e supporto tecnico** per accedere ai file della Guida oppure effettuare una ricerca nella Knowledge Base ESET. Per ulteriore assistenza, è possibile inviare una richiesta di supporto. Il Supporto tecnico ESET risponderà rapidamente alle domande degli utenti e li aiuterà a trovare una soluzione ai loro problemi.

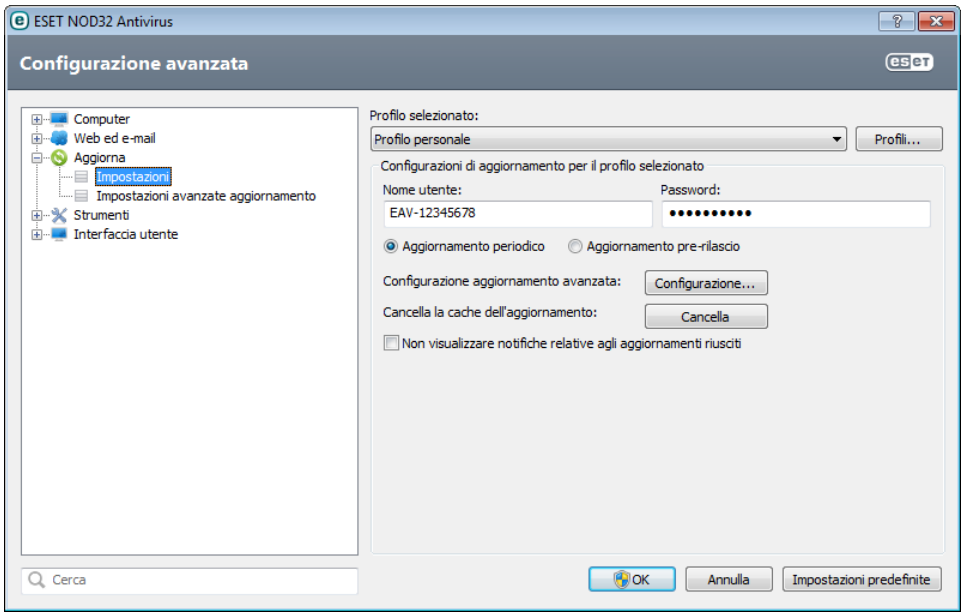
3.2 Aggiornamenti

L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire la protezione del sistema contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e al funzionamento. Nel menu principale, fare clic su **Aggiorna**, quindi su **Aggiorna adesso** per verificare la disponibilità di un aggiornamento del database delle firme antivirali.

Se durante l'attivazione di ESET NOD32 Antivirus non sono stati specificati Nome utente e Password, verrà richiesto di inserirli in questa fase.

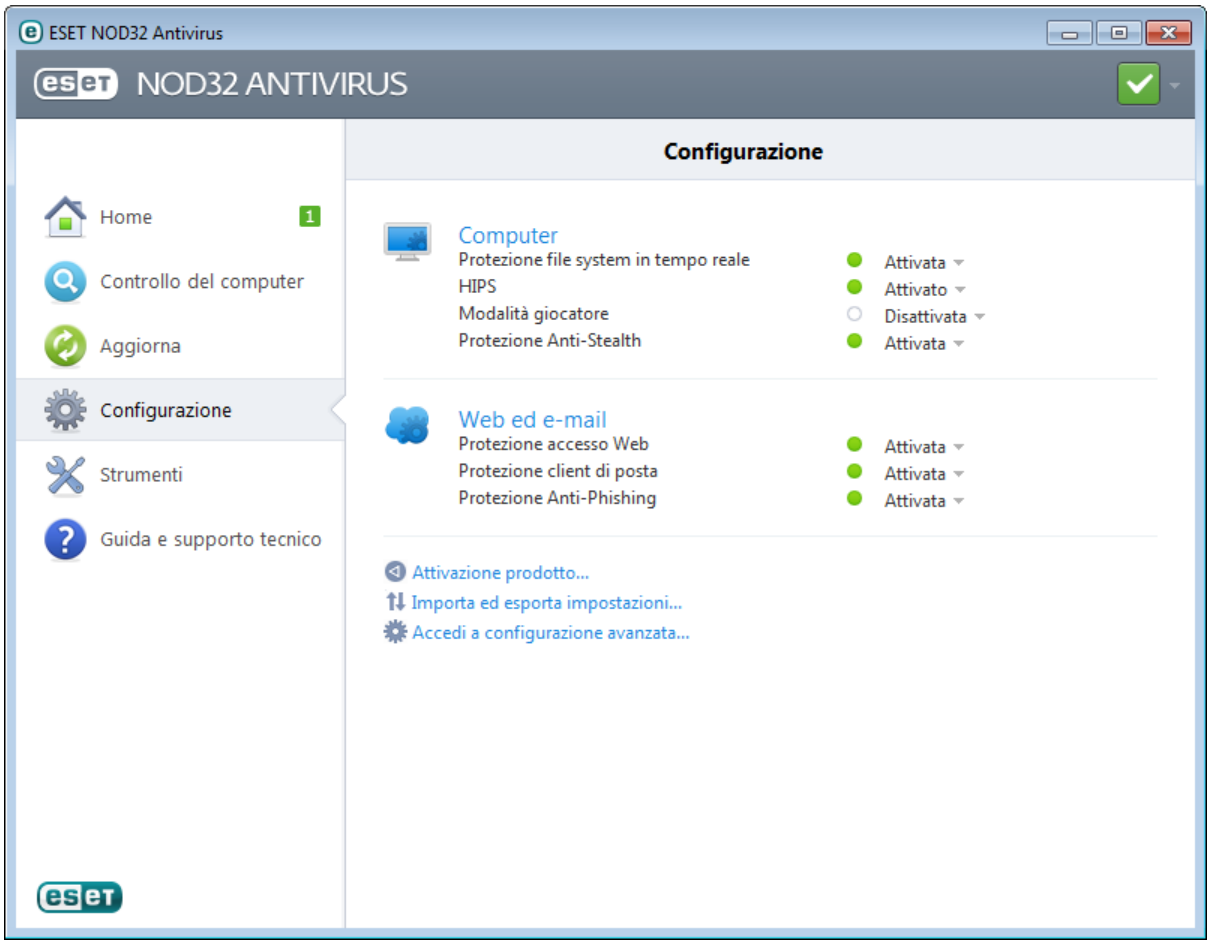


Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi su **Accedi a configurazione avanzata...** oppure premere **F5** sulla tastiera) sono disponibili opzioni di aggiornamento aggiuntive. Fare clic su **Aggiorna** > **Impostazioni** nella struttura Configurazione avanzata sulla sinistra. Per configurare le opzioni di aggiornamento avanzate, come ad esempio la modalità di aggiornamento, l'accesso al server proxy e le connessioni LAN, fare clic su **Configurazione...** nella finestra **Aggiornamento**.



4. Utilizzo di ESET NOD32 Antivirus

Le opzioni di configurazione di ESET NOD32 Antivirus consentono di regolare i livelli di protezione del computer.



Il menu **Configurazione** contiene le opzioni seguenti:

- **Computer**
- **Web ed e-mail**

Fare clic su un componente per regolare le impostazioni avanzate del modulo di protezione corrispondente.

L'impostazione della protezione **Computer** consente di attivare o disattivare i componenti seguenti:

- **Protezione file system in tempo reale** - Tutti i file vengono sottoposti a controllo per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer.
- **HIPS** - Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a una serie personalizzata di regole.
- **Modalità giocatore** - Attiva o disattiva la Modalità giocatore. Quando si attiva la Modalità giocatore, viene visualizzato un messaggio di avviso (potenziale rischio per la protezione) e la finestra principale diventa arancione.
- **Protezione Anti-Stealth** - Rileva programmi pericolosi, tra cui rootkit, che si nascondono dal sistema operativo e dalle tradizionali tecniche di testing.

La configurazione di protezione **Web ed e-mail** consente di attivare o disattivare i seguenti componenti:

- **Protezione accesso Web** - Se questa opzione è attivata, viene eseguito il controllo di tutto il traffico HTTP o HTTPS per la ricerca di software dannoso.
- **Protezione client di posta** - Monitora le comunicazioni ricevute mediante il protocollo POP3 e IMAP.
- **Protezione Anti-Phishing** - Filtra i siti Web per i quali si sospetta una distribuzione di contenuti concepiti allo scopo di manipolare gli utenti facendo loro inviare informazioni riservate.

Per attivare nuovamente la protezione del componente di protezione disattivato, fare clic su **Disattivato**, quindi su

Attiva.

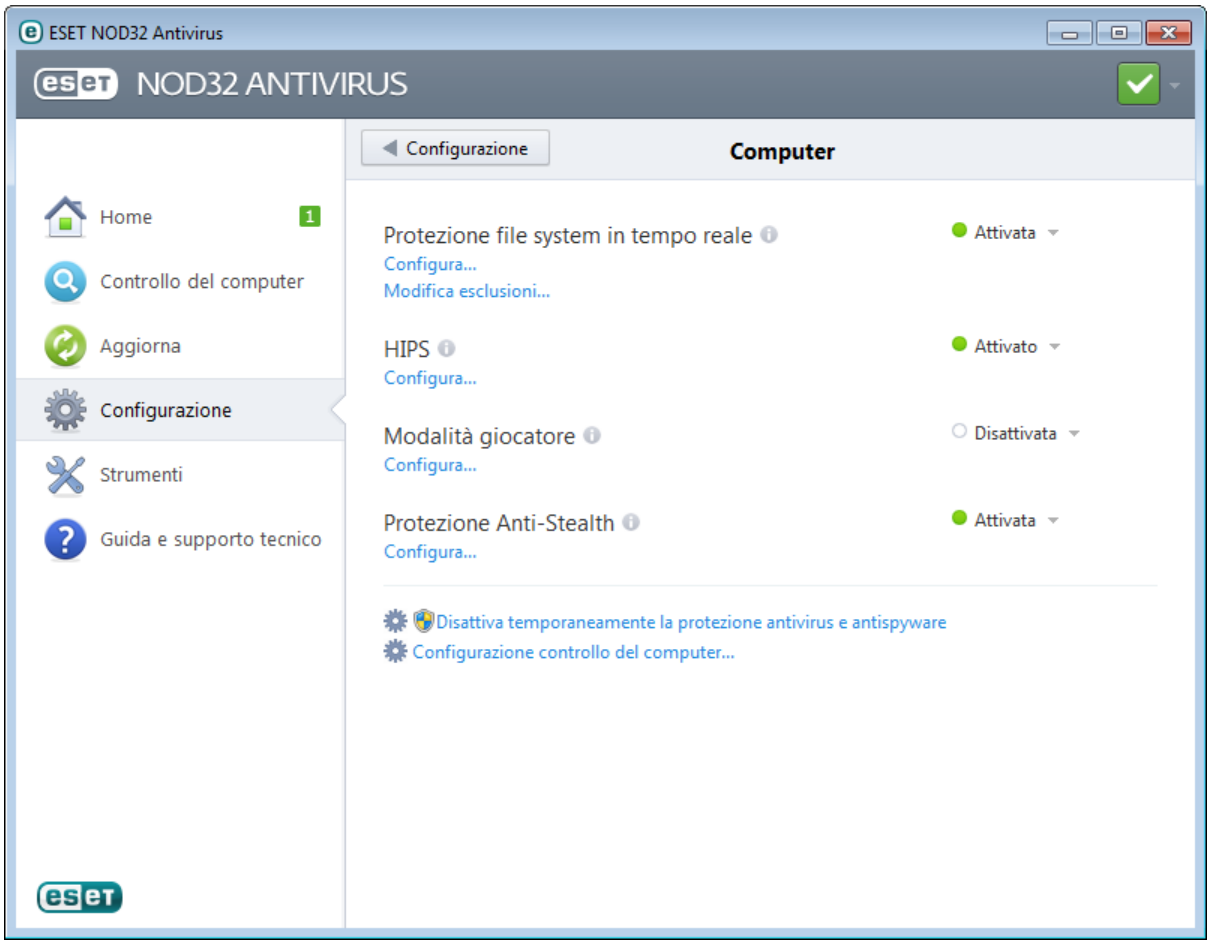
NOTA: quando si disattiva la protezione mediante questo metodo, tutte le parti disattivate della protezione saranno attivate dopo aver riavviato il computer.

Nella parte inferiore della finestra di configurazione sono disponibili ulteriori opzioni. Usare il collegamento **Attivazione prodotto...** per accedere al modulo di registrazione che consente di attivare il prodotto di protezione ESET e ricevere un messaggio e-mail contenente i dati per l'autenticazione (nome utente e password). Per caricare i parametri di impostazione mediante un file di configurazione *.xml* o per salvare i parametri di impostazione correnti su un file di configurazione, selezionare l'opzione **Importa ed esporta impostazioni...**.

4.1 Computer

Il modulo **Computer** è disponibile nel riquadro **Configurazione** facendo clic sul titolo **Computer**. Questa finestra mostra una panoramica di tutti i moduli di protezione. Per disattivare temporaneamente i singoli moduli, fare clic su **Attivato** > **Disattiva per...** accanto al modulo desiderato. Tenere presente che in questo modo si potrebbe ridurre il livello di protezione del computer. Per accedere alle impostazioni dettagliate di ciascun modulo, fare clic su **Configura...**.

Fare clic su **Modifica esclusioni...** per aprire la finestra di configurazione Esclusione, che consente di escludere i file e le cartelle dal controllo.



Disattiva temporaneamente la protezione antivirus e antispyware - Disattiva tutti i moduli di protezione antivirus e antispyware. Una volta disattivata la protezione, comparirà la finestra **Disattiva temporaneamente la protezione**, che consente all'utente di determinare la durata della disattivazione della protezione mediante la selezione di un valore dal menu a discesa **Intervallo di tempo**. Fare clic su **OK** per confermare.

Configurazione controllo computer... - Fare clic per regolare i parametri del controllo su richiesta (controllo eseguito manualmente).

4.1.1 Antivirus e antispyware

La Protezione antivirus e antispyware difende il sistema da attacchi dannosi controllando file, messaggi e-mail e comunicazioni su Internet. Il modulo antivirus è in grado di eliminare una minaccia con codice dannoso rilevata. L'oggetto viene dapprima bloccato, poi pulito, cancellato o messo in quarantena.

Le opzioni scanner per tutti i moduli di protezione (ad esempio, protezione file system in tempo reale, protezione accesso Web, ecc.) consentono di attivare o disattivare il rilevamento dei seguenti elementi:

- Le **Applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso.
  Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.
- Le **Applicazioni potenzialmente pericolose** sono software legali e commerciali che potrebbero essere utilizzati in modo non legale per scopi illegittimi. Esempi di applicazioni potenzialmente pericolose sono strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente). Questa opzione è disattivata per impostazione predefinita.
  Per ulteriori informazioni su questi tipi di applicazione, consultare la relativa voce del glossario.
- Le **Applicazioni potenzialmente sospette** includono programmi compressi con programmi di compressione o protettori. Questi tipi di programmi di protezione sono spesso utilizzati dagli autori di malware per eludere il rilevamento.

La tecnologia Anti-Stealth è un sistema sofisticato che consente di rilevare programmi pericolosi, come ad esempio i rootkit, che sono in grado di nascondersi dal sistema operativo. Ciò significa che non è possibile rilevarli utilizzando le normali tecnologie di testing.

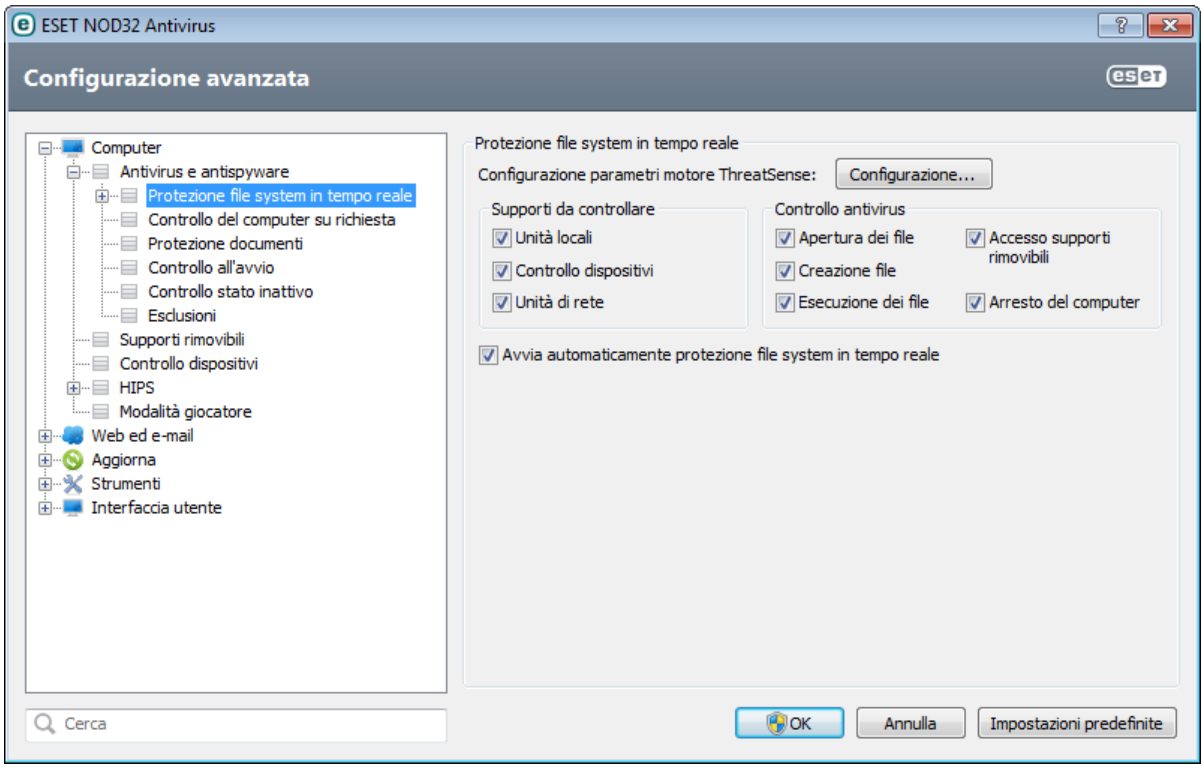
4.1.1.1 Protezione file system in tempo reale

La funzione di Protezione file system in tempo reale consente di controllare tutti gli eventi correlati all'antivirus nel sistema. Tutti i file vengono sottoposti a controllo alla ricerca di codice dannoso nel momento in cui vengono aperti, creati o eseguiti sul computer. La funzione Protezione file system in tempo reale viene avviata all'avvio del sistema.

La Protezione file system in tempo reale, che viene attivata da vari eventi di sistema, tra cui l'accesso a un file, controlla tutti i tipi di supporti. Grazie ai metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione configurazione parametri motore ThreatSense), è possibile configurare la Protezione file system in tempo reale in modo da gestire i file di nuova creazione in modo diverso rispetto a quelli esistenti. Ad esempio, la Protezione file system in tempo reale può essere configurata in modo da monitorare più da vicino i file di nuova creazione.

Per ridurre al minimo l'impatto sul sistema della protezione in tempo reale, i file che sono già stati controllati verranno ignorati, eccetto nel caso in cui siano state apportate modifiche. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database delle firme antivirali. Questo comportamento viene configurato mediante la funzione **Ottimizzazione Smart**. Se questa funzione non è attiva, verrà eseguito un controllo di tutti i file a cui viene effettuato l'accesso. Per modificare questa opzione, premere **F5** per aprire la finestra Configurazione avanzata ed espandere **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale**. Fare clic su **Configurazione...** accanto a **configurazione parametri motore ThreatSense** > **Altro** e selezionare o deselezionare **Attiva ottimizzazione intelligente**.

In base alle impostazioni predefinite, la Protezione file system in tempo reale viene avviata automaticamente all'avvio del sistema operativo e fornisce un controllo ininterrotto. In casi particolari (ad esempio, in caso di conflitto con un altro scanner in tempo reale), la protezione in tempo reale può essere disattivata deselezionando **Avvia automaticamente la protezione file system in tempo reale** nella sezione **Protezione file system in tempo reale** della Configurazione avanzata.



Supporti da controllare

Per impostazione predefinita, vengono controllati tutti i tipi di supporto alla ricerca di eventuali minacce:

Dischi locali - Consente di controllare tutti gli hard disk del sistema.
Controllo dispositivi - CD/DVD, supporti di archiviazione USB, dispositivi Bluetooth e così via.
Dischi di rete - Consente di eseguire il controllo di tutte le unità mappate.

Si consiglia di mantenere le impostazioni predefinite e di modificarle solo in casi specifici, ad esempio quando il controllo di alcuni supporti rallenta notevolmente il trasferimento dei dati.

Controllo al verificarsi di un evento

Per impostazione predefinita, tutti i file sono sottoposti a controllo all'apertura, durante la creazione o l'esecuzione. Si consiglia di mantenere le seguenti impostazioni predefinite per garantire il massimo livello di protezione in tempo reale per il computer in uso:

- **Apertura dei file** - Attiva/disattiva il controllo dei file aperti.
- **Creazione dei file** - Attiva/disattiva il controllo dei file appena creati o modificati.
- **Esecuzione dei file** - Attiva/disattiva il controllo dei file eseguiti.
- **Accesso supporti rimovibili** - Attiva o disattiva il controllo attivato dall'accesso a determinati supporti rimovibili dotati di uno spazio di archiviazione.
- **Arresto computer** - Attiva o disattiva il controllo attivato dall'arresto del computer.

4.1.1.1.1 Opzioni avanzate di controllo

In **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale** > **Configurazione avanzata** sono disponibili opzioni di configurazione più dettagliate.

Parametri ThreatSense aggiuntivi per i file appena creati e modificati - I file appena creati hanno maggiore possibilità di essere infettati rispetto a quelli esistenti. Per questo motivo il programma controlla tali file con parametri aggiuntivi. Oltre ai comuni metodi di controllo basati sulle firme, viene utilizzata la funzione di euristica avanzata che è in grado di rilevare le nuove minacce prima che l'aggiornamento del database delle firme antivirali venga rilasciato. Oltre che sui file appena creati, il controllo viene eseguito anche sui file autoestraenti (SFX) e sugli eseguibili compressi, ovvero file eseguibili compressi a livello interno. Per impostazione predefinita, gli archivi vengono analizzati fino al 10° livello di nidificazione e controllati indipendentemente dalla loro dimensione effettiva. Per modificare le impostazioni di controllo dell'archivio, deselezionare **Impostazioni predefinite controllo degli archivi**.

Parametri ThreatSense aggiuntivi per i file eseguiti - Per impostazione predefinita, quando i file vengono eseguiti non viene usata l'euristica avanzata. In alcuni casi potrebbe tuttavia essere utile attivare questa opzione (selezionando **Euristica avanzata all'esecuzione dei file**). È possibile che l'euristica avanzata rallenti l'esecuzione di alcuni programmi a causa dell'aumento dei requisiti di sistema. Se, dopo aver attivato **Euristica avanzata all'esecuzione dei file da supporti rimovibili**, si desidera escludere alcune porte dei supporti rimovibili (USB) dal controllo con euristica avanzata all'esecuzione dei file, fare clic su **Eccezioni...** per aprire la finestra delle esclusioni dei supporti rimovibili. In questa finestra, è possibile personalizzare le impostazioni selezionando o deselezionando le caselle di controllo relative a ogni porta.

4.1.1.1.2 Livelli di pulizia

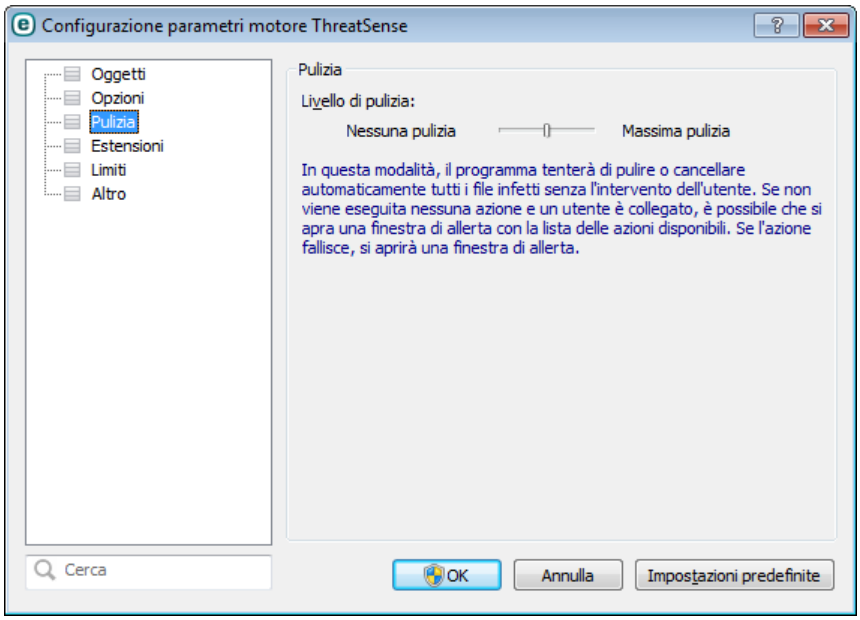
La protezione in tempo reale prevede tre livelli di pulizia (per accedere, fare clic su **Configurazione...** nella sezione **Protezione file system in tempo reale**, quindi su **Pulizia**).

Nessuna pulizia - I file infetti non vengono puliti automaticamente. Verrà visualizzata una finestra di avviso per consentire all'utente di scegliere un'azione. Questo livello è indicato per utenti più esperti in grado di eseguire le azioni appropriate in caso di infiltrazione.

Pulitura standard - Il programma tenterà di pulire o eliminare automaticamente un file infetto in base a un'azione predefinita (a seconda del tipo di infiltrazione). Una notifica nell'angolo in basso a destra della schermata segnalerà il rilevamento e l'eliminazione di un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma offre altre azioni di follow-up. Lo stesso si verifica se non è stato possibile completare un'azione predefinita.

Massima pulizia - Il programma pulirà o eliminerà tutti i file infetti. Le uniche eccezioni sono costituite dai file di sistema. Nel caso in cui non sia possibile pulirli, verrà visualizzata una finestra di avviso con la possibilità di scegliere un'azione da eseguire.

Attenzione: se un archivio contiene uno o più file infetti, sono disponibili due opzioni per gestire tale archivio. In modalità standard (Pulitura standard), l'intero archivio viene eliminato se tutti i file in esso contenuti sono infetti. In modalità **Massima pulizia**, l'archivio viene eliminato se contiene almeno un file infetto, indipendentemente dallo stato degli altri file contenuti nell'archivio.



4.1.1.1.3 Quando modificare la configurazione della protezione in tempo reale

La protezione in tempo reale è il componente più importante per la sicurezza di un sistema. Prestare la massima attenzione quando si modificano i relativi parametri. È consigliabile modificarli solo in casi specifici,

Dopo l'installazione di ESET NOD32 Antivirus, tutte le impostazioni sono ottimizzate al fine di offrire il massimo livello di protezione del sistema agli utenti. Per ripristinare le impostazioni predefinite, fare clic su **Impostazioni predefinite** in basso a destra della finestra **Protezione file system in tempo reale** (**Configurazione avanzata** > **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale**).

4.1.1.1.4 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare un file di test da eicar.com. Questo file di test è un file innocuo e rilevabile da tutti i programmi antivirus. Il file è stato creato da EICAR (European Institute for Computer Antivirus Research) per testare la funzionalità dei programmi antivirus. Può essere scaricato all'indirizzo http://www.eicar.org/download/eicar.com

4.1.1.1.5 Cosa fare se la protezione in tempo reale non funziona

In questo capitolo, verranno illustrati i problemi che potrebbero verificarsi durante l'utilizzo della protezione in tempo reale e le modalità di risoluzione.

La protezione in tempo reale è disattivata

Se la protezione in tempo reale è stata inavvertitamente disattivata da un utente, sarà necessario riattivarla. Per riattivare la protezione in tempo reale, selezionare **Configurazione** nella finestra principale del programma e fare clic su **Protezione file system in tempo reale**.

Se la protezione in tempo reale non viene lanciata all'avvio del sistema, è probabile che l'opzione **Avvia automaticamente la protezione file system in tempo reale** non sia stata selezionata. Per attivare l'opzione, accedere a Configurazione avanzata (**F5**) e fare clic su **Computer** > **Antivirus e antispyware** > **Protezione file system in tempo reale** nella struttura Configurazione avanzata. Nella sezione **Configurazione avanzata** nella parte inferiore della finestra, verificare che la casella di controllo **Avvia automaticamente la protezione file system in tempo reale** sia selezionata.

La protezione in tempo reale non rileva né pulisce le infiltrazioni

Verificare che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus presenti nel sistema prima di installare ESET.

La protezione in tempo reale non viene avviata

Se la protezione in tempo reale non viene lanciata all'avvio del sistema (e l'opzione **Avvia automaticamente la protezione file system in tempo reale** è attivata), ciò potrebbe dipendere da un conflitto con altri programmi. Per ricevere assistenza nella risoluzione del problema, si prega di contattare il Supporto tecnico ESET.

4.1.1.2 Controllo del computer

Lo scanner su richiesta è una parte importante della soluzione antivirus. Viene utilizzato per eseguire il controllo di file e di cartelle sul computer in uso. Dal punto di vista della protezione, è essenziale che i controlli del computer non vengano eseguiti solo quando si sospetta un'infezione, ma periodicamente, nell'ambito delle normali misure di protezione. Si consiglia di eseguire periodicamente controlli approfonditi del sistema al fine di rilevare virus che non sono stati rilevati dalla Protezione file system in tempo reale quando sono stati scritti sul disco. Ciò può verificarsi se la Protezione file system in tempo reale era disattivata in quel momento, il database antivirus era obsoleto o il file non è stato rilevato come virus quando è stato salvato sul disco.

Sono disponibili due tipologie di **Controllo del computer**. **Controllo intelligente**, che consente di eseguire rapidamente il controllo del sistema senza che sia necessario configurare ulteriori parametri. **Controllo personalizzato**, che consente di selezionare uno dei profili di controllo predefiniti per l'analisi di percorsi specifici, nonché di scegliere specifiche destinazioni di controllo.

Controllo intelligente

La funzione Controllo intelligente consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio del Controllo intelligente consiste nella facilità di utilizzo e nel fatto che non è richiesta una configurazione di controllo dettagliata. Il Controllo intelligente consente di effettuare un controllo di tutti i file presenti nei dischi locali, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di pulizia viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di pulizia, consultare la sezione Pulizia.

Controllo personalizzato

Il controllo personalizzato consente di specificare parametri di controllo quali destinazioni e metodi di controllo. Il vantaggio del Controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare le configurazioni come profili di controllo definiti dagli utenti che risultano particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri.

Controllo supporti rimovibili

Simile al Controllo intelligente - consente di lanciare velocemente un controllo dei supporti rimovibili (come ad esempio CD/DVD/USB) attualmente collegati al computer. Questa opzione può essere utile in caso di connessione di una memoria USB ad un computer e nel caso in cui si desideri controllarne il contenuto alla ricerca di malware o di altre potenziali minacce.

Questo tipo di controllo può anche essere avviato facendo clic su **Controllo personalizzato**, quindi selezionando **Supporti rimovibili** dal menu a discesa **Destinazioni di controllo** e facendo clic su **Controllo**.

Per ulteriori informazioni sull'avanzamento del controllo, consultare il capitolo Avanzamento controllo.

È consigliabile eseguire un controllo del computer almeno una volta al mese. Il controllo può essere configurato come attività pianificata in **Strumenti** > **Pianificazione attività**.

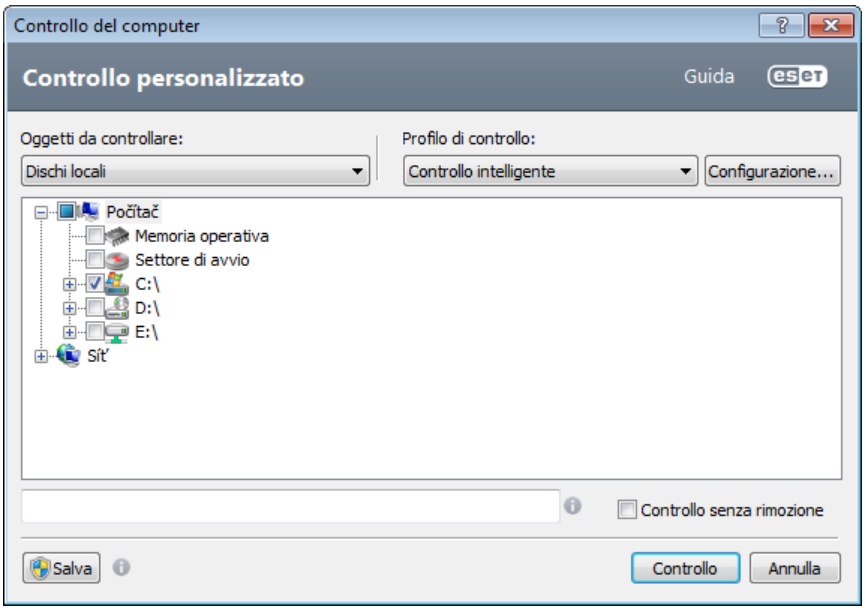
4.1.1.2.1 Launcher controllo personalizzato

Se non si desidera controllare l'intero spazio su disco ma solo una specifica destinazione, è possibile utilizzare lo strumento del Controllo personalizzato facendo clic su **Controllo computer** > **Controllo personalizzato** e selezionando un'opzione dal menu a discesa **Oggetti da controllare** oppure selezionando destinazioni specifiche dalla struttura (ad albero) della cartella.

La finestra Oggetti da controllare consente di definire gli oggetti (memoria, unità, settori, file e cartelle) che verranno sottoposti a controllo alla ricerca di infiltrazioni. Selezionare gli oggetti dalla struttura ad albero contenente un elenco di tutti i supporti disponibili nel computer. Il menu a discesa **Oggetti da controllare** consente di selezionare gli oggetti da controllare predefiniti.

- **Attraverso le impostazioni di profilo** - Consente di selezionare le destinazioni nel profilo di controllo selezionato.
- **Supporti rimovibili** - Consente di selezionare dischetti, supporti di archiviazione USB, CD/DVD.
- **Unità locali** - Consente di selezionare tutti gli hard disk del sistema.
- **Unità di rete** - Consente di selezionare tutte le unità di rete mappate.
- **Nessuna selezione** - Consente di annullare tutte le selezioni.

Per visualizzare rapidamente una destinazione di controllo o per aggiungere direttamente una destinazione desiderata (cartella o file), inserirla nel campo vuoto sotto all'elenco delle cartelle. Ciò è possibile solo se nella struttura ad albero non sono state selezionate destinazioni e il menu **Oggetti da controllare** è impostato su **Nessuna selezione**.



Gli elementi infetti non vengono puliti automaticamente. Il controllo senza rimozione può essere utilizzato per ottenere una panoramica dello stato di protezione corrente. Se si desidera effettuare solo un controllo del sistema senza azioni di pulizia aggiuntive, selezionare **Controlla senza pulire**. È inoltre possibile scegliere tra tre livelli di pulizia facendo clic su **Configurazione...** > **Pulizia**. Le informazioni relative alla scansione vengono salvate in un rapporto di scansione.

È possibile scegliere un profilo dal menu a discesa **Profilo di controllo** da utilizzare per il controllo delle destinazioni scelte. Il profilo predefinito è **Controllo intelligente**. Esistono due altri profili predefiniti chiamati **Controllo approfondito** e **Controllo menu contestuale**. Questi profili di controllo utilizzano parametri del motore ThreatSense diversi. Fare clic su **Configurazione...** per configurare i dettagli del profilo di controllo scelto nel menu Profilo di controllo. Le opzioni disponibili sono descritte in Impostazione scanner.

Fare clic su **Salva** per salvare le modifiche apportate alle selezioni di destinazioni, comprese quelle relative alla struttura delle cartelle.

Fare clic su **Controlla** per eseguire il controllo utilizzando i parametri personalizzati configurati dall'utente.

Effettua controllo come Amministratore consente di eseguire il controllo mediante l'account Amministratore. Selezionare questa opzione se l'utente corrente non dispone dei privilegi per accedere ai file appropriati da controllare. Nota: questo pulsante non è disponibile se l'utente corrente non può invocare operazioni UAC come Amministratore.

4.1.1.2.2 Avanzamento controllo

Nella finestra di avanzamento del controllo viene mostrato lo stato attuale del controllo e informazioni sul numero di file rilevati che contengono codice dannoso.

NOTA: è normale che alcuni file, ad esempio file protetti con password o file che vengono utilizzati esclusivamente dal sistema (in genere il file *pagefile.sys* e alcuni file di registro), non possano essere sottoposti al controllo.

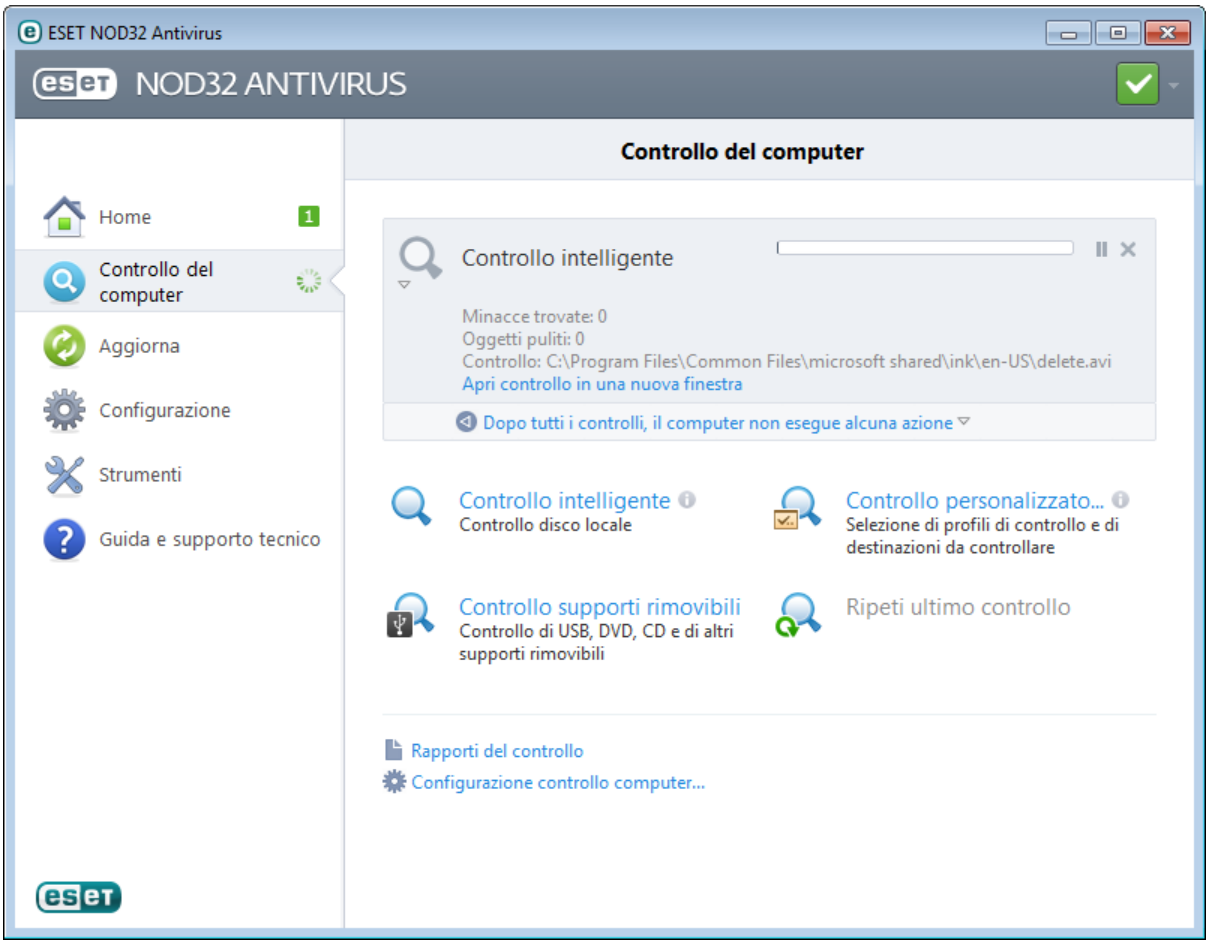
La barra di avanzamento mostra la percentuale di oggetti già sottoposti a controllo rispetto a quelli in attesa di essere sottoposti al controllo. Il valore è derivato in base al numero totale di oggetti inclusi in un controllo.

Suggerimenti

Fare clic sulla lente di ingrandimento o sulla freccia per visualizzare i dettagli sul controllo attualmente in esecuzione.
È possibile eseguire un altro controllo parallelo facendo clic su **Controllo intelligente** o **Controllo personalizzato...**.

Oggetti - Consente di visualizzare il numero totale di file controllati, minacce rilevate e minacce pulite durante un controllo.

Destinazione - Nome dell'oggetto in fase di controllo e relativo percorso.



Dopo tutti i controlli il computer non esegue alcuna azione - Attiva un arresto o un riavvio pianificato al termine del controllo del computer. Una volta terminato il controllo, verrà visualizzata una finestra di dialogo in cui viene richiesto all'utente di confermare l'arresto entro 60 secondi. Fare nuovamente clic su questa opzione per disattivare l'azione selezionata.

4.1.1.2.3 Profili di scansione

È possibile salvare i parametri di scansione preferiti per i controlli futuri. È consigliabile creare un profilo di scansione differente (con diversi oggetti da controllare, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Computer** > **Antivirus e antispyware** > **Controllo computer su richiesta** > **Profili...**. Nella finestra **Profili di configurazione** è disponibile un menu a discesa **Profili selezionati** contenente i profili di scansione esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza nella creazione di un profilo di scansione adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione della scansione.

Esempio: si supponga di voler creare il proprio profilo di scansione e che la configurazione del Controllo intelligente sia appropriata solo in parte, in quanto non si desidera eseguire la scansione di eseguibili compressi o di applicazioni potenzialmente pericolose, bensì si intende applicare l'opzione **Massima pulizia**. Nella finestra **Profili di configurazione**, fare clic su **Aggiungi...**. Immettere il nome del nuovo profilo nel campo **Nome profilo**, quindi selezionare **Controllo intelligente** dal menu a discesa **Copia impostazioni dal profilo**. Regolare i parametri rimanenti per soddisfare le specifiche esigenze e salvare il nuovo profilo.

4.1.1.3 Controllo all'avvio

Per impostazione predefinita, all'avvio del sistema e durante gli aggiornamenti del database delle firme antivirali, verrà eseguito il controllo automatico del file di avvio. Questo controllo dipende dalla configurazione di Pianificazione configurazione e attività.

Le opzioni di controllo all'avvio fanno parte della pianificazione dell'attività **Controllo del file di avvio del sistema**. Per modificare le impostazioni, accedere a **Strumenti** > **Pianificazione attività**, fare clic su **Controllo automatico file di avvio**, quindi su **Modifica...**. Nell'ultimo passaggio verrà visualizzata la finestra Controllo automatico file di avvio (per ulteriori informazioni, vedere il capitolo seguente).

Per ulteriori informazioni sulla creazione e sulla gestione di Pianificazione attività, vedere Creazione di nuove attività.

4.1.1.3.1 Controllo automatico file di avvio

Durante la creazione di un'attività pianificata di controllo del file di avvio del sistema, sono disponibili varie opzioni per regolare i parametri seguenti:

Il menu a discesa **Livello di controllo** consente di specificare il livello di controllo dei file eseguiti all'avvio del sistema. I file sono visualizzati in ordine crescente in base ai seguenti criteri:

- **Solo i file utilizzati più di frequente** (ultimi file sottoposti al controllo)
- **File utilizzati di frequente**
- **File utilizzati comunemente**
- **File utilizzati raramente**
- **Tutti i file registrati** (la maggior parte dei file sottoposti al controllo)

Sono inoltre inclusi due gruppi del **Livello di controllo** specifici:

- **File eseguiti prima dell'accesso utente** - Contiene file da posizioni a cui è possibile accedere senza che l'utente abbia eseguito la registrazione (include quasi tutte le posizioni di avvio quali servizi, oggetti browser helper, notifiche Winlogon, voci della pianificazione attività di Windows, dll noti e così via).
- **File eseguiti dopo l'accesso utente** - Contiene file da posizioni a cui è possibile accedere solo dopo che un utente ha eseguito la registrazione (include file che sono eseguiti solo per un utente specifico, in genere i file in *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*).

Per ogni gruppo summenzionato, vengono definiti elenchi di file da sottoporre al controllo.

Priorità di controllo - Il livello di priorità utilizzato per determinare il momento di avvio di un controllo:

- **Normale** - con un carico di sistema medio
- **Basso** - con un carico di sistema basso
- **Più basso** - con un carico di sistema minimo
- **Quando inattivo** - l'attività verrà eseguita solo quando il sistema è inattivo

4.1.1.4 Controllo stato inattivo

Lo scanner dello stato inattivo può essere configurato e attivato nella sezione **Configurazione avanzata** in **Computer** > **Antivirus e antispyware** > **Controllo stato inattivo**. Se il computer si trova nello stato inattivo, verrà eseguito un controllo del computer silenzioso su tutti i dischi locali. Consultare la sezione Metodi di attivazione del rilevamento stato inattivo per un elenco completo di condizioni che è necessario soddisfare per attivare lo scanner dello stato inattivo.

Per impostazione predefinita, lo scanner dello stato inattivo non verrà eseguito in caso di alimentazione del computer (notebook) a batteria. È possibile ignorare questa impostazione selezionando la casella di controllo accanto a **Esegui anche se il computer è alimentato a batteria** in Configurazione avanzata.

Selezionare **Attiva registrazione** in Configurazione avanzata per registrare il risultato di un controllo del computer nella sezione File di rapporto (nella finestra principale del programma, fare clic su **Strumenti** > **File di rapporto** e selezionare **Controllo del computer** dal menu a discesa **Rapporto**).

L'ultima impostazione di questa sezione è configurazione parametri motore ThreatSense. Fare clic su **Configurazione...** se si desidera modificare vari parametri di controllo (ad esempio, metodi di rilevamento).

4.1.1.5 Esclusioni

Le esclusioni consentono di escludere file e cartelle dalla scansione. Per garantire che la ricerca delle minacce venga eseguita su tutti gli oggetti, si consiglia di creare esclusioni solo se assolutamente necessario. Tuttavia, esistono situazioni in cui potrebbe essere necessario escludere un oggetto, ad esempio il caso di voci di database di grandi dimensioni che rallenterebbero il computer durante il controllo o di un software che entra in conflitto con il controllo.

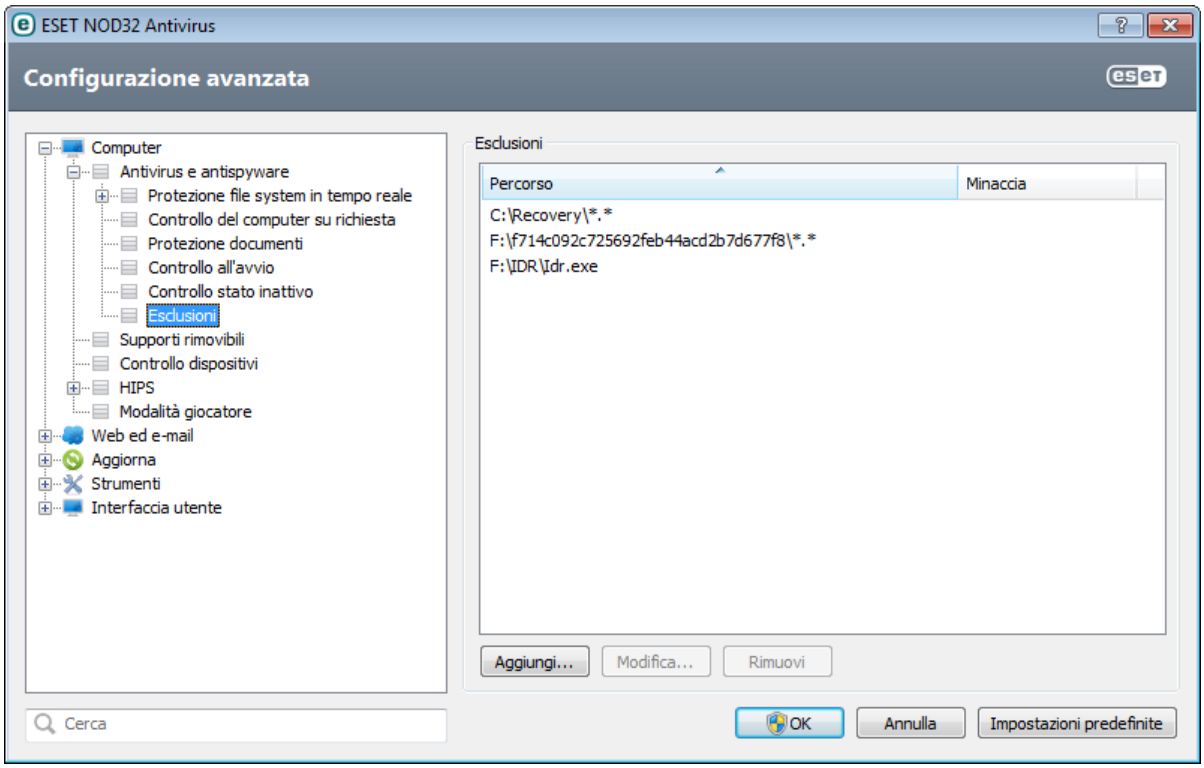
Per escludere un oggetto dalla scansione:

1. Fare clic su **Aggiungi...**,
2. Immettere il percorso di un oggetto oppure selezionarlo nella struttura ad albero.

È possibile utilizzare i caratteri jolly per includere un gruppo di file. Un punto interrogativo (?) rappresenta un carattere variabile singolo, mentre un asterisco (*) rappresenta una stringa variabile di zero o più caratteri.

Esempi

- Se si desidera escludere tutti i file presenti in una cartella, digitare il percorso della cartella e utilizzare la maschera "*.*".
- Per escludere un'unità intera, compresi tutti i file e le sottocartelle, usare la maschera "D:*".
- Se si desidera escludere solo i file DOC, utilizzare la maschera "*.doc".
- Se il nome di un file eseguibile contiene un determinato numero di caratteri (e i caratteri variano) e si è sicuri solo della prima lettera (ad esempio "D"), utilizzare il formato seguente: "D????.exe". I punti interrogativi sostituiscono i caratteri mancanti (sconosciuti).



Nota: una minaccia all'interno di un file non sarà rilevata dal modulo di protezione file system in tempo reale o dal modulo del controllo del computer se un file soddisfa i criteri dell'esclusione dal controllo.

Percorso - Percorso dei file e delle cartelle esclusi.

Minaccia - Se è presente il nome di una minaccia accanto a un file escluso, significa che il file viene escluso solo per la minaccia indicata e non per tutte. Se il file si infetta successivamente con altri malware, verrà rilevato dal modulo antivirus. Questo tipo di esclusione può essere utilizzato solo per alcuni tipi di infiltrazioni e può essere creato nella finestra di avviso minaccia che segnala l'infiltrazione (fare clic su **Mostra opzioni avanzate**, quindi selezionare

Escludi dal rilevamento) oppure facendo clic su **Configurazione** > **Quarantena**, quindi facendo clic con il pulsante destro del mouse sul file in quarantena e selezionando **Ripristina ed escludi dal rilevamento** dal menu contestuale.

Aggiungi... - Esclude gli oggetti dal rilevamento

Modifica... - Consente all'utente di modificare le voci selezionate

Rimuovi - Rimuove le voci selezionate

4.1.1.6 Configurazione parametri motore ThreatSense

ThreatSense è una tecnologia che prevede numerosi metodi di rilevamento delle minacce complesse. Questa tecnologia è proattiva, ovvero fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Il programma utilizza una combinazione di analisi del codice, emulazione del codice, firme generiche e firme antivirali che operano in modo integrato per potenziare enormemente la protezione del sistema. Il motore di scansione è in grado di controllare contemporaneamente diversi flussi di dati, ottimizzando l'efficienza e la percentuale di rilevamento. La tecnologia ThreatSense è inoltre in grado di eliminare i rootkit.

Le opzioni di configurazione del motore ThreatSense consentono all'utente di specificare vari parametri di controllo:

- Tipi ed estensioni dei file da controllare
- Combinazione di diversi metodi di rilevamento
- Livelli di pulizia e così via.

Per aprire la finestra di configurazione, fare clic su **Configurazione...** nella finestra Configurazione avanzata di qualsiasi modulo che utilizza la tecnologia ThreatSense (vedere sezione sottostante). Scenari di protezione diversi potrebbero richiedere configurazioni diverse. In considerazione di questo, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- Protezione file system in tempo reale,
- Protezione documenti,
- Protezione client di posta,
- Protezione accesso Web,
- Controllo del computer.

I parametri ThreatSense sono ottimizzati per ciascun modulo e la relativa modifica può influire in modo significativo sul funzionamento del sistema. Ad esempio, la modifica dei parametri per il controllo degli eseguibili compressi o per consentire l'euristica avanzata nel modulo della protezione file system in tempo reale potrebbe causare un rallentamento del sistema (questi metodi di controllo vengono applicati generalmente solo ai file di nuova creazione). È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, ad eccezione di Controllo computer.

4.1.1.6.1 Oggetti

Nella sezione **Oggetti** è possibile definire i componenti e file del computer che saranno sottoposti a scansione per la ricerca di infiltrazioni.

Memoria operativa - Consente di eseguire la scansione per la ricerca di minacce che attaccano la memoria operativa del sistema.

Settori di avvio - Consente di controllare i settori di avvio alla ricerca di virus nel record di avvio principale.

File di e-mail - Il programma supporta le estensioni seguenti: DBX (Outlook Express) ed EML.

Archivi - Il programma supporta le estensioni seguenti: ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE e molti altri ancora.

Archivi autoestraenti - Gli archivi autoestraenti (SFX) sono archivi che non necessitano di programmi speciali, ovvero archivi, per decomprimersi.

Eseguibili compressi - Dopo l'esecuzione, gli eseguibili compressi (diversamente dai tipi di archivio standard) si decomprimono nella memoria. Oltre ai programmi statici standard (UPS, yoda, ASPack, FSG e così via), lo scanner

supporta (grazie all'emulazione del codice) numerosi altri tipi di programmi di compressione.

4.1.1.6.2 Opzioni

La sezione **Opzioni** consente di selezionare i metodi utilizzati durante una scansione del sistema per il rilevamento di eventuali infiltrazioni. Sono disponibili le seguenti opzioni:

Euristica - L'euristica è un algoritmo che analizza l'attività (dannosa) dei programmi. Il vantaggio principale consiste nella capacità di identificare software dannoso precedentemente inesistente o non identificato dai database delle firme antivirali precedenti. Lo svantaggio è una piccola probabilità di falsi allarmi.

Euristica avanzata/DNA/Firme Smart - L'euristica avanzata rappresenta una delle tecnologie utilizzate da ESET NOD32 Antivirus per offrire un rilevamento proattivo delle minacce. Questa funzionalità è in grado di rilevare malware sconosciuti mediante il sistema dell'emulazione. Il nuovo traduttore binario consente di aggirare gli stratagemmi anti-emulazione utilizzati dagli autori di malware. La versione più recente della funzionalità introduce un nuovo metodo di emulazione del codice basato sulla traduzione binaria. Il nuovo traduttore binario consente di aggirare gli stratagemmi anti-emulazione utilizzati dagli autori di malware. Oltre ai miglioramenti summenzionati, è stato eseguito un importante aggiornamento del controllo basato sul DNA che consente di effettuare rilevamenti generici ottimizzati e una migliore gestione dei malware attualmente in circolazione.

ESET Live Grid - La tecnologia di reputazione di ESET consente di verificare le informazioni sui file controllati rispetto ai dati provenienti da ESET Live Grid basato sul cloud, allo scopo di migliorare il rilevamento e la velocità di controllo.

4.1.1.6.3 Pulizia

Le impostazioni di pulizia determinano il comportamento dello scanner durante la pulizia di file infetti. Sono disponibili 3 livelli di pulizia.

4.1.1.6.4 Estensioni

Un'estensione è una parte del nome di un file delimitata da un punto. Un'estensione definisce il tipo e il contenuto di un file. Questa sezione delle impostazioni parametri ThreatSense consente di definire i tipi di file da sottoporre a controllo.

Per impostazione predefinita, tutti i file vengono sottoposti a scansione indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dalla scansione. Deselezionando **Controlla tutti i file**, l'elenco verrà modificato per mostrare le estensioni di tutti i file sottoposti al controllo.

Per attivare il controllo dei file senza estensione, selezionare **Controlla file senza estensione**. **Non eseguire controllo dei file senza estensione** diventerà disponibile attivando **Controlla tutti i file**.

L'esclusione di file è un'operazione utile nel caso in cui il controllo di determinati tipi di file impedisca il corretto funzionamento di uno specifico programma che utilizza determinate estensioni. Ad esempio, potrebbe essere consigliabile escludere le estensioni EDB, EML e TMP durante l'utilizzo dei server Microsoft Exchange.

I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire la scansione di estensioni di file specifiche. Digitando un'**Estensione** si attiva il pulsante **Aggiungi** che consente di aggiungere la nuova estensione all'elenco. Per eliminare un'estensione dall'elenco, selezionarla e fare clic su **Rimuovi**.

È possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri, mentre il punto interrogativo sostituisce qualsiasi simbolo. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, poiché l'elenco deve contenere solo indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente.

Per eseguire solo il controllo del gruppo di estensioni predefinito, fare clic su **Impostazioni predefinite**, quindi su **Sì** per confermare.

4.1.1.6.5 Limiti

La sezione Limiti consente di specificare la dimensione massima degli oggetti e i livelli di nidificazione degli archivi sui quali eseguire la scansione:

Dimensioni massima oggetto - Determina la dimensione massima degli oggetti su cui eseguire la scansione. Il modulo antivirus eseguirà unicamente la scansione degli oggetti di dimensioni inferiori a quelle specificate. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dalla scansione. Il valore predefinito è: *illimitato*.

Durata massima scansione dell'oggetto (sec.) - Consente di definire il valore massimo di tempo destinato alla scansione di un oggetto. Se è stato immesso un valore definito dall'utente, il modulo antivirus interromperà la scansione dell'oggetto una volta raggiunto tale valore, indipendentemente dal fatto che la scansione sia stata completata. Il valore predefinito è: *illimitato*.

Livello di nidificazione degli archivi - Specifica il livello massimo di scansione degli archivi. Il valore predefinito è: *10*.

Dimensioni massima file in archivio - Questa opzione consente di specificare le dimensioni massime dei file contenuti all'interno degli archivi, i quali, una volta estratti, saranno sottoposti a scansione. Il valore predefinito è: *illimitato*.

Se per tali motivi il controllo dell'archivio viene terminato anticipatamente, la relativa casella di controllo rimarrà deselezionata.

Nota: si consiglia di non modificare i valori predefiniti. In circostanze normali, non sussiste alcun motivo per farlo.

4.1.1.6.6 Altro

Nella sezione **Altro** è possibile configurare le seguenti opzioni:

Registra tutti gli oggetti - Se questa opzione è selezionata, il file di rapporto riporta tutti i file sottoposti a scansione, anche quelli non infetti. Se ad esempio viene individuata un'infiltrazione all'interno di un archivio, nel rapporto verranno elencati anche i file puliti presenti all'interno dell'archivio.

Attiva ottimizzazione Smart - Al fine di garantire il miglior livello di scansione, l'attivazione dell'ottimizzazione Smart consente l'utilizzo delle impostazioni più efficienti alla velocità di scansione più elevata. I vari moduli di protezione eseguono la scansione in modo intelligente, utilizzando metodi di scansione differenti e applicandoli a tipi di file specifici. Se l'opzione di ottimizzazione Smart non è attivata, durante la scansione vengono applicate solo le impostazioni definite dall'utente nell'architettura ThreatSense di moduli specifici.

Quando si configurano i parametri del motore ThreatSense per l'esecuzione di un Controllo computer, sono disponibili le seguenti opzioni:

Flussi di dati alternativi (ADS) - I flussi di dati alternativi utilizzati dal file system NTFS sono associazioni di file e cartelle invisibili alle normali tecniche di controllo. Molte infiltrazioni cercano di non essere rilevate presentandosi come flussi di dati alternativi.

Esegui scansioni in background con priorità bassa - Ogni sequenza di scansione utilizza una determinata quantità di risorse del sistema. Se si utilizzano programmi che necessitano di molte risorse di sistema, è possibile attivare la scansione in background con priorità bassa e risparmiare risorse per le applicazioni.

Mantieni timestamp ultimo accesso - Selezionare questa opzione per mantenere l'ora di accesso originale ai file controllati anziché aggiornarla (ad esempio, per l'utilizzo con sistemi di backup di dati).

Scorri rapporto di controllo - Questa opzione consente di abilitare/disabilitare lo scorrimento del rapporto. Se viene selezionata, è possibile scorrere le informazioni verso l'alto nella finestra di visualizzazione.

4.1.1.7 Rilevamento di un'infiltrazione

Le infiltrazioni possono raggiungere il sistema da diversi accessi, ad esempio pagine Web, cartelle condivise, messaggi e-mail o dispositivi rimovibili (USB, dischi esterni, CD, DVD, dischetti e così via).

Comportamento standard

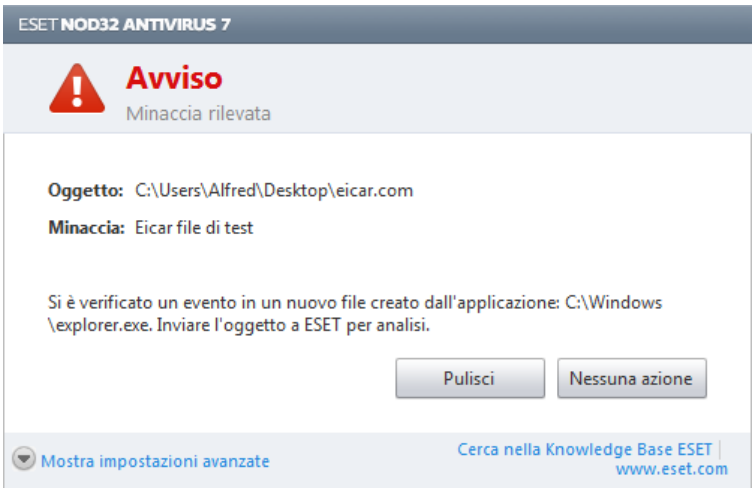
In linea generale, ESET NOD32 Antivirus gestisce le infiltrazioni utilizzando i seguenti strumenti per la rilevazione:

- Protezione file system in tempo reale
- Protezione accesso Web
- Protezione client di posta
- Controllo del computer su richiesta

Ciascuna di tali opzioni utilizza il livello di pulizia standard e tenta di pulire il file e di spostarlo nella Quarantena o di interrompere la connessione. Una finestra di avviso viene visualizzata nell'area di notifica posta nell'angolo in basso a destra della schermata. Per ulteriori informazioni sui livelli di pulizia e sul comportamento, vedere Pulizia.

Pulizia ed eliminazione

In assenza di azioni predefinite per l'esecuzione della Protezione file system in tempo reale, verrà chiesto all'utente di selezionare un'opzione nella finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, in quanto i file infettati non verranno puliti. È opportuno selezionare questa opzione solo quando si è certi che un file non è pericoloso e che si tratta di un errore di rilevamento.



Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto un codice dannoso. In tal caso, tentare innanzitutto di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codice dannoso, verrà eliminato.

Se un file infetto è "bloccato" o utilizzato da un processo del sistema, verrà eliminato solo dopo essere stato rilasciato (generalmente dopo il riavvio del sistema).

Più minacce

Se durante un controllo del computer i file infetti non sono stati puliti (o se il Livello di pulizia era impostato su **Nessuna pulizia**), viene visualizzata una finestra di avviso che richiede di selezionare un'azione per i file in questione. Selezionare le azioni da eseguire sui file (le azioni vengono impostate singolarmente per ciascun file

presente nell'elenco), quindi fare clic su **Fine**.

Eliminazione dei file negli archivi

In modalità di pulizia predefinita, l'intero archivio verrà eliminato solo nel caso in cui contenga file infetti e nessun file pulito. In pratica, gli archivi non vengono eliminati nel caso in cui dovessero contenere anche file puliti non dannosi. Durante l'esecuzione di un controllo di massima pulizia, si consiglia di agire con estrema prudenza, in quanto, in caso di rilevamento di un file infetto, verrà eliminato l'intero archivio di appartenenza dell'oggetto, indipendentemente dallo stato degli altri file.

Se il computer mostra segnali di infezione malware, ad esempio appare più lento, si blocca spesso e così via, è consigliabile attenersi alle seguenti istruzioni:

- Aprire ESET NOD32 Antivirus e fare clic su Controllo del computer
- Fare clic su **Controllo intelligente** (per ulteriori informazioni, consultare Controllo del computer)
- Al termine del controllo, consultare il rapporto per conoscere il numero di file controllati, infetti e puliti

Se si desidera controllare solo una parte del disco, fare clic su **Controllo personalizzato** e selezionare le destinazioni su cui effettuare un controllo antivirus.

4.1.1.8 Protezione documenti

La funzione Protezione documenti consente di eseguire il controllo dei documenti di Microsoft Office prima della loro apertura e dei file scaricati automaticamente da Internet Explorer, ad esempio gli elementi di Microsoft ActiveX. La funzione Protezione documenti offre un livello di protezione aggiuntivo rispetto alla protezione file system in tempo reale e può essere disattivata per ottimizzare le prestazioni di sistemi non esposti a volumi elevati di documenti Microsoft Office.

Integrazione nel sistema consente di attivare il sistema di protezione. Per modificare questa opzione, premere F5 per aprire la finestra Configurazione avanzata e fare clic su **Computer** > **Antivirus e antispyware** > **Protezione documenti** nella struttura Configurazione avanzata.

Questa funzione è attivata dalle applicazioni che utilizzano Microsoft Antivirus API (ad esempio Microsoft Office 2000 e versioni successive o Microsoft Internet Explorer 5.0 e versioni successive).

4.1.2 Supporti rimovibili

ESET NOD32 Antivirus offre il controllo automatico dei supporti rimovibili (CD/DVD/USB/...). Questo modulo consente di controllare un supporto inserito. Questa funzionalità può essere utile se l'amministratore del computer desidera impedire l'utilizzo di supporti rimovibili con contenuti non desiderati da parte degli utenti.

Per modificare il comportamento dell'azione che verrà eseguita quando nel computer viene inserito un supporto rimovibile (CD/DVD/USB/...), premere **F5** per aprire la finestra Configurazione avanzata ed espandere **Computer** > **Antivirus e antispyware** > **Supporti rimovibili** e selezionare l'azione predefinita **Azione da eseguire dopo aver inserito i supporti rimovibili** dal menu a discesa. Se è selezionata l'opzione **Mostra opzioni di scansione**, verrà visualizzata una notifica che consente di scegliere un'azione desiderata:

- **Controlla ora** - Viene eseguito il controllo del computer su richiesta del supporto rimovibile inserito.
- **Controlla più tardi** - Non verrà eseguita alcuna azione e la finestra **Rilevato nuovo dispositivo** verrà chiusa.
- **Configurazione...** - Consente di accedere alla sezione di configurazione del supporto rimovibile.

4.1.3 Controllo dispositivi

ESET NOD32 Antivirus offre un controllo automatico dei dispositivi (CD/DVD/USB/...). Questo modulo consente di controllare, bloccare o regolare le estensioni dei filtri o delle autorizzazioni e di definire la capacità dell'utente di accedere e di utilizzare un determinato dispositivo. Questa funzionalità potrebbe rivelarsi utile nel caso in cui l'amministratore di un computer desideri impedire l'utilizzo di dispositivi con contenuti non desiderati da parte degli utenti.

Dispositivi esterni supportati

- CD/DVD
- Archiviazione su disco
- Archiviazione FireWire

Nota: il controllo eseguito da ESET Endpoint Security o ESET Endpoint Antivirus in un ambiente aziendale supporta varie tipologie di dispositivi esterni.

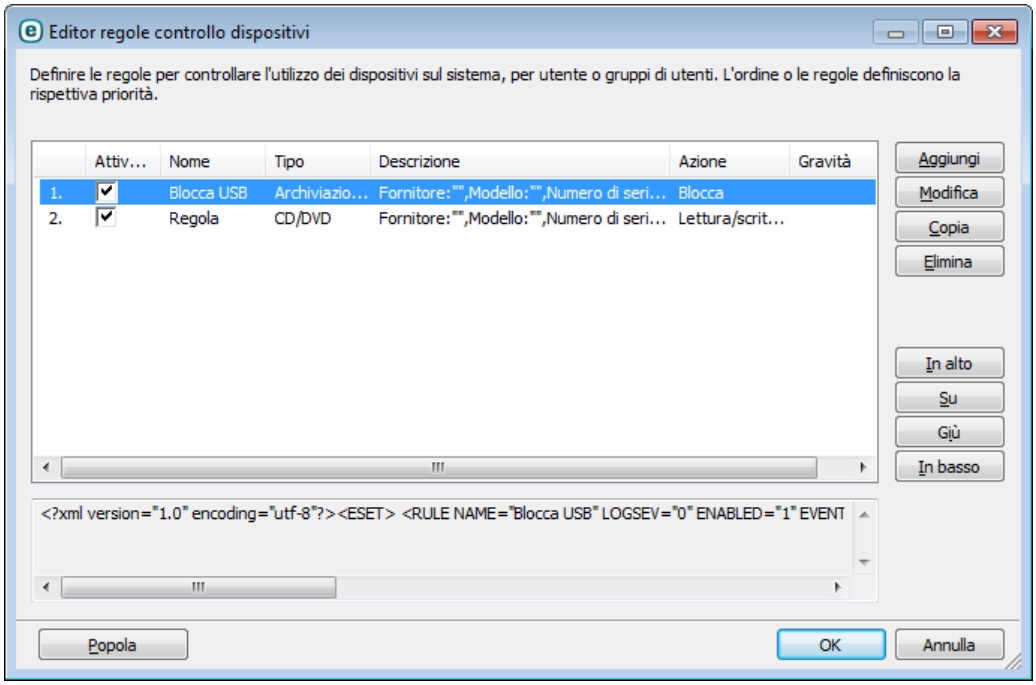
Le opzioni di configurazione del controllo dispositivi possono essere modificate in **Configurazione avanzata** (F5) > **Computer** > **Controllo dispositivi**.

Selezionando la casella di controllo accanto a **Integra nel sistema**, è possibile attivare la funzione Controllo dispositivi in ESET NOD32 Antivirus. Per rendere effettiva questa modifica, sarà necessario riavviare il computer. Dopo aver attivato il Controllo dispositivi, si attiverà l'opzione **Configura regole...**, che consentirà all'utente di aprire la finestra Editor regole controllo dispositivi.

Se il dispositivo esterno inserito applica una regola esistente che esegue l'azione **Blocca**, nell'angolo in basso a destra comparirà una finestra popup di notifica e l'accesso al dispositivo verrà negato.

4.1.3.1 Regole per il controllo dispositivi

Nella finestra **Editor regole controllo dispositivi**, in cui vengono visualizzate le regole esistenti, è possibile effettuare un controllo accurato dei dispositivi esterni collegati dagli utenti al computer.



È possibile consentire o bloccare specifici dispositivi per ciascun utente o gruppo di utenti e sulla base di parametri aggiuntivi del dispositivo che è possibile specificare nella configurazione delle regole. L'elenco delle regole contiene varie descrizioni tra cui nome, tipo di dispositivo esterno, azione da eseguire dopo aver collegato un dispositivo esterno al computer e gravità del rapporto.

Fare clic su **Aggiungi** o **Modifica** per gestire una regola. Fare clic su **Copia** per creare una nuova regola con le opzioni predefinite utilizzate per un'altra regola selezionata. Le stringhe XML visualizzate quando si seleziona una regola possono essere copiate negli Appunti in modo da aiutare gli amministratori di sistema a esportare/importare questi dati e utilizzarli, ad esempio, in ESET Remote Administrator.

Premere CTRL e fare clic per selezionare più regole e applicare azioni, come ad esempio elimina o sposta in alto o in basso nell'elenco, a tutte le regole selezionate. La casella di controllo **Attivata** consente di disattivare o attivare una regola. Questa opzione è utile se non si desidera eliminare definitivamente una regola in modo da poterla utilizzare in futuro.

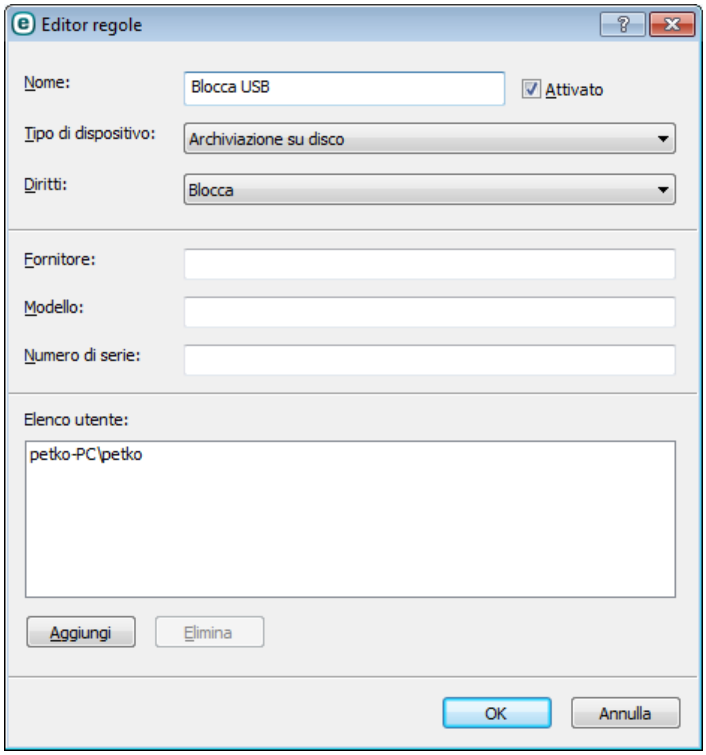
Il controllo viene eseguito mediante regole classificate in base al rispettivo ordine di priorità (le regole con priorità maggiore saranno posizionate in alto).

Fare clic con il pulsante destro del mouse su una regola per visualizzare il menu contestuale. Qui è possibile impostare il livello di dettaglio (gravità) delle voci di rapporto di una regola. Le voci del rapporto possono essere visualizzate nella finestra principale di ESET NOD32 Antivirus in **Strumenti** > **File di rapporto**.

Fare clic su **Popola** per popolare automaticamente i parametri dei supporti rimovibili per i dispositivi collegati al computer.

4.1.3.2 Aggiunta di regole per il controllo dispositivi

Una regola per il controllo dispositivi definisce l'azione che verrà intrapresa quando viene effettuata una connessione tra il computer e un dispositivo che soddisfa i criteri della regola.



Inserire una descrizione della regola nel campo **Nome** per consentire una migliore identificazione. Selezionare la casella di controllo accanto ad **Attivata** per disattivare o attivare questa regola. Questa opzione può essere utile se non si desidera eliminare definitivamente la regola.

Tipo di dispositivo

Scegliere il tipo di dispositivo esterno dal menu a discesa (USB/Bluetooth/FireWire/...). I tipi di dispositivi vengono ereditati dal sistema operativo e possono essere visualizzati in Gestione dispositivi del sistema, a condizione che un dispositivo sia collegato al computer. Il tipo di dispositivo **Supporto di archiviazione ottico** nel menu a discesa si riferisce all'archiviazione dei dati su un supporto a lettura ottica (ad esempio, CD e DVD). I supporti di archiviazione includono dischi esterni o lettori tradizionali di schede di memoria collegati tramite USB o FireWire. I lettori di smart card prevedono circuiti integrati incorporati, come ad esempio schede SIM o schede di autenticazione. Esempi di dispositivi di acquisizione immagini sono gli scanner o le fotocamere, che non forniscono informazioni sugli utenti, ma solo sulle azioni. Ciò implica che i dispositivi di acquisizione immagini possono essere bloccati solo a livello globale.

Diritti

È possibile negare o consentire l'accesso ai supporti non di archiviazione. Le regole dei supporti di archiviazione consentono invece di scegliere uno dei seguenti diritti:

- **Blocca** - L'accesso al supporto sarà bloccato.
- **Solo lettura** - Sul dispositivo sarà consentito solo l'accesso alla lettura.
- **Lettura/scrittura** - Sarà consentito l'accesso completo al dispositivo.

Tenere presente che non sono disponibili tutti i diritti (azioni) per tutti i tipi di dispositivi. Se su un dispositivo è presente spazio di archiviazione, saranno disponibili tutte e tre le azioni. Per i dispositivi non di archiviazione, sono disponibili solo due azioni (ad esempio, l'azione **Solo lettura** non è disponibile per il sistema Bluetooth. Ciò significa che i dispositivi Bluetooth possono essere solo consentiti o bloccati).

Altri parametri che possono essere utilizzati per ottimizzare le regole e personalizzarle in base ai dispositivi in uso. Tutti i parametri non fanno distinzione tra lettere maiuscole e minuscole:

- **Fornitore** - Filtraggio in base al nome o identificativo del fornitore.
- **Modello** - Nome specifico del dispositivo.
- **Numero di serie** - Generalmente, a ogni dispositivo esterno è associato un numero di serie. Nel caso di CD/DVD, il numero di serie è associato al supporto specifico e non all'unità CD.

Nota: se le tre voci precedenti non sono specificate, questi campi verranno ignorati dalla regola durante la ricerca delle corrispondenze. I parametri di filtraggio in tutti i campi testuali distinguono tra maiuscole e minuscole e i caratteri jolly (*, ?) non sono supportati. I parametri devono essere identici a quelli del fornitore.

Suggerimento: per trovare i parametri di un dispositivo, creare una regola di autorizzazione per il tipo appropriato di dispositivi, collegare il dispositivo al computer, quindi controllare le proprietà del dispositivo in Rapporto controllo dispositivi.

Le regole possono essere limitate a determinati utenti o gruppi di utenti aggiunti all'**Elenco utenti**:

- **Aggiungi** - Apre la finestra di dialogo **Tipo di oggetto: Utenti o Gruppi**, che consente di selezionare gli utenti desiderati.
- **Elimina** - Rimuove l'utente selezionato dal filtro.

Tenere presente che non tutti i dispositivi possono essere limitati dalle regole dell'utente (ad esempio, i dispositivi di acquisizione di immagini non forniscono informazioni sugli utenti, ma solo sulle azioni invocate).

4.1.4 HIPS

Il **Sistema anti-intrusione basato su host** (HIPS) protegge il sistema da malware o attività indesiderate che tentano di compromettere la sicurezza del computer. L'HIPS utilizza un'analisi comportamentale avanzata unita alle capacità di rilevamento del filtraggio di rete per il monitoraggio dei processi in esecuzione, dei file e delle chiavi del registro. L'HIPS è indipendente dalla protezione file system in tempo reale e non è un firewall, in quanto monitora solo i processi eseguiti all'interno del sistema operativo.

Le impostazioni HIPS sono disponibili in **Configurazione avanzata** (F5). Per accedere all'HIPS nella struttura Configurazione avanzata, fare clic su **Computer** > **HIPS**. Lo stato HIPS (attivato/disattivato) è visualizzato nella finestra principale di ESET NOD32 Antivirus, nel riquadro **Configurazione**, a destra della sezione Computer.

Attenzione: è consigliabile che le modifiche alle impostazioni HIPS siano apportate solo dagli utenti avanzati.

ESET NOD32 Antivirus presenta una tecnologia di *Autoprotezione* integrata che impedisce ai software dannosi di corrompere o disattivare la protezione antivirus e antispyware del computer. La funzione *Autoprotezione* protegge i file e le chiavi di registro considerati cruciali per il funzionamento di ESET NOD32 Antivirus e garantisce la mancanza di privilegi per il software potenzialmente dannoso nell'apportare modifiche a tali percorsi.

Le modifiche alle impostazioni **Attiva HIPS** e **Attiva l'Autoprotezione** avranno effetto solo dopo aver il riavvio di Windows. Per avere effetto, la disattivazione del sistema **HIPS** richiede anche un riavvio del computer.

L'**Exploit Blocker** è progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

Lo **Scanner memoria avanzato** lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscazione e/o crittografia. Per ulteriori informazioni su questo tipo di protezione, consultare il glossario.

Il filtraggio HIPS può essere eseguito in una delle quattro modalità seguenti:

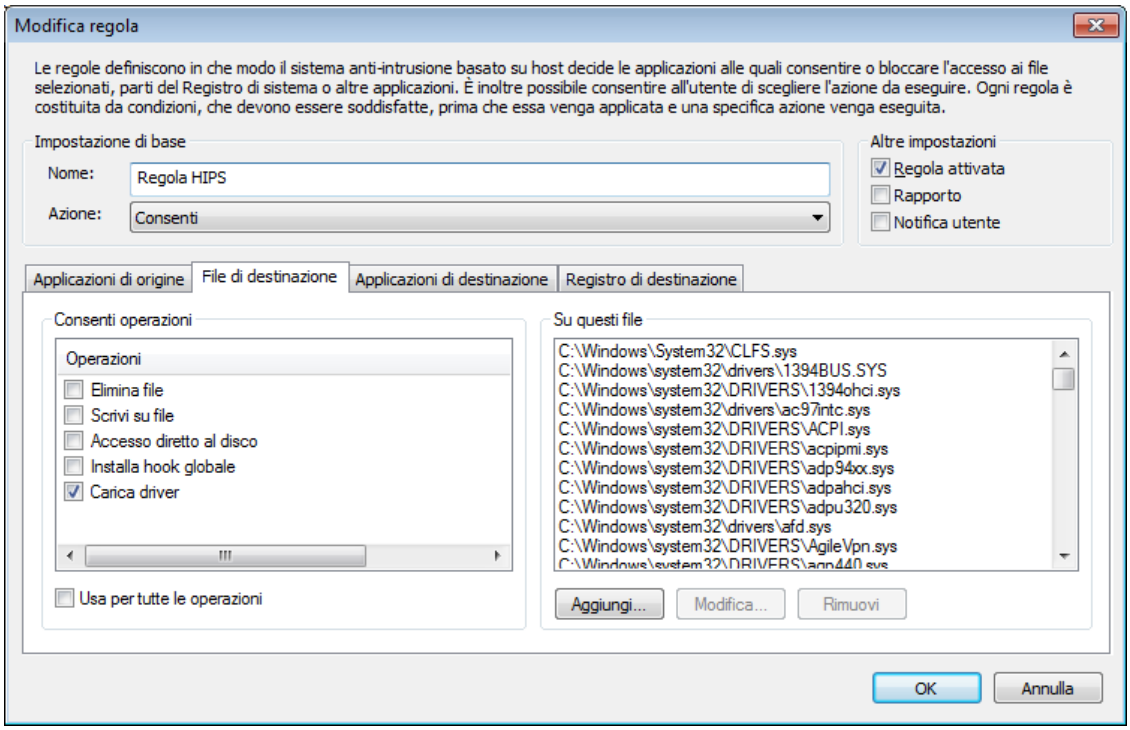
- **Modalità automatica con regole** - Le operazioni sono attivate e viene utilizzata una serie di regole predefinite per proteggere il sistema.
- **Modalità interattiva** - All'utente verrà chiesto di confermare le operazioni.
- **Modalità basata su criteri** - Le operazioni non definite da una regola possono essere bloccate.
- **Modalità riconoscimento** - Le operazioni sono attivate e dopo ogni operazione viene creata una regola. Le regole create in questa modalità possono essere visualizzate nell'**Editor regole**, ma la loro priorità è inferiore rispetto alla priorità delle regole create manualmente o in modalità automatica. Dopo aver selezionato **Modalità riconoscimento**, l'opzione **Notifica scadenza modalità riconoscimento entro x giorni** diventa disponibile. Una

volta scaduto il periodo di tempo definito in **Notifica scadenza modalità riconoscimento entro x giorni**, la modalità di riconoscimento viene nuovamente disattivata. Il periodo di tempo massimo è 14 giorni. Alla scadenza di tale intervallo di tempo, viene visualizzata una finestra popup in cui è possibile modificare le regole e selezionare una modalità di filtraggio differente.

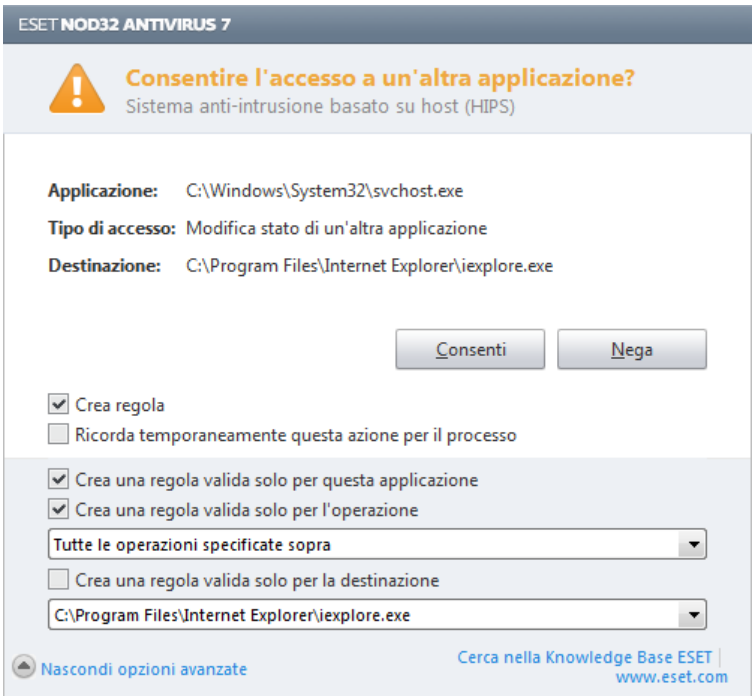
Il sistema HIPS monitora gli eventi all'interno del sistema operativo e reagisce in base a regole simili a quelle utilizzate dal rapporto del Personal firewall in ESET Smart Security. Fare clic su **Configura regole...** per aprire la finestra di gestione delle regole HIPS. In questa sezione è possibile selezionare, creare, modificare o eliminare regole.

Nell'esempio seguente viene spiegato come limitare il comportamento indesiderato delle applicazioni:

1. Denominare la regola e selezionare **Blocca** nel menu a discesa **Azione**.
2. Aprire la scheda **Applicazioni di destinazione**. Lasciare vuota la scheda **Applicazioni di origine** per applicare la nuova regola a tutte le applicazioni che tentano di eseguire una delle operazioni selezionate nell'elenco **Operazioni** sulle applicazioni nell'elenco **Su queste applicazioni**.
3. Selezionare **Modifica stato di un'altra applicazione** (tutte le operazioni sono descritte nella guida del prodotto, a cui è possibile accedere premendo F1).
4. **Aggiungi** una o più applicazioni che si desidera proteggere.
5. Selezionare la casella di controllo **Notifica utente** per visualizzare una notifica tutte le volte che viene applicata una regola.
6. Fare clic su **OK** per salvare la nuova regola.



Selezionando **Chiedi** come azione predefinita, ESET NOD32 Antivirus consentirà di visualizzare una finestra di dialogo all'esecuzione di ogni operazione. È possibile scegliere di **Negare** o **Consentire** l'operazione. Se non viene scelta alcuna azione, il sistema ne selezionerà una sulla base delle regole predefinite.



La finestra di dialogo **Consenti l'accesso a un'altra applicazione** consente di creare una regola in base a una nuova azione rilevata dall'HIPS e di definire le condizioni in base alle quali consentire o negare l'azione. Fare clic su **Mostra opzioni** per definire i parametri esatti della nuova regola. Le regole create in questo modo sono considerate equivalenti alle regole create manualmente. La regola creata da una finestra di dialogo può quindi essere meno specifica rispetto a quella che ha attivato la finestra di dialogo. Ciò significa che, dopo la creazione di una regola, la stessa operazione attiva un'altra finestra di dialogo se i parametri del set di regole precedente non si applicano alla specifica situazione.

Ricorda temporaneamente questa azione per il processo causa un'azione (**Consenti** /**Nega**) da utilizzare finché non verrà apportata una modifica alle regole o alle modalità di filtraggio oppure non verrà eseguito un aggiornamento del modulo HIPS o un riavvio del sistema. In seguito a una di queste azioni, le regole temporanee verranno eliminate.

4.1.5 Modalità giocatore

La modalità giocatore è una funzionalità per gli utenti che desiderano utilizzare il software senza essere interrotti, che non desiderano essere disturbati dalle finestre popup e che desiderano ridurre al minimo l'utilizzo della CPU. La modalità giocatore può essere utilizzata anche durante le presentazioni che non possono essere interrotte dall'attività antivirus. Attivando questa funzionalità, tutte le finestre popup vengono disattivate e l'attività di Pianificazione attività verrà completamente interrotta. La protezione del sistema è ancora in esecuzione in background ma non richiede alcun intervento da parte dell'utente.

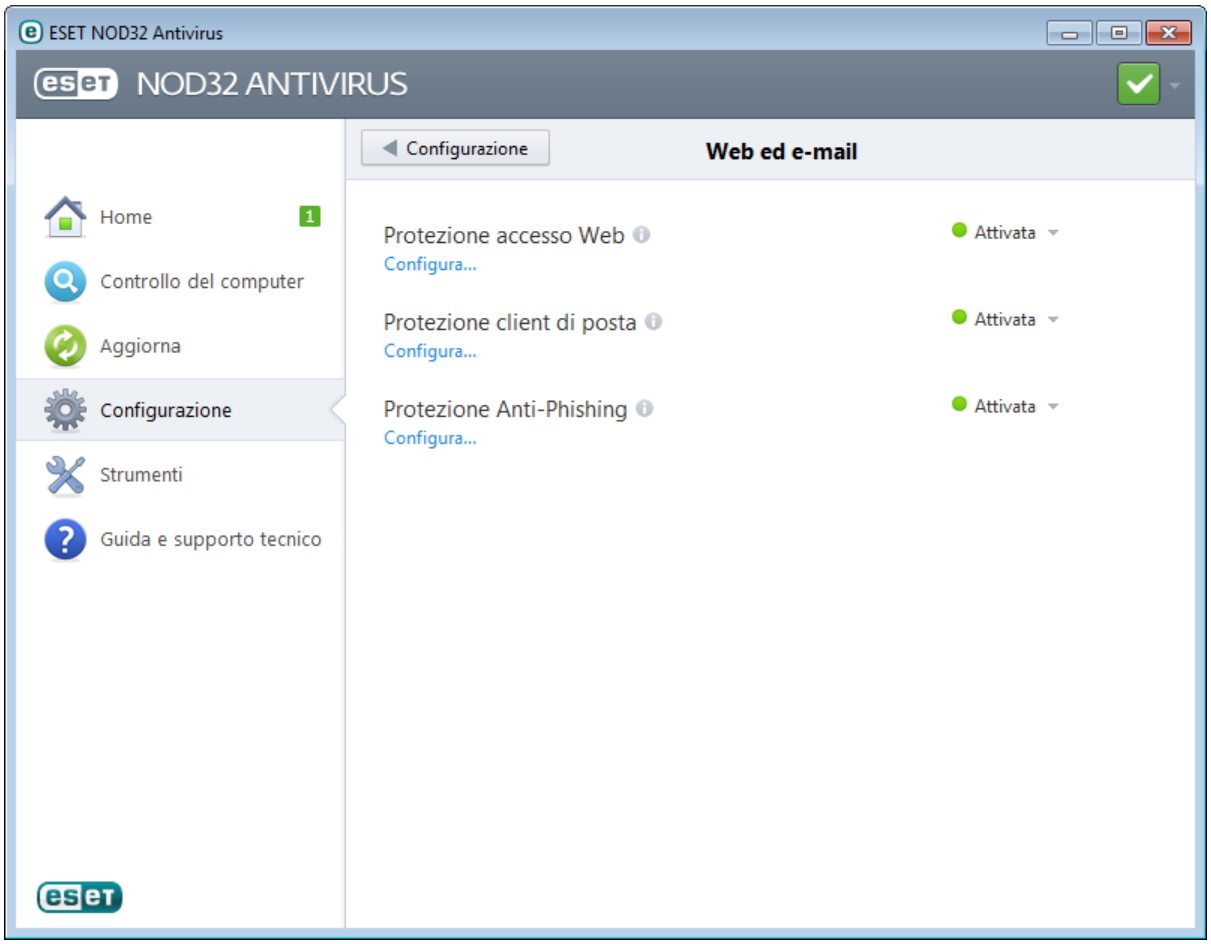
La modalità giocatore può essere attivata o disattivata nella finestra principale del programma facendo clic su **Configurazione** > **Computer** > **Attiva** in **Modalità giocatore**. In alternativa, è possibile attivarla nella struttura Configurazione avanzata (F5) espandendo **Computer**, facendo clic su **Modalità giocatore** e selezionando la casella di controllo accanto a **Attiva modalità giocatore**. L'attivazione della modalità giocatore rappresenta un potenziale rischio per la protezione. Per tale motivo, l'icona relativa allo stato della protezione sulla barra delle attività diventa di colore arancione e viene visualizzato un avviso. Questo avviso verrà inoltre visualizzato nella finestra principale del programma dove **Modalità giocatore attivata** comparirà in arancione.

Selezionando **Attiva modalità giocatore quando vengono eseguite automaticamente applicazioni in modalità a schermo intero**, la modalità giocatore si attiverà all'avvio di un'applicazione in modalità a schermo intero e si interromperà automaticamente all'uscita dall'applicazione. Questa funzionalità si rivela particolarmente utile per l'attivazione della modalità giocatore all'avvio di un gioco, di un'applicazione in modalità a schermo intero o di una presentazione.

È inoltre possibile selezionare **Disattiva automaticamente la modalità giocatore dopo X minuti** per definire l'intervallo di tempo (il valore predefinito è 1 minuto) in seguito al quale la modalità giocatore verrà automaticamente disattivata.

4.2 Web ed e-mail

Le opzioni di configurazione del Web ed e-mail sono disponibili nel riquadro **Configurazione** facendo clic su **Web ed e-mail**. Da qui è possibile accedere alle impostazioni dettagliate del programma.



La connettività Internet è una funzione standard dei personal computer. Purtroppo, Internet è diventato lo strumento principale per la distribuzione di codice dannoso. Per questo motivo, è essenziale gestire attentamente le impostazioni di **Protezione accesso Web**.

Fare clic su **Configura** per aprire le impostazioni di protezione Web/e-mail/anti-phishing in Configurazione avanzata.

La **Protezione client di posta** garantisce il controllo delle comunicazioni via e-mail ricevute mediante il protocollo POP3 e IMAP. Utilizzando il programma plug-in per il client di posta in uso, ESET NOD32 Antivirus controlla tutte le comunicazioni da e verso il client di posta (POP3, MAPI, IMAP, HTTP).

La **Protezione Anti-Phishing** consente all'utente di bloccare le pagine Web che distribuiscono notoriamente contenuti phishing. Si consiglia vivamente di lasciare attivata l'opzione Anti-Phishing.

È possibile disattivare temporaneamente il modulo di protezione Web/e-mail Web/e-mail/anti-phishing facendo clic su **Attivato**.

4.2.1 Protezione client di posta

La Protezione client e-mail garantisce il controllo delle comunicazioni via e-mail ricevute mediante i protocolli POP3 e IMAP. Utilizzando il plug-in per Microsoft Outlook e altri client e-mail, ESET NOD32 Antivirus controlla tutte le comunicazioni dal client e-mail (POP3, MAPI, IMAP, HTTP). Durante la verifica dei messaggi in arrivo, il programma utilizza tutti i metodi di controllo avanzato previsti nel motore di controllo ThreatSense. Ciò significa che il rilevamento di programmi dannosi viene eseguito ancora prima del confronto con il database delle firme antivirali. La scansione delle comunicazioni mediante i protocolli POP3 e IMAP non dipende dal client e-mail in uso.

Le opzioni per questa funzionalità sono disponibili nella sezione **Configurazione avanzata** > **Web ed e-mail** > **Protezione client di posta**.

Configurazione parametri motore ThreatSense - La configurazione avanzata dello scanner antivirus consente di configurare gli oggetti da controllare, i metodi di rilevamento e così via. Fare clic su **Configurazione...** per visualizzare la finestra della configurazione dettagliata dello scanner antivirus.

Dopo che un messaggio e-mail è stato controllato, una notifica contenente i risultati di scansione può essere aggiunta al messaggio. È possibile selezionare **Aggiungi notifiche alle e-mail ricevute e lette** o **Aggiungi notifiche alle e-mail inviate**. Tenere presente che, in rare occasioni, le notifiche potrebbero essere omesse in messaggi HTML problematici o create da specifici virus. Le notifiche possono essere aggiunte sia alle e-mail ricevute e lette sia alle e-mail inviate. Le opzioni disponibili sono:

- **Mai** - Non viene aggiunta alcuna notifica.
- **Solo per l'e-mail infetta** - Solo i messaggi contenenti software dannoso vengono contrassegnati come controllati (impostazione predefinita).
- **Per tutte le e-mail** - Il programma aggiunge la notifica a tutte le e-mail sottoposte a scansione.

Aggiungi nota all'oggetto di e-mail infette ricevute e lette/inviate - Selezionare questa casella di controllo se si desidera che la protezione e-mail includa un allarme antivirus nell'oggetto di un'e-mail infetta. Questa funzione consente di filtrare in modo semplice le e-mail infette in base all'oggetto (se supportata dal programma e-mail in uso). Aumenta inoltre il livello di credibilità del destinatario e, in caso di rilevamento di un'infiltrazione, fornisce informazioni utili sul livello di minaccia di un determinato messaggio e-mail o mittente.

Template aggiunto all'oggetto dell'e-mail infetta - Modificare questo template se si desidera cambiare il formato predefinito dell'oggetto di un'e-mail infetta. Questa funzione sostituirà l'oggetto del messaggio *"Ciao"* con un determinato valore predefinito *"[virus]"* nel seguente formato: *"[virus] Ciao"*. La variabile *%VIRUSNAME%* rappresenta la minaccia rilevata.

4.2.1.1 Integrazione con client e-mail

L'integrazione di ESET NOD32 Antivirus con i client e-mail aumenta il livello di protezione attiva contro codici dannosi nei messaggi e-mail. Se il client di posta in uso è supportato, è possibile attivare l'integrazione in ESET NOD32 Antivirus. In caso di attivazione dell'integrazione, la barra degli strumenti di ESET NOD32 Antivirus viene inserita direttamente nel client di posta, garantendo in tal modo una protezione e-mail più efficace. Le impostazioni di integrazione sono disponibili nella sezione **Configurazione** > **Accedi a configurazione avanzata...** > **Web ed e-mail** > **Protezione client e-mail** > **Integrazione con client e-mail**.

I client e-mail attualmente supportati includono Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. Per un elenco completo dei client e-mail supportati e delle relative versioni, fare riferimento al seguente articolo della Knowledge Base ESET.

Selezionare la casella di controllo accanto a **Disattiva il controllo alla modifica del contenuto della posta in arrivo** se si riscontra un rallentamento del sistema durante l'utilizzo del client di posta. Ciò può accadere durante il recupero di e-mail da Kerio Outlook Connector Store.

Anche se l'integrazione non è attivata, la comunicazione e-mail rimane comunque protetta tramite il modulo di protezione client e-mail (POP3, IMAP).

4.2.1.1.1 Configurazione della protezione client di posta

Il modulo di protezione client di posta supporta i seguenti client di posta: Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail e Mozilla Thunderbird. Per questi programmi la protezione e-mail esegue la stessa funzione di un plugin. Il vantaggio principale offerto dal plugin consiste nella sua indipendenza dal protocollo utilizzato. Quando il client di posta riceve un messaggio crittografato, questo viene decodificato e inviato al programma di scanner antivirus.

E-mail per il controllo

E-mail ricevute - Attiva/disattiva la verifica dei messaggi ricevuti.
E-mail inviate - Attiva/disattiva la verifica dei messaggi inviati.
E-mail lette - Attiva/disattiva la verifica dei messaggi letti.

Azione da eseguire sull'e-mail infetta

Nessuna azione - Se questa opzione è attivata, il programma identificherà gli allegati infetti senza tuttavia eseguire alcuna azione.
Elimina e-mail - Il programma notificherà all'utente le eventuali infiltrazioni ed eliminerà il messaggio.
Sposta e-mail nella cartella Posta eliminata - I messaggi e-mail infetti verranno spostati automaticamente nella cartella **Posta eliminata**.
Sposta e-mail nella cartella - Specificare la cartella personalizzata in cui si desidera spostare le e-mail infette che sono state rilevate.

Altro

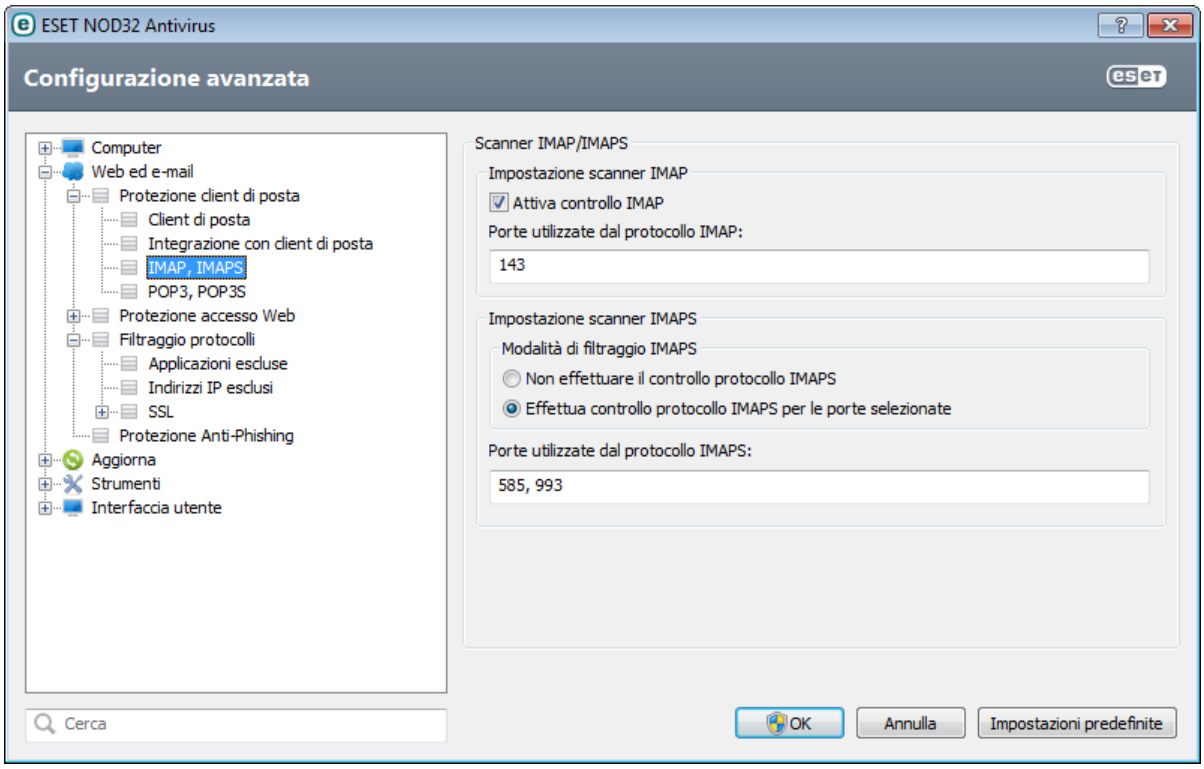
Ripeti controllo dopo l'aggiornamento - Attiva/disattiva un nuovo controllo dopo l'aggiornamento del database delle firme antivirali.
Accetta i risultati del controllo da altri moduli - Selezionando questa opzione, il modulo di protezione e-mail accetterà i risultati del controllo di altri moduli di protezione.

4.2.1.2 Scanner IMAP, IMAPS

IMAP (Internet Message Access Protocol) è un altro protocollo Internet per il recupero dei messaggi e-mail. Il protocollo IMAP offre alcuni vantaggi rispetto al protocollo POP3, tra cui, ad esempio, la possibilità di connettere simultaneamente più di un client alla stessa casella di posta e conservare informazioni sullo stato del messaggio (lettura, invio di risposta o eliminazione). ESET NOD32 Antivirus offre protezione per questo protocollo, indipendentemente dal client di posta utilizzato.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Il controllo del protocollo IMAP viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono sottoposte a scansione tutte le comunicazioni della porta 143, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a Verifica protocollo SSL nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **Filtro protocolli** > **SSL** e selezionare l'opzione **Effettua sempre la scansione del protocollo SSL**.



4.2.1.3 Filtro POP3, POP3S

Il protocollo POP3 è quello più diffuso per la ricezione di comunicazioni e-mail in un'applicazione client e-mail. ESET NOD32 Antivirus offre la protezione per questo protocollo, indipendentemente dal client e-mail in uso.

Il modulo di protezione che fornisce questo controllo viene avviato automaticamente all'avvio del sistema e resta quindi attivo in memoria. Perché il modulo funzioni correttamente, verificare che sia attivato: il controllo del protocollo POP3 viene eseguito automaticamente senza che sia necessario riconfigurare il client di posta. Per impostazione predefinita, vengono sottoposte a scansione tutte le comunicazioni della porta 110, ma se necessario è possibile aggiungere altre porte di comunicazione. I numeri delle porte devono essere separati da una virgola.

La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a Verifica protocollo SSL nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **Filtro protocolli** > **SSL** e selezionare l'opzione **Effettua sempre la scansione del protocollo SSL**.

In questa sezione è possibile configurare il controllo dei protocolli POP3 e POP3S.

Attiva controllo e-mail - Se questa opzione è attivata, tutto il traffico POP3 viene monitorato per rilevare il software dannoso.

Porte utilizzate dal protocollo POP3 - Elenco delle porte usate dal protocollo POP3 (110 per impostazione predefinita).

ESET NOD32 Antivirus supporta anche il controllo del protocollo POP3S. Questo tipo di comunicazione utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla le comunicazioni utilizzando i metodi di crittografia SSL (Secure Socket Layer) e TLS (Transport Layer Security).

Non effettuare il controllo POP3S - La comunicazione crittografata non verrà controllata.

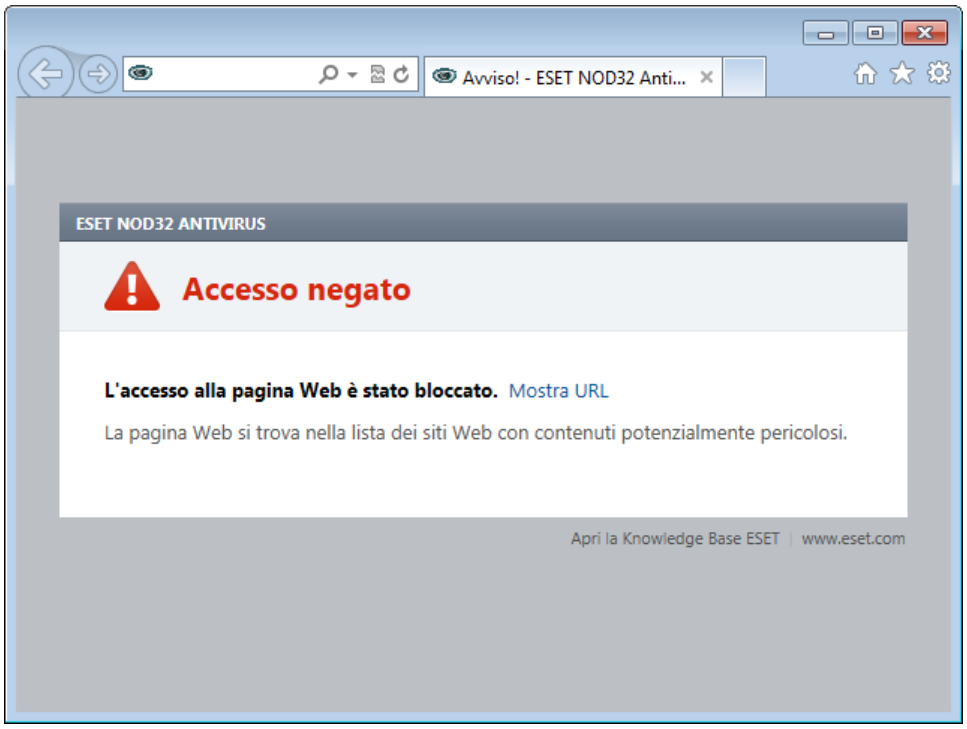
Effettua controllo protocollo POP3S per le porte selezionate - Selezionare questa opzione per attivare il controllo POP3S solo per le porte definite in **Porte utilizzate dal protocollo POP3S**.

Porte utilizzate dal protocollo POP3S - Elenco delle porte POP3S da controllare (995 per impostazione predefinita).

4.2.2 Protezione accesso Web

La connettività Internet è una funzione standard in un personal computer. Purtroppo è diventato anche lo strumento principale per il trasferimento di codice dannoso. La Protezione accesso Web monitora la comunicazione tra i browser Web e i server remoti ed è conforme alle regole HTTP (Hypertext Transfer Protocol) e HTTPS (comunicazione crittografata).

Si consiglia vivamente di attivare l'opzione Protezione accesso Web. L'opzione è disponibile dalla finestra principale di ESET NOD32 Antivirus accedendo a **Configurazione** > **Web ed e-mail** > **Protezione accesso Web**. L'accesso a pagine Web note con contenuti dannosi è sempre bloccato.



4.2.2.1 HTTP, HTTPS

Per impostazione predefinita, ESET NOD32 Antivirus è configurato in modo da utilizzare gli standard della maggior parte dei browser Internet. Le opzioni di configurazione dello scanner HTTP possono tuttavia essere modificate in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione accesso Web** > **HTTP, HTTPS**. Nella finestra principale **Scanner HTTP/HTTPS**, è possibile selezionare o deselezionare **Attiva controllo HTTP**. È inoltre possibile definire i numeri delle porte utilizzate per la comunicazione HTTP. L'impostazione predefinita per i numeri delle porte è 80 (HTTP), 8080 e 3128 (per il server proxy).

ESET NOD32 Antivirus supporta il controllo del protocollo HTTPS. La comunicazione HTTPS utilizza un canale crittografato per trasferire le informazioni tra server e client. ESET NOD32 Antivirus controlla le comunicazioni utilizzando i metodi di crittografia SSL (Secure Socket Layer) e TLS (Transport Layer Security). Il controllo HTTPS può essere impostato con le seguenti modalità:

Non effettuare il controllo del protocollo HTTPS - La comunicazione crittografata non verrà controllata.

Effettua il controllo del protocollo HTTPS per le porte selezionate - Il programma eseguirà il controllo solo sulle applicazioni specificate nella sezione Web e client di posta e che utilizzano le porte definite in **Porte utilizzate dal protocollo HTTPS**. La porta 443 rappresenta l'impostazione predefinita.

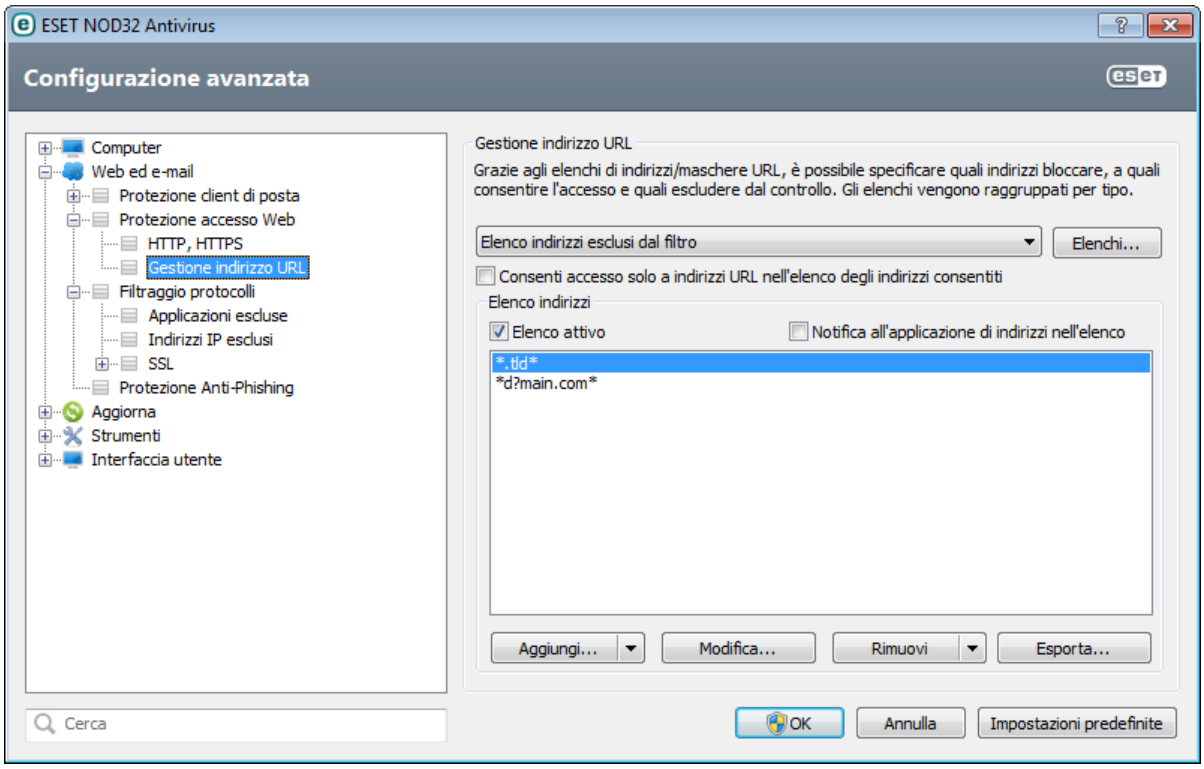
La comunicazione crittografata non verrà controllata. Per attivare il controllo sulla comunicazione crittografata e visualizzare l'impostazione scanner, accedere a Verifica protocollo SSL nella sezione Configurazione avanzata, fare clic su **Web ed e-mail** > **Filtro protocolli** > **SSL** e selezionare l'opzione **Effettua sempre la scansione del protocollo SSL**.

4.2.2.2 Gestione indirizzo URL

La sezione Gestione indirizzo URL consente di specificare gli indirizzi HTTP da bloccare, consentire o escludere dal controllo. **Aggiungi**, **Modifica**, **Rimuovi** ed **Esporta** vengono utilizzati per gestire l'elenco degli indirizzi. Non sarà possibile accedere ai siti Web presenti nell'elenco degli indirizzi bloccati. Durante l'accesso, i siti Web presenti nell'elenco degli indirizzi esclusi non vengono sottoposti al controllo per rilevare il codice dannoso. Selezionando **Consenti accesso solo a indirizzi URL nell'elenco degli indirizzi consentiti**, sarà possibile accedere solo agli indirizzi presenti nell'elenco degli indirizzi consentiti, mentre tutti gli altri indirizzi HTTP verranno bloccati.

Se si aggiunge un indirizzo URL all'**Elenco indirizzi esclusi dal filtro**, l'indirizzo verrà escluso dal controllo. È inoltre possibile consentire o bloccare determinati indirizzi aggiungendoli all'**Elenco di indirizzi consentiti** o all'**Elenco di indirizzi bloccati**. Fare clic su **Elenchi...** per aprire la finestra **Elenchi indirizzi/maschere HTTP**, dove è possibile **Aggiungere** o **Rimuovere** elenchi di indirizzi. Per aggiungere un indirizzo URL HTTPS all'elenco, è necessario selezionare l'opzione **Effettua sempre controllo del protocollo SSL**.

In tutti gli elenchi è possibile utilizzare i simboli speciali * (asterisco) e ? (punto interrogativo). L'asterisco sostituisce qualsiasi stringa di caratteri, mentre il punto interrogativo sostituisce qualsiasi simbolo. Prestare particolare attenzione quando si specificano gli indirizzi esclusi dal controllo, poiché l'elenco deve contenere solo indirizzi affidabili e sicuri. Allo stesso modo, è necessario verificare che in questo elenco i simboli * e ? siano utilizzati correttamente. Per attivare l'elenco, selezionare l'opzione **Elenco attivo**. Se si desidera ricevere una notifica quando viene inserito un indirizzo dall'elenco corrente, selezionare **Notifica all'applicazione di indirizzi nell'elenco**.



Aggiungi.../Da file - Consente di aggiungere un indirizzo all'elenco, manualmente (facendo clic su **Aggiungi**) o da un semplice file di testo (facendo clic su **Da file**). L'opzione **Da file** consente all'utente di aggiungere indirizzi URL/ maschere multipli salvati in un file di testo.

Modifica... - Consente di modificare manualmente gli indirizzi aggiungendo, ad esempio, una maschera ("*" e "?").

Rimuovi/Rimuovi tutto - Fare clic su **Rimuovi** per rimuovere l'indirizzo selezionato dall'elenco. Per rimuovere tutti gli indirizzi, selezionare **Rimuovi tutto**.

Esporta... - Consente di salvare gli indirizzi dall'elenco corrente in un file di testo.

4.2.3 Filtraggio protocolli

La protezione antivirus per i protocolli dell'applicazione viene fornita tramite il motore di scansione di ThreatSense, che integra perfettamente tutte le tecniche di scansione avanzata dei malware. Il controllo funziona automaticamente, indipendentemente dal browser o dal client e-mail in uso. Per la comunicazione crittografata (SSL) vedere **Filtraggio protocolli** > **SSL**.

Integra nel sistema - Attiva il driver per la funzionalità del filtraggio protocolli di ESET NOD32 Antivirus.

Attiva filtro del contenuto del protocollo di applicazioni - Se questa opzione è attivata, tutto il traffico HTTP(S), POP3(S) e IMAP(S) verrà controllato dallo scanner antivirus.

NOTA: in Windows Vista Service Pack 1, Windows 7 e Windows Server 2008 per il controllo delle comunicazioni di rete viene utilizzata la nuova architettura Windows Filtering Platform (WFP). Poiché la tecnologia WPF fa uso di tecniche di monitoraggio particolari, le opzioni seguenti non sono disponibili:

- **Porte HTTP, POP3 e IMAP** – Consente di limitare l'instradamento del traffico sul server proxy interno solo alle porte corrispondenti.
- **Applicazioni contrassegnate come browser Internet e client e-mail** - Consente di limitare l'instradamento del traffico sul server proxy interno solo alle applicazioni contrassegnate come browser e client e-mail (**Web ed e-mail** > **Filtraggio protocolli** > **Web e client e-mail**).
- **Porte e applicazioni contrassegnate come browser Web o client di posta** – Consente l'instradamento di tutto il traffico sulle porte corrispondenti oltre che delle comunicazioni delle applicazioni contrassegnate come browser e client di posta sul server proxy interno.

4.2.3.1 Web e client di posta

NOTA: in Windows Vista Service Pack 1 e Windows Server 2008 per il controllo delle comunicazioni di rete viene utilizzata la nuova architettura Windows Filtering Platform (WFP). Poiché la tecnologia WPF utilizza speciali tecniche di monitoraggio, la sezione **Web e client di posta** non è disponibile.

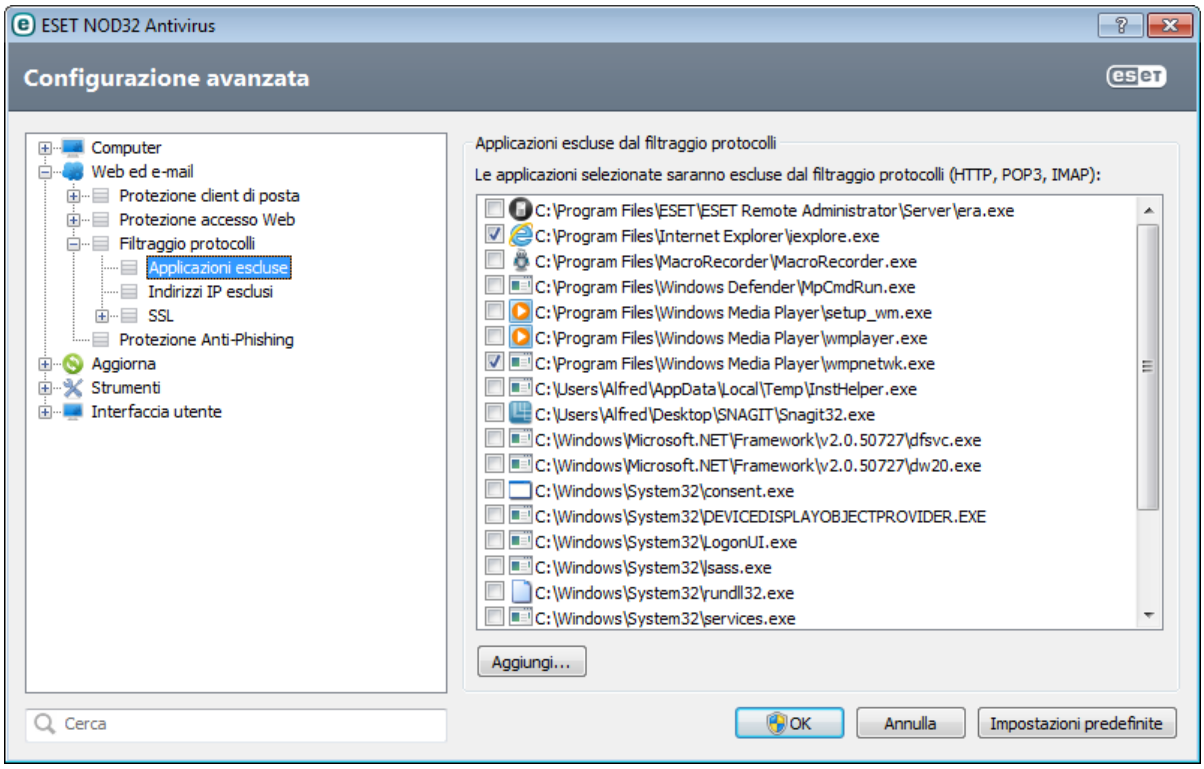
A causa dell'enorme quantità di codice dannoso che circola su Internet, una navigazione Internet sicura è essenziale per la protezione del computer. Le vulnerabilità dei browser Web e i collegamenti fraudolenti aiutano il codice dannoso a penetrare inosservato nel sistema. Per tale motivo, ESET NOD32 Antivirus si focalizza sulla sicurezza dei browser Web. Ogni applicazione che accede alla rete può essere contrassegnata come un browser. La casella di controllo presenta due stati:

- **Deselezionata** - La comunicazione delle applicazioni viene filtrata solo per le porte specificate.
- **Selezionata** - La comunicazione viene sempre filtrata (anche se viene impostata una porta differente).

4.2.3.2 Applicazioni escluse

Per escludere la comunicazione di specifiche applicazioni di rete dal filtraggio dei contenuti, selezionarle nell'elenco. Sulla comunicazione HTTP/POP3/IMAP delle applicazioni selezionate non verrà eseguito il rilevamento delle minacce. È consigliabile usare questa opzione solo per le applicazioni che non funzionano correttamente se la rispettiva comunicazione viene sottoposta a controllo.

L'esecuzione di applicazioni e servizi sarà disponibile automaticamente. Fare clic su **Aggiungi...** per selezionare manualmente un'applicazione non visualizzata nell'elenco del filtraggio protocolli.

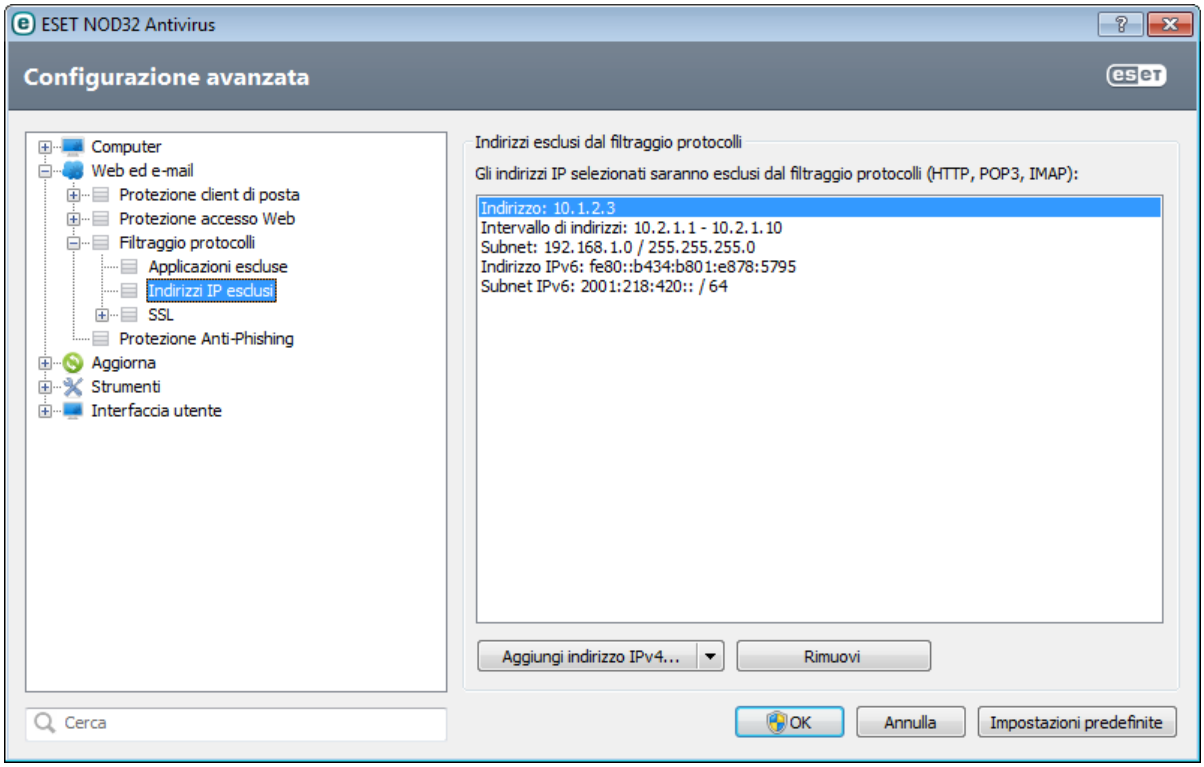


4.2.3.3 Indirizzi IP esclusi

Le voci presenti nell'elenco saranno escluse dal filtraggio del contenuto del protocollo. Sulla comunicazione HTTP/POP3/IMAP da/verso gli indirizzi selezionati non verrà eseguito il rilevamento delle minacce. È consigliabile utilizzare questa opzione solo per gli indirizzi di cui è nota l'affidabilità.

Aggiungi indirizzo IPv4/IPv6 - Fare clic per aggiungere un indirizzo IP/intervallo di indirizzi/subnet di un punto remoto a cui viene applicata una regola.

Rimuovi - Rimuove dall'elenco le voci selezionate.



4.2.3.3.1 Aggiungi indirizzo IPv4

Ciò consente di aggiungere un indirizzo/intervallo di indirizzi/subnet IP di un punto remoto a cui si applica la regola. Sebbene sia il più vecchio, il protocollo Internet versione 4 è quello maggiormente utilizzato.

Indirizzo singolo - Aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola, ad esempio *192.168.0.10*.

Intervallo di indirizzi - Immettere il primo e l'ultimo indirizzo IP per specificare l'intervallo IP (di più computer) per cui deve essere applicata la regola, ad esempio da *192.168.0.1* a *192.168.0.99*.

Subnet - Subnet (gruppo di computer) definita da un indirizzo IP e da una maschera.

Ad esempio, *255.255.255.0* è la maschera di rete per il prefisso *192.168.1.0/24*, che indica l'intervallo di indirizzi compreso tra *192.168.1.1* e *192.168.1.254*.

4.2.3.3.2 Aggiungi indirizzo IPv6

Ciò consente di aggiungere un indirizzo/una subnet IPv6 di un punto remoto a cui si applica la regola. Si tratta della versione più recente del protocollo Internet e sostituirà la versione precedente 4.

Indirizzo singolo - Aggiunge l'indirizzo IP di un singolo computer a cui deve essere applicata la regola, ad esempio *2001:718:1c01:16:214:22ff:fec9:ca5*.

Subnet - Subnet (gruppo di computer) definita da un indirizzo IP e da una maschera, ad esempio *2002:c0a8:6301:1::1/64*).

4.2.3.4 Verifica protocollo SSL

ESET NOD32 Antivirus consente di verificare i protocolli incapsulati nel protocollo SSL. È possibile utilizzare varie modalità di scansione per le comunicazioni protette mediante il protocollo SSL utilizzando certificati attendibili, certificati sconosciuti o certificati che sono esclusi dalla verifica delle comunicazioni protette mediante il protocollo SSL.

Effettua sempre la scansione del protocollo SSL - Selezionare questa opzione per verificare tutte le comunicazioni protette mediante il protocollo SSL ad eccezione delle comunicazioni protette mediante i certificati esclusi dalla verifica. Se viene stabilita una nuova comunicazione usando un certificato firmato sconosciuto, all'utente non verrà inviata alcuna notifica e la comunicazione verrà filtrata in modo automatico. Quando si accede a un server con un certificato non attendibile contrassegnato come attendibile (aggiunto quindi all'elenco dei certificati attendibili), la comunicazione con il server è consentita e il contenuto del canale di comunicazione viene filtrato.

Chiedi conferma sui siti non visitati (possono essere impostate esclusioni) - Se si accede a un nuovo sito protetto SSL (con un certificato sconosciuto), verrà visualizzata una finestra di dialogo in cui è possibile scegliere l'azione da eseguire. Questa modalità consente di creare un elenco di certificati SSL che verranno esclusi dal controllo.

Non controllare il protocollo SSL - Se viene selezionata questa opzione, il programma non eseguirà la scansione delle comunicazioni su SSL.

Applica le eccezioni create in base ai certificati - Consente di attivare l'utilizzo delle esclusioni specificate nei certificati attendibili ed esclusi per la scansione della comunicazione SSL. Questa opzione è disponibile se si seleziona **Effettua sempre la scansione del protocollo SSL**.

Blocca le comunicazioni crittografate che utilizzano il protocollo obsoleto SSL v2 - La comunicazione che utilizza la versione precedente del protocollo SSL verrà automaticamente bloccata.

4.2.3.4.1 Certificati

Affinché le comunicazioni SSL funzionino in modo adeguato nei browser/client di posta, è fondamentale che il certificato radice per ESET sia aggiunto all'elenco dei certificati radice noti (autori). È necessario attivare **Aggiungi il certificato radice ai browser conosciuti**. Selezionare questa opzione per aggiungere automaticamente il certificato radice di ESET ai browser conosciuti (ad esempio, Opera e Firefox). Per i browser che utilizzano l'archivio di certificazioni di sistema, il certificato viene aggiunto automaticamente (ad esempio, Internet Explorer). Per applicare il certificato a browser non supportati, fare clic su **Visualizza certificato** > **Dettagli** > **Copia su file...**, quindi importarlo manualmente nel browser.

In alcuni casi non è possibile verificare la validità del certificato mediante l'archivio Autorità di certificazione radice attendibili (ad esempio VeriSign). Ciò significa che il certificato è auto-firmato da qualcuno (ad esempio, l'amministratore di un server Web o una piccola azienda) e considerare questo certificato come attendibile non rappresenta sempre un rischio per la sicurezza. La maggior parte delle principali aziende (ad esempio, le banche) utilizza un certificato firmato da TRCA. Dopo aver selezionato **Chiedi conferma della validità dei certificati** (impostazione predefinita), all'utente verrà richiesto di selezionare un'azione da eseguire in caso di comunicazione crittografata. Verrà visualizzata una finestra di dialogo in cui l'utente potrà scegliere se contrassegnare il certificato come attendibile o escluso. Nel caso in cui il certificato non sia presente nell'elenco TRCA, la finestra sarà rossa. In caso contrario, sarà di colore verde.

È possibile selezionare **Blocca la comunicazione che utilizza il certificato** per terminare sempre una connessione crittografata al sito che utilizza il certificato non verificato.

Se il certificato non è valido oppure è danneggiato, significa che è scaduto o che l'auto-firma era errata. In questo caso, è consigliabile bloccare la comunicazione che utilizza il certificato.

4.2.3.4.1.1 Certificati attendibili

In aggiunta all'Archivio Autorità di certificazione radice attendibili integrato dove ESET NOD32 Antivirus archivia i certificati attendibili, è possibile creare un elenco personalizzato di certificati attendibili che possono essere visualizzati in **Configurazione avanzata** (F5) > **Web ed e-mail** > **Filtro protocolli** > **SSL** > **Certificati** > **Certificati attendibili**. ESET NOD32 Antivirus verificherà il contenuto delle comunicazioni crittografate che utilizzano i certificati presenti nell'elenco.

Per eliminare dall'elenco le voci selezionate, fare clic su **Rimuovi**. Fare clic su **Mostra** (oppure fare doppio clic sul certificato) per visualizzare le informazioni sul certificato selezionato.

4.2.3.4.1.2 Certificati esclusi

La sezione Certificati esclusi contiene i certificati ritenuti sicuri. Il contenuto delle comunicazioni crittografate che utilizzano i certificati nell'elenco non verrà verificato alla ricerca di minacce. È consigliabile escludere solo i certificati Web che sono garantiti come sicuri e i casi in cui la comunicazione che utilizza tali certificati non richiede una verifica. Per eliminare le voci selezionate dall'elenco, fare clic su **Rimuovi**. Fare clic su **Mostra** (oppure fare doppio clic sul certificato) per visualizzare le informazioni sul certificato selezionato.

4.2.3.4.1.3 Comunicazioni SSL crittografate

Se il computer è configurato per la scansione del protocollo SSL, potrebbe essere visualizzata una finestra di dialogo mediante la quale viene chiesto di scegliere un'azione da eseguire quando si tenta di stabilire una connessione crittografata (usando un certificato sconosciuto). La finestra di dialogo contiene le seguenti informazioni: nome dell'applicazione che ha avviato la comunicazione e del certificato utilizzato.

Se non si trova nell'Archivio Autorità di certificazione radice attendibili, il certificato è considerato non attendibile.

Per i certificati sono disponibili le azioni seguenti:

Sì - Il certificato verrà temporaneamente contrassegnato come attendibile - per la durata della sessione corrente, la finestra di avviso non verrà visualizzata al successivo tentativo di utilizzo del certificato.

Sì, sempre - Contrassegna il certificato come attendibile e lo aggiunge all'elenco dei certificati attendibili - per i certificati attendibili non verrà visualizzata alcuna finestra di avviso.

No - Contrassegna il certificato come non attendibile per la sessione corrente. La finestra di avviso verrà visualizzata al successivo tentativo di utilizzo del certificato.

Escludi - Aggiunge il certificato all'elenco dei certificati esclusi. I dati trasferiti sul canale crittografato fornito non verranno controllati.

4.2.4 Protezione Anti-Phishing

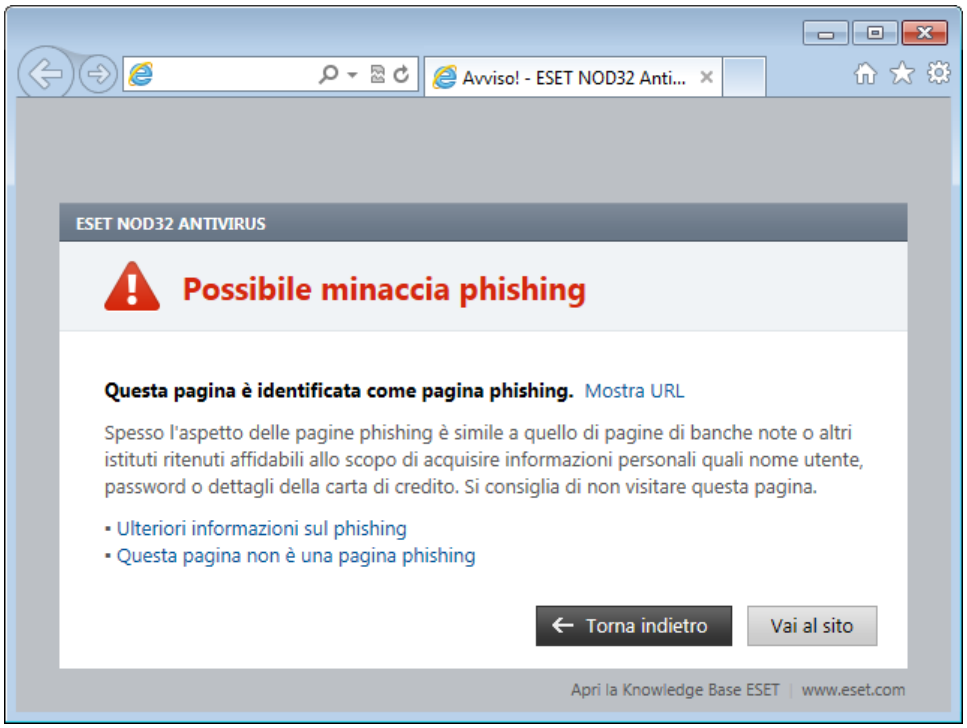
Il termine phishing definisce un'attività illegale che si avvale dell'ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni riservate). Il phishing viene spesso utilizzato per ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via. Per ulteriori informazioni su questa attività, consultare il glossario. ESET NOD32 Antivirus fornisce protezione antiphishing, ovvero una funzione che permette di bloccare pagine Web note per la distribuzione di questo tipo di contenuto.

Si consiglia vivamente di attivare la funzione Anti-Phishing in ESET NOD32 Antivirus. È possibile accedere a questa opzione da **Configurazione avanzata** (F5) > **Web ed e-mail** > **Protezione Anti-Phishing**.

Per una versione aggiornata e più dettagliata di questa pagina della Guida, consultare anche il relativo articolo della Knowledge Base.

Accesso ad un sito Web phishing

Accedendo ad un sito Web phishing, nel browser Web comparirà la seguente finestra di dialogo. Facendo clic su **Vai al sito** (scelta non consigliata), sarà possibile accedere al sito Web senza visualizzare un messaggio di avviso.



NOTA: per impostazione predefinita, i potenziali siti Web phishing che sono stati inseriti nella whitelist scadranno dopo alcune ore. Per consentire un sito Web in modo permanente, è possibile utilizzare lo strumento Gestione indirizzi URL. Da **Configurazione avanzata** (F5), fare clic su **Web ed e-mail** > **Protezione accesso Web** > **Gestione indirizzi URL** e, dal menu a discesa **Gestione indirizzi URL**, selezionare **Elenco di indirizzi consentiti** e aggiungere il sito Web all'elenco.

Segnalazione di un sito phishing

Il collegamento Segnala un sito phishing consente di segnalare un sito Web phishing/dannoso a ESET per l'analisi.

NOTA: prima di inviare un sito Web a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:
- il sito Web non viene rilevato,
- il sito Web viene erroneamente rilevato come una minaccia. In questo caso, consultare il collegamento Rimuovi sito phishing.

In alternativa, è possibile inviare il sito Web tramite e-mail. Inviare l'e-mail a campioni@eset.com. Ricordare di utilizzare una descrizione nel campo dell'oggetto e di fornire il maggior numero possibile di informazioni sul sito Web, ad esempio l'indirizzo del sito Web dal quale è stato scaricato, come si è venuti a conoscenza del sito, ecc.).

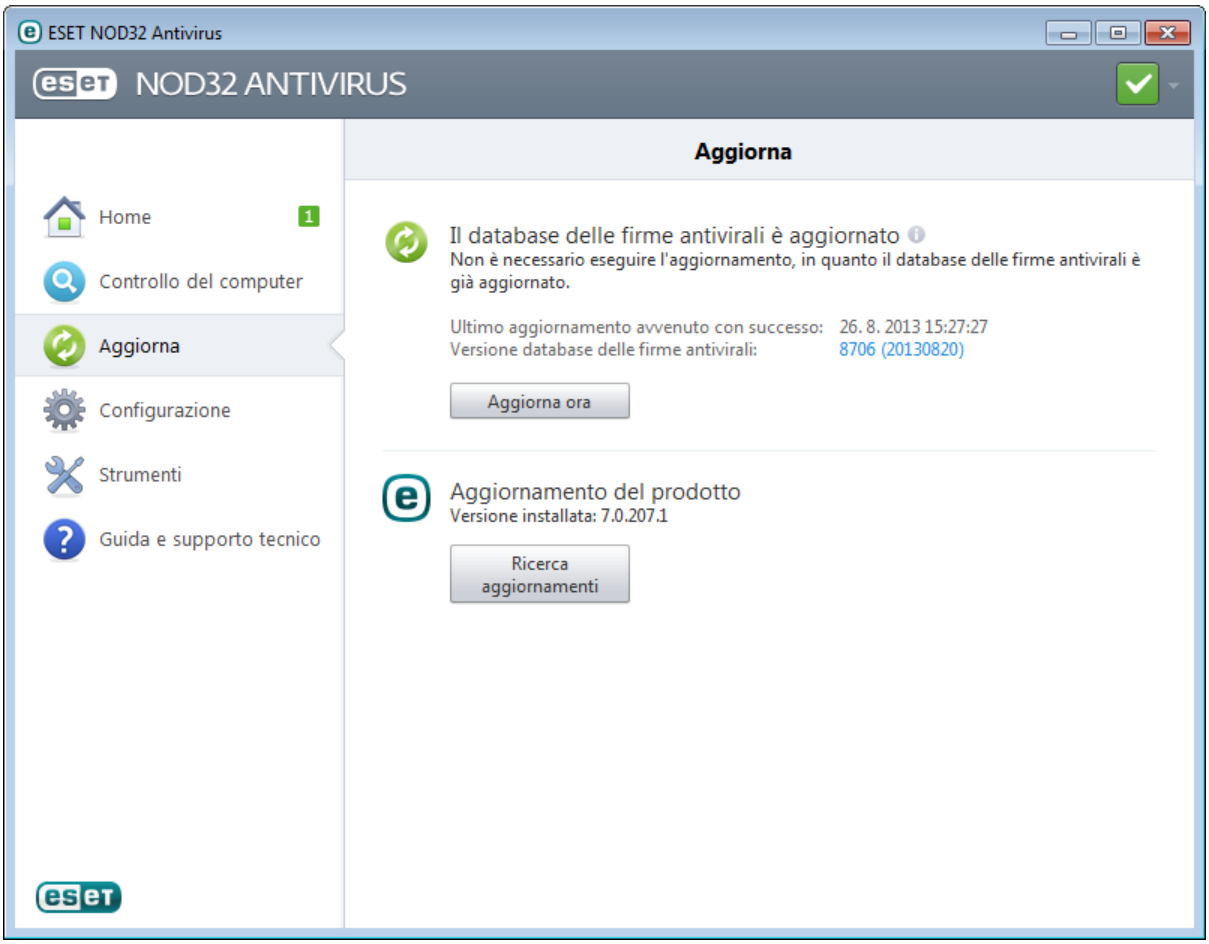
4.3 Aggiornamento del programma

L'aggiornamento periodico di ESET NOD32 Antivirus rappresenta il metodo migliore per garantire il livello massimo di protezione del computer. Il modulo di aggiornamento garantisce in due modi che il programma sia sempre aggiornato: attraverso l'aggiornamento rispettivamente del database delle firme antivirali e dei componenti del sistema.

Facendo clic su **Aggiorna** nella finestra principale del programma, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento eseguito correttamente e valutare se sia necessario un aggiornamento. Nella finestra principale sono inoltre contenute informazioni sulla versione del database delle firme antivirali. Questo indicatore numerico rappresenta un collegamento attivo al sito Web di ESET, in cui vengono riportate tutte le firme aggiunte nel corso dell'aggiornamento in questione.

Oltre agli aggiornamenti automatici, è possibile fare clic su **Aggiorna adesso** per avviare un aggiornamento manualmente. L'aggiornamento del database delle firme antivirali e dei componenti del programma costituisce un aspetto importante per garantire una protezione completa contro codici dannosi. È opportuno prestare particolare attenzione alla relativa configurazione e al funzionamento. Se durante l'installazione non si inseriscono informazioni sulla Licenza (Nome utente e Password), è possibile inserirle durante l'aggiornamento per accedere ai server di aggiornamento ESET.

NOTA: il Nome utente e la Password vengono forniti da ESET dopo l'acquisto di ESET NOD32 Antivirus.



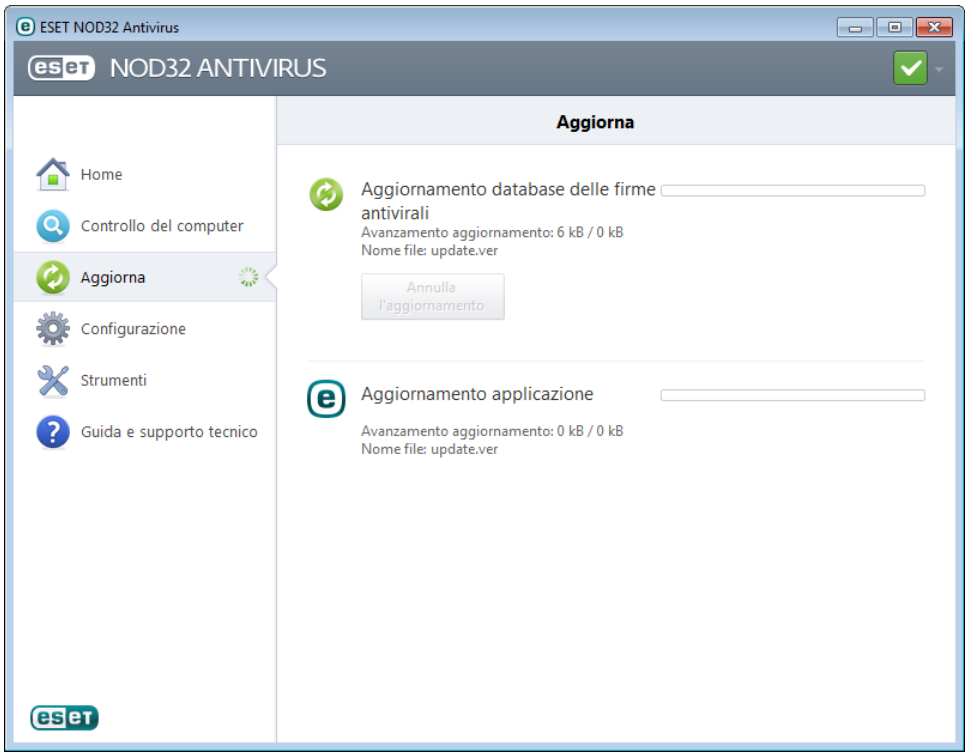
Ultimo aggiornamento riuscito - Data dell'ultimo aggiornamento. Se non viene visualizzata una data recente, il database delle firme antivirali potrebbe non essere aggiornato.

Versione del database delle firme antivirali - Numero del database delle firme antivirali, che rappresenta anche un collegamento attivo al sito Web ESET. Selezionare per visualizzare un elenco di tutte le firme aggiunte in un aggiornamento specifico.

Fare clic su **Ricerca aggiornamenti** per verificare la disponibilità della versione di ESET NOD32 Antivirus più recente.

Processo di aggiornamento

Dopo aver selezionato **Aggiorna adesso**, verrà avviato il processo di download. Verranno visualizzati una barra di avanzamento del download e il tempo rimanente per il completamento dell'operazione. Per interrompere l'aggiornamento, fare clic su **Annulla l'aggiornamento**.

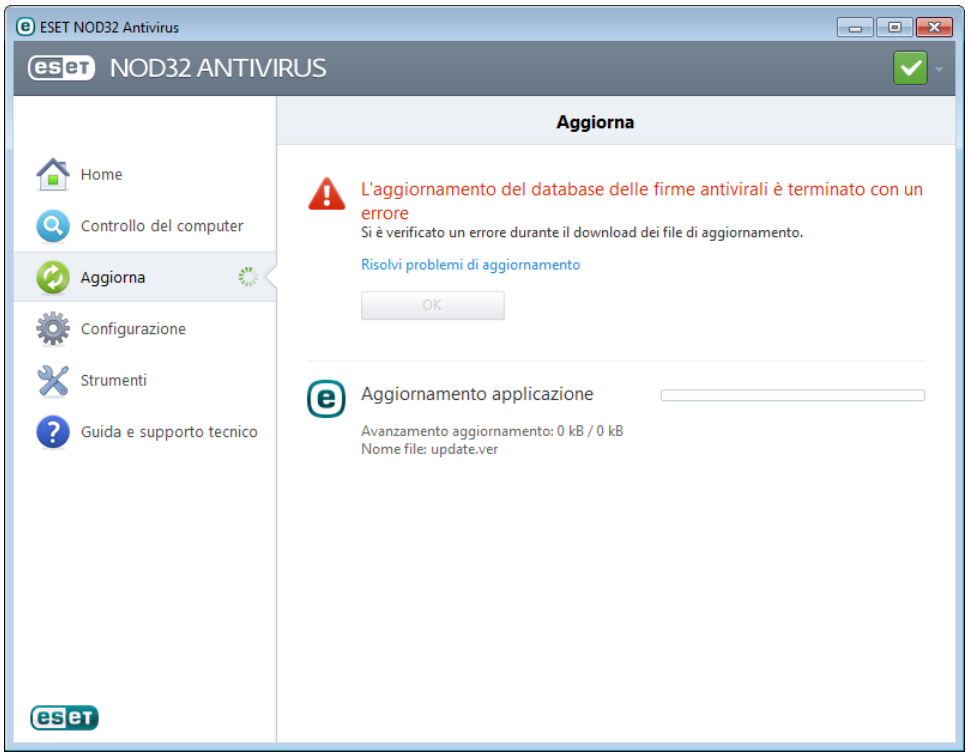


Importante: in circostanze normali, quando gli aggiornamenti sono scaricati correttamente, nella finestra **Aggiorna** viene visualizzato il messaggio **Aggiornamento non necessario. Il database delle firme antivirali è aggiornato**. In caso contrario, il programma è obsoleto ed è maggiormente esposto alle infezioni. Aggiornare il database delle firme antivirali appena possibile. In caso contrario, viene visualizzato uno dei seguenti messaggi:

Il database delle firme antivirali è obsoleto - Questo errore viene visualizzato dopo diversi tentativi non riusciti di aggiornamento del database delle firme antivirali. Si consiglia di controllare le impostazioni di aggiornamento. I motivi più comuni alla base di questo errore consistono in un inserimento errato dei dati di autenticazione o in una configurazione non corretta delle impostazioni di connessione.

Il messaggio di notifica precedente è correlato ai due messaggi **Aggiornamento del database delle firme antivirali terminato con un errore** seguenti, relativi agli aggiornamenti non riusciti:

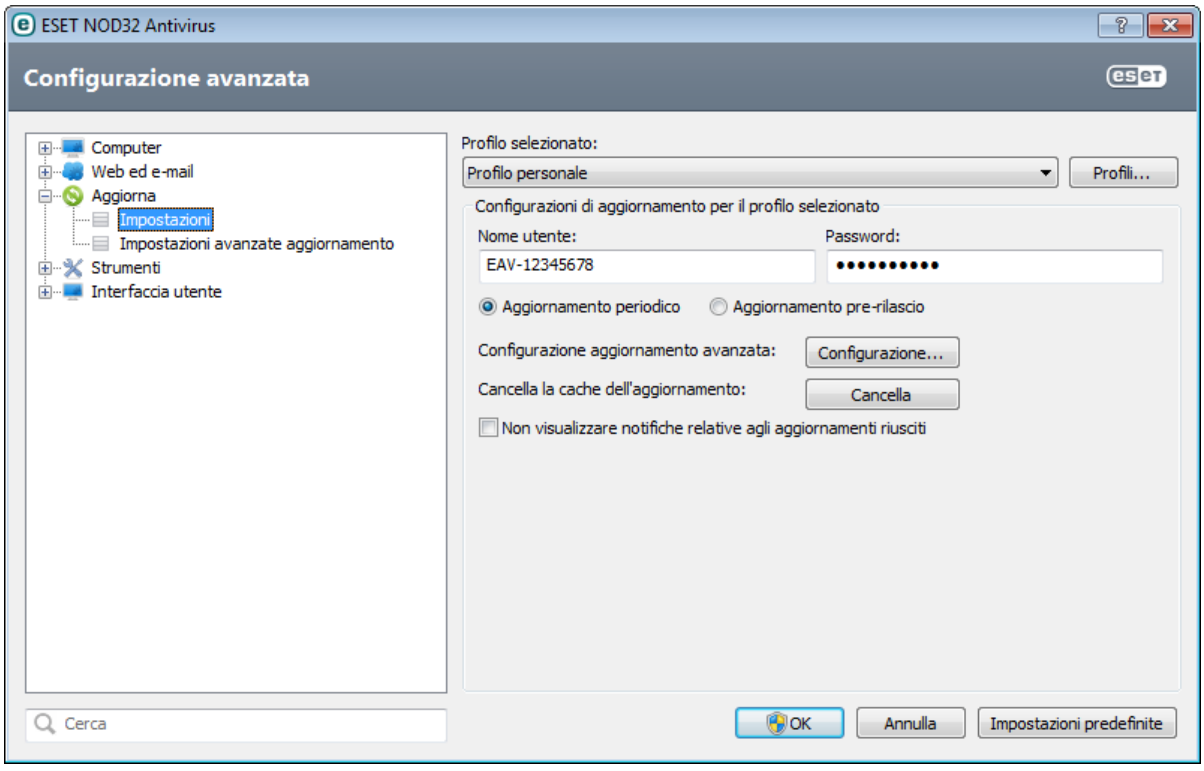
1. **Nome utente e/o Password non validi** - Il Nome utente e la Password non sono stati inseriti correttamente nella configurazione dell'aggiornamento. Si consiglia di verificare i propri dati di autenticazione. Nella finestra Configurazione avanzata (fare clic su **Configurazione** nel menu principale, quindi selezionare **Accedi a configurazione avanzata...** oppure premere F5 sulla tastiera) sono disponibili ulteriori opzioni di aggiornamento. Fare clic su **Aggiorna** > **Impostazioni** nella struttura Configurazione avanzata per inserire un nuovo Nome utente e una nuova Password.
2. **Si è verificato un errore durante il download dei file di aggiornamento** - L'errore potrebbe essere causato da Impostazioni di connessione Internet non corrette. Si consiglia di verificare la connettività Internet (aprendo un qualsiasi sito Web nel browser). Se il sito Web non si apre, è possibile che la connessione Internet non sia presente o che si siano verificati problemi di connettività nel computer in uso. Se la connessione Internet non è attiva, contattare il proprio Provider di servizi Internet (ISP).



4.3.1 Impostazioni di aggiornamento

Le opzioni di configurazione dell'aggiornamento sono disponibili nella struttura **Configurazione avanzata** (tasto F5), facendo clic su **Aggiornamento** > **Impostazioni**. Questa sezione consente di specificare informazioni sull'origine dell'aggiornamento, come ad esempio i server di aggiornamento e i dati per l'autenticazione di tali server. Nella versione home dei prodotti ESET, l'utente non può scegliere il proprio server di aggiornamento. I file di aggiornamento verranno scaricati automaticamente dal server ESET con l'ultimo traffico di rete. Il menu a discesa **Server di aggiornamento** è disponibile solo in ESET Endpoint Antivirus o ESET Endpoint Security.

Affinché gli aggiornamenti vengano scaricati correttamente, occorre inserire correttamente tutte le informazioni di aggiornamento. Se si utilizza un firewall, assicurarsi che sia stata consentita la comunicazione del programma con Internet (la comunicazione HTTP è attiva).



Il profilo di aggiornamento corrente viene visualizzato nel menu a discesa **Profilo selezionato**. Per creare un nuovo

profilo, fare clic su **Profili...**.

L'autenticazione per i server di aggiornamento si basa sul **Nome utente** e sulla **Password** generati e inviati dopo aver acquistato il programma. Per impostazione predefinita, non è richiesta alcuna verifica e i campi **Nome utente** e **Password** sono lasciati vuoti.

Gli aggiornamenti pre-rilascio (opzione **Aggiornamento pre-rilascio**) sono aggiornamenti sottoposti ad approfondite verifiche interne che saranno presto disponibili per tutti. Gli aggiornamenti pre-rilascio consentono di accedere ai metodi di rilevamento e correzioni più recenti. È tuttavia probabile che tali aggiornamenti non siano sempre sufficientemente stabili e NON devono pertanto essere utilizzati su server di produzione e workstation dove è richiesta massima disponibilità e stabilità. L'elenco dei moduli correnti è disponibile in **Guida e supporto tecnico** > **Informazioni su ESET NOD32 Antivirus**. È consigliabile lasciare attivata l'opzione **Aggiornamento periodico** selezionata per impostazione predefinita.

Fare clic su **Configurazione...** accanto a **Impostazione aggiornamento avanzata** per visualizzare una finestra contenente le opzioni di aggiornamento avanzate.

In caso di problemi di aggiornamento, fare clic su **Cancella** per eliminare i file di aggiornamento temporanei.

Non visualizzare la notifica dopo il completamento dell'aggiornamento - Disattiva la notifica sulla barra delle applicazioni nell'angolo in basso a destra della schermata. È utile selezionare questa opzione se è in esecuzione un'applicazione a schermo intero o un videogioco. Tenere presente che se è attiva la Modalità giocatore, tutte le notifiche saranno disattivate.

4.3.1.1 Aggiorna profili

Per varie configurazioni e attività di aggiornamento è possibile creare profili di aggiornamento. La creazione dei profili di aggiornamento è particolarmente utile per gli utenti mobili che necessitano di un profilo alternativo per le proprietà di connessione a Internet, soggette a periodici cambiamenti.

Nel menu a discesa **Profilo selezionato** è possibile visualizzare il profilo correntemente selezionato, configurato per impostazione predefinita come **Profilo personale**. Per creare un nuovo profilo, fare clic su **Profili...**, quindi su **Aggiungi...** e inserire il **Nome profilo**. Quando si crea un nuovo profilo, è possibile copiare le impostazioni da uno esistente selezionandolo dal menu a discesa **Copia impostazioni dal profilo**.

Nella finestra di configurazione del profilo è possibile specificare il server di aggiornamento da un elenco di server disponibili oppure aggiungere un nuovo server. L'elenco dei server di aggiornamento esistenti è disponibile nel menu a discesa **Server di aggiornamento**. Per aggiungere un nuovo server di aggiornamento, fare clic su **Modifica** nella sezione **Impostazioni di aggiornamento per il profilo selezionato**, quindi su **Aggiungi**.

4.3.1.2 Impostazione aggiornamento avanzata

Per visualizzare la Configurazione aggiornamento avanzata, fare clic su **Configurazione...**. Le opzioni relative alla configurazione aggiornamento avanzata includono la configurazione della **Modalità di aggiornamento**, del **Proxy HTTP** e della **LAN**.

4.3.1.2.1 Modalità di aggiornamento

La scheda **Modalità di aggiornamento** contiene opzioni correlate all'aggiornamento dei componenti di programma. Il programma consente di preimpostare le azioni da eseguire quando è disponibile un nuovo aggiornamento dei componenti di programma.

Gli aggiornamenti dei componenti di programma (PCU) includono nuove funzioni oppure modifiche alle funzioni delle versioni precedenti. I PCU possono essere eseguiti automaticamente senza alcun intervento da parte dell'utente oppure è possibile scegliere di ricevere una notifica a ogni esecuzione. Dopo che è stato installato l'aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer. Nella sezione **Aggiornamento componenti programma** sono disponibili tre opzioni:

- **Non aggiornare mai i componenti di programma** - L'aggiornamento dei componenti di programma non viene eseguito. Questa opzione è adatta alle installazioni su server, poiché di norma i server possono essere riavviati solo durante la manutenzione.
- **Aggiorna sempre i componenti di programma** - L'aggiornamento dei componenti di programma verrà scaricato e installato automaticamente. Ricordare che potrebbe essere necessario riavviare il computer.
- **Chiedi prima di scaricare i componenti di programma** - Opzione predefinita. All'utente verrà chiesto di confermare o rifiutare gli aggiornamenti dei componenti di programma, quando disponibili.

Dopo aver eseguito un aggiornamento dei componenti di programma, potrebbe essere necessario riavviare il computer in modo da garantire il corretto funzionamento di tutti i moduli. La sezione **Riavvia dopo l'aggiornamento dei componenti di programma** consente di selezionare una delle opzioni seguenti:

- **Non riavviare mai il computer** - Non sarà richiesto di riavviare il computer, anche se è necessario. Questa opzione non è consigliata poiché il computer potrebbe non funzionare correttamente fino al riavvio successivo.
- **Proponi il riavvio del computer se necessario** - Opzione predefinita. Dopo l'aggiornamento dei componenti di programma verrà visualizzata una finestra di dialogo con la richiesta di riavviare il computer.
- **Se necessario, riavvia il computer senza notifica** - Dopo l'aggiornamento dei componenti di programma, il computer verrà riavviato (se necessario).

NOTA: la scelta dell'opzione più adatta dipende dalla workstation sulla quale saranno applicate le impostazioni. Si tenga presente che esistono delle differenze tra le workstation e i server. Ad esempio, il riavvio automatico del server dopo l'aggiornamento di un programma potrebbe causare gravi danni al sistema.

Selezionando l'opzione **Chiedi prima di scaricare l'aggiornamento**, verrà visualizzata una notifica ogni volta che sarà disponibile un nuovo aggiornamento.

Se la dimensione del file di aggiornamento supera il valore indicato nel campo **Chiedi se un file di aggiornamento è maggiore di**, verrà visualizzata una notifica.

L'opzione **Controlla periodicamente la disponibilità di una versione del prodotto più recente** attiverà l'attività pianificata **Controlla periodicamente la disponibilità di una versione del prodotto più recente** (vedere Pianificazione attività).

4.3.1.2.2 Server proxy

Per accedere alle opzioni di configurazione del server proxy per uno specifico profilo di aggiornamento, fare clic su **Aggiorna** nella struttura Configurazione avanzata (F5), quindi su **Configurazione...** a destra di **Configurazione aggiornamento avanzata**. Fare clic sulla scheda **Proxy HTTP** e selezionare una delle tre opzioni seguenti:

- **Utilizza impostazioni server proxy globali**
- **Non utilizzare server proxy**
- **Connessione tramite server proxy**

Se si seleziona l'opzione **Utilizza impostazioni server proxy globali**, verranno utilizzate le opzioni di configurazione del server proxy già specificate all'interno della sottostruttura **Strumenti** > **Server proxy** della struttura Configurazione avanzata.

Selezionare **Non utilizzare server proxy** per specificare che non verrà utilizzato alcun server proxy per l'aggiornamento di ESET NOD32 Antivirus.

Selezionare l'opzione **Connessione tramite server proxy** nei seguenti casi:

- È necessario utilizzare un server proxy per aggiornare ESET NOD32 Antivirus e tale server proxy è differente da quello specificato nelle impostazioni globali (**Strumenti** > **Server proxy**). In questo caso, sarà necessario fornire alcune informazioni aggiuntive: Indirizzo del **Server proxy**, **Porta** di comunicazione e **Nome utente** e **Password** del server proxy, se richiesti.
- Le impostazioni del server proxy non sono state impostate a livello globale. ESET NOD32 Antivirus si connetterà tuttavia a un server proxy per verificare la disponibilità di aggiornamenti.
- Il computer è connesso a Internet tramite un server proxy. Le impostazioni vengono estrapolate da Internet Explorer durante l'installazione del programma, ma se successivamente vengono modificate, ad esempio se si cambia il provider di servizi Internet (ISP), verificare che le impostazioni del proxy HTTP elencate in questa finestra siano corrette. In caso contrario, il programma non sarà in grado di connettersi ai server di aggiornamento.

L'impostazione predefinita per il server proxy è **Utilizza impostazioni server proxy globali**.

NOTA: i dati di autenticazione, come ad esempio il **Nome utente** e la **Password**, sono necessari per accedere al server proxy. Compilare questi campi solo se sono richiesti un nome utente e una password. Tenere presente che questi campi, in cui non è necessario inserire il Nome utente e la Password per ESET NOD32 Antivirus, devono essere completati solo se è richiesta una password di accesso a Internet mediante un server proxy.

4.3.1.2.3 Connessione alla LAN

Durante l'aggiornamento da un server locale con un sistema operativo basato su NT, per impostazione predefinita è richiesta l'autenticazione per ciascuna connessione di rete.

Per configurare tale account, fare clic sulla scheda **LAN**. Nella sezione **Connetti a LAN come** sono disponibili le opzioni **Account di sistema (predefinito)**, **Utente attuale** e **Utente specificato**.

Selezionare l'opzione **Account di sistema (predefinito)** per utilizzare l'account di sistema per l'autenticazione. In genere non viene eseguito alcun processo di autenticazione se nella sezione principale di impostazione dell'aggiornamento non sono specificati dati di autenticazione.

Per essere certi che il programma esegua l'autenticazione utilizzando l'account di un utente che ha eseguito correntemente l'accesso, selezionare **Utente attuale**. Lo svantaggio di questa opzione consiste nel fatto che il programma non è in grado di connettersi al server di aggiornamento se nessun utente ha eseguito correntemente l'accesso.

Selezionare **Utente specificato** se si desidera che il programma utilizzi un account utente specifico per l'autenticazione. Utilizzare questo metodo quando la connessione con l'account di sistema predefinito non riesce. Tenere presente che l'account dell'utente specificato deve disporre dell'accesso alla directory dei file di aggiornamento sul server locale. In caso contrario, il programma non sarà in grado di stabilire una connessione e scaricare gli aggiornamenti.

Avviso: Se si seleziona **Utente attuale** o **Utente specificato**, è possibile che si verifichi un errore quando si modifica l'identità del programma per l'utente desiderato. È consigliabile immettere i dati di autenticazione della LAN nella sezione principale di configurazione dell'aggiornamento. In questa sezione di impostazione dell'aggiornamento, i dati di autenticazione devono essere inseriti come segue: *nome_dominio**utente* (se si tratta di un gruppo di lavoro, immettere *none_gruppodilavoro**nome*) e la password utente. Per l'aggiornamento dalla versione HTTP del server locale, non è richiesta alcuna autenticazione.

Selezionare **Disconnetti dal server dopo l'aggiornamento** se la connessione al server rimane attiva anche dopo il download degli aggiornamenti.

4.3.2 Rollback aggiornamento

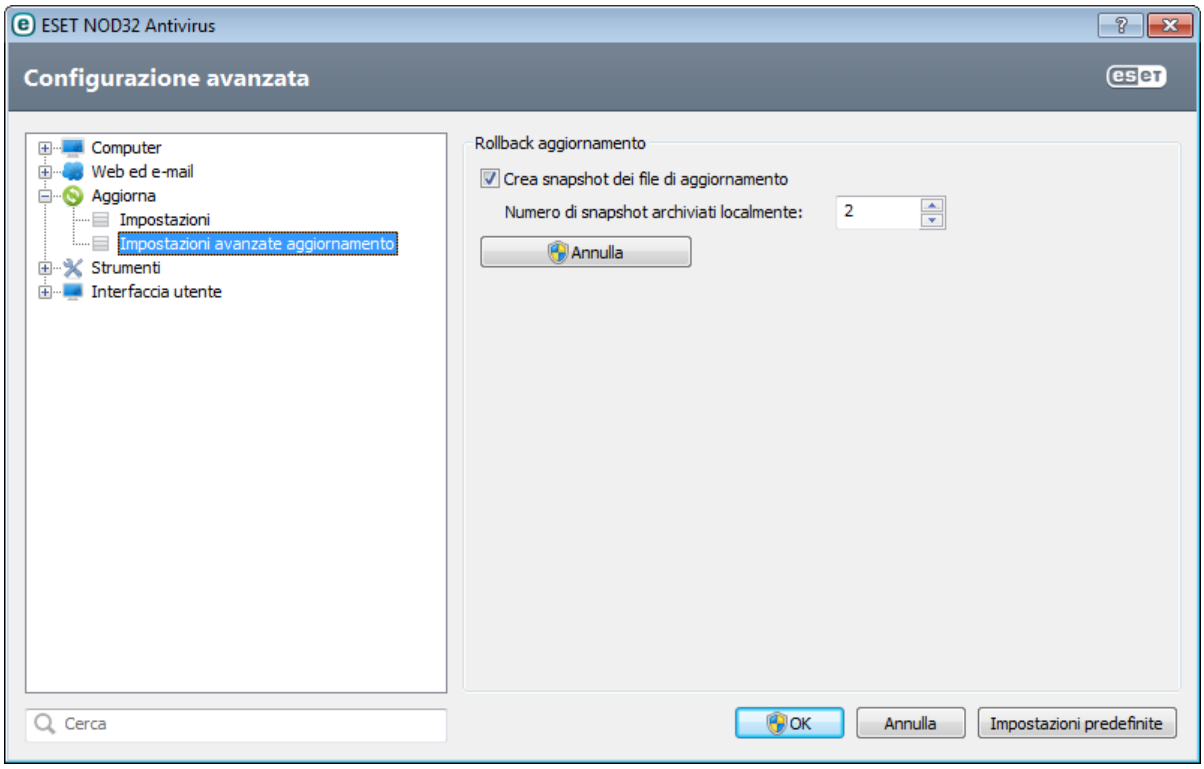
Se si sospetta che un nuovo aggiornamento del database antivirus e/o dei moduli del programma possa essere instabile o danneggiato, è possibile ripristinare la versione precedente e disattivare gli aggiornamenti per un determinato periodo di tempo. In alternativa, è possibile attivare gli aggiornamenti precedentemente disattivati in caso di rimando indefinito da parte dell'utente.

ESET NOD32 Antivirus registra gli snapshot del database delle firme antivirali e dei moduli del programma da utilizzare con la funzione *annullamento*. Per creare snapshot del database antivirus, lasciare selezionata la casella di controllo **Crea snapshot dei file di aggiornamento**. Il campo **Numero di snapshot memorizzati localmente** definisce il numero di snapshot del database antivirale precedentemente archiviati.

Dopo aver selezionato **Roll back** (**Configurazione avanzata** (F5) > **Aggiornamento** > **Rollback aggiornamento**), è necessario scegliere un intervallo di tempo nel menu a discesa **Sospendi aggiornamenti** che indica il periodo di tempo nel quale gli aggiornamenti del database delle firme antivirali e del modulo del programma verranno sospesi.

Selezionare **Fino a revoca** per rimandare in modo indefinito gli aggiornamenti periodici finché l'utente non avrà ripristinato la funzionalità degli aggiornamenti manualmente. Non è consigliabile selezionare questa opzione in quanto rappresenta un potenziale rischio per la protezione.

Se viene eseguito un rollback, il pulsante **Annulla** si trasforma in **Consenti aggiornamenti**. Non saranno consentiti aggiornamenti per l'intervallo di tempo selezionato nel menu a discesa **Sospendi aggiornamenti**. La versione del database delle firme antivirali viene ripristinata alla versione più vecchia a disposizione e memorizzata come uno snapshot nel file system del computer locale.



Esempio: Si presupponga che la versione più recente del database delle firme antivirali corrisponda al numero 6871. Le versioni 6870 e 6868 sono memorizzate come snapshot del database delle firme antivirali. Si noti che la versione

6869 non è disponibile poiché, ad esempio, il computer è stato spento ed è stato reso disponibile un aggiornamento più recente prima che venisse scaricata la versione 6869. Se il campo **Numero di snapshot memorizzati localmente** è impostato su 2 e si fa clic su **Annulla**, il database delle firme antivirali (compresi i moduli del programma) viene ripristinato al numero di versione 6868. L'operazione potrebbe richiedere alcuni minuti. Verificare se la versione del database delle firme antivirali è stata ripristinata a una versione precedente dalla finestra principale del programma di ESET NOD32 Antivirus nella sezione Aggiornamento.

4.3.3 Come creare attività di aggiornamento

È possibile avviare gli aggiornamenti manualmente selezionando l'opzione **Aggiorna database delle firme antivirali** nella finestra principale visualizzata dopo aver selezionato l'opzione **Aggiorna** dal menu principale.

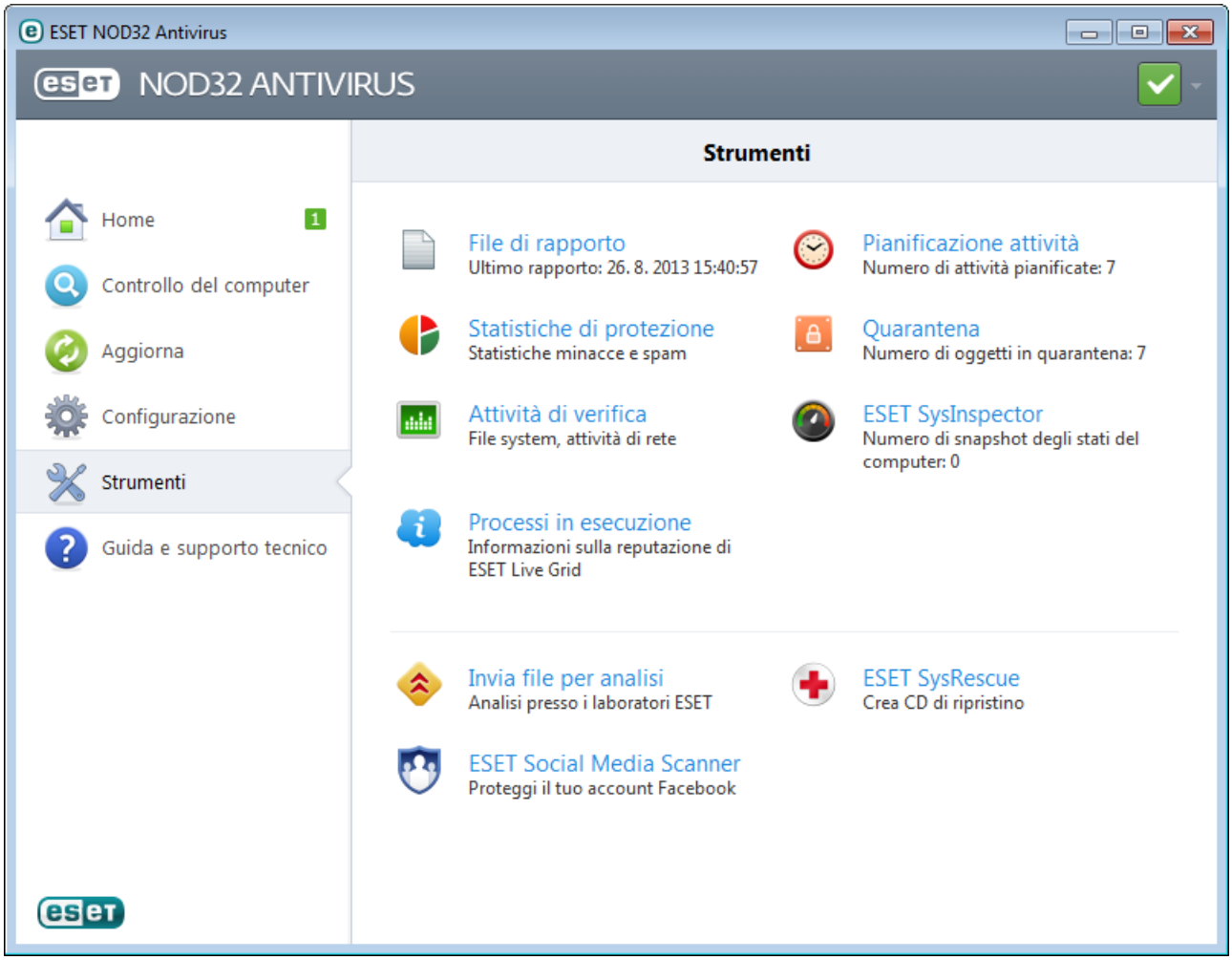
Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Per impostazione predefinita, in ESET NOD32 Antivirus sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna delle attività di aggiornamento in base alle proprie esigenze. Oltre alle attività di aggiornamento predefinite, è possibile creare nuove attività di aggiornamento con una configurazione definita dall'utente. Per ulteriori dettagli sulla creazione e sulla configurazione delle attività di aggiornamento, consultare la sezione Pianificazione attività.

4.4 Strumenti

Il menu **Strumenti** include moduli che consentono di semplificare l'amministrazione del programma, offrendo opzioni aggiuntive per gli utenti esperti.



Questo menu contiene i seguenti strumenti:

- File di rapporto
- Statistiche di protezione
- Attività di verifica
- Processi in esecuzione (se ESET Live Grid è attivato in ESET NOD32 Antivirus)
- Pianificazione attività
- Quarantena
- ESET SysInspector

Invia file per analisi - Consente di inviare un file sospetto al laboratorio antivirus ESET per l'analisi. La finestra di dialogo visualizzata dopo aver selezionato questa opzione è descritta nella sezione Invio di file per l'analisi.

ESET SysRescue - Avvia la procedura di creazione guidata di ESET SysRescue.

Nota: ESET SysRescue in ESET NOD32 Antivirus 6 non è attualmente disponibile per Windows 8. Si consiglia di creare un disco SysRescue di ESET su un'altra versione di Microsoft Windows.

ESET Social Media Scanner - Collegamento ad un'applicazione di social network (ad esempio Facebook) pensato allo scopo di proteggere gli utenti dei social network dalle minacce. Questa applicazione è indipendente da altri prodotti ESET ed è completamente gratuita.

4.4.1 File di rapporto

I file di rapporto contengono informazioni relative a tutti gli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate. La registrazione rappresenta una parte essenziale dell'analisi del sistema, del rilevamento delle minacce e della risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento da parte dell'utente. Le informazioni vengono registrate in base alle impostazioni del livello di dettaglio di rapporto correnti. È possibile visualizzare i messaggi di testo e i rapporti direttamente dall'ambiente di ESET NOD32 Antivirus, nonché dai registri di archivio.

È possibile accedere ai file di rapporto dalla finestra principale del programma facendo clic su **Strumenti** > **File di rapporto**. Selezionare il tipo di rapporto desiderato nel menu a discesa **Rapporto**. Sono disponibili i rapporti seguenti:

- **Minacce rilevate** - Nel rapporto delle minacce sono contenute informazioni dettagliate sulle infiltrazioni rilevate da ESET NOD32 Antivirus. Le informazioni includono l'ora del rilevamento, il nome dell'infiltrazione, la posizione, l'azione eseguita e il nome dell'utente registrato nel momento in cui è stata rilevata l'infiltrazione. Fare doppio clic su una voce qualsiasi del rapporto per visualizzarne il contenuto dettagliato in una finestra separata.
- **Eventi** - Tutte le azioni importanti eseguite da ESET NOD32 Antivirus vengono registrate nel rapporto eventi. Il rapporto eventi contiene informazioni sugli eventi e sugli errori che si sono verificati nel programma. È utile agli amministratori di sistema e agli utenti per risolvere i problemi. Spesso le informazioni visualizzate in questo rapporto consentono di trovare la soluzione a un problema che si verifica nel programma.
- **Controllo computer** - In questa finestra vengono visualizzati i risultati di tutti i controlli manuali o pianificati completati. Ogni riga corrisponde a un singolo controllo del computer. Fare doppio clic su una voce per visualizzare i dettagli del rispettivo controllo.
- **HIPS** - Contiene i record di specifiche regole HIPS che sono stati contrassegnati per la registrazione. Nel protocollo viene mostrata l'applicazione che ha attivato l'operazione, il risultato (ovvero se la regola era consentita o vietata) e il nome della regola creata.
- **Siti Web filtrati** - Questo elenco è utile se si desidera visualizzare un elenco di siti Web che sono stati bloccati dalla Protezione accesso Web. In questi rapporti è possibile visualizzare l'ora, l'indirizzo URL, l'utente e l'applicazione che hanno creato una connessione a un sito Web specifico.
- **Controllo dispositivi** - Contiene record relativi ai supporti rimovibili o ai dispositivi collegati al computer. Nel file di rapporto saranno registrati solo i dispositivi con le rispettive regole di Controllo dispositivi. Se la regola non corrisponde a un dispositivo collegato, non verrà creata alcuna voce di rapporto relativa a tale evento. Qui è possibile visualizzare anche dettagli relativi al tipo di dispositivo, numero di serie, nome del fornitore e

dimensioni del supporto (ove disponibili).

In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti (tasto di scelta rapida Ctrl + C), selezionando la voce desiderata e facendo clic su **Copia**. Per selezionare più voci, usare i tasti CTRL e MAIUSC.

Fare clic con il pulsante destro del mouse su una voce specifica per visualizzare il menu contestuale. Nel menu contestuale sono disponibili le seguenti opzioni:

- **Filtra record dello stesso tipo** - Dopo aver attivato questo filtro, verranno visualizzati solo record dello stesso tipo (diagnostica, avvisi, ecc.).
- **Filtro.../Trova...** - Dopo aver attivato questa opzione, verrà visualizzata la finestra **Filtraggio rapporti** in cui è possibile definire i criteri di filtraggio.
- **Disattiva filtro** - Consente di annullare tutte le impostazioni del filtro (come descritto in precedenza).
- **Copia tutto** - Copia le informazioni su tutti i record nella finestra.
- **Elimina/Elimina tutto** - Elimina i record selezionati o tutti i record visualizzati. Per poter eseguire questa operazione è necessario disporre dei privilegi amministrativi.
- **Esporta** - Consente di esportare le informazioni sui record in formato XML.
- **Scorri registro** - Lasciare attivata questa opzione per scorrere i rapporti meno recenti e osservare i rapporti attivi nella finestra **File di rapporto**.

4.4.1.1 Manutenzione rapporto

La configurazione della registrazione di ESET NOD32 Antivirus è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Accedi a configurazione avanzata...** > **Strumenti** > **File di rapporto**. La sezione relativa ai rapporti viene utilizzata per definire come verranno gestiti. Il programma elimina automaticamente i rapporti meno recenti per liberare spazio sull'unità disco rigido. Per i file di rapporto è possibile specificare le opzioni seguenti:

Livello di dettaglio di registrazione minimo - Specifica il livello di dettaglio minimo degli eventi da registrare.

- **Diagnostica** - Registra tutte le informazioni necessarie per l'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativi** - Messaggi di record informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza.
- **Allarmi** - Consente di registrare errori critici e messaggi di allarme.
- **Errori** - Verranno registrati errori quali *"Errore durante il download del file"* ed errori critici.
- **Critici** - Registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

Le voci del rapporto più vecchie del numero specificato di giorni nel campo **Elimina automaticamente i record più vecchi di X giorni** verranno eliminate automaticamente.

Ottimizza automaticamente file di rapporto - Se questa opzione è selezionata, i file di rapporto vengono automaticamente deframmentati se la percentuale è superiore al valore specificato nel campo **Se il numero di record inutilizzati supera (%)**.

Fare clic su **Ottimizza ora** per avviare la deframmentazione dei file di rapporto. Per migliorare le prestazioni e potenziare la velocità di elaborazione dei rapporti, durante questo processo vengono rimosse le voci vuote. Tale miglioramento può essere rilevato in particolare se i rapporti contengono un numero elevato di elementi.

4.4.2 Pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con configurazione e proprietà predefinite.

È possibile accedere alla Pianificazione attività nella finestra principale del programma di ESET NOD32 Antivirus facendo clic su **Strumenti** > **Pianificazione attività**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, ad esempio data, ora e profilo di controllo predefiniti utilizzati.

La Pianificazione attività consente di pianificare le attività seguenti: aggiornamento del database delle firme antivirali, attività di scansione, controllo dei file di avvio del sistema e manutenzione dei rapporti. È possibile

aggiungere o modificare attività direttamente dalla finestra principale Pianificazione attività, facendo clic su **Aggiungi...** o **Elimina** nella parte inferiore della finestra. Fare clic con il pulsante destro del mouse in qualsiasi punto della finestra Pianificazione attività per eseguire le azioni seguenti: visualizzare informazioni dettagliate, eseguire immediatamente l'attività, aggiungere una nuova attività ed eliminare un'attività esistente. Utilizzare le caselle di controllo accanto a ciascuna voce per attivare o disattivare le attività.

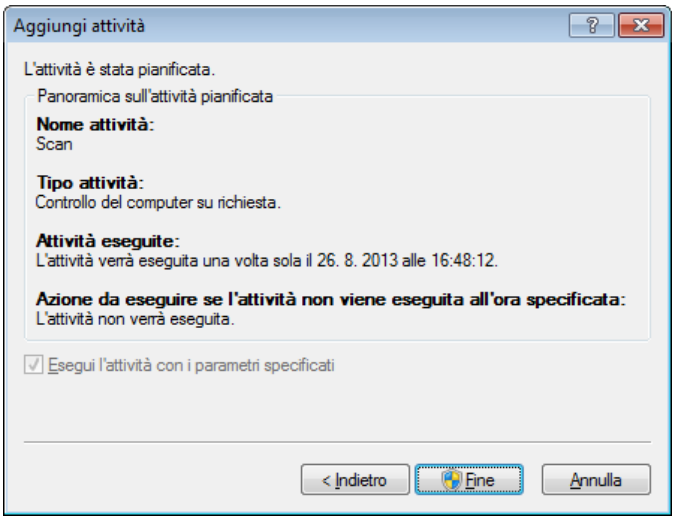
Per impostazione predefinita, in **Pianificazione attività** vengono visualizzate le attività pianificate seguenti:

- **Manutenzione rapporto**
- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo la connessione remota**
- **Aggiornamento automatico dopo l'accesso dell'utente**
- **Controlla periodicamente la disponibilità di una versione del prodotto più recente** (vedere Modalità di aggiornamento)
- **Controllo automatico file di avvio** (dopo l'accesso utente)
- **Controllo automatico file di avvio** (dopo il completamento dell'aggiornamento del database delle firme antivirali)
- **Primo controllo automatico**

Per modificare la configurazione di un'attività pianificata esistente (predefinita o definita dall'utente), fare clic con il pulsante destro del mouse sull'attività e selezionare **Modifica...** oppure selezionare l'attività che si desidera modificare e fare clic su **Modifica...**.

Aggiunta di un nuova attività

1. Fare clic su **Aggiungi...** nella parte inferiore della finestra.
2. Selezionare l'attività desiderata dal menu a discesa.
3. Immettere il nome dell'attività e selezionare l'intervallo di tempo desiderato:
   - **Una volta** - L'attività verrà eseguita solo una volta, alla data e all'ora predefinite.
   - **Ripetutamente** - L'attività verrà eseguita in base all'intervallo specificato (in ore).
   - **Ogni giorno** - L'attività verrà eseguita ogni giorno all'ora specificata.
   - **Ogni settimana** - L'attività verrà eseguita una o più volte alla settimana, nei giorni e nelle ore specificati.
   - **Quando si verifica un evento** - L'attività verrà eseguita quando si verifica un evento specifico.
4. A seconda dell'intervallo di tempo selezionato nel passaggio precedente, verrà visualizzata una delle seguenti finestra di dialogo:
   - **Una volta** - L'attività verrà eseguita alla data e all'ora predefinite.
   - **Ripetutamente** - L'attività verrà eseguita in base all'intervallo di tempo specificato.
   - **Ogni giorno** - L'attività verrà eseguita periodicamente ogni giorno all'ora specificata.
   - **Ogni settimana** - L'attività verrà eseguita nel giorno e nell'ora selezionati.
5. Se l'attività non è stata eseguita all'ora predefinita, è possibile specificare il momento in cui dovrà essere nuovamente eseguita:
   - Attendi il successivo intervallo pianificato
   - Esegui l'attività appena possibile
   - Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera -- ore
6. Nell'ultimo passaggio, è possibile verificare l'attività da pianificare. Fare clic su **Fine** per confermare l'attività.



4.4.3 Statistiche di protezione

Per visualizzare un grafico dei dati statistici relativi ai moduli di protezione ESET NOD32 Antivirus, fare clic su **Strumenti** > **Statistiche di protezione**. Selezionare il modulo di protezione desiderato dal menu a discesa **Statistiche** per visualizzare il grafico e la legenda corrispondenti. Se si passa il mouse su un elemento nella legenda, verranno visualizzati solo i dati di quell'elemento nel grafico.

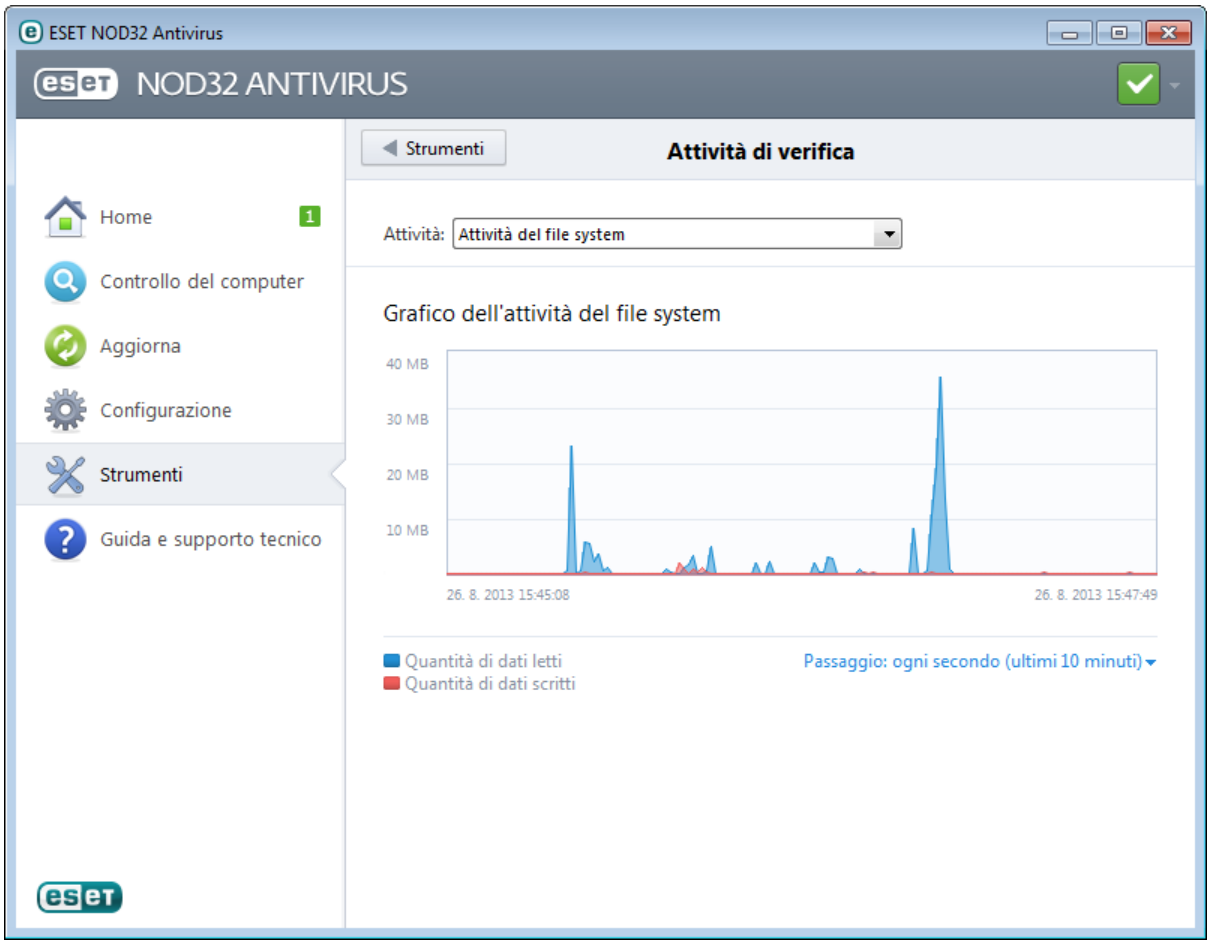
Sono disponibili i seguenti grafici statistici:

- **Protezione antivirus e antispyware** - Consente di visualizzare il numero di oggetti infetti e puliti.
- **Protezione file system** - Consente di visualizzare solo gli oggetti che sono stati scritti o letti sul file system.
- **Protezione client e-mail** - Consente di visualizzare solo gli oggetti inviati o ricevuti dai client e-mail.
- **Protezione accesso Web e Anti-Phishing** - Consente di visualizzare solo gli oggetti scaricati dai browser Web.

Sotto il grafico delle statistiche è visualizzato il numero degli oggetti totali sottoposti a controllo, l'ultimo oggetto sottoposto a controllo e la data e l'ora delle statistiche. Fare clic su **Azzeramento** per cancellare tutte le informazioni statistiche.

4.4.4 Attività di verifica

Per visualizzare l'**Attività di file system** corrente in un grafico, fare clic su **Strumenti** > **Attività di verifica**. Nella parte inferiore del grafico è presente una linea cronologica che registra in tempo reale le attività del file system in base all'intervallo di tempo selezionato. Per modificare l'intervallo di tempo, fare clic su **Passaggio: 1...** collocato nell'angolo in basso a destra della finestra.



Sono disponibili le seguenti opzioni:

- **Passaggio: 1 secondo (ultimi 10 minuti)** - Il grafico si aggiorna ogni secondo e l'intervallo di tempo copre gli ultimi 10 minuti
- **Passaggio: 1 minuto (ultime 24 ore)** - Il grafico si aggiorna ogni minuto e l'intervallo di tempo copre le ultime 24 ore
- **Passaggio: 1 ora (ultimo mese)** - Il grafico si aggiorna ogni ora e l'intervallo di tempo copre l'ultimo mese
- **Passaggio: 1 ora (mese selezionato)** - Il grafico si aggiorna ogni ora e l'intervallo di tempo copre gli ultimi X mesi selezionati

L'asse verticale del **Grafico dell'attività del file system** rappresenta i dati letti (blu) e scritti (rosso). Entrambi i valori sono espressi in KB (kilobyte)/MB/GB. Facendo scorrere il mouse sui dati letti o scritti nella didascalia sottostante il grafico, è possibile visualizzare unicamente i dati relativi a quella specifica attività.

4.4.5 ESET SysInspector

ESET SysInspector è un'applicazione che esamina a fondo il computer, raccoglie informazioni dettagliate sui componenti del sistema, quali i driver e le applicazioni installati, le connessioni di rete o le voci di registro importanti e valuta il livello di rischio di ciascun componente. Tali informazioni possono risultare utili per determinare la causa di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

Nella finestra di dialogo SysInspector sono visualizzate le seguenti informazioni sui rapporti creati:

- **Ora** - Ora di creazione del rapporto.
- **Commento** - Breve commento.
- **Utente** - Nome dell'utente che ha creato il rapporto.
- **Stato** - Stato di creazione del rapporto.

Sono disponibili le azioni seguenti:

- **Confronta** - Consente di mettere a confronto due rapporti esistenti.
- **Crea...** - Consente di creare un nuovo rapporto. Attendere il completamento del rapporto di ESET SysInspector (**Stato**: Creato).
- **Elimina** - Rimuove dall'elenco i rapporti selezionati.

Fare clic con il pulsante destro del mouse su uno o più rapporti selezionati per visualizzare le opzioni seguenti del menu contestuale:

- **Mostra** - Visualizza il rapporto selezionato in ESET SysInspector (funzione uguale all'esecuzione di un doppio clic su un rapporto).
- **Elimina tutto** - Consente di eliminare tutti i rapporti.
- **Esporta...** - Esporta il rapporto su un file *XML* o su un file *XML* compresso.

4.4.6 ESET Live Grid

ESET Live Grid (sviluppato sul sistema avanzato di allarme immediato ESET ThreatSense.Net) utilizza i dati inviati dagli utenti ESET di tutto il mondo e li invia al laboratorio antivirus ESET. Grazie all'invio di campioni e metadati "from the wild" sospetti, ESET Live Grid consente a ESET di soddisfare le esigenze dei clienti e di gestire le minacce più recenti in modo tempestivo. Per ulteriori informazioni su ESET Live Grid, consultare il glossario.

Un utente può controllare la reputazione dei processi in esecuzione e dei file direttamente dall'interfaccia del programma o dal menu contestuale. Ulteriori informazioni sono disponibili su ESET Live Grid. Sono disponibili due opzioni:

1. È possibile scegliere di non attivare ESET Live Grid. Non verranno perse funzionalità del software, che continuerà ad offrire la migliore protezione in assoluto.
2. È possibile configurare ESET Live Grid per l'invio di informazioni anonime sulle nuove minacce e laddove sia presente il nuovo codice dannoso. Il file può essere inviato a ESET per un'analisi dettagliata. Lo studio di queste minacce sarà d'aiuto ad ESET per aggiornare le proprie capacità di rilevamento.

ESET Live Grid raccoglierà informazioni sul computer degli utenti in relazione alle nuove minacce rilevate. Tali informazioni possono includere un campione o una copia del file in cui è contenuta la minaccia, il percorso al file, il nome del file, informazioni su data e ora, il processo in base al quale la minaccia è apparsa sul computer e informazioni sul sistema operativo del computer.

Per impostazione predefinita, ESET NOD32 Antivirus viene configurato per l'invio di file sospetti al laboratorio antivirus ESET per l'analisi dettagliata. Sono sempre esclusi file con determinate estensioni, ad esempio *DOC* o *XLS*. È inoltre possibile aggiungere altre estensioni qualora sussistano specifici file che l'utente o la società dell'utente non desidera inviare.

Nel menu di configurazione ESET Live Grid, sono disponibili varie opzioni di attivazione/disattivazione di ESET Live Grid, uno strumento utile per l'invio di file sospetti e di informazioni statistiche anonime ai laboratori ESET. È accessibile dalla struttura di Configurazione avanzata selezionando **Strumenti** > **ESET Live Grid**.

Partecipa a ESET Live Grid (scelta consigliata) - Consente di attivare/disattivare ESET Live Grid, uno strumento utile per l'invio di file sospetti e di informazioni statistiche anonime ai laboratori ESET.

Non inviare statistiche - Selezionare questa opzione se non si desidera inviare informazioni anonime sul computer raccolte da ESET Live Grid. Queste informazioni sono correlate alle minacce più recenti rilevate e possono comprendere il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione di ESET NOD32 Antivirus, la versione del sistema operativo in uso e le impostazioni di ubicazione. Solitamente, le statistiche vengono inviate ai server ESET una o due volte al giorno.

Non inviare file - I file sospetti che somigliano a infiltrazioni per il loro contenuto o comportamento non vengono inviati a ESET per essere analizzati con la tecnologia ESET Live Grid.

Configurazione avanzata... - Apre una finestra contenente impostazioni aggiuntive per ESET Live Grid.

Se ESET Live Grid è già stato utilizzato in precedenza ed è stato disattivato, potrebbero essere ancora presenti pacchetti di dati da inviare. Anche dopo la disattivazione, tali pacchetti verranno inviati a ESET all'occasione successiva. Successivamente, non verrà più creato alcun pacchetto.

4.4.6.1 File sospetti

La scheda **File** nella configurazione avanzata di ESET Live Grid consente all'utente di configurare le modalità di invio delle minacce ai laboratori antivirus ESET per l'analisi.

Se si rileva un file sospetto, è possibile inviarlo per l'analisi ai ThreatLabs. Se viene individuata un'applicazione dannosa, essa verrà aggiunta al successivo aggiornamento delle firme antivirali.

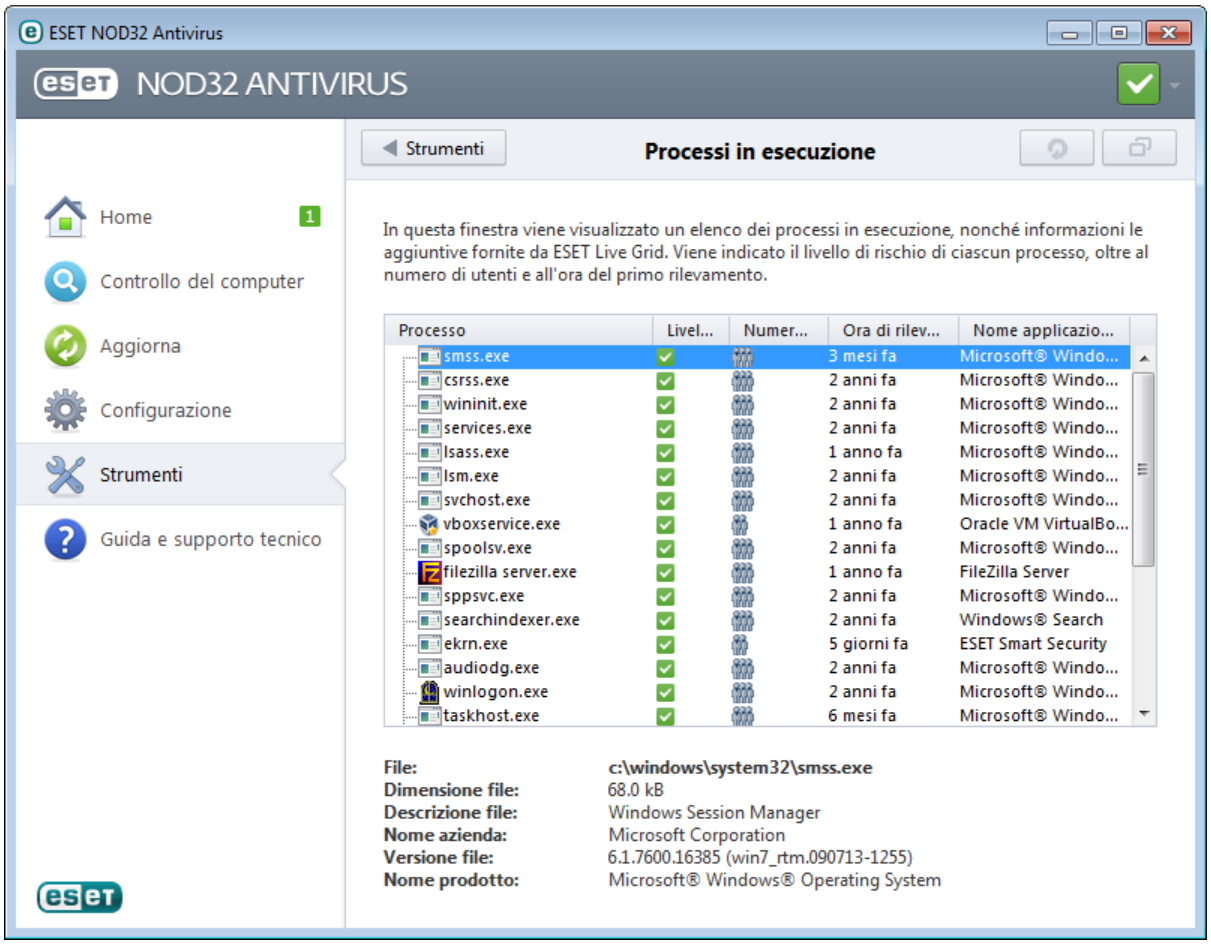
Filtro di esclusione - Il Filtro di esclusione consente di escludere dall'invio determinati file/cartelle. I file elencati non verranno mai inviati ai laboratori ESET per l'analisi, anche se contengono codice sospetto. È ad esempio utile escludere file che potrebbero contenere informazioni riservate, quali documenti o fogli di calcolo. Per impostazione predefinita, vengono esclusi i tipi di file più comuni (con estensione DOC e così via). È possibile aggiungerli alla lista degli elementi esclusi dalla scansione.

Contatto e-mail (facoltativo) - Il contatto e-mail può essere inviato insieme ai file sospetti e potrebbe essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. Tenere presente che non si riceverà alcuna risposta da ESET, a meno che non siano richieste ulteriori informazioni.

Selezionare **Attiva registrazione** per creare un rapporto di eventi sul quale sono registrati gli invii dei file e delle informazioni statistiche. Ciò attiverà la registrazione sul Rapporto eventi durante l'invio di file o statistiche.

4.4.7 Processi in esecuzione

I processi in esecuzione consentono di visualizzare i programmi o processi in esecuzione sul computer e inviare informazioni tempestive e costanti a ESET sulle nuove infiltrazioni. ESET NOD32 Antivirus fornisce informazioni dettagliate sui processi in esecuzione allo scopo di proteggere gli utenti che utilizzano la tecnologia ESET Live Grid.



Processo - Nome immagine del programma o del processo attualmente in esecuzione sul computer. Per visualizzare tutti i processi in esecuzione sul computer è inoltre possibile utilizzare Windows Task Manager. Per aprire il Task Manager, fare clic con il pulsante destro del mouse su un'area vuota sulla barra delle attività, quindi scegliere **Task Manager** oppure premere Ctrl+Maiusc+Esc sulla tastiera.

Livello rischio - Nella maggior parte dei casi, ESET NOD32 Antivirus e la tecnologia ESET Live Grid assegnano livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ogni oggetto e quindi ne valutano le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso).

NOTA: Le applicazioni note contrassegnate come Non a rischio (verde) sono definitivamente pulite (inserite nella whitelist) e saranno escluse dal controllo in modo da aumentare la velocità di esecuzione del controllo del computer su richiesta o della protezione file system in tempo reale sul dispositivo.

Numero di utenti - Numero di utenti che utilizzano una determinata applicazione. Queste informazioni sono raccolte mediante la tecnologia ESET Live Grid.

Ora di rilevamento - Periodo di tempo da quando l'applicazione è stata rilevata dalla tecnologia ESET Live Grid.

NOTA: se un'applicazione è contrassegnata con un livello di rischio Sconosciuto (arancione), non si tratta necessariamente di software dannoso. In genere si tratta di una nuova applicazione. In caso di dubbi sul file, selezionare l'opzione invia file per analisi al laboratorio antivirus ESET. Se il file si rivela essere un'applicazione dannosa, il suo rilevamento verrà aggiunto in uno degli aggiornamenti successivi.

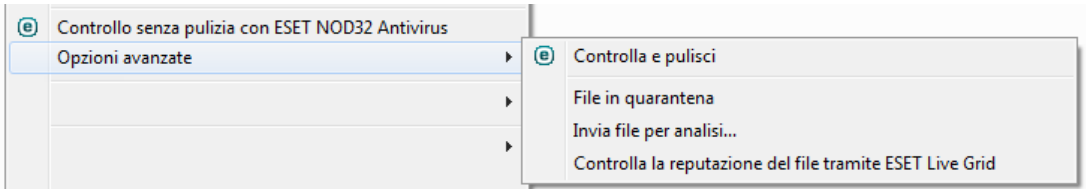
Nome applicazione - Nome specifico di un programma o processo.

Apri una nuova finestra - Le informazioni sui processi in esecuzione verranno visualizzate in una nuova finestra.

Fare clic sulla parte inferiore di una determinata applicazione per visualizzare le seguenti informazioni nella parte inferiore della finestra:

- **File** - Posizione di un'applicazione sul computer.
- **Dimensioni file** - Dimensione del file in B (byte).
- **Descrizione file** - Caratteristiche del file basate sulla relativa descrizione del sistema operativo.
- **Nome società** - Nome del fornitore o del processo applicativo.
- **Versione file** - Informazioni estrapolate dall'autore dell'applicazione.
- **Nome prodotto** - Nome dell'applicazione e/o nome commerciale.

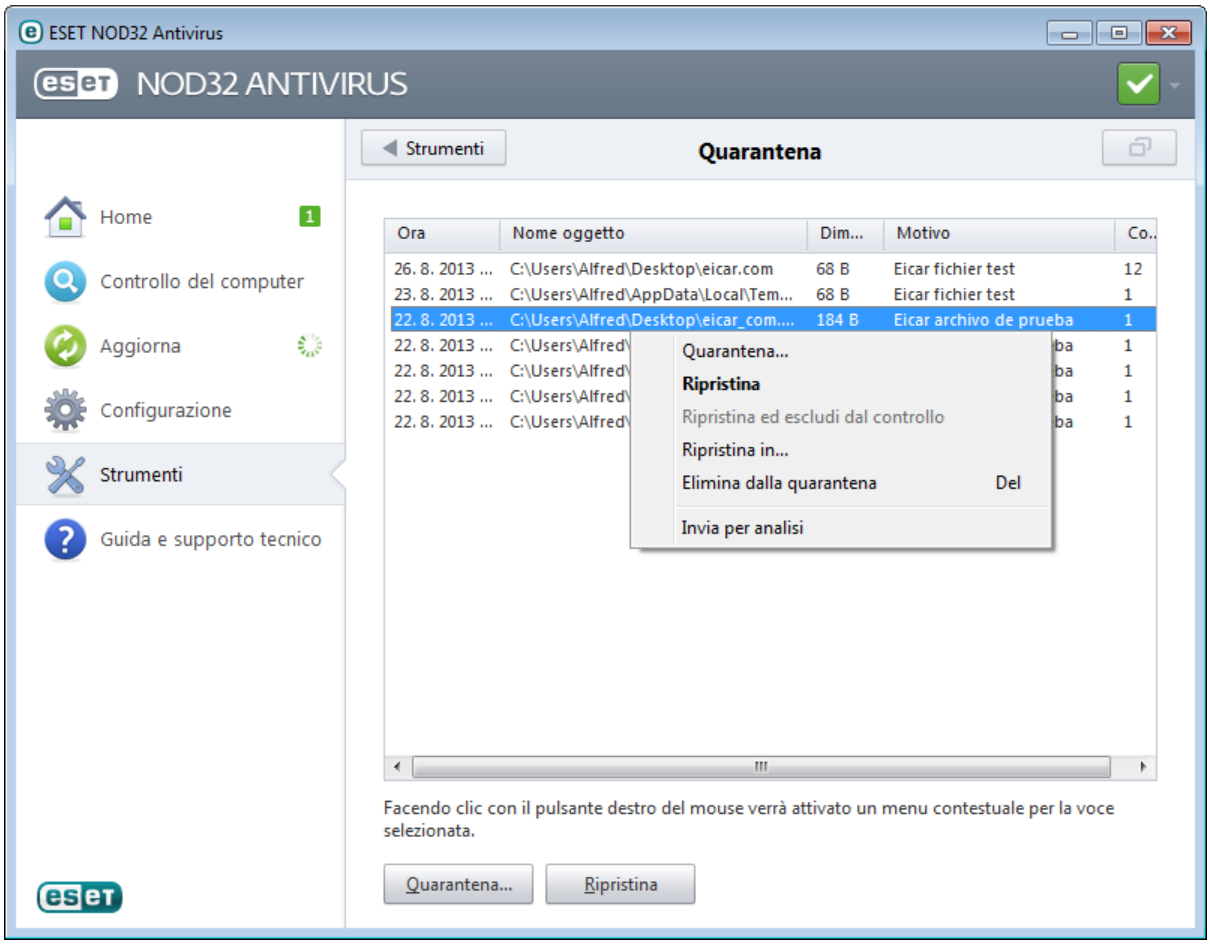
NOTA: La reputazione può essere controllata anche sui file che non agiscono come programmi/processi in esecuzione - contrassegnare i file che si desidera controllare, fare clic con il pulsante destro del mouse su di essi e selezionare **Opzioni avanzate** > **Controlla la reputazione del file tramite ESET Live Grid**.



4.4.8 Quarantena

La funzione principale della quarantena è archiviare i file infetti in modo sicuro. I file devono essere messi in quarantena se non è possibile pulirli, se non è sicuro o consigliabile eliminarli o, infine, se vengono erroneamente rilevati come minacce da ESET NOD32 Antivirus.

È possibile mettere in quarantena qualsiasi tipo di file. È una procedura consigliata nel caso in cui un file si comporti in modo sospetto ma non viene rilevato dallo scanner antivirus. I file messi in quarantena possono essere inviati al laboratorio antivirus ESET per l'analisi.



I file salvati nella cartella della quarantena possono essere visualizzati in una tabella contenente la data e l'ora della quarantena, il percorso originale del file infetto, la dimensione in byte, il motivo (ad esempio, oggetto aggiunto

dall'utente) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni).

Mettere file in quarantena

ESET NOD32 Antivirus mette automaticamente in quarantena i file eliminati (qualora l'utente non abbia provveduto ad annullare questa opzione nella finestra di avviso). Se necessario, è possibile mettere manualmente in quarantena i file sospetti selezionando **Quarantena...**. In tal caso, il file originale non verrà rimosso dalla posizione di origine. Per questa operazione è possibile utilizzare anche il menu contestuale: fare clic con il pulsante destro del mouse sulla finestra **Quarantena** e selezionare l'opzione **Quarantena...**.

Ripristino dalla quarantena

È possibile ripristinare nella posizione di origine i file messi in quarantena. Utilizzare a tale scopo la funzione **Ripristina**, disponibile nel menu contestuale visualizzato facendo clic con il pulsante destro del mouse su un file specifico nella finestra Quarantena. Se un file è contrassegnato come applicazione potenzialmente indesiderata, l'opzione **Ripristina ed escludi dal controllo** è attivata. Per ulteriori informazioni su questo tipo di applicazione, consultare la relativa voce del glossario. Il menu contestuale contiene anche l'opzione **Ripristina in...**, che consente di ripristinare i file in una posizione diversa da quella di origine da cui sono stati eliminati.

NOTA: se il programma ha messo in quarantena per errore un file non dannoso, escludere il file dal controllo dopo averlo ripristinato e inviarlo al Supporto tecnico ESET.

Invio di un file dalla cartella Quarantena

Se un file sospetto che non è stato rilevato dal programma è stato messo in quarantena o se un file è stato segnalato erroneamente come infetto (ad esempio, mediante un'analisi euristica del codice) e quindi messo in quarantena, è necessario inviarlo al laboratorio antivirus ESET. Per inviare un file dalla cartella di quarantena, fare clic con il pulsante destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.

4.4.9 Configurazione del server proxy

Nelle reti LAN di grandi dimensioni, la connessione del computer dell'utente a Internet può essere mediata da un server proxy. In questo caso, occorre definire le impostazioni seguenti. In caso contrario, il programma non sarà in grado di aggiornarsi automaticamente. In ESET NOD32 Antivirus, il server proxy può essere configurato in due sezioni differenti della struttura Configurazione avanzata.

Le impostazioni del server proxy possono innanzitutto essere configurate in **Configurazione avanzata** da **Strumenti** > **Server proxy**. Specificando il server proxy a questo livello, si definiscono le impostazioni globali del server proxy per l'intera applicazione ESET NOD32 Antivirus. Questi parametri vengono utilizzati da tutti i moduli che richiedono una connessione a Internet.

Per specificare le impostazioni del server proxy per questo livello, selezionare la casella di controllo **Usa server proxy**, quindi inserire l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di **Porta** del server proxy.

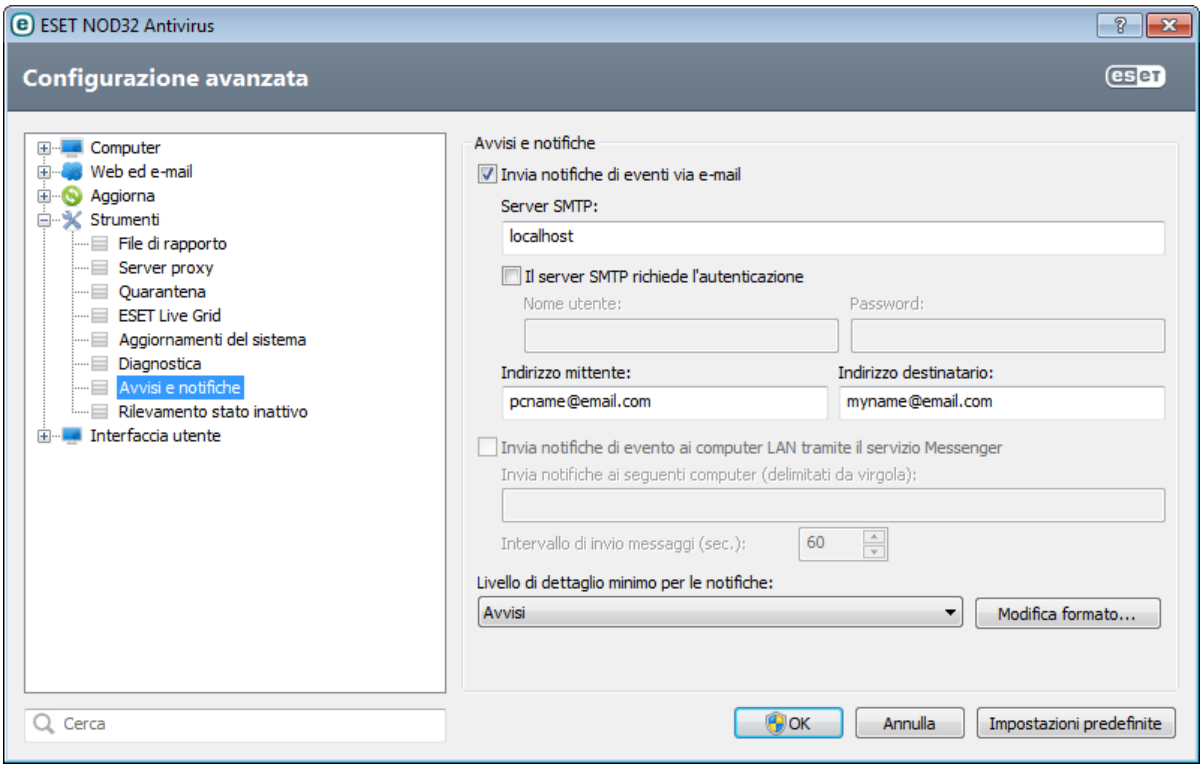
Se la comunicazione con il server proxy richiede l'autenticazione, selezionare la casella di controllo **Il server proxy richiede l'autenticazione** e inserire un **Nome utente** e una **Password** validi nei rispettivi campi. Fare clic su **Rileva server proxy** per rilevare e popolare automaticamente le impostazioni del server proxy. Verranno copiati i parametri specificati in Internet Explorer.

NOTA: questa funzione non consente di recuperare i dati sull'autenticazione (nome utente e password). Tali informazioni devono quindi essere immesse dall'utente.

Le impostazioni del server proxy possono inoltre essere definite nell'ambito dell'impostazione aggiornamento avanzata (sezione **Aggiorna** della struttura di **Configurazione avanzata**). Questa impostazione è applicabile al profilo di aggiornamento fornito ed è consigliata sui notebook che ricevono spesso aggiornamenti delle firme antivirali da diverse postazioni. Per ulteriori informazioni su questa impostazione, consultare la sezione Configurazione aggiornamento avanzata.

4.4.10 Avvisi e notifiche

ESET NOD32 Antivirus supporta l'invio di e-mail nel caso in cui si verifichi un evento con il livello di dettaglio selezionato. Fare clic sulla casella di controllo **Invia notifiche di eventi via e-mail** per attivare questa funzione e le notifiche e-mail.



Server SMTP - Il server SMTP utilizzato per l'invio delle notifiche.

Nota: ESET NOD32 Antivirus non supporta i server SMTP con crittografia SSL/TLS.

Il server SMTP richiede l'autenticazione - Se il server SMTP richiede l'autenticazione, questi campi devono essere compilati con nome utente e password validi per l'accesso al server SMTP.

Indirizzo mittente - Questo campo specifica l'indirizzo del mittente che verrà visualizzato nell'intestazione delle e-mail di notifica.

Indirizzo destinatario - Questo campo specifica l'indirizzo del destinatario che verrà visualizzato nell'intestazione delle e-mail di notifica.

Invia notifiche di evento ai computer LAN tramite il servizio Messenger - Selezionare questa casella di controllo per inviare messaggi ai computer LAN tramite il servizio di messaggeria di Windows®.

Invia notifiche ai seguenti computer (delimitati da virgola) - Immettere i nomi dei computer che riceveranno le notifiche tramite il servizio Messenger di Windows®.

Intervallo di invio messaggi (sec.) - Per modificare la lunghezza dell'intervallo tra le notifiche inviate tramite LAN, immettere l'intervallo di tempo desiderato in secondi.

Livello di dettaglio minimo per le notifiche - Specifica il livello di dettaglio minimo delle notifiche da inviare.

Modifica formato... - Le comunicazioni tra il programma e un utente remoto o un amministratore di sistema avvengono tramite e-mail o messaggi LAN (utilizzando il servizio Messenger di Windows®. Il formato predefinito dei messaggi e delle notifiche di avviso è adatto alla maggior parte delle situazioni. Tuttavia, qualora fosse necessario modificare il formato del messaggio, fare clic su Modifica formato....

4.4.10.1 Formato dei messaggi

In questa sezione è possibile configurare il formato dei messaggi di evento che vengono visualizzati sui computer remoti.

Gli avvisi di minaccia e i messaggi di notifica dispongono di un formato predefinito. Si consiglia di non modificare questo formato. Tuttavia, in alcuni casi (ad esempio, se si dispone di un sistema di elaborazione della posta automatizzato) potrebbe essere necessario modificare il formato dei messaggi.

Nel messaggio, le parole chiave (stringhe separate dai segni %) vengono sostituite dalle informazioni effettive specificate. Sono disponibili le parole chiave seguenti:

- **%TimeStamp%** - Data e ora dell'evento
- **%Scanner%** - Modulo interessato
- **%ComputerName%** - Nome del computer in cui si è verificato l'avviso
- **%ProgramName%** - Programma che ha generato l'avviso
- **%InfectedObject%** - Nome del file, del messaggio, ecc. infetto
- **%VirusName%** - Identificazione dell'infezione
- **%ErrorDescription%** - Descrizione di un evento non virus

Le parole chiave **%InfectedObject%** e **%VirusName%** vengono utilizzate solo nei messaggi di allarme delle minacce, mentre **%ErrorDescription%** viene utilizzata solo nei messaggi di evento.

Utilizza caratteri alfabetici locali - Converte un messaggio e-mail nella codifica dei caratteri ANSI in base alle impostazioni della lingua di Windows (ad esempio windows-1250). Se si lascia deselezionata questa opzione, il messaggio verrà convertito e codificato in ACSII a 7 bit (ad esempio, "á" verrà modificata in "a" e un simbolo sconosciuto verrà modificato in "?").

Utilizza codifica caratteri locali - L'origine del messaggio e-mail verrà codificata in formato QP (Quoted-printable) che utilizza i caratteri ASCII ed è in grado di trasmettere correttamente speciali caratteri nazionali tramite e-mail nel formato a 8-bit (áéíóú).

4.4.11 Invio di campioni per l'analisi

La finestra di dialogo per l'invio dei file consente di inviare un file o un sito a ESET ai fini dell'analisi ed è disponibile in **Strumenti** > **Invia campione per l'analisi**. Se è stato trovato un file con un comportamento sospetto nel computer in uso o un sito sospetto su Internet, è possibile inviarlo al laboratorio antivirus ESET per l'analisi. Se il file si rivela essere un'applicazione o un sito Web dannoso, il suo rilevamento verrà aggiunto in un aggiornamento successivo.

In alternativa, è possibile inviare il file tramite e-mail. Se si preferisce questa opzione, comprimere il file o i file con WinRAR/ZIP, proteggere l'archivio con la password "infected" e inviarlo a campioni@eset.com. Ricordare di inserire una descrizione nel campo dell'oggetto e di fornire il maggior numero di informazioni possibile sul file (ad esempio, l'indirizzo del sito Web dal quale è stato scaricato).

NOTA: Prima di inviare un file a ESET, assicurarsi che soddisfi uno o più dei criteri seguenti:
- il file non viene rilevato
- il file viene erroneamente rilevato come una minaccia

Non verrà inviata alcuna risposta a meno che non siano richieste ulteriori informazioni ai fini dell'analisi.

Selezionare la descrizione dal menu a discesa **Motivo per l'invio del file** che si avvicina maggiormente alla propria motivazione:
- **File sospetto**
- **Sito sospetto** (un sito Web infettato da un malware),
- **File falso positivo** (file che è stato rilevato come un'infezione ma che in realtà non è infetto),
- **Sito falso positivo**
- **Altro**

File/Sito - Il percorso del file o del sito Web che si intende inviare.

E-mail contatto - Una e-mail di contatto viene inviata a ESET insieme ai file sospetti e può essere utilizzata per contattare il mittente qualora fossero necessarie ulteriori informazioni ai fini dell'analisi. L'immissione

dell'indirizzo e-mail di contatto è facoltativa. ESET non invierà alcuna risposta a meno che non siano richieste ulteriori informazioni. Ogni giorno i server ESET ricevono decine di migliaia di file e non è pertanto possibile rispondere a tutti.

4.4.12 Aggiornamenti del sistema

La funzione di aggiornamento di Windows è un componente importante per la protezione del computer da software dannosi. Per questo motivo, è fondamentale installare gli aggiornamenti di Microsoft Windows non appena disponibili. ESET NOD32 Antivirus invia notifiche all'utente relative agli aggiornamenti mancanti in base al livello specificato. Sono disponibili i livelli seguenti:

- **Nessun aggiornamento** - Per il download non viene offerto nessun aggiornamento del sistema.
- **Aggiornamenti facoltativi** - Per il download vengono offerti aggiornamenti con priorità bassa e di livello superiore.
- **Aggiornamenti consigliati** - Per il download vengono offerti aggiornamenti contrassegnati come comuni o di livello superiore.
- **Aggiornamenti importanti** - Per il download vengono offerti aggiornamenti contrassegnati come importanti o di livello superiore.
- **Aggiornamenti critici** - Per il download vengono offerti unicamente gli aggiornamenti critici.

Fare clic su **OK** per salvare le modifiche. Dopo la verifica dello stato mediante il server di aggiornamento, viene visualizzata la finestra Aggiornamenti del sistema. Le informazioni sull'aggiornamento del sistema non saranno pertanto disponibili immediatamente dopo il salvataggio delle modifiche.

4.5 Interfaccia utente

La sezione **Interfaccia utente** consente di configurare il comportamento dell'interfaccia grafica utente (GUI) del programma.

Tramite lo strumento Grafica, è possibile regolare l'aspetto e gli effetti del programma.

Configurando gli Avvisi e notifiche, è possibile modificare il comportamento degli avvisi sulle minacce rilevate e le notifiche di sistema. in modo da adattarli alle proprie esigenze.

Se si sceglie di non visualizzare alcune notifiche, esse verranno visualizzate nell'area Finestre di notifica nascoste. In tali finestre è possibile verificarne lo stato, visualizzare ulteriori dettagli oppure rimuoverle.

Per assicurare la massima protezione del software di protezione, è possibile impedire l'esecuzione di modifiche non autorizzate proteggendo le impostazioni mediante una password tramite lo strumento Impostazione dell'accesso.

Il Menu contestuale viene visualizzato dopo aver fatto clic con il pulsante destro del mouse su un oggetto. Utilizzare questo strumento per integrare gli elementi controllo ESET NOD32 Antivirus nel menu contestuale.

4.5.1 Grafica

Le opzioni di configurazione dell'interfaccia utente in ESET NOD32 Antivirus consentono di modificare l'ambiente di lavoro per adattarlo alle esigenze specifiche dell'utente. Queste opzioni di configurazione sono accessibili nella struttura Configurazione avanzata espandendo l'**Interfaccia utente** e facendo clic su **Grafica**.

Nella sezione **Elementi dell'interfaccia utente**, è necessario disattivare l'opzione **Interfaccia grafica utente** qualora gli elementi grafici rallentino le prestazioni del computer o causino altri problemi. Potrebbe inoltre essere necessario disattivare l'interfaccia grafica per gli utenti con problemi visivi in quanto potrebbe creare conflitto con determinate applicazioni utilizzate per leggere il testo visualizzato sullo schermo.

Se si desidera disattivare la schermata iniziale di ESET NOD32 Antivirus, deselezionare **Mostra schermata iniziale all'avvio**.

Scegliere **Seleziona elemento controllo attivo** per far sì che il sistema evidenzi l'elemento presente al momento nell'area attiva del cursore del mouse. Per attivare l'elemento evidenziato, fare clic su di esso.

Per attivare l'utilizzo di icone animate che consentono di visualizzare lo stato di avanzamento di varie operazioni, selezionare **Utilizza icone animate per stato avanzamento**.

Se si desidera che ESET NOD32 Antivirus emetta un suono al verificarsi di eventi importanti durante un controllo, ad esempio in caso di rilevamento di una minaccia o al termine di un controllo, selezionare **Utilizza segnale audio**.

4.5.2 Avvisi e notifiche

La sezione **Avvisi e notifiche** nell'**Interfaccia utente** consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema (ad esempio messaggi di aggiornamenti riusciti) in ESET NOD32 Antivirus. È inoltre possibile impostare l'ora di visualizzazione e il livello di trasparenza delle notifiche sulla barra delle applicazioni (applicabile solo ai sistemi che supportano le notifiche sulla barra delle applicazioni).

Deselezionare la casella di controllo vicino a **Visualizza avvisi** per annullare tutte le finestre di avviso. Questa operazione è adatta solo in alcune situazioni. Nella maggior parte dei casi, è consigliabile lasciare attivata l'opzione (impostazione predefinita).

Le notifiche visualizzate sul desktop sono solo a titolo informativo e non consentono o richiedono l'interazione da parte dell'utente. Vengono visualizzati nell'area di notifica posta nell'angolo in basso a destra della schermata. Per attivare la visualizzazione delle notifiche sul desktop, selezionare **Visualizza notifiche sul desktop**. Per modificare opzioni più dettagliate, ad esempio l'orario di visualizzazione della notifica e la trasparenza della finestra, fare clic su **Configura notifiche**. Per visualizzare in anteprima il funzionamento delle notifiche, fare clic su **Anteprima**. Per eliminare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero, selezionare **Non visualizzare le notifiche quando vengono eseguite applicazioni in modalità a schermo intero**.

Per chiudere automaticamente le finestre popup dopo un determinato periodo di tempo, selezionare **Chiudi automaticamente le finestre di messaggio dopo (sec.)**. Se non vengono chiuse manualmente, le finestre di avviso vengono chiuse automaticamente una volta trascorso il periodo di tempo specificato.

Fare clic su **Impostazione avanzata** per accedere a ulteriori opzioni di configurazione degli **Avvisi e notifiche**.

4.5.2.1 Configurazione avanzata

Nel menu a discesa **Livello di dettaglio minimo degli eventi da visualizzare** è possibile selezionare il livello iniziale di gravità degli avvisi e delle notifiche da visualizzare.

- **Diagnostica** - Registra tutte le informazioni necessarie per l'ottimizzazione del programma e di tutti i record indicati in precedenza.
- **Informativi** - Messaggi di record informativi che includono gli aggiornamenti riusciti e tutti i record indicati in precedenza.
- **Allarmi** - Consente di registrare errori critici e messaggi di allarme.
- **Errori** - Verranno registrati errori quali *"Errore durante il download del file"* ed errori critici.
- **Critici** - Registra solo gli errori critici (errore che avvia la protezione antiviruse così via).

L'ultima funzione in questa sezione consente di configurare la destinazione delle notifiche in un ambiente multi-utente. Nel campo **In sistemi multiutente, visualizza le notifiche sullo schermo di questo utente** viene specificato l'utente che riceverà le notifiche di sistema e di altro tipo sui sistemi che consentono la connessione simultanea di più utenti. In genere si tratta di un amministratore di sistema o di rete. Questa opzione è utile soprattutto per i server di terminali, a condizione che tutte le notifiche di sistema vengano inviate all'amministratore.

4.5.3 Finestre di notifica nascoste

Se per le finestre di notifica (avvisi) visualizzate in precedenza è stata selezionata l'opzione **Non visualizzare più questo messaggio**, questa notifica verrà visualizzata nell'elenco delle finestre di notifica nascoste. Le azioni eseguite automaticamente vengono visualizzate nella colonna **Conferma**.

Mostra - Mostra un'anteprima delle finestre di notifica al momento non visualizzate e per le quali è configurata un'azione automatica.

Rimuovi - Rimuove voci dall'elenco **Finestre di messaggio nascoste**. Tutte le finestre di notifica rimosse dall'elenco verranno visualizzate nuovamente.

4.5.4 Configurazione dell'accesso

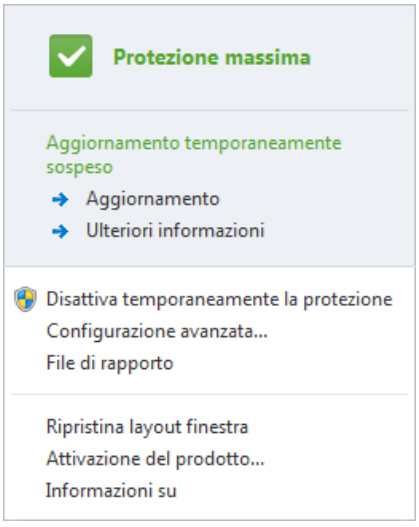
Le impostazioni ESET NOD32 Antivirus rappresentano una parte cruciale dei criteri di protezione. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Per proteggere con password i parametri di configurazione, nel menu principale fare clic su **Configurazione** > **Accedi a configurazione avanzata...** > **Interfaccia utente** > **Impostazione dell'accesso**, selezionare **Proteggi impostazioni con password** e fare clic su **Imposta password**. Tenere presente che la password fa distinzione tra maiuscole e minuscole.

Richiedi diritti di amministratore completi per gli account con diritti limitati - Selezionare questa opzione per richiedere all'utente corrente (nel caso non disponga dei diritti di amministratore) di inserire un nome utente e una password di amministratore per la modifica di alcuni parametri del sistema (analogo a Controllo dell'account utente (UAC) in Windows Vista e Windows 7). Tali modifiche includono la disattivazione dei moduli di protezione. Sui sistemi Windows XP, in cui l'UAC non è in esecuzione, gli utenti avranno a disposizione l'opzione **Richiedi diritti di amministratore (sistema senza supporto Controllo dell'account utente)**.

Mostra finestra timeout protezione - Selezionando questa opzione, tutte le volte che la protezione verrà disattivata temporaneamente dall'utente dal menu del programma oppure nella sezione **ESET NOD32 Antivirus** > **Configurazione**, verrà visualizzata una finestra di dialogo che indica il tempo residuo della disattivazione della protezione.

4.5.5 Menu del programma

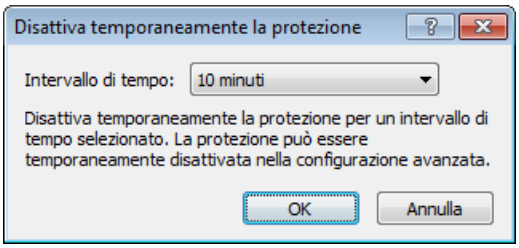
Il menu del programma principale contiene alcune delle funzioni e delle opzioni di impostazione più importanti.



Usato frequentemente - Consente di visualizzare le parti di ESET NOD32 Antivirus che vengono utilizzate più frequentemente. È possibile accedervi rapidamente dal menu del programma.

Disattiva temporaneamente la protezione - Consente di visualizzare la finestra di dialogo di conferma per disattivare la Protezione antivirus e antispyware che protegge da attacchi dannosi al sistema controllando file e comunicazioni Web ed e-mail. Selezionare **Non ripetere più la domanda** per non visualizzare più questo messaggio.

Il menu a discesa **Intervallo di tempo** rappresenta l'intervallo di tempo durante il quale la Protezione antivirus e antispyware verrà disattivata.



Configurazione avanzata... - Selezionare questa opzione per accedere alla struttura **Configurazione avanzata**. Vi sono anche altri modi per aprire la Configurazione avanzata, ad esempio, premendo il tasto F5 oppure accedendo a **Configurazione** > **Accedi a configurazione avanzata...**.

File di rapporto - I File di rapporto contengono informazioni relative agli eventi di programma importanti che si sono verificati e forniscono una panoramica delle minacce rilevate.

Ripristina layout finestra - Ripristina le dimensioni predefinite e la posizione sullo schermo della finestra di ESET NOD32 Antivirus.

Attivazione del prodotto... - Selezionare questa opzione se non è ancora stato attivato il prodotto di protezione ESET oppure inserire nuovamente le credenziali di attivazione del prodotto dopo aver rinnovato la licenza.

Informazioni su - Vengono fornite informazioni sul sistema, dettagli sulla versione installata di ESET NOD32 Antivirus e sui relativi moduli di programma installati. In questa sezione è anche possibile trovare la data di scadenza della licenza e le informazioni relative al sistema operativo e alle risorse di sistema.

4.5.6 Menu contestuale

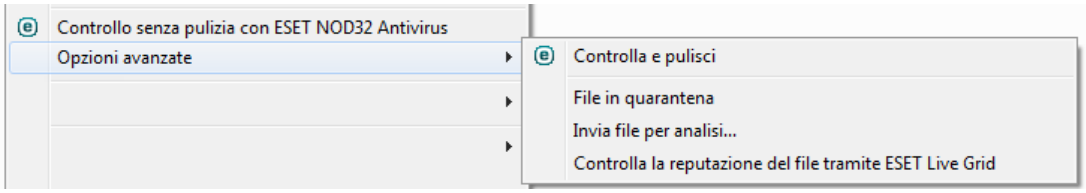
Il menu contestuale viene visualizzato dopo aver fatto clic con il pulsante destro del mouse su un oggetto. Nel menu sono elencate tutte le opzioni disponibili da eseguire sull'oggetto.

È possibile integrare gli elementi controllo ESET NOD32 Antivirus nel menu contestuale. Sono disponibili opzioni di configurazione più dettagliate per questa funzionalità nella struttura Configurazione avanzata in **Interfaccia utente** > **Menu contestuale**.

Integra nel menu contestuale - Integrare gli elementi controllo ESET NOD32 Antivirus nel menu contestuale.

Nel menu a discesa **Tipo di menu** sono disponibili le seguenti opzioni:

- **Completo (esegui prima controllo)** - Attiva tutte le opzioni del menu contestuale. Nel menu principale verrà visualizzato **Controllo senza pulizia con ESET NOD32 Antivirus** come prima opzione e **Controllo e pulizia** come seconda opzione.
- **Completo (esegui prima pulitura)** - Attiva tutte le opzioni del menu contestuale. Nel menu principale verrà visualizzato **Controllo con ESET NOD32 Antivirus** come prima opzione e **Controllo senza pulizia** come seconda opzione.



- **Solo controllo** - Nel menu contestuale verrà visualizzato solo **Controlla senza pulizia con ESET NOD32 Antivirus**.
- **Solo pulizia** - Nel menu contestuale verrà visualizzato solo **Controllo con ESET NOD32 Antivirus**.

5. Utente avanzato

5.1 Gestione profili

La Gestione profili viene utilizzata in due modi all'interno di ESET NOD32 Antivirus: nella sezione **Controllo computer su richiesta** e nella sezione **Aggiorna**.

Controllo del computer

È possibile salvare i parametri di scansione preferiti per i controlli futuri. È consigliabile creare un profilo di scansione differente (con diversi oggetti da controllare, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, aprire la finestra Configurazione avanzata (F5) e fare clic su **Computer** > **Antivirus e antispyware** > **Controllo computer su richiesta** > **Profili...**. Nella finestra **Profili di configurazione** è disponibile un menu a discesa **Profili selezionati** contenente i profili di scansione esistenti e l'opzione per crearne di nuovi. Per ricevere assistenza nella creazione di un profilo di scansione adatto alle proprie esigenze, consultare la sezione Configurazione parametri motore ThreatSense contenente una descrizione di ciascun parametro di configurazione della scansione.

Esempio: si supponga di voler creare il proprio profilo di scansione e che la configurazione del Controllo intelligente sia appropriata solo in parte, in quanto non si desidera eseguire la scansione di eseguibili compressi o di applicazioni potenzialmente pericolose, bensì si intende applicare l'opzione **Massima pulizia**. Nella finestra **Profili di configurazione**, fare clic su **Aggiungi...**. Immettere il nome del nuovo profilo nel campo **Nome profilo**, quindi selezionare **Controllo intelligente** dal menu a discesa **Copia impostazioni dal profilo**. Regolare i parametri rimanenti per soddisfare le specifiche esigenze e salvare il nuovo profilo.

Aggiorna

L'editor dei profili nella sezione Impostazione aggiornamento consente agli utenti di creare nuovi profili di aggiornamento. Creare e utilizzare i profili personalizzati (diversi dal **Profilo personale** predefinito) solo se il computer utilizza vari metodi di connessione ai server di aggiornamento.

Ad esempio, un computer portatile che si connette normalmente a un server locale (Mirror) nella rete locale ma scarica gli aggiornamenti direttamente dai server di aggiornamento ESET durante la disconnessione (trasferta di lavoro) potrebbe utilizzare due profili: il primo per connettersi al server locale e il secondo per connettersi ai server ESET. Dopo aver configurato questi profili, accedere a **Strumenti** > **Pianificazione attività** e modificare i parametri delle attività di aggiornamento. Indicare un profilo come principale e l'altro come secondario.

Profilo selezionato - Il profilo di aggiornamento attualmente utilizzato. Per modificarlo, scegliere un profilo dal menu a discesa.

Aggiungi... - Consente di creare nuovi profili di aggiornamento.

Nella parte inferiore della finestra è visualizzato l'elenco dei profili esistenti.

5.2 Tasti di scelta rapida

I tasti di scelta rapida che è possibile utilizzare con ESET NOD32 Antivirus sono:

Ctrl+G	disattiva l'interfaccia utente nel prodotto
Ctrl+I	apre la pagina ESET SysInspector
Ctrl+L	apre la pagina File di rapporto
Ctrl+S	apre la pagina Pianificazione attività
Ctrl+Q	apre la pagina Quarantena
Ctrl+U	apre una configurazione per nome utente e password
Ctrl+R	ripristina le dimensioni predefinite e la posizione sullo schermo della finestra

Per una migliore navigazione del prodotto ESET, è possibile utilizzare i seguenti tasti di scelta rapida:

F1	apre le pagine della Guida
F5	apre la Configurazione avanzata
Tasti Su/Giù	navigazione all'interno delle voci del prodotto
*	ingrandisce il nodo della struttura Configurazione avanzata
-	comprime i nodi della struttura Configurazione avanzata
TAB	sposta il cursore in una finestra
Esc	chiude la finestra di dialogo attiva

5.3 Diagnostica

La diagnostica fornisce dump sulle interruzioni delle applicazioni correlate ai processi ESET (ad esempio, *ekrn*). In caso di interruzione di un'applicazione, verrà generato un dump, che può aiutare gli sviluppatori a eseguire il debug e correggere vari problemi di ESET NOD32 Antivirus. Sono disponibili due tipi di dump:

- **Dump memoria completo** - Registra tutti i contenuti della memoria di sistema quando l'applicazione viene interrotta inaspettatamente. Un dump memoria completo può contenete dati estrapolati dai processi in esecuzione quando è stato raccolto il dump di memoria.
- **Minidump** - Registra il minor numero possibile di informazioni utili che possono aiutare a identificare il motivo alla base dell'arresto inaspettato dell'applicazione. Questo tipo di file dump risulta utile in caso di limitazioni di spazio. A causa delle informazioni limitate incluse, gli errori che non sono stati causati direttamente dalla minaccia in esecuzione quando si è verificato il problema potrebbero tuttavia non essere rilevati a seguito di un'analisi del file in questione.
- Selezionare **Non generare dump di memoria** (impostazione predefinita) per disattivare questa funzione.

Directory di destinazione - Directory nella quale verrà generato il dump durante l'arresto imprevisto. Fare clic su **...** per aprire questa directory in una nuova finestra di *Windows Explorer*.

5.4 Importa ed esporta impostazioni

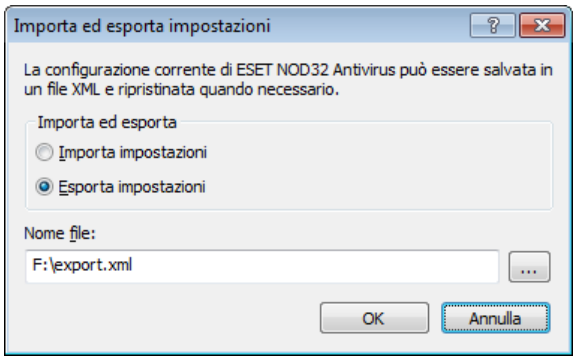
È possibile importare o esportare il file di configurazione personalizzato in formato .xml di ESET NOD32 Antivirus dal menu **Configurazione**.

I file di importazione e di esportazione sono utili se si necessita effettuare un backup della configurazione corrente di ESET NOD32 Antivirus da utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per gli utenti che desiderano utilizzare la configurazione preferita su più sistemi. In tal modo, sarà possibile importare facilmente un file *.xml* per il trasferimento di queste impostazioni.

L'importazione della configurazione è molto semplice. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni...** quindi selezionare **Importa impostazioni**. Inserire il percorso del file di configurazione o fare clic sul pulsante **...** per ricercare il file di configurazione che si vuole importare.

Le operazioni per esportare una configurazione sono molto simili. Nella finestra principale del programma, fare clic su **Configurazione** > **Importa ed esporta impostazioni...**. Selezionare **Esporta impostazioni** e inserire il percorso del file di configurazione (ad esempio, *export.xml*). Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.

Nota: durante l'esportazione delle impostazioni potrebbe comparire un errore se non si dispone degli idonei diritti di scrittura del file esportato nella directory specificata.



5.5 Rilevamento stato inattivo

Le impostazioni del rilevamento stato inattivo possono essere configurate nella sezione **Configurazione avanzata** in **Strumenti** > **Rilevamento stato inattivo**. Queste impostazioni specificano l'attivazione del Controllo stato inattivo se:

- è attivo lo screen saver,
- il computer è bloccato,
- un utente si disconnette.

Utilizzare le caselle di controllo per attivare o disattivare i vari metodi di attivazione del rilevamento dello stato inattivo.

5.6 ESET SysInspector

5.6.1 Introduzione a ESET SysInspector

L'applicazione ESET SysInspector ispeziona il computer in modo approfondito e visualizza i dati raccolti in modo globale. La raccolta di informazioni su driver e applicazioni, su connessioni di rete o importanti voci di registro semplifica il controllo di comportamenti sospetti del sistema, siano essi dovuti a incompatibilità software o hardware o infezioni malware.

È possibile accedere a ESET SysInspector in due modi: dalla versione integrata nelle soluzioni ESET Security o scaricando gratuitamente la versione indipendente (SysInspector.exe) dal sito Web ESET. Le funzionalità e i comandi di entrambe le versioni sono identici. L'unica differenza consiste nella gestione dei risultati. La versione indipendente e quella integrata consentono entrambe di esportare snapshot del sistema su un file *XML* e salvarli su disco. La versione integrata consente tuttavia anche di memorizzare gli snapshot di sistema direttamente in **Strumenti** > **ESET SysInspector** (tranne ESET Remote Administrator). Per ulteriori informazioni, vedere la sezione ESET SysInspector come componente di ESET NOD32 Antivirus.

È necessario attendere qualche minuto per consentire a ESET SysInspector di controllare il computer. A seconda della configurazione hardware, del sistema operativo e del numero di applicazioni installate nel computer in uso, questa operazione potrebbe richiedere da 10 secondi ad alcuni minuti.

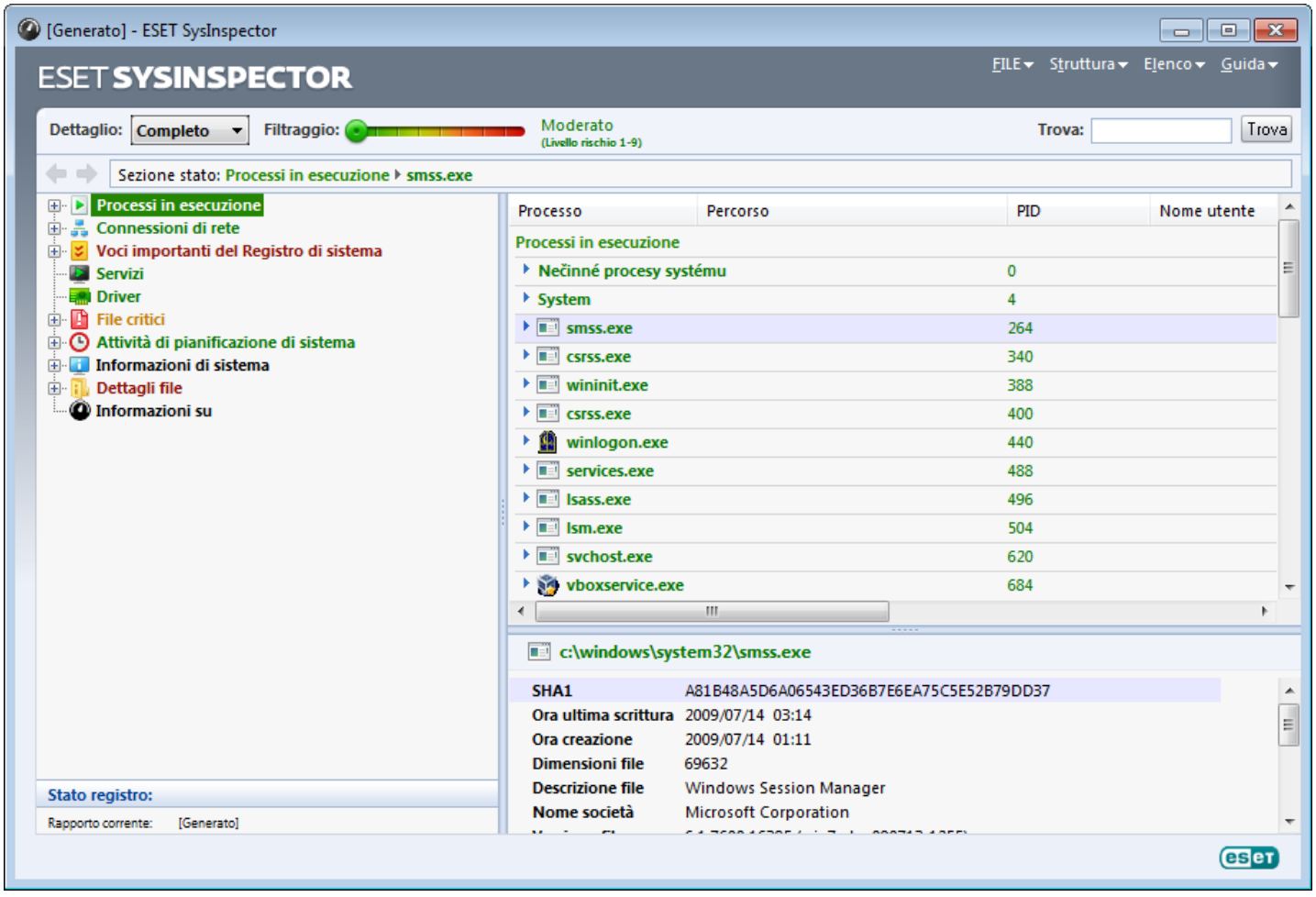
5.6.1.1 Avvio di ESET SysInspector

Per avviare ESET SysInspector è sufficiente eseguire il file eseguibile *SysInspector.exe* scaricato dal sito Web ESET. Se è già installata una delle soluzioni ESET Security, è possibile eseguire ESET SysInspector direttamente dal menu Start (fare clic su **Programmi** > **ESET** > **ESET NOD32 Antivirus**).

Si prega di attendere che l'applicazione abbia esaminato il sistema in uso. Questa operazione potrebbe richiedere diversi minuti.

5.6.2 Interfaccia utente e utilizzo dell'applicazione

Per chiarezza, la finestra principale del programma è stata divisa in quattro sezioni principali: i comandi del programma sono posizionati nella parte superiore della finestra; a sinistra viene visualizzata la finestra di spostamento, a destra è disponibile la finestra Descrizione e, infine, nella parte inferiore della schermata, viene visualizzata la finestra Dettagli. Nella sezione Stato registro sono elencati i parametri principali di un rapporto (filtro usato, tipo di filtro, se il rapporto è il risultato di un confronto e così via).



5.6.2.1 Comandi del programma

La presente sezione contiene la descrizione di tutti i comandi del programma disponibili in ESET SysInspector.

File

Selezionare **File** per memorizzare lo stato attuale del sistema per un'analisi futura oppure aprire un rapporto precedentemente archiviato. Ai fini della pubblicazione, è consigliabile generare un rapporto **Idoneo all'invio**. In questo formato, nel rapporto vengono omesse informazioni riservate (nome utente attuale, nome computer, nome dominio, privilegi utente attuale, variabili d'ambiente e così via).

NOTA: è possibile aprire i rapporti di ESET SysInspector precedentemente archiviati trascinandoli nella finestra principale del programma.

Struttura

Consente di espandere o chiudere tutti i nodi e di esportare le sezioni selezionate sullo script di servizio.

Elenco

Contiene funzioni per uno spostamento più pratico all'interno del programma e varie altre funzioni, ad esempio la ricerca di informazioni su Internet.

Guida

Contiene informazioni sull'applicazione e sulle relative funzioni.

Dettaglio

Questa impostazione influenza le informazioni visualizzate nella finestra principale del programma al fine di semplificarne l'utilizzo. Nella modalità "Base" si ha accesso alle informazioni utilizzate per trovare soluzioni a problemi comuni del sistema. Nella modalità "Media" il programma visualizza i dettagli meno utilizzati, mentre nella modalità "Completa", ESET SysInspector mostra tutte le informazioni necessarie alla soluzione di problemi specifici.

Filtraggio

Il filtraggio elementi viene utilizzato soprattutto per individuare file o voci di registro sospetti all'interno del sistema. Regolando il cursore, è possibile filtrare gli elementi in base al livello di rischio. Se il cursore si trova all'estrema sinistra (Livello di rischio 1) vengono visualizzati tutti gli elementi. Spostando il cursore a destra, il programma esclude tutti gli elementi meno rischiosi rispetto al livello di rischio corrente, consentendo di visualizzare solo gli elementi che risultano più sospetti rispetto al livello visualizzato. Quando il cursore si trova all'estrema destra, il programma visualizza solo gli elementi dannosi conosciuti.

Tutti gli elementi contrassegnati con un livello di rischio compreso tra 6 e 9 rappresentano un rischio per la sicurezza. Se ESET SysInspector ha rilevato un elemento di questo tipo, si consiglia di eseguire il controllo del sistema con ESET Online Scanner, se non si utilizza una soluzione di protezione di ESET. ESET Online Scanner è un servizio gratuito.

NOTA: il Livello di rischio di un elemento può essere determinato rapidamente confrontandone il colore con quello del cursore Livello di rischio.

Confronta

Durante il confronto di due rapporti, è possibile scegliere di visualizzare tutti gli elementi, solo gli elementi aggiunti, solo gli elementi rimossi o solo gli elementi sostituiti.

Trova

L'opzione Cerca può essere utilizzata per individuare rapidamente un elemento specifico in base al nome o parte di esso. I risultati della richiesta di ricerca vengono visualizzati nella finestra Descrizione.

Ritorna

Facendo clic sulle frecce indietro o avanti, è possibile tornare alle informazioni precedentemente visualizzate nella finestra Descrizione. È possibile utilizzare i tasti Cancella e Barra spaziatrice anziché fare clic su Avanti e Indietro.

Sezione stato

Visualizza il nodo corrente nella finestra di spostamento.

Importante: gli elementi evidenziati in rosso sono sconosciuti. Per tale motivo, il programma li segna come potenzialmente pericolosi. Se un elemento è segnalata in rosso, non significa automaticamente che sia possibile eliminare il file. Prima di procedere all'eliminazione, assicurarsi che i file siano effettivamente pericolosi o non necessari.

5.6.2.2 Navigare in ESET SysInspector

ESET SysInspector divide vari tipi di informazioni in numerose sezioni di base, dette nodi. Se disponibili, ulteriori dettagli saranno visualizzabili espandendo ciascun nodo nei relativi sottonodi. Per espandere o comprimere un nodo, fare doppio clic sul nome del nodo oppure fare clic su ⊞ o ⊟ accanto al nome del nodo. Spostandosi nella struttura ad albero di nodi e sottonodi della finestra di spostamento, sono disponibili vari dettagli su ciascun nodo presente nella finestra Descrizione. Navigando tra gli elementi della finestra Descrizione, è possibile visualizzare ulteriori dettagli per ciascun elemento nella finestra Dettagli.

Di seguito vengono riportate le descrizioni dei nodi principali presenti nella finestra di spostamento e le relative informazioni delle finestre Descrizione e Dettagli.

Processi in esecuzione

Questo nodo contiene informazioni sulle applicazioni e sui processi in esecuzione durante la generazione del rapporto. Nella finestra Descrizione sono disponibili dettagli aggiuntivi su ciascun processo, ad esempio le librerie dinamiche utilizzate dal processo e la loro posizione nel sistema, il nome del produttore dell'applicazione e il livello di rischio del file.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

NOTA: un sistema operativo è basato su diversi componenti kernel, costantemente in esecuzione, che forniscono funzioni fondamentali e di base per le altre applicazioni utente. In alcuni casi, tali processi sono visualizzati nello strumento ESET SysInspector con il percorso file preceduto da \??\. Quei simboli forniscono un'ottimizzazione per i processi in questione prima di avviarli e risultano sicuri per il sistema.

Connessioni di rete

La finestra Descrizione contiene un elenco di processi e applicazioni che comunicano sulla rete utilizzando il protocollo selezionato nella finestra di spostamento (TCP o UDP), unitamente all'indirizzo remoto a cui è collegata l'applicazione. È inoltre possibile verificare gli indirizzi IP dei server DNS.

La finestra Dettagli contiene informazioni aggiuntive sugli elementi selezionati nella finestra Descrizione, quali le dimensioni del file o il relativo hash.

Voci importanti del Registro di sistema

Contiene un elenco delle voci di registro selezionate che sono spesso correlate a vari problemi del sistema, ad esempio quelle indicano i programmi di avvio, oggetti browser helper (BHO) e così via.

Nella finestra Descrizione è possibile visualizzare i file correlati a voci di registro specifiche. Nella finestra Dettagli è possibile visualizzare maggiori informazioni.

Servizi

La finestra Descrizione contiene un elenco di file registrati come Servizi Windows. Nella finestra Dettagli è possibile controllare il modo in cui è impostato l'avvio del servizio insieme ai dettagli specifici del file.

Driver

Un elenco di driver installati nel sistema.

File critici

Nella finestra Descrizione è visualizzato il contenuto dei file critici relativi al sistema operativo Microsoft Windows.

Attività di pianificazione di sistema

Contiene un elenco delle attività avviate dall'Utilità di pianificazione di Windows a un orario/intervallo specificato.

Informazioni di sistema

Contiene informazioni dettagliate sull'hardware e sul software, oltre a informazioni sulle variabili d'ambiente

impostate, sui diritti utente e sui rapporti eventi di sistema.

Dettagli file

Un elenco di file di sistema importanti e di file presenti nella cartella Programmi. Per maggiori informazioni sui file in questione, fare riferimento alle finestre Descrizione e Dettagli.

Informazioni su

Informazioni sulla versione di ESET SysInspector ed elenco dei moduli del programma.

5.6.2.2.1 Tasti di scelta rapida

I tasti di scelta rapida che possono essere utilizzati con ESET SysInspector includono:

File

Ctrl+O	apre il rapporto esistente
Ctrl+S	salva i rapporti creati

Genera

Ctrl+G	genera uno snapshot di stato computer standard
Ctrl+H	genera uno snapshot di stato computer che potrebbe registrare anche informazioni sensibili

Filtraggio elementi

1, O	non a rischio, visualizzati gli elementi con livello di rischio 1-9
2	non a rischio, visualizzati gli elementi con livello di rischio 2-9
3	non a rischio, visualizzati gli elementi con livello di rischio 3-9
4, U	sconosciuto, visualizzati gli elementi con livello di rischio 4-9
5	sconosciuto, visualizzati gli elementi con livello di rischio 5-9
6	sconosciuto, visualizzati gli elementi con livello di rischio 6-9
7, B	a rischio, visualizzati gli elementi con livello di rischio 7-9
8	a rischio, visualizzati gli elementi con livello di rischio 8-9
9	a rischio, visualizzati gli elementi con livello di rischio 9
-	diminuisce il livello di rischio
+	aumenta il livello di rischio
Ctrl+9	modalità di filtraggio, livello uguale o più alto
Ctrl+0	modalità di filtraggio, solo livello uguale

Visualizza

Ctrl+5	visualizza per fornitore, tutti i fornitori
Ctrl+6	visualizza per fornitore, solo Microsoft
Ctrl+7	visualizza per fornitore, tutti gli altri fornitori
Ctrl+3	mostra tutti i dettagli
Ctrl+2	livello di dettaglio medio
Ctrl+1	visualizzazione di base
Cancella	indietro di un passaggio
Barra spaziatrice	avanti di un passaggio
Ctrl+W	espande la struttura
Ctrl+Q	comprime la struttura

Altri comandi

Ctrl+T	va alla posizione originale dell'elemento dopo averlo selezionato nei risultati di ricerca
Ctrl+P	visualizza informazioni di base su un elemento
Ctrl+A	visualizza informazioni complete di un elemento
Ctrl+C	copia la struttura dell'elemento attuale
Ctrl+X	copia gli elementi

Ctrl+B	trova su Internet le informazioni sui file selezionati
Ctrl+L	apre la cartella dove si trova il file selezionato
Ctrl+R	apre la voce corrispondente nell'editor del Registro di sistema
Ctrl+Z	copia un percorso di un file (se l'elemento è relativo a un file)
Ctrl+F	passa al campo di ricerca
Ctrl+D	chiude i risultati di ricerca
Ctrl+E	esegue lo script di servizio

Confronto

Ctrl+Alt+O	apre il rapporto originale/comparativo
Ctrl+Alt+R	annulla il confronto
Ctrl+Alt+1	visualizza tutti gli elementi
Ctrl+Alt+2	visualizza solo gli elementi aggiunti, il rapporto mostrerà gli elementi presenti nel rapporto attuale
Ctrl+Alt+3	visualizza solo gli elementi rimossi, il rapporto mostrerà gli elementi presenti nel rapporto precedente
Ctrl+Alt+4	visualizza solo gli elementi sostituiti (compresi i file)
Ctrl+Alt+5	visualizza solo le differenze tra i rapporti
Ctrl+Alt+C	visualizza il confronto
Ctrl+Alt+N	visualizza il rapporto attuale
Ctrl+Alt+P	apre il rapporto precedente

Varie

F1	visualizza la guida
Alt+F4	chiude il programma
Alt+Maiusc+F4	chiude il programma senza chiedere
Ctrl+I	statistiche registro

5.6.2.3 Confronta

La funzione Confronta consente di mettere a confronto due rapporti esistenti. Il risultato di questa funzione è una serie di elementi non comuni ai due rapporti. È la soluzione ideale se si desidera individuare le modifiche nel sistema ed è un utile strumento per il rilevamento di codice dannoso.

Dopo l'avvio, l'applicazione crea un nuovo rapporto, visualizzato in una nuova finestra. Fare clic su **File** > **Salva rapporto** per salvare un rapporto in un file. I file di rapporto possono essere aperti e visualizzati in un secondo momento. Per aprire un rapporto esistente, fare clic su **File** > **Apri rapporto**. Nella finestra principale del programma, ESET SysInspector visualizza sempre un rapporto alla volta.

Il confronto tra due rapporti offre il vantaggio di visualizzare un rapporto attualmente attivo e uno salvato in un file. Per confrontare i rapporti, fare clic su **File** > **Confronta rapporto** e scegliere **Seleziona file**. Il rapporto selezionato verrà confrontato con quello attivo nelle finestre principali del programma. Nel rapporto comparativo saranno visualizzate solo le differenze tra i due.

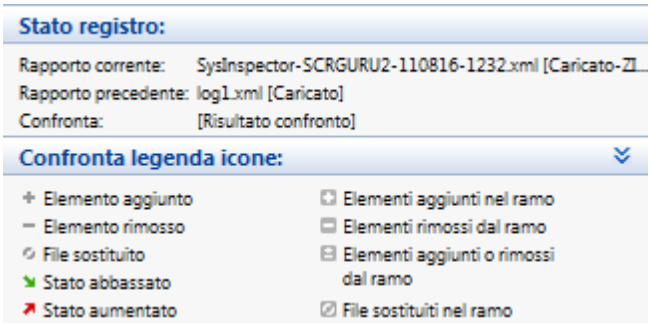
NOTA: se si mettono a confronto due file di rapporto, facendo clic su **File** > **Salva rapporto** e salvandoli in un file ZIP, verranno salvati entrambi i file. Se si apre il file in un secondo momento, i rapporti contenuti verranno automaticamente messi a confronto.

Accanto agli elementi visualizzati, ESET SysInspector mostra i simboli che identificano le differenze tra i rapporti confrontati.

Descrizione di tutti i simboli che possono essere visualizzati accanto agli elementi:

- + nuovo valore, non presente nel rapporto precedente
- la sezione della struttura contiene nuovi valori
- – valore rimosso, presente solo nel rapporto precedente
- la sezione della struttura contiene i valori rimossi
- il valore/file è stato modificato
- la sezione della struttura contiene valori/file modificati
- il livello di rischio è diminuito/era più alto nel precedente rapporto
- il livello di rischio è aumentato/era più basso nel precedente rapporto

Nella sezione di descrizione visualizzata nell'angolo in basso a sinistra vengono descritti tutti i simboli e mostrati i nomi dei rapporti confrontati.



Qualsiasi rapporto comparativo può essere salvato in un file e aperto successivamente.

Esempio

Generare e salvare un rapporto, registrando le informazioni originali sul sistema, in un file denominato previous.xml. Dopo aver effettuato le modifiche al sistema, aprire ESET SysInspector e attendere che venga eseguito un nuovo rapporto. Salvarlo in un file denominato *current.xml*.

Al fine di rilevare le modifiche tra i due rapporti, fare clic su **File** > **Confronta rapporti**. Il programma crea un rapporto comparativo che visualizza solo le differenze tra i due.

È possibile ottenere lo stesso risultato utilizzando la seguente opzione della riga di comando:

SysIsnpector.exe current.xml previous.xml

5.6.3 Parametri della riga di comando

ESET SysInspector supporta la generazione di rapporti dalla riga di comando con i seguenti parametri:

/gen	genera rapporto direttamente dalla riga di comando senza avviare l'interfaccia grafica utente (GUI)
/privacy	genera rapporto omettendo le informazioni sensibili
/zip	salva rapporto in un archivio zip compresso
/silent	non visualizzare finestra di avanzamento durante la creazione del rapporto dalla riga di comando
/blank	avvia ESET SysInspector senza generare/caricare il rapporto

Esempi

Utilizzo:

```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

Per caricare un rapporto specifico direttamente nel browser, utilizzare: *SysInspector.exe .\clientlog.xml*
Per generare il rapporto dalla riga di comando, utilizzare: *SysInspector.exe /gen=.\mynewlog.xml*
Per generare un rapporto escludendo le informazioni sensibili direttamente in un file compresso, utilizzare: *SysInspector.exe /gen=.\mynewlog.zip /privacy /zip*
Per confrontare due file di rapporto ed esaminare le differenze, utilizzare: *SysInspector.exe new.xml old.xml*

NOTA: Se il nome di un file/cartella contiene uno spazio vuoto, è necessario inserirlo tra virgolette.

5.6.4 Script di servizio

Lo script di servizio è uno strumento utile per i clienti che utilizzano ESET SysInspector in quanto consente di rimuovere facilmente gli oggetti indesiderati dal sistema.

Lo script di servizio consente all'utente di esportare l'intero rapporto di ESET SysInspector o le parti selezionate. Al termine dell'esportazione, è possibile selezionare gli oggetti indesiderati da eliminare. È quindi possibile eseguire il rapporto modificato per eliminare gli oggetti contrassegnati.

Lo script di servizio è adatto agli utenti avanzati che hanno già esperienza nella diagnostica dei problemi del sistema. Le modifiche effettuate da persone non qualificate potrebbero causare danni al sistema operativo.

Esempio

Se si sospetta che il computer sia infettato da un virus non rilevato dal programma antivirus, attenersi alle seguenti istruzioni dettagliate:

1. Eseguire ESET SysInspector per generare un nuovo snapshot del sistema.
2. Selezionare il primo elemento della sezione a sinistra (nella struttura ad albero), premere Shift ed evidenziare l'ultimo elemento per selezionarli tutti.
3. Fare clic con il pulsante destro del mouse sugli oggetti selezionati e scegliere **Esporta sezioni selezionate a script di servizio**.
4. Gli oggetti selezionati verranno esportati in un nuovo rapporto.
5. Questo è il passaggio più importante dell'intera procedura: aprire il nuovo rapporto e cambiare l'attributo - in + per tutti gli oggetti che si desidera rimuovere. Fare attenzione a non contrassegnare file/oggetti importanti del sistema operativo.
6. Aprire ESET SysInspector, fare clic su **File** > **Esegui script di servizio** e immettere il percorso dello script.
7. Fare clic su **OK** per eseguire lo script.

5.6.4.1 Generazione dello script di servizio

Per generare uno script, fare clic con il pulsante destro del mouse su qualsiasi voce della struttura del menu (nel riquadro a sinistra) nella finestra principale di ESET SysInspector. Selezionare l'opzione **Esporta tutte le sezioni a script di servizio** o **Esporta sezioni selezionate a script di servizio** nel menu contestuale.

NOTA: non è possibile esportare lo script di servizio quando vengono confrontati due rapporti.

5.6.4.2 Struttura dello script di servizio

Nella prima riga dell'intestazione dello script sono disponibili informazioni sulla versione del motore (ev), sulla versione dell'interfaccia utente (gv) e sulla versione del rapporto (lv). Questi dati possono essere utilizzati per tenere traccia delle possibili variazioni nel file XML che genera lo script e prevenire eventuali incoerenze durante l'esecuzione. Non modificare questa parte dello script.

La restante parte del file è suddivisa in sezioni in cui è possibile modificare gli elementi (indicare quelli che saranno elaborati dallo script). È possibile contrassegnare gli elementi da elaborare sostituendo il carattere "-" davanti a un elemento con il carattere "+". Le sezioni dello script sono separate tra loro mediante una riga vuota. A ogni sezione viene assegnato un numero e un titolo.

01) Processi in esecuzione

Questa sezione contiene un elenco di tutti i processi in esecuzione nel sistema. Ogni processo è identificato mediante il proprio percorso UNC e, successivamente, dal rispettivo codice hash CRC16 tra asterischi (*).

Esempio:

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Nell'esempio, è stato selezionato un processo, module32.exe (contrassegnato dal carattere "+"). Il processo

terminerà all'esecuzione dello script.

02) Moduli caricati

In questa sezione sono contenuti i moduli di sistema attualmente in uso.

Esempio:

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Nell'esempio, il modulo khbekhb.dll è stato contrassegnato con "+". All'esecuzione dello script, i processi che eseguono tale modulo specifico verranno riconosciuti e interrotti.

03) Connessioni TCP

Questa sezione contiene informazioni sulle connessioni TCP esistenti.

Esempio:

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

All'esecuzione dello script, verrà individuato il proprietario del socket nelle connessioni TCP contrassegnate e il socket verrà interrotto, liberando le risorse del sistema.

04) Endpoint UDP

Questa sezione contiene informazioni sugli endpoint UDP esistenti.

Esempio:

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

All'esecuzione dello script, verrà isolato il proprietario del socket sugli endpoint UDP contrassegnati e il socket verrà interrotto.

05) Voci server DNS

Questa sezione contiene informazioni sulla configurazione del server DNS corrente.

Esempio:

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

All'esecuzione dello script, le voci del server DNS contrassegnate verranno rimosse.

06) Voci importanti del Registro di sistema

Questa sezione contiene informazioni su importanti voci del Registro di sistema.

Esempio:

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

All'esecuzione dello script, le voci contrassegnate verranno eliminate, ridotte a valori a 0 byte o ripristinate sui valori predefiniti. L'azione da eseguire su una particolare voce dipende dalla categoria della voce stessa e dal valore principale nel Registro di sistema specifico.

07) Servizi

In questa sezione sono riportati i servizi registrati all'interno del sistema.

Esempio:

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

All'esecuzione dello script, i servizi contrassegnati e i relativi servizi dipendenti verranno interrotti e disinstallati.

08) Driver

In questa sezione sono riportati i driver installati.

Esempio:

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Quando si esegue lo script, i driver selezionati verranno arrestati. Tenere presente che alcuni driver non possono essere arrestati.

09) File critici

Questa sezione contiene informazioni sui file critici per il corretto funzionamento del sistema operativo.

Esempio:

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Gli elementi selezionati saranno eliminati o ripristinati sui valori originali.

5.6.4.3 Esecuzione degli script di servizio

Contrassegnare tutti gli elementi desiderati, quindi salvare e chiudere lo script. Eseguire lo script modificato direttamente dalla finestra principale di ESET SysInspector selezionando l'opzione **Esegui script di servizio** dal menu File. All'apertura di uno script, verrà visualizzato il seguente messaggio: **Eseguire lo script di servizio "%Scriptname %"?** Dopo aver confermato, verrà visualizzato un altro messaggio per segnalare che lo script di servizio che si sta cercando di eseguire non è stato firmato. Fare clic su **Esegui** per avviare lo script.

Verrà visualizzata una finestra di dialogo per confermare la corretta esecuzione dello script.

Se lo script è stato eseguito solo parzialmente, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio è stato eseguito parzialmente. Visualizzare il rapporto degli errori?** Selezionare **Sì** per visualizzare un rapporto completo degli errori in cui sono indicate le operazioni non eseguite.

Se lo script non viene riconosciuto, verrà visualizzata una finestra di dialogo contenente il seguente messaggio: **Lo script di servizio selezionato non è firmato. L'esecuzione di script sconosciuti o non firmati potrebbe causare seri danni ai dati nel computer. Eseguire lo script e le azioni?** Ciò potrebbe essere causato da incoerenze all'interno dello script (intestazione danneggiata, titolo della sezione danneggiato, linea vuota tra le sezioni e così via). È possibile riaprire il file script e correggere gli errori all'interno dello script o creare un nuovo script di servizio.

5.6.5 Domande frequenti

ESET SysInspector richiede privilegi di amministratore per l'esecuzione?

Anche se per eseguire ESET SysInspector non sono necessari privilegi di amministratore, alcune informazioni raccolte possono essere visualizzate solo da un account amministratore. Eseguendo il programma come utente standard o utente con restrizioni, si raccoglieranno meno informazioni sull'ambiente operativo in uso.

ESET SysInspector crea un file di rapporto?

ESET SysInspector può creare un file di rapporto della configurazione del proprio computer. Per salvarne uno, fare clic su **File** > **Salva rapporto** nella finestra principale del programma. I rapporti vengono salvati nel formato XML. Per impostazione predefinita, i file vengono salvati nella directory *%USERPROFILE%\Documenti*, con una convenzione di denominazione file "SysInpsector-%COMPUTERNAME%-AAMMGG-HHMM.XML". Se preferibile, è possibile modificare la posizione e il nome del file di rapporto prima di salvarlo.

Come si visualizza il file di rapporto di ESET SysInspector?

Per visualizzare un file di rapporto creato da ESET SysInspector, eseguire il programma e fare clic su **File** > **Apri rapporto** nella finestra principale del programma. È anche possibile trascinare i file di rapporto all'interno dell'applicazione ESET SysInspector. Se è necessario consultare frequentemente i file di rapporto di ESET SysInspector, è consigliabile creare un collegamento sul Desktop al file SYSINSPECTOR.EXE, quindi sarà sufficiente trascinare i file di rapporto sopra di esso per poterli visualizzare. Per motivi di protezione, in Windows Vista/7 la funzione di trascinamento della selezione tra finestre con differenti autorizzazioni di protezione potrebbe non

essere disponibile.

È disponibile una specifica per il formato del file di rapporto? E per quanto riguarda un SDK?

Attualmente non è disponibile né una specifica per il file di rapporto né un SDK, in quanto il programma è ancora in fase di sviluppo. Dopo il rilascio del programma, potrebbero essere forniti sulla base dei commenti e delle richieste dei clienti.

In che modo ESET SysInspector valuta il rischio di un determinato oggetto?

Nella maggior parte dei casi, ESET SysInspector assegna livelli di rischio agli oggetti (file, processi, chiavi di registro, ecc.), utilizzando una serie di regole euristiche che esaminano le caratteristiche di ogni oggetto e quindi ne valutano le potenzialità come attività dannosa. Sulla base di tali euristiche, agli oggetti viene assegnato un livello di rischio da 1 - Non a rischio (verde) a 9 - A rischio (rosso). Nel riquadro di spostamento a sinistra, le sezioni sono colorate sulla base del livello di rischio più elevato di un oggetto al loro interno.

Un livello di rischio "6 - Sconosciuto (rosso)" significa che un oggetto è pericoloso?

Le valutazioni di ESET SysInspector non garantiscono che un oggetto sia dannoso. Questa affermazione dovrebbe essere eseguita da un esperto di sicurezza. ESET SysInspector è progettato per fornire una rapida valutazione agli esperti di sicurezza, in modo da informarli su quali oggetti del sistema potrebbero richiedere una loro ulteriore analisi in presenza di comportamento anomalo.

Perché ESET SysInspector si collega a Internet quando viene avviato?

Al pari di molte applicazioni, ESET SysInspector è provvisto di firma digitale, un certificato che garantisce la pubblicazione del software da parte di ESET e l'assenza di alterazione dello stesso. Al fine di verificare il certificato, il sistema operativo contatta un'autorità di certificazione per verificare l'identità dell'autore del software. Si tratta di una procedura comune eseguita su tutti i programmi con firma digitale eseguiti in Microsoft Windows.

Cos'è la tecnologia Anti-Stealth?

La tecnologia Anti-Stealth assicura un efficace rilevamento di rootkit.

Se il sistema viene attaccato da codice dannoso che si comporta come un rootkit, l'utente può essere esposto al rischio di perdita o furto dei dati. In assenza di uno strumento speciale anti-rootkit, è quasi impossibile rilevarli.

Perché a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente?

Quando si cerca di identificare la firma digitale di un file eseguibile, ESET SysInspector verifica innanzitutto se nel file è incorporata una firma digitale. Se viene trovata una firma digitale, il file verrà convalidato usando tali informazioni. Se la firma digitale non viene trovata, ESI inizia a ricercare il file CAT corrispondente (Catalogo di protezione - *%systemroot%\system32\catroot*) contenente informazioni sul file eseguibile elaborato. Nel caso in cui dovesse trovare il file CAT appropriato, nel processo di convalida del file eseguibile verrà applicata la firma digitale di tale file CAT.

Per tale motivo, a volte i file contrassegnati come "Firmati da MS", hanno contemporaneamente un "Nome aziendale" differente.

Esempio:

Windows 2000 include l'applicazione HyperTerminal nel percorso *C:\Programmi\Windows NT*. Il file eseguibile dell'applicazione principale non è firmato a livello digitale, ma ESET SysInspector lo contrassegna come file firmato da Microsoft. Ciò dipende da un riferimento in *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* che punta a *C:\Programmi\Windows NT\hypertrm.exe* (il principale file eseguibile dell'applicazione HyperTerminal) e *sp4.cat* è firmato a livello digitale da Microsoft.

5.6.6 ESET SysInspector come componente di ESET NOD32 Antivirus

Per aprire la sezione ESET SysInspector in ESET NOD32 Antivirus, fare clic su **Strumenti** > **ESET SysInspector**. Il sistema di gestione della finestra di ESET SysInspector è simile a quello dei rapporti di scansione del computer o delle attività pianificate. Tutte le operazioni con gli snapshot del sistema (crea, visualizza, confronta, rimuovi ed esporta) sono accessibili con pochi clic.

La finestra di ESET SysInspector contiene informazioni di base sugli snapshot creati, quali data e ora di creazione, breve commento, nome dell'utente che ha creato lo snapshot e stato dello snapshot.

Per eseguire il confronto, la creazione o l'eliminazione degli snapshot, utilizzare i pulsanti corrispondenti nella parte inferiore della finestra di ESET SysInspector. Quelle opzioni sono disponibili anche dal menu contestuale. Per visualizzare lo snapshot di sistema selezionato, scegliere **Mostra** dal menu contestuale. Per esportare lo snapshot selezionato in un file, fare clic con il pulsante destro del mouse, quindi selezionare **Esporta...**.

Di seguito viene fornita una descrizione dettagliata delle opzioni disponibili:

- **Confronta** - Consente di confrontare due rapporti esistenti. È idonea se si desidera rilevare le modifiche tra il rapporto attuale e uno precedente. Per utilizzare questa opzione, selezionare due snapshot da mettere a confronto.
- **Crea...** - Consente di creare un nuovo record. È prima necessario inserire un breve commento sul record. Per visualizzare lo stato di avanzamento della procedura di creazione dello snapshot (relativamente allo snapshot in corso di generazione), fare riferimento alla colonna **Stato**. Tutti gli snapshot completati sono contrassegnati dallo stato **Creato**.
- **Elimina/Elimina tutto** - Consente di rimuovere le voci dall'elenco.
- **Esporta...** - Salva la voce selezionata in un file XML (anche in una versione compressa).

5.7 ESET SysRescue

ESET SysRescue è un'utilità che consente di creare un disco di avvio contenente una delle soluzioni ESET Security: può essere ESET NOD32 Antivirus, ESET Smart Security o anche uno dei prodotti per server. Il vantaggio principale offerto da ESET SysRescue consiste nel fatto che la soluzione ESET Security viene eseguita indipendentemente dal sistema operativo che la ospita e, al tempo stesso, dispone dell'accesso diretto al disco e all'intero file system. Ciò consente di rimuovere infiltrazioni che non sarebbe stato possibile eliminare in una situazione ordinaria, ad esempio durante l'esecuzione del sistema operativo.

5.7.1 Requisiti minimi

ESET SysRescue è eseguibile su Microsoft Windows Preinstallation Environment (Windows PE) versione 2.x, basato su Windows Vista.

Poiché Windows PE è incluso nel pacchetto gratuito Windows Automated Installation Kit (Windows AIK) o Windows Assesment and Deployment Kit (WADK), questi ultimi devono essere installati prima di procedere alla creazione di ESET SysRescue (http://go.eset.eu/AIK, http://www.microsoft.com/en-us/download/details.aspx?id=30652). La scelta di uno di questi pacchetti dipende dalla versione del sistema operativo. A causa del supporto della versione a 32 bit di Windows PE, è necessario utilizzare un pacchetto di installazione della soluzione ESET Security a 32 bit durante la creazione di ESET SysRescue su sistemi a 64 bit. ESET SysRescue supporta Windows AIK 1.1 e versioni successive, nonché WADK 1.0 e versioni successive.

Per effettuare l'installazione di Windows ADK, scegliere di installare esclusivamente gli strumenti di distribuzione di pacchetti e l'ambiente di preinstallazione di Windows (Windows PE). Poiché questi pacchetti hanno dimensioni superiori a 3,0 GB, per il download si consiglia una connessione a Internet ad alta velocità.

ESET SysRescue è disponibile nelle soluzioni ESET Security 4.0 e versioni successive.

Windows ADK supporta:

- Windows 8
- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2

Nota: ESET SysRescue potrebbe non essere disponibile per Windows 8 in versioni precedenti di prodotti di protezione ESET. In questo caso, si consiglia di effettuare l'upgrade del prodotto o di creare un disco ESET SysRescue su un'altra versione di Microsoft Windows.

Windows AIK supporta:

- Windows 7
- Windows Vista
- Windows XP Service Pack 2 con KB926044
- Windows XP Service Pack 3

5.7.2 Come creare un CD di ripristino

Per avviare la procedura guidata di ESET SysRescue, fare clic su **Start** > **Programmi** > **ESET** > **ESET NOD32 Antivirus** > **ESET SysRescue**.

Innanzitutto, la procedura guidata ricerca Windows AIK o ADK e un dispositivo adatto alla creazione di un supporto di avvio. Se Windows AIK o ADK non è installato sul computer (o è danneggiato o installato in modo errato), la procedura guidata consentirà di installarlo o di inserire il percorso della cartella di Windows AIK o ADK (http://go.eset.eu/AIK, http://www.microsoft.com/en-us/download/details.aspx?id=30652).

NOTA: poiché Windows AIK è superiore a 1 GB, per il download è necessaria una connessione a Internet ad alta velocità.

Per effettuare l'installazione di Windows ADK, scegliere di installare esclusivamente gli strumenti di distribuzione di pacchetti e l'ambiente di preinstallazione di Windows (Windows PE). Poiché questi pacchetti hanno dimensioni superiori a 3,0 GB, per il download è necessaria una connessione a Internet ad alta velocità.

Al passaggio successivo, selezionare il supporto di destinazione in cui si desidera posizionare ESET SysRescue.

5.7.3 Selezione delle destinazioni

Oltre che su CD/DVD/USB, è possibile scegliere di salvare ESET SysRescue anche in un file ISO. Successivamente, sarà possibile masterizzare l'immagine ISO su un CD/DVD o utilizzarla in altro modo (ad esempio, in ambienti virtuali quali VmWare o Virtualbox).

Se è stato selezionato il dispositivo USB come supporto di destinazione, è possibile che su alcuni computer non sia possibile eseguire l'avvio. Alcune versioni del BIOS possono riportare problemi di comunicazione con Boot manager (ad esempio, con Windows Vista) e durante l'avvio vengono visualizzati i seguenti messaggi di errore:

```
file : \boot\bcd
stato : 0xc000000e
informazioni : si è verificato un errore durante il tentativo di leggere i dati della configurazione di avvi
```

Nel caso si verificasse questo tipo di errore, si consiglia di selezionare un supporto CD anziché USB.

5.7.4 Impostazioni

Prima di avviare la creazione di ESET SysRescue, nella procedura di installazione guidata vengono visualizzati i parametri di compilazione. Tali parametri possono essere modificati facendo clic sul pulsante **Cambia...**. Le opzioni disponibili includono:

- Cartelle
- Antivirus ESET
- Avanzate
- Protocollo Internet
- Supporto USB di avvio (quando è selezionato il supporto USB di destinazione)
- Masterizzazione (quando è selezionata l'unità CD/DVD di destinazione)

L'opzione **Crea** rimane inattiva se non viene specificato alcun pacchetto di installazione MSI o se nel computer non viene installata alcuna soluzione ESET Security. Per selezionare un pacchetto di installazione, fare clic su **Cambia**, quindi sulla scheda **ESET Antivirus**. Se non si inseriscono nome utente e password (**Cambia** > **ESET Antivirus**), l'opzione **Crea** non è disponibile.

5.7.4.1 Cartelle

La **Cartella temporanea** è una cartella di lavoro per i file richiesti per la compilazione di ESET SysRescue.

Cartella ISO è una cartella in cui vengono salvati, al termine della compilazione, i file ISO.

L'elenco presente in questa scheda riporta tutti i dischi di rete locali e mappati insieme allo spazio disponibile residuo. Se alcune cartelle si trovano in un disco che non dispone di spazio sufficiente, si consiglia di selezionare un disco alternativo che disponga di maggiore spazio. In caso contrario, è possibile che la compilazione si interrompa in modo anomalo a causa della mancanza di spazio libero su disco.

Applicazioni esterne - Consente di specificare programmi aggiuntivi che saranno eseguiti o installati dopo il riavvio da un supporto ESET SysRescue.

Includi applicazioni esterne - Consente di aggiungere programmi esterni alla compilazione di ESET SysRescue.

Cartella selezionata - Cartella in cui si trovano i programmi da aggiungere al disco di ESET SysRescue.

5.7.4.2 Antivirus ESET

Per la creazione del CD ESET SysRescue, è possibile scegliere tra due origini di file ESET utilizzabili dal compilatore:

Cartella ESS/EAV - File già contenuti nella cartella da cui la soluzione ESET Security è stata installata nel computer.

File MSI - Vengono utilizzati i file contenuti nel programma di installazione di MSI.

È quindi possibile scegliere di aggiornare il percorso dei file (nup). Normalmente deve essere selezionata l'opzione predefinita **Cartella ESS/EAV/File MSI**. In alcuni casi, è possibile scegliere una **Cartella di aggiornamento** personalizzata, ad esempio per utilizzare una versione precedente o più recente del database delle firme antivirali.

È possibile utilizzare una delle due origini seguenti di nome utente e password:

ESS/EAV installato - Il nome utente e la password saranno copiati dalla soluzione ESET Security attualmente installata.

Da utente - Verranno utilizzati il nome utente e la password inseriti nei campi corrispondenti.

NOTA: La soluzione ESET Security su ESET SysRescue CD viene aggiornata da Internet o dalla soluzione ESET Security installata nel computer sul quale è in esecuzione ESET SysRescue CD.

5.7.4.3 Impostazioni avanzate

La scheda **Avanzate** consente di ottimizzare ESET SysRescue CD rispetto alle dimensioni della memoria del computer. Selezionare **576 MB o più** per scrivere il contenuto del CD nella memoria operativa (RAM). Se si seleziona **meno di 576 MB**, durante l'esecuzione di WinPE sarà sempre possibile accedere al CD di ripristino.

Nella sezione **Driver esterni** è possibile immettere i driver per gli hardware specifici utilizzati dall'utente (in genere, la scheda di rete). Sebbene WinPE sia basato su Windows Vista SP1, che supporta un'ampia gamma di hardware, talvolta l'hardware non viene riconosciuto. È quindi necessario aggiungere il driver manualmente. Esistono due modi per introdurre un driver nella compilazione di ESET SysRescue: manualmente (fare clic su **Aggiungi**) e automaticamente (fare clic su **Ricerca aut.**). In caso di introduzione manuale, è necessario selezionare il percorso del file .inf corrispondente (è inoltre necessario che in questa cartella sia presente il file *.sys applicabile). In caso di introduzione automatica, il driver viene rilevato automaticamente nel sistema operativo di un determinato computer. Si consiglia di utilizzare l'introduzione automatica unicamente se ESET SysRescue viene utilizzato su un computer che dispone della stessa scheda di rete utilizzata dal computer in cui è stato creato ESET SysRescue CD. Durante la creazione, il driver di ESET SysRescue viene introdotto nella compilazione in modo tale che l'utente non debba cercarlo in seguito.

5.7.4.4 Protocollo Internet

Questa sezione consente di configurare le impostazioni di rete di base e le connessioni predefinite dopo aver eseguito ESET SysRescue.

Selezionare **Indirizzo IP privato automatico** per ottenere l'indirizzo IP automaticamente dal server DHCP (Dynamic Host Configuration Protocol).

In alternativa, questa connessione di rete può utilizzare un indirizzo IP specificato a livello manuale, anche noto come indirizzo IP statico. Selezionare **Personalizzato** per configurare le impostazioni IP appropriate. Se si seleziona questa opzione, è necessario specificare un **Indirizzo IP** e, per le connessioni LAN e Internet ad alta velocità, una **Maschera subnet**. In **Server DNS preferito** e **Server DNS alternativo**, digitare gli indirizzi del server DNS primario e secondario.

5.7.4.5 Dispositivo USB di avvio

Se è stato selezionato il dispositivo USB come supporto di destinazione, è possibile selezionare uno dei supporti USB disponibili nella scheda **Dispositivo USB di avvio** (nel caso siano presenti più dispositivi USB).

Selezionare il **Dispositivo** di destinazione appropriato sul quale verrà installato ESET SysRescue.

Avviso: durante la creazione di ESET SysRescue, il supporto USB selezionato verrà formattato. Tutti i dati sul supporto verranno cancellati.

Se si seleziona **Formattazione rapida**, la formattazione rimuove tutti i file dalla partizione ma non esegue il controllo del disco alla ricerca di settori errati. Usare questa opzione se il supporto USB è stato precedentemente formattato e si è certi che non sia danneggiato.

5.7.4.6 Masterizza

Se il supporto di destinazione selezionato è CD/DVD, è possibile specificare parametri aggiuntivi di masterizzazione nella scheda **Masterizza**.

Elimina file ISO - Selezionare per eliminare il file ISO temporaneo dopo la creazione del ESET SysRescue.

Eliminazione attivata - Consente di selezionare le opzioni per l'eliminazione rapida e completa.

Dispositivo di masterizzazione - Selezionare l'unità da utilizzare per la masterizzazione.

Attenzione: questa è l'opzione predefinita. Se viene utilizzato un CD/DVD riscrivibile, tutti i dati in esso contenuti verranno eliminati.

La sezione Supporto contiene informazioni sul supporto nel dispositivo CD/DVD in uso.

Velocità di masterizzazione - Selezionare la velocità desiderata dal menu a discesa. Quando si seleziona la velocità di masterizzazione è necessario tener conto delle capacità del dispositivo di masterizzazione e del tipo di CD/DVD utilizzati.

5.7.5 Utilizzo di ESET SysRescue

Affinché il CD/DVD/USB di ripristino funzioni in maniera ottimale, è necessario avviare il computer dal supporto ESET SysRescue. È possibile modificare la priorità di avvio nel BIOS. In alternativa, è possibile utilizzare il menu di avvio durante l'inizializzazione del computer. In genere si utilizzano i tasti F9 o F12 a seconda della versione della scheda madre/BIOS in uso.

Dopo l'avvio dal supporto di avvio, la soluzione ESET Security viene inizializzata. Poiché ESET SysRescue viene utilizzato solo in situazioni specifiche, non è richiesto l'utilizzo di alcuni moduli di protezione e di alcune funzioni del programma disponibili nella versione standard della soluzione ESET Security. L'elenco di tali funzioni e moduli è limitato alle operazioni di **Controllo del computer**, **Aggiorna** e alcune sezioni in **Configurazione** e **Strumenti**. La funzionalità più importante di ESET SysRescue è la capacità di aggiornare il database delle firme antivirali. Prima di avviare un controllo del computer, è pertanto consigliabile eseguire un aggiornamento del programma.

5.7.5.1 Utilizzo di ESET SysRescue

Si supponga che i computer nella rete siano stati infettati da un virus che modifica i file eseguibili (EXE). La soluzione ESET Security è in grado di pulire tutti i file infetti ad eccezione di *explorer.exe*, che non può essere pulito neanche in modalità sicura. Ciò dipende dal fatto che anche *explorer.exe*, in qualità di uno dei processi Windows essenziali, viene lanciato in modalità sicura. La soluzione ESET Security non riuscirebbe ad eseguire alcuna azione sul file che rimarrebbe quindi infettato.

In questo tipo di scenario, è possibile usare ESET SysRescue per risolvere il problema. ESET SysRescue non richiede l'utilizzo di alcun componente del sistema operativo che lo ospita ed è pertanto in grado di elaborare (pulire, eliminare) qualsiasi file sul disco.

5.8 Riga di comando

Il modulo antivirus di ESET NOD32 Antivirus può essere avviato dalla riga di comando, manualmente con il comando "ecls" oppure con un file batch ("bat"). Utilizzo dello scanner della riga di comando ESET:

```
ecls [OPTIONS..] FILES..
```

È possibile utilizzare i parametri e le opzioni riportati di seguito quando viene eseguita una scansione su richiesta dalla riga di comando:

Opzioni

/base-dir=FOLDER	carica moduli da CARTELLA
/quar-dir=FOLDER	CARTELLA di quarantena
/exclude=MASK	escludi dalla scansione i file corrispondenti a MASCHERA
/subdir	esegui controllo delle sottocartelle (impostazione predefinita)
/no-subdir	non eseguire controllo delle sottocartelle
/max-subdir-level=LEVEL	sottolivello massimo delle cartelle all'interno di cartelle su cui eseguire la scansione
/symlink	segui i collegamenti simbolici (impostazione predefinita)
/no-symlink	ignora collegamenti simbolici
/ads	esegui la scansione di ADS (impostazione predefinita)
/no-ads	non eseguire la scansione di ADS
/log-file=FILE	registra output nel FILE
/log-rewrite	sovrascrivi il file di output (impostazione predefinita: aggiungi)
/log-console	registra l'output nella console (impostazione predefinita)
/no-log-console	non registrare l'output nella console
/log-all	registra anche file puliti
/no-log-all	non registrare file puliti (impostazione predefinita)
/aind	mostra indicatore di attività
/auto	controlla e disinfetta automaticamente tutti i dischi locali

Opzioni scanner

/files	esegui controllo dei file (impostazione predefinita)
/no-files	non eseguire controllo dei file
/memory	esegui scansione della memoria
/boots	esegui la scansione dei settori di avvio
/no-boots	non eseguire la scansione dei settori di avvio (impostazione predefinita)
/arch	esegui controllo degli archivi (impostazione predefinita)
/no-arch	non eseguire controllo degli archivi
/max-obj-size=SIZE	esegui solo la scansione dei file inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/max-arch-level=LEVEL	sottolivello massimo degli archivi all'interno di archivi (archivi nidificati) su cui eseguire la scansione
/scan-timeout=LIMIT	esegui scansione degli archivi per LIMITE secondi al massimo
/max-arch-size=SIZE	esegui la scansione dei file di un archivio solo se inferiori a DIMENSIONE (impostazione predefinita 0 = illimitato)
/max-sfx-size=SIZE	esegui la scansione dei file di un archivio autoestraente solo se inferiori a DIMENSIONE megabyte (impostazione predefinita 0 = illimitato)
/mail	esegui la scansione dei file di e-mail (impostazione predefinita)
/no-mail	non eseguire controllo dei file di e-mail
/mailbox	esegui la scansione delle caselle di posta (impostazione predefinita)
/no-mailbox	non eseguire la scansione delle caselle di posta
/sfx	esegui la scansione degli archivi autoestraenti (impostazione predefinita)
/no-sfx	non eseguire controllo degli archivi autoestraenti
/rtp	esegui la scansione degli eseguibili compressi (impostazione predefinita)
/no-rtp	non eseguire la scansione degli eseguibili compressi
/adware	esegui la scansione di Adware/Spyware/Riskware (impostazione predefinita)
/no-adware	non eseguire la scansione di Adware/Spyware/Riskware
/unsafe	esegui la scansione delle applicazioni potenzialmente pericolose
/no-unsafe	non eseguire la scansione delle applicazioni potenzialmente pericolose (impostazione predefinita)
/unwanted	esegui la scansione delle applicazioni potenzialmente indesiderate
/no-unwanted	non eseguire la scansione delle applicazioni potenzialmente indesiderate (impostazione predefinita)
/pattern	utilizza le firme digitali (impostazione predefinita)
/no-pattern	non utilizzare le firme digitali
/heur	attiva l'euristica (impostazione predefinita)
/no-heur	disattiva l'euristica
/adv-heur	attiva l'euristica avanzata (impostazione predefinita)
/no-adv-heur	disattiva l'euristica avanzata
/ext=EXTENSIONS	esegui scansione solo di ESTENSIONI delimitate da due punti
/ext-exclude=EXTENSIONS	escludi dal controllo le ESTENSIONI delimitate da due punti
/clean-mode=MODE	utilizza la MODALITÀ pulitura per gli oggetti infetti. Opzioni disponibili: nessuna, standard (valore predefinito), massima, rigorosa, eliminazione
/quarantena	copiare i file infettati (se puliti) in Quarantena (integra l'azione eseguita durante la pulizia)
/no-quarantena	non copiare file infettati in Quarantena

Opzioni generali

/help	mostra guida ed esci
/version	mostra informazioni sulla versione ed esci
/preserve-time	mantieni indicatore data e ora dell'ultimo accesso

Codici di uscita

0	nessuna minaccia rilevata

1	minaccia rilevata e pulita
10	impossibile controllare alcuni file (potrebbero essere minacce)
50	trovata minaccia
100	errore

NOTA: i codici di uscita superiori a 100 indicano che non è stata eseguita la scansione del file, il quale potrebbe quindi essere infetto.

6. Glossario

6.1 Tipi di infiltrazioni

Un'infiltrazione è una parte di software dannoso che tenta di entrare e/o danneggiare il computer di un utente.

6.1.1 Virus

Un virus è un pezzo di codice dannoso che è pre-incorporato o viene aggiunto ai file esistenti nel computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro. Il termine "virus" viene spesso utilizzato in maniera errata per indicare qualsiasi tipo di minaccia. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

I virus attaccano principalmente i file eseguibili e i documenti. In breve, un virus funziona nel seguente modo: dopo aver eseguito un file infetto, il codice dannoso viene chiamato ed eseguito prima dell'esecuzione dell'applicazione originale. Un virus può infettare qualsiasi file sul quale l'utente corrente dispone dei diritti di scrittura.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché sono in grado di eliminare deliberatamente i file da un disco rigido. Altri, invece, non causano veri e propri danni, poiché il loro scopo consiste esclusivamente nell'infastidire l'utente e dimostrare le competenze tecniche dei rispettivi autori.

Se il computer è stato infettato da un virus e non è possibile rimuoverlo, inviarlo ai laboratori ESET ai fini di un esame accurato. In alcuni casi, i file infetti possono essere modificati a un livello tale da impedirne la pulizia. In questo caso, è necessario sostituire i file con una copia non infetta.

6.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite la rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di propagarsi autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi e-mail all'interno della lista dei contatti degli utenti oppure sfruttano le vulnerabilità delle applicazioni di rete.

I worm sono pertanto molto più attivi rispetto ai virus. Grazie all'ampia disponibilità di connessioni Internet, possono espandersi in tutto il mondo entro poche ore o persino pochi minuti dal rilascio. Questa capacità di replicarsi in modo indipendente e rapido li rende molto più pericolosi rispetto ad altri tipi di malware.

Un worm attivato in un sistema può provocare diversi inconvenienti: può eliminare file, ridurre le prestazioni del sistema e perfino disattivare programmi. La sua natura lo qualifica come "mezzo di trasporto" per altri tipi di infiltrazioni.

Se il computer è infettato da un worm, si consiglia di eliminare i file infetti poiché è probabile che contengano codice dannoso.

6.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di minacce che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli così a eseguirli.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- **Downloader** - Programmi dannosi in grado di scaricare altre minacce da Internet.
- **Dropper** - Programmi dannosi in grado di installare sui computer compromessi altri tipi di malware.
- **Backdoor** - Programmi dannosi che comunicano con gli autori degli attacchi remoti, consentendo loro di ottenere l'accesso al computer e assumerne il controllo.
- **Keylogger** (registratore delle battute dei tasti) - Un programma che registra ogni battuta di tasto effettuata da un utente e che invia le informazioni agli autori degli attacchi remoti.
- **Dialer** - Programmi dannosi progettati per connettersi a numeri con tariffe telefoniche molto elevate anziché ai

provider dei servizi Internet dell'utente. È quasi impossibile che un utente noti che è stata creata una nuova connessione. I dialer possono causare danni solo agli utenti con connessione remota che ormai viene utilizzata sempre meno frequentemente.

Se sul computer in uso viene rilevato un trojan horse, si consiglia di eliminarlo, poiché probabilmente contiene codice dannoso.

6.1.4 Rootkit

I rootkit sono programmi dannosi che forniscono agli autori degli attacchi su Internet l'accesso illimitato a un sistema, nascondendo tuttavia la loro presenza. I rootkit, dopo aver effettuato l'accesso a un sistema (di norma, sfruttando una vulnerabilità del sistema), utilizzano le funzioni del sistema operativo per non essere rilevate dal software antivirus: nascondono i processi, i file e i dati del Registro di sistema di Windows. Per tale motivo, è quasi impossibile rilevarli utilizzando le tradizionali tecniche di testing.

Per bloccare i rootkit, sono disponibili due livelli di rilevamento:

1. Quando tentano di accedere ad un sistema: Non sono ancora presenti e pertanto sono inattivi. La maggior parte dei sistemi antivirus è in grado di eliminare i rootkit a questo livello (presupponendo che riescano effettivamente a rilevare tali file come infetti).
2. Quando sono nascosti dal normale testing: ESET NOD32 Antivirus gli utenti hanno il vantaggio di poter utilizzare la tecnologia Anti-Stealth che è in grado di rilevare ed eliminare anche i rootkit attivi.

6.1.5 Adware

Adware è l'abbreviazione di software con supporto della pubblicità (advertising-supported software). Rientrano in questa categoria i programmi che visualizzano materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenenti pubblicità all'interno di un browser Internet oppure ne modificano la pagina iniziale. I programmi adware vengono spesso caricati insieme a programmi freeware, che consentono ai loro sviluppatori di coprire i costi di sviluppo delle applicazioni che, in genere, sono molto utili.

L'adware non è di per sé pericoloso, anche se gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento e registrazione, al pari dei programmi spyware.

Se si decide di utilizzare un prodotto freeware, è opportuno prestare particolare attenzione al programma di installazione. Nei programmi di installazione viene in genere visualizzata una notifica dell'installazione di un programma adware aggiuntivo. Spesso è possibile annullarla e installare il programma senza adware.

Alcuni programmi non vengono installati senza adware. In caso contrario, le rispettive funzionalità saranno limitate. Ciò significa che l'adware potrebbe accedere di frequente al sistema in modo "legale", poiché l'utente ne ha dato il consenso. In questi casi, vale il proverbio secondo il quale la prudenza non è mai troppa. Se in un computer viene rilevato un file adware, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

6.1.6 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/consapevolezza dell'utente. Gli spyware si avvalgono di funzioni di monitoraggio per inviare dati statistici di vario tipo, tra cui un elenco dei siti Web visitati, indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che lo scopo di tali tecniche è raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è legato al fatto che non esiste una distinzione chiara tra applicazioni utili e dannose e che nessuno può essere sicuro del fatto che le informazioni raccolte verranno utilizzate correttamente. I dati ottenuti dalle applicazioni spyware possono contenere codici di sicurezza, PIN, numeri di conti bancari e così via. I programmi spyware sono frequentemente accoppiati a versioni gratuite di un programma creato dal relativo autore per generare profitti o per offrire un incentivo all'acquisto del software. Spesso, gli utenti sono informati della presenza di un'applicazione spyware durante l'installazione di un programma che li esorta a eseguire l'aggiornamento a una versione a pagamento che non lo contiene.

Esempi di prodotti freeware noti associati a programmi spyware sono le applicazioni client delle reti P2P (peer-to-

peer). Spyfalcon o Spy Sheriff (e molti altri ancora) appartengono a una sottocategoria di spyware specifica, poiché si fanno passare per programmi antispyware ma in realtà sono essi stessi applicazioni spyware.

Se in un computer viene rilevato un file spyware, è consigliabile eliminarlo in quanto è molto probabile che contenga codice dannoso.

6.1.7 Programmi di compressione

Un programma di compressione è un eseguibile compresso autoestraente che riunisce vari tipi di malware in un unico pacchetto.

I programmi di compressione più comuni sono UPX, PE_Compact, PKLite e ASPack. Lo stesso malware può essere rilevato in modo diverso se compresso mediante l'utilizzo di un programma di compressione diverso. I programmi di compressione sono anche in grado di mutare le proprie "firme" nel tempo, rendendo più complessi il rilevamento e la rimozione dei malware.

6.1.8 Applicazioni potenzialmente pericolose

Esistono molti programmi legali utili per semplificare l'amministrazione dei computer in rete. Tuttavia, nelle mani sbagliate, possono essere utilizzati per scopi illegittimi. ESET NOD32 Antivirus offre la possibilità di rilevare tali minacce.

Applicazioni potenzialmente pericolose è la classificazione utilizzata per il software legale e commerciale. Questa classificazione include programmi quali strumenti di accesso remoto, applicazioni di password cracking e applicazioni di keylogging (programmi che registrano tutte le battute dei tasti premuti da un utente).

Se si rileva la presenza di un'applicazione potenzialmente pericolosa in esecuzione sul computer (che non è stata installata dall'utente) rivolgersi all'amministratore di rete o rimuovere l'applicazione.

6.1.9 Applicazioni potenzialmente indesiderate

Le **applicazioni potenzialmente indesiderate** (PUA) non sono necessariamente dannose. Potrebbero tuttavia influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso prima dell'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- Nuove finestre mai visualizzate in precedenza (popup, annunci pubblicitari)
- Attivazione ed esecuzione di processi nascosti
- Maggiore utilizzo delle risorse del sistema
- Modifiche dei risultati di ricerca
- Applicazioni che comunicano con server remoti.

6.2 Tecnologia ESET

6.2.1 Exploit Blocker

L'Exploit Blocker è progettato per rafforzare i tipi di applicazione comunemente utilizzati come browser Web, lettori PDF, client di posta e componenti di MS Office. Il sistema si basa sul monitoraggio del comportamento dei processi ai fini del rilevamento di attività sospette che potrebbero indicare un exploit.

Nel momento in cui l'Exploit Blocker identifica un processo sospetto, lo interrompe immediatamente e registra i dati relativi alla minaccia, che vengono quindi inviati al sistema cloud di ESET Live Grid. Le informazioni vengono elaborate dal laboratorio delle minacce ESET e utilizzate ai fini di una maggiore protezione degli utenti contro minacce sconosciute e attacchi zero-day (malware di nuova concezione per i quali non sono disponibili soluzioni preconfigurate).

6.2.2 Scanner memoria avanzato

Lo Scanner memoria avanzato lavora congiuntamente all'Exploit Blocker per rafforzare il livello di protezione contro malware concepiti allo scopo di eludere il rilevamento dei prodotti antimalware mediante l'utilizzo di pratiche di offuscazione e/o crittografia. Qualora i metodi di emulazione o di euristica ordinari non siano in grado di rilevare una minaccia, lo Scanner memoria avanzato identifica il comportamento sospetto ed effettua un controllo delle minacce presenti nella memoria del sistema. Questa soluzione si rivela efficace persino contro i malware che utilizzano pratiche di offuscamento ottimizzate.

Diversamente dall'Exploit Blocker, lo Scanner memoria avanzato rappresenta un metodo post-esecuzione. Ciò implica un rischio di esecuzione di attività dannose prima del rilevamento di una minaccia. Tuttavia, qualora le varie tecniche di rilevamento disponibili non si rivelino efficaci, questo sistema offre un livello aggiuntivo di sicurezza.

6.2.3 ESET Live Grid

Sviluppato sul sistema avanzato di allarme immediato ThreatSense.Net®, ESET Live Grid utilizza i dati inviati dagli utenti ESET di tutto il mondo e li invia al laboratorio antivirus ESET. Grazie all'invio di campioni e metadati "from the wild" sospetti, ESET Live Grid consente a ESET di soddisfare le esigenze dei clienti e di gestire le minacce più recenti in modo tempestivo. I ricercatori dei malware ESET utilizzano le informazioni per creare un'istantanea accurata della natura e dell'ambito delle minacce globali, che consente a ESET di puntare il mirino sugli obiettivi appropriati. I dati ESET Live Grid giocano un ruolo importante nella definizione delle priorità nell'ambito dei sistemi di elaborazione automatici.

Questo strumento consente inoltre di implementare un sistema di reputazione che contribuisce al potenziamento dell'efficienza complessiva delle soluzioni anti-malware ESET. Durante l'analisi di un file eseguibile o di un archivio sul sistema di un utente, il relativo hashtag viene dapprima confrontato rispetto a un database di elementi della whitelist e della blacklist. Se presente nella whitelist, il file analizzato viene considerato pulito e contrassegnato ai fini dell'esclusione da controlli futuri. Se presente nella blacklist, verranno intraprese azioni appropriate in base alla natura della minaccia. In caso di mancata corrispondenza, il file viene sottoposto a un controllo completo. Sulla base dei risultati del controllo, i file vengono categorizzati come minacce o non minacce. Questo approccio registra un impatto positivo importante sulle prestazioni del controllo.

Il sistema di reputazione consente di effettuare un rilevamento efficace di campioni di malware anche prima dell'invio delle relative firme al computer dell'utente, mediante il database antivirus aggiornato (tale azione si ripete più di una volta al giorno).

6.3 E-mail

L'e-mail o electronic mail è una moderna forma di comunicazione che presenta numerosi vantaggi. È flessibile, veloce e diretta e ha svolto un ruolo cruciale nella proliferazione di Internet all'inizio degli anni novanta.

Purtroppo, a causa dell'elevato livello di anonimità, i messaggi e-mail e Internet lasciano ampio spazio ad attività illegali come lo spam. Lo spamming include annunci pubblicitari non desiderati, hoax e proliferazione di software dannoso o malware. Ad aumentare ulteriormente i disagi e i pericoli è il fatto che i costi di invio dello spamming sono minimi e gli autori dispongono di numerosi strumenti per acquisire nuovi indirizzi e-mail. Il volume e la varietà dello spamming ne rende inoltre estremamente difficoltoso il monitoraggio. Maggiore è il periodo di utilizzo dell'indirizzo e-mail, più elevata sarà la possibilità che finisca in un database per motori di spamming. Di seguito sono riportati alcuni suggerimenti per la prevenzione di messaggi e-mail indesiderati:

- Se possibile, evitare di pubblicare il proprio indirizzo e-mail su Internet
- Fornire il proprio indirizzo e-mail solo a utenti considerati attendibili
- Se possibile, non utilizzare alias comuni. Maggiore è la complessità degli alias, minore sarà la probabilità che vengano rilevati
- Non rispondere a messaggi di spam già recapitati nella posta in arrivo
- Quando si compilano moduli su Internet, prestare particolare attenzione a selezionare opzioni quali "Sì, desidero ricevere informazioni".
- Utilizzare indirizzi e-mail "specifici", ad esempio uno per l'ufficio, uno per comunicare con gli amici e così via.
- Cambiare di tanto in tanto l'indirizzo e-mail
- Utilizzare una soluzione antispam

6.3.1 Pubblicità

La pubblicità su Internet è una delle forme di pubblicità in maggior crescita. I vantaggi principali dal punto di vista del marketing sono i costi ridotti e un livello elevato di immediatezza. I messaggi vengono inoltre recapitati quasi immediatamente. Molte società utilizzano strumenti di marketing via e-mail per comunicare in modo efficace con i clienti attuali e potenziali.

Questo tipo di pubblicità è legittimo, perché si potrebbe essere interessati a ricevere informazioni commerciali su determinati prodotti. Molte società inviano tuttavia messaggi di contenuto commerciale non desiderati. In questi casi, la pubblicità tramite e-mail supera il limite e diventa spam.

La quantità di messaggi e-mail non desiderati diventa così un problema e non sembra diminuire. Gli autori di messaggi e-mail non desiderati tentano spesso di mascherare i messaggi spam come messaggi legittimi.

6.3.2 Hoax: truffe e bufale

Un hoax è un messaggio contenente informazioni non veritiere diffuso su Internet. che viene in genere inviato via e-mail e tramite strumenti di comunicazione come ICQ e Skype. Il messaggio stesso è in genere una burla o una leggenda metropolitana.

Gli hoax virus tentano di generare paura, incertezza e dubbio (FUD, Fear, Uncertainty and Doubt) nei destinatari, inducendoli a credere che nei relativi sistemi è presente un "virus non rilevabile" in grado di eliminare file e recuperare password o di eseguire altre attività dannose.

Alcuni hoax richiedono ai destinatari di inoltrare messaggi ai loro contatti, aumentandone così la diffusione. Esistono hoax via cellulare, richieste di aiuto, offerte di denaro dall'estero e così via. Spesso è impossibile determinare l'intento dell'autore del messaggio.

È molto prababile che i messaggi che invitano ad essere inoltrati a tutti i propri conoscenti siano hoax. Su Internet sono presenti molti siti Web in grado di verificare l'autenticità di un messaggio e-mail. Prima di inoltrarlo, effettuare una ricerca in Internet per qualsiasi messaggio si sospetti essere hoax.

6.3.3 Phishing

Il termine phishing definisce un'attività illegale che si avvale di tecniche di ingegneria sociale (ovvero di manipolazione degli utenti al fine di ottenere informazioni confidenziali). Lo scopo è quello di ottenere l'accesso a dati sensibili quali numeri di conti bancari, codici PIN e così via.

Di norma, l'accesso viene ricavato tramite l'invio di messaggi e-mail che imitano quelli di una persona o società affidabile (istituto finanziario, compagnia di assicurazioni). Il messaggio e-mail sembra autentico e presenta immagini e contenuti che possono indurre a credere che provenga effettivamente da un mittente affidabile. Tali messaggi chiedono all'utente, con vari pretesti (verifica dati, operazioni finanziarie), di immettere alcuni dati personali: numeri di conto bancario o nomi utente e password. Tali dati, se inviati, possono essere rubati e utilizzati in modo illegale.

Le banche, le compagnie di assicurazioni e altre società legittime non chiederanno mai di rivelare nomi utente e password in messaggi e-mail non desiderati.

6.3.4 Riconoscimento messaggi spamming

In genere, esistono alcuni indicatori che consentono di identificare i messaggi spamming (e-mail non desiderate) nella cassetta postale. Un messaggio può essere considerato un messaggio spamming se soddisfa almeno alcuni dei criteri riportati di seguito.

- L'indirizzo del mittente non appartiene a nessuno degli utenti presenti nell'elenco dei contatti.
- Agli utenti viene offerta una grossa somma di denaro, purché si impegnino tuttavia ad anticipare una piccola somma di denaro.
- Viene chiesto di immettere con vari pretesti (verifica di dati, operazioni finanziarie) alcuni dati personali, quali numero di conto bancario, nome utente, password e così via.
- È scritto in una lingua straniera.
- Viene chiesto di acquistare un prodotto a cui non si è interessati. Se tuttavia si decide di acquistarlo, è consigliabile verificare che il mittente del messaggio sia un fornitore attendibile (contattare il produttore originale).
- Alcuni termini contengono errori di ortografia nel tentativo di aggirare il filtro di spamming, ad esempio "vaigra" invece di "viagra" e così via