ESET NOD32 Antivirus 4

Business Edition per Mac OS X

Manuale di installazione e Guida utente

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

ESET NOD32 Antivirus 4

Supporto tecnico globale: www.eset.com/support

REV. 5. 9. 2011

Contenuti

1. ESET NOD32 Antivirus....4
1.1 Requisiti di sistema....4
2. Installazione....5
2.1 Installazione tipica....5
2.2 Installazione personalizzata....5
2.3 Installazione remota....6
2.3.1 Creazione pacchetto installazione remota....6
2.3.2 Installazione remota su computer di destinazione....7
2.3.3 Disinstallazione remota....7
2.3.4 Aggiornamento remoto....7
2.4 Inserimento nome utente e password....7
2.5 Controllo computer su richiesta....7
3. Guida introduttiva....8
3.1 Introduzione all'interfaccia utente: modalità....8
3.1.1 Verifica del funzionamento del sistema....8
3.1.2 Cosa fare se il programma non funziona correttamente....8
4. Utilizzo di ESET NOD32 Antivirus....10
4.1 Protezione antivirus e antispyware....10
4.1.1 Protezione file system in tempo reale....10
4.1.1.1 Impostazione protezione in tempo reale....10
4.1.1.1.1 Scansione al verificarsi di un evento....10
4.1.1.1.2 Opzioni avanzate di scansione....10
4.1.1.1.3 Esclusioni da scansione....10
4.1.1.2 Quando modificare la configurazione della protezione in tempo reale....11
4.1.1.3 Controllo della protezione in tempo reale....11
4.1.1.4 Cosa fare se la protezione in tempo reale non funziona....11
4.1.2 Controllo computer su richiesta....11
4.1.2.1 Tipo di scansione....12
4.1.2.1.1 Controllo Smart....12
4.1.2.1.2 Controllo personalizzato....12
4.1.2.2 Destinazioni di scansione specifiche....12
4.1.2.3 Profili di scansione....12
4.1.3 Configurazione parametri motore ThreatSense....13
4.1.3.1 Oggetti....13
4.1.3.2 Opzioni....13
4.1.3.3 Pulizia....14
4.1.3.4 Estensioni....14
4.1.3.5 Limiti....14
4.1.3.6 Altri....14
4.1.4 Rilevamento di un'infiltrazione....14
4.2 Aggiornamento del programma....15
4.2.1 Aggiornamento a una nuova build....15
4.2.2 Impostazione dell'aggiornamento....16
4.2.3 Come creare attività di aggiornamento....16
4.3 Pianificazione attività....16
4.3.1 Scopo della pianificazione attività....17
4.3.2 Creazione di nuove attività....17
4.4 Quarantena....17
4.4.1 Mettere file in quarantena....18
4.4.2 Ripristino dalla quarantena....18
4.4.3 Invio di file dalla Quarantena....18
4.5 File di rapporto....18
4.5.1 Manutenzione rapporto....18
4.5.2 Filtraggio rapporti....18
4.6 Interfaccia utente....18
4.6.1 Avvisi e notifiche....19
4.6.1.1 Configurazione avanzata avvisi e notifiche....19
4.6.2 Privilegi....19
4.6.3 Menù contestuale....19
4.7 ThreatSense.Net....20
4.7.1 File sospetti....20
5. Utente avanzato....21
5.1 Importa ed esporta impostazioni....21
5.1.1 Importa impostazioni....21
5.1.2 Esporta impostazioni....21
5.2 Configurazione del server proxy....21
5.3 Blocco supporti rimovibili....21
5.4 Amministrazione remota....21
6. Glossario....23
6.1 Tipi di infiltrazioni....23
6.1.1 Virus....23
6.1.2 Worm....23
6.1.3 Trojan horse....23
6.1.4 Adware....23
6.1.5 Spyware....24
6.1.6 Applicazioni potenzialmente pericolose....24
6.1.7 Applicazioni potenzialmente indesiderate....24

1. ESET NOD32 Antivirus

Come conseguenza della sempre crescente diffusione dei sistemi operativi basati su Unix, i creatori di malware stanno sviluppando nuove minacce per colpire gli utenti di Mac. ESET NOD32 Antivirus offre una protezione potente ed efficace contro le minacce. ESET NOD32 Antivirus consente di allontanare le minacce di Windows, proteggendo gli utenti di Mac durante le loro interazioni con gli utenti Windows e viceversa. Sebbene i malware Windows non rappresentino una minaccia diretta per Mac, la disattivazione dei malware che ha determinato l'infezione di una macchina Mac consentirà di evitarne la diffusione su computer Windows attraverso una rete locale o Internet.

1.1 Requisiti di sistema

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

ESET NOD32 Antivirus:

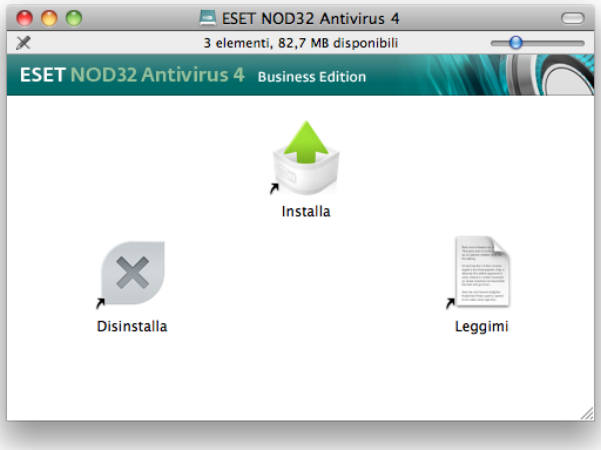
	Requisiti di sistema
Architettura processore	32bit, 64bit Intel®
Sistema operativo	Mac OS X 10.5.x e successivo
Memoria	512 MB
Spazio su disco	100 MB

2. Installazione

Prima di cominciare la procedura di installazione, chiudere tutti i programmi aperti sul computer. In ESET NOD32 Antivirus sono contenuti componenti che possono creare conflitto con altri programmi antivirus già installati nel computer. Si consiglia di rimuovere altri programmi per impedire l'insorgere di eventuali problemi. È possibile installare ESET NOD32 Antivirus tramite il CD di installazione o mediante un file disponibile per il download sul sito Web ESET.

Per avviare la procedura di installazione, procedere in uno dei modi descritti di seguito:

- Se si utilizza il CD di installazione, inserirlo nell'unità CD-ROM. Fare doppio clic sull'icona di installazione ESET NOD32 Antivirus per avviare il programma di installazione.
- Se si utilizza un file scaricato dal sito Web, fare doppio clic sul file scaricato per avviare il programma di installazione.



Dopo aver avviato il programma di installazione, l'installazione guidata condurrà l'utente attraverso le fasi di configurazione di base. Dopo aver accettato i termini di licenza dell'utente finale, è possibile scegliere uno dei seguenti tipi di installazione:

- Installazione tipica 5
- Installazione personalizzata 5
- Installazione remota 6

2.1 Installazione tipica

L'installazione tipica comprende le opzioni di configurazione adatte alla maggior parte degli utenti. Le impostazioni garantiscono livelli massimi di sicurezza, nonché prestazioni ottimali del sistema. L'installazione tipica rappresenta l'opzione predefinita consigliata nel caso in cui gli utenti non abbiano particolari necessità relative a impostazioni specifiche.

Dopo aver selezionato la modalità di installazione **Tipica (impostazioni consigliate)**, verrà visualizzata una finestra di dialogo in cui sarà necessario immettere nome utente e password per attivare gli aggiornamenti automatici del programma. Ciò svolge un ruolo fondamentale per garantire una protezione costante del sistema. Immettere nei campi corrispondenti **Nome utente** e **Password** (ovvero i dati di autenticazione ottenuti dopo l'acquisto o la registrazione del prodotto). Se non si dispone ancora di nome utente e password, è possibile selezionare l'opzione **Imposta i parametri di aggiornamento più tardi** per procedere con l'installazione.

Il **Sistema di allarme immediato ThreatSense.Net** consente di garantire che ESET sia informata in modo tempestivo e continuato sulle nuove infiltrazioni per proteggere gli utenti in modo immediato. Il sistema consente l'invio di nuove minacce al laboratorio ESET preposto allo studio delle minacce, dove queste verranno analizzate, elaborate e aggiunte al database delle firme antivirali. Di default, viene selezionata l'opzione **Attiva Sistema di allarme immediato ThreatSense.Net**. Fare clic su **Configurazione...** per modificare le impostazioni dettagliate per l'invio di file sospetti. (Per ulteriori informazioni, vedere ThreatSense.Net 20).

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. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile notarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente. Selezionare l'opzione **Attiva rilevamento delle applicazioni potenzialmente indesiderate** per consentire a ESET NOD32 Antivirus di rilevare questo tipo di minaccia (scelta consigliata). Se non si desidera attivare tale funzione, selezionare l'opzione **Disattiva rilevamento delle applicazioni potenzialmente indesiderate**.

Fare clic su **Installa** per installare ESET NOD32 Antivirus su un disco **Macintosh HD** standard. Se si desidera selezionare un altro disco, fare clic su **Modifica percorso di installazione...**

2.2 Installazione personalizzata

L'installazione personalizzata è indicata per utenti esperti che desiderano modificare le impostazioni avanzate durante il processo di installazione.

Dopo aver selezionato la modalità di installazione **Personalizzata**, sarà necessario inserire **Nome utente** e **Password** (ovvero i dati di autenticazione ottenuti dopo l'acquisto o la registrazione del prodotto) nei campi corrispondenti. Se non si dispone ancora di nome utente e password, è possibile selezionare l'opzione **Imposta i parametri di aggiornamento più tardi** per procedere con l'installazione. È possibile inserire nome utente e password in un secondo momento.

In caso di utilizzo di un server proxy, è possibile definirne i parametri durante questa fase selezionando l'opzione **Utilizzo un server proxy**. 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 (in base alle impostazioni predefinite, la porta 3128). Nel caso in cui il server proxy richieda l'autenticazione, sarà necessario

immettere un **Nome utente** e una **Password** validi, per consentire l'accesso al server proxy. Se si è certi di non utilizzare un server proxy, scegliere l'opzione **Non utilizzo un server proxy**.In caso di dubbi, è possibile utilizzare le impostazioni di sistema correnti selezionando **Utilizza le impostazioni di sistema (scelta consigliata)**.

Se ESET NOD32 Antivirus sarà amministrato da ESET Remote Administrator (ERA), sarà possibile impostare i parametri ERA Server (nome del server, porta e password) per collegare automaticamente ESET NOD32 Antivirus a ERA Server dopo l'installazione.

Nella fase successiva è possibile **Definire gli utenti con privilegi** che saranno in grado di modificare la configurazione del programma. Dalla lista di utenti sulla sinistra, è possibile scegliere gli utenti e **Aggiungerli** alla lista degli **Utenti con privilegi**. Per visualizzare tutti gli utenti del sistema, selezionare l'opzione **Mostra tutti gli utenti**.

Il **Sistema di allarme immediato ThreatSense.Net** consente di garantire che ESET sia informata in modo tempestivo e continuato sulle nuove infiltrazioni per proteggere gli utenti in modo immediato. Il sistema consente l'invio di nuove minacce al laboratorio ESET preposto allo studio delle minacce, dove queste verranno analizzate, elaborate e aggiunte al database delle firme antivirali. Di default, viene selezionata l'opzione **Attiva Sistema di allarme immediato ThreatSense.Net**. Fare clic su **Configurazione...** per modificare le impostazioni dettagliate per l'invio di file sospetti. Per ulteriori informazioni, vedere ThreatSense.Net 20.

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. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile notarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente. Selezionare l'opzione **Attiva rilevamento delle applicazioni potenzialmente indesiderate** per consentire a ESET NOD32 Antivirus di rilevare questo tipo di minaccia (scelta consigliata).

Fare clic su **Installa** per installare ESET NOD32 Antivirus su un disco **Macintosh HD**. Se si desidera selezionare un altro disco, fare clic su **Modifica percorso di installazione...**

2.3 Installazione remota

L'installazione remota consente di creare un pacchetto di installazione che è possibile installare su computer di destinazione attraverso un software di desktop remoto. ESET NOD32 Antivirus può quindi essere gestito in remoto attraverso ESET Remote Administrator.

L'installazione remota avviene in due fasi:

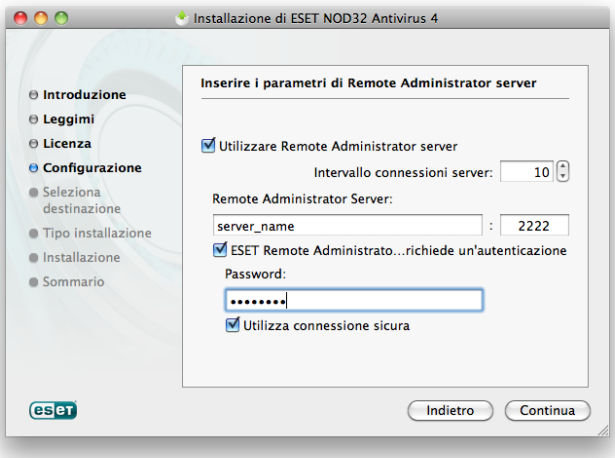
1. Creazione di un pacchetto di installazione remota tramite il programma di installazione ESET 6
2. Installazione remota attraverso l'utilizzo di un software di desktop remoto 7

2.3.1 Creazione pacchetto installazione remota

Dopo aver selezionato la modalità di installazione **Remota**, verrà visualizzata una finestra di dialogo in cui sarà necessario immettere nome utente e password per attivare gli aggiornamenti automatici di ESET NOD32 Antivirus. Immettere nei campi corrispondenti **Nome utente** e **Password** (ovvero i dati di autenticazione ottenuti dopo l'acquisto o la registrazione del prodotto). Se non si dispone ancora di nome utente e password, è possibile selezionare l'opzione **Imposta i parametri di aggiornamento più tardi** per procedere con l'installazione. È possibile inserire nome utente e password direttamente all'interno del programma in un secondo momento.

La fase successiva consiste nella configurazione della connessione Internet. In caso di utilizzo di un server proxy, è possibile definirne i parametri durante questa fase selezionando l'opzione **Utilizzo un server proxy**. Se si è certi di non utilizzare un server proxy, è possibile scegliere l'opzione **Non utilizzo un server proxy**. In caso di dubbi, è possibile utilizzare le impostazioni di sistema correnti selezionando **Utilizza le impostazioni di sistema**.

Impostare i parametri ERA Server (nome del server, porta e password) per connettere automaticamente ESET NOD32 Antivirus a ERA Server dopo l'installazione.



Nella fase successiva è possibile **Definire gli utenti con privilegi** che saranno in grado di modificare la configurazione del programma. Dalla lista di utenti sulla sinistra, è possibile scegliere gli utenti e **Aggiungerli** alla lista degli **Utenti con**

privilegi. Per visualizzare tutti gli utenti del sistema, selezionare l'opzione **Mostra tutti gli utenti**.

Il **Sistema di allarme immediato ThreatSense.Net** consente di garantire che ESET sia informata in modo tempestivo e continuato sulle nuove infiltrazioni per proteggere gli utenti in modo immediato. Il sistema consente l'invio di nuove minacce al laboratorio ESET preposto allo studio delle minacce, dove queste verranno analizzate, elaborate e aggiunte al database delle firme antivirali. Di default, viene selezionata l'opzione **Attiva Sistema di allarme immediato ThreatSense.Net**. Fare clic su **Configurazione...** per modificare le impostazioni dettagliate per l'invio di file sospetti. Per ulteriori informazioni, vedere ThreatSense.Net 20.

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. Applicazioni di questo tipo sono spesso legate all'installazione di altri programmi e potrebbe essere difficile notarle durante il processo di installazione. Sebbene tali applicazioni consentano di visualizzare una notifica durante il processo di installazione, esse possono essere installate facilmente senza il consenso dell'utente. Selezionare l'opzione **Attiva rilevamento delle applicazioni potenzialmente indesiderate** per consentire a ESET NOD32 Antivirus di rilevare questo tipo di minaccia (scelta consigliata).

Nell'ultima fase della procedura di installazione guidata, scegliere una cartella di destinazione. Il programma di installazione ESET creerà il pacchetto di installazione *(EAV4_Remote_Install.pkg)* e lo script shell di disinstallazione *(EAV4_Remote_UnInstall.sh)*.

2.3.2 Installazione remota su computer di destinazione

ESET NOD32 Antivirus può essere installato su computer di destinazione attraverso il Desktop remoto Apple o qualsiasi altro strumento in grado di supportare l'installazione di pacchetti Mac standard (*.pkg*), copiando i file ed eseguendo gli script shell su computer di destinazione.

Per installare ESET NOD32 Antivirus utilizzando il Desktop remoto Apple, eseguire il comando **Installa pacchetti…**, individuare il file *EAV4_Remote_Install.pkg* e fare clic su **Installa**.

Per istruzioni più dettagliate sulle modalità di gestione dei computer client attraverso ESET Remote Administrator si rimanda alla Guida utente ESET Remote Administrator.

2.3.3 Disinstallazione remota

Per disinstallare ESET NOD32 Antivirus dai computer client:

1. utilizzare il comando **Copia gli elementi…** nel Desktop remoto Apple, individuare lo script shell della disinstallazione *(EAV4_Remote_UnInstall.sh* - creato insieme al pacchetto di installazione) e copiarlo sui computer target.
2. eseguire il **Comando invia a Unix…** nel Desktop remoto Apple. Una volta completata con successo la disinstallazione, verrà visualizzato un registro della console.

2.3.4 Aggiornamento remoto

L'aggiornamento remoto di ESET NOD32 Antivirus viene effettuato attraverso il comando **Installa pacchetti…** nel Desktop remoto Apple.

NOTA: Le impostazioni salvate nel pacchetto di installazione remota ESET non vengono applicate ai computer di destinazione durante il processo di aggiornamento. ESET Remote Administrator deve essere utilizzato per configurare ESET NOD32 Antivirus da remoto dopo l'aggiornamento.

2.4 Inserimento nome utente e password

Per garantire una funzionalità ottimale, è importante che il programma scarichi automaticamente gli aggiornamenti dei database delle firme antivirali. Ciò è possibile solo se il **Nome utente** e la **Password** vengono immessi correttamente nella Configurazione dell'aggiornamento 16.

2.5 Controllo computer su richiesta

Dopo aver installato ESET NOD32 Antivirus, è necessario eseguire un controllo del computer per la ricerca di codici dannosi. Nella finestra principale del programma, fare clic su **Controllo computer** quindi fare clic su **Controllo Smart**. Per ulteriori informazioni sui controlli del computer su richiesta, si rimanda alla sezione Controllo computer su richiesta 11.

3. Guida introduttiva

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

3.1 Introduzione all'interfaccia utente: modalità

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. Se è attivata la **Modalità avanzata** verrà visualizzato il sottomenu **Statistiche**.
- **Controllo computer** - Questa opzione consente di configurare e avviare la **Controllo computer su richiesta**.
- **Aggiorna** - Consente di visualizzare informazioni relative agli aggiornamenti del database delle firme antivirali.
- **Configurazione** - Selezionare questa opzione per regolare il livello di protezione del computer. Se è attivata la **Modalità avanzata** verrà visualizzato il sottomenu **Antivirus e antispyware**.
- **Strumenti** - Consente di accedere ai **File di rapporto**, alla **Quarantena** e alla **Pianificazione attività**. Questa opzione può essere visualizzata esclusivamente in **Modalità avanzata**.
- **Guida** - Fornisce informazioni relative al programma, all'accesso ai file della guida, alla Knowledge Base su Internet e al sito web ESET.

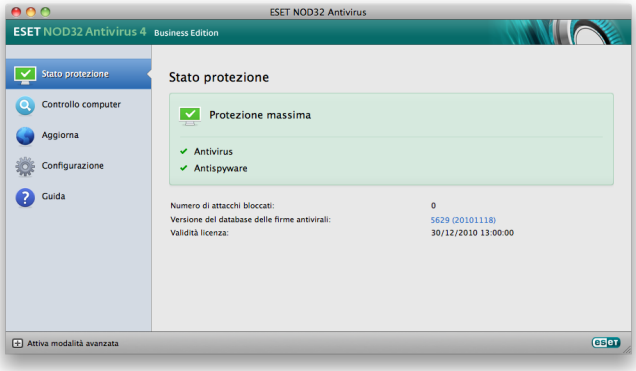
L'interfaccia utente ESET NOD32 Antivirus consente agli utenti di alternare le modalità Standard e Avanzata. La modalità standard consente l'accesso alle funzioni necessarie per le normali operazioni. Tale modalità non consente di visualizzare opzioni avanzate. Per passare da una modalità all'altra, fare clic sull'icona "più" (**+**) vicino ad **Attiva modalità avanzata**/ **Attiva modalità standard** nell'angolo in basso a sinistra della finestra principale del programma.

La modalità standard consente l'accesso alle funzioni necessarie per le normali operazioni. Tale modalità non consente di visualizzare opzioni avanzate.

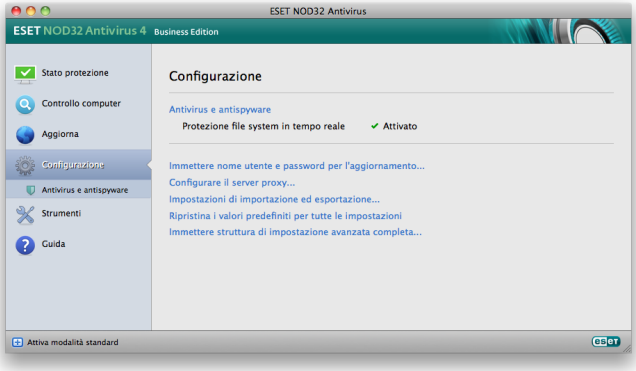
Quando si passa alla modalità avanzata, viene aggiunta l'opzione **Strumenti** al menu principale. L'opzione **Strumenti** consente di accedere ai sottomenu per i **File di rapporto**, la **Quarantena** e la **Pianificazione attività**.

NOTA: Tutte le istruzioni rimanenti della guida si riferiscono alla **modalità avanzata**.

Modalità standard:

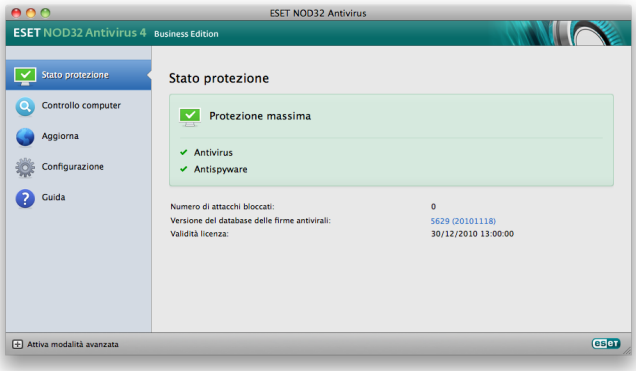


Modalità avanzata:



3.1.1 Verifica del funzionamento del sistema

Per visualizzare lo **Stato protezione**, fare clic sull'opzione in alto nel menu principale. Nel rapporto di funzionamento di ESET NOD32 Antivirus è possibile visualizzare la finestra principale, nonché un sottomenu con le **Statistiche**. Selezionarlo per visualizzare informazioni più dettagliate e statistiche relative ai controlli del computer eseguiti sul sistema. La finestra Statistiche è disponibile esclusivamente in modalità avanzata.



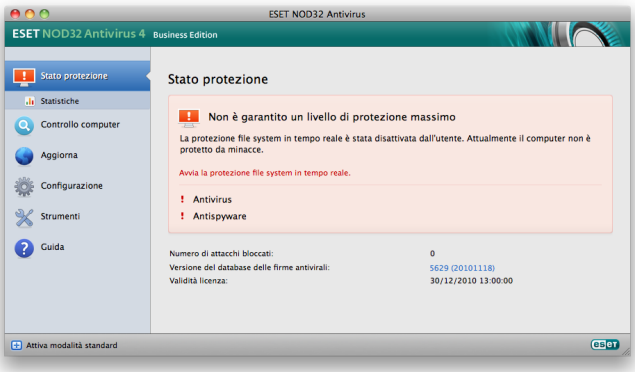
3.1.2 Cosa fare se il programma non funziona correttamente

Se i moduli attivati funzionano correttamente, verrà visualizzata un'icona di controllo verde. In caso contrario, verrà visualizzato un punto esclamativo rosso o un'icona di notifica arancione e, nella parte superiore della finestra, verranno visualizzate ulteriori informazioni sul modulo. Verrà inoltre visualizzata una soluzione consigliata per la riparazione del modulo. Per modificare lo stato dei singoli moduli, scegliere **Configurazione** dal menu principale e fare clic sul

modulo desiderato.

Qualora non si riuscisse a risolvere un problema ricorrendo alle soluzioni consigliate, fare clic su **Guida** per accedere ai file della Guida o effettuare una ricerca nella knowledge base.

Per assistenza, è possibile contattare il Supporto tecnico ESET sul sito web ESET. Essa risponderà rapidamente alle domande degli utenti e li aiuterà a ricercare una soluzione ai loro problemi.



4. Utilizzo di ESET NOD32 Antivirus

4.1 Protezione antivirus e antispyware

La protezione antivirus difende il sistema da attacchi dannosi, modificando i file che rappresentano minacce potenziali. In caso di rilevamento di una minaccia costituita da codice dannoso, il modulo antivirus è in grado di eliminarla bloccandola e pulendola, eliminandola o mettendola in quarantena.

4.1.1 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 scansione per la ricerca di codici dannosi al momento dell'apertura, creazione o esecuzione sul computer. La funzione di protezione del file system in tempo reale viene avviata all'avvio del sistema.

4.1.1.1 Impostazione protezione in tempo reale

La protezione del file system in tempo reale controlla tutti i tipi di supporto quando si verificano determinati eventi. Grazie ai metodi di rilevamento della tecnologia ThreatSense (descritti nella sezione intitolata Configurazione parametri motore ThreatSense 13), la protezione file system in tempo reale potrebbe variare per i file di nuova creazione e per i file esistenti. Nel caso di file appena creati, è possibile applicare un livello di controllo maggiore.

In base alle impostazioni predefinite, la protezione in tempo reale viene avviata automaticamente all'avvio del sistema operativo e fornisce un controllo ininterrotto. In casi speciali, ad esempio in caso di conflitto con un altro scanner in tempo reale, la protezione in tempo reale può essere interrotta facendo clic sull'icona ESET NOD32 Antivirus sulla barra dei menu (sulla parte superiore dello schermo) e selezionando quindi l'opzione **Disattiva la protezione file system in tempo reale**. La protezione in tempo reale può anche essere interrotta dalla finestra del programma principale (**Configurazione** > **Antivirus e antispyware** > **Disattiva**).

Per modificare le impostazioni avanzate della protezione in tempo reale, fare clic su **Configurazione** > **Inserisci preferenze applicazione ...** > **Protezione** > **Protezione in tempo reale** e fare clic sul pulsante **Configurazione...** vicino a **Opzioni avanzate** (descritte nella sezione intitolata Opzioni avanzate di scansione 10).

4.1.1.1.1 Scansione al verificarsi di un evento

In base alle impostazioni predefinite, il controllo viene effettuato all'**Apertura dei file**, durante la **Creazione dei file** o l'**Esecuzione dei file**. È consigliabile mantenere le impostazioni predefinite che offrono il massimo livello di protezione in tempo reale per il computer.

4.1.1.1.2 Opzioni avanzate di scansione

In questa finestra è possibile definire le tipologie di oggetti da sottoporre a scansione da parte del motore ThreatSense e attivare/disattivare l'opzione di **Euristica avanzata** nonché modificare le impostazioni degli archivi e della cache file.

Si consiglia di non modificare i valori predefiniti nella sezione **Impostazioni predefinite archivi** salvo nel caso in cui fosse necessario risolvere un problema specifico, poiché livelli di ricerca degli archivi troppo elevati possono ostacolare le prestazioni del sistema.

È possibile passare alla scansione Euristica avanzata ThreatSense per i file eseguiti nonché per i file creati e modificati separatamente facendo clic sulla casella di controllo **Euristica avanzata** nelle rispettive sezioni dei parametri ThreatSense.

Al fine di determinare un impatto minimo sul sistema durante l'utilizzo della protezione in tempo reale, è possibile definire le dimensioni della cache di ottimizzazione. Tale comportamento è attivo nel momento in cui si sceglie l'opzione **Attiva pulisci cache file**. Quando questa funzione è disattivata, tutti i file vengono sottoposti a scansione ad ogni accesso. I file non verranno sottoposti a scansione ripetutamente dopo essere stati memorizzati nella cache (salvo il caso in cui siano stati modificati) fino alle dimensioni definite della cache. I file vengono controllati nuovamente subito dopo ogni aggiornamento del database di firme antivirali.

Fare clic su **Attiva pulisci cache file** per attivare/disattivare questa funzione. Per impostare il numero di file da memorizzare nella cache, basta indicare il valore desiderato nel campo di inserimento accanto alla voce **Dimensioni cache**.

È possibile impostare ulteriori parametri di scansione nella finestra **Configurazione motore ThreatSense**. È possibile definire il tipo di **Oggetti** da sottoporre a scansione, le **Opzioni** da utilizzare e il livello di **Pulizia**, nonché definire le **Estensioni** e i **Limiti** delle dimensioni dei file per la protezione file system in tempo reale. È possibile accedere alla finestra di configurazione del motore ThreatSense facendo clic sul pulsante **Configurazione...** vicino a **Motore ThreatSense** nella finestra di Configurazione avanzata. Per ulteriori informazioni relative ai parametri del motore ThreatSense si rimanda alla sezione Configurazione parametri motore ThreatSense 13.

4.1.1.1.3 Esclusioni da scansione

Questa sezione consente di escludere alcuni file e cartelle dalla scansione.

- **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. Pertanto, se il file si infetta successivamente con altri malware, esso verrà rilevato dal modulo antivirus.

- **Aggiungi...**- esclude gli oggetti dal rilevamento. Inserire il percorso ad un oggetto (è anche possibile utilizzare i caratteri jolly * and ?) o selezionare la cartella o il file dalla struttura ad albero.
- **Modifica...** - consente di modificare le voci selezionate
- **Elimina** - rimuove le voci selezionate
- **Impostazioni predefinite** - annulla tutte le esclusioni.

4.1.1.2 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. Agire con prudenza nel momento in cui si modificano i parametri della protezione in tempo reale. È consigliabile modificarli solo in casi specifici, come ad esempio il caso in cui si verifichi un conflitto con una determinata applicazione o con lo scanner in tempo reale di un altro programma antivirus.

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 sul pulsante **Impostazioni predefinite** posizionato nell'angolo in basso a sinistra della finestra **Protezione in tempo reale** (**Configurazione** > **Inserisci preferenze applicazione ...** > **Protezione** > **Protezione in tempo reale**).

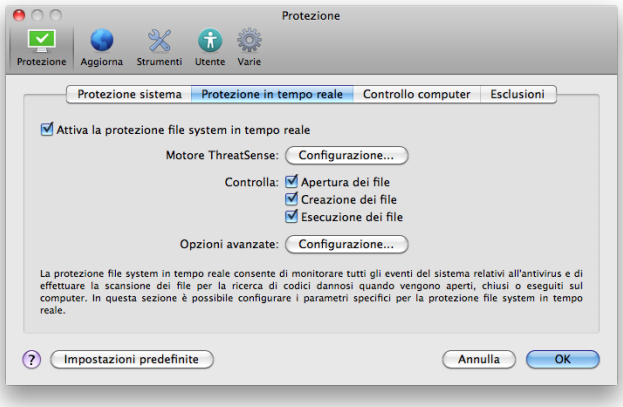
4.1.1.3 Controllo della protezione in tempo reale

Per verificare che la protezione in tempo reale funzioni e sia in grado di rilevare virus, utilizzare il file di test eicar.com. Questo file di test è un file innocuo, speciale, 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.

4.1.1.4 Cosa fare se la protezione in tempo reale non funziona

Nel prossimo capitolo verranno illustrate situazioni problematiche che si possono verificare quando si utilizza la protezione in tempo reale e verranno descritte le relative 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** > **Antivirus e antispyware** e fare clic sul link **Attiva la protezione file system in tempo reale** (sulla destra) nella finestra principale del programma. In alternativa, è possibile attivare la protezione file system in tempo reale nella finestra delle Impostazioni avanzate in **Protezione** > **Protezione in tempo reale** selezionando l'opzione **Attiva protezione file system in tempo reale**.



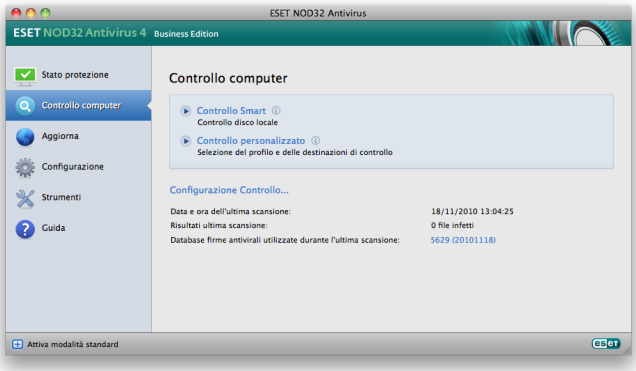
La protezione in tempo reale non rileva né pulisce le infiltrazioni
Assicurarsi che nel computer non siano installati altri programmi antivirus. Se sono attivati contemporaneamente due scudi di protezione in tempo reale, essi possono entrare in conflitto. È consigliabile disinstallare gli altri programmi antivirus che potrebbero essere presenti nel sistema.

La protezione in tempo reale non viene avviata
Se la protezione in tempo reale non si attiva all'avvio del sistema, ciò potrebbe dipendere da conflitti con altri programmi. In tal caso, consultare gli specialisti del Supporto tecnico ESET.

4.1.2 Controllo computer su richiesta

Se si sospetta che il computer sia infetto perché non funziona normalmente, eseguire un **Controllo computer** > **Controllo Smart** per cercare eventuali infiltrazioni nel computer. Per garantire un livello massimo di protezione, è necessario eseguire regolarmente controlli del computer come parte delle misure di sicurezza di routine, anziché limitarsi ad eseguirle in caso di infezioni sospette. Una scansione regolare consente di rilevare infiltrazioni non rilevate dallo scanner in tempo reale se salvate su disco. Ciò accade se, al momento dell'infezione, lo scanner in tempo reale è stato disattivato o quando il database di firme antivirali è obsoleto.

È consigliabile eseguire una scansione su richiesta del computer almeno una volta al mese. La scansione può essere configurata come attività pianificata in **Strumenti** > **Pianificazione attività**.



4.1.2.1 Tipo di scansione

Sono disponibili due tipologie di controllo del computer su richiesta. **Controllo Smart**, 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 scansione predefiniti, nonché di scegliere destinazioni di scansione specifiche.

4.1.2.1.1 Controllo Smart

La funzione Controllo Smart consente di avviare velocemente un controllo del computer e di pulire i file infetti senza l'intervento dell'utente. Il vantaggio principale è la semplicità della procedura, che non richiede una configurazione di scansione dettagliata. Il Controllo Smart consente di effettuare un controllo di tutti i file presenti nelle cartelle, nonché una pulizia o un'eliminazione automatica delle infiltrazioni rilevate. Il livello di disinfezione viene impostato automaticamente sul valore predefinito. Per ulteriori informazioni sui tipi di disinfezione, si rimanda alla sezione dedicata alla Pulizia 14.

4.1.2.1.2 Controllo personalizzato

Il **Controllo personalizzato** rappresenta una soluzione ottimale se si desidera specificare parametri di scansione quali destinazioni e metodi di scansione. Il vantaggio del controllo personalizzato consiste nella possibilità di configurare i parametri in dettaglio. È possibile salvare diverse configurazioni come profili di scansione definiti dagli utenti. Questi sono particolarmente utili se il controllo viene eseguito più volte con gli stessi parametri.

Per scegliere le destinazioni di scansione, selezionare **Controllo computer** > **Controllo personalizzato** quindi selezionare **Destinazioni di scansione** specifiche dalla struttura ad albero. Una destinazione di scansione può anche essere specificata in modo più preciso, immettendo il percorso alla cartella del/i file che si desidera includere nel controllo. Se si è interessati esclusivamente alla scansione del sistema senza ulteriori azioni di pulizia, selezionare l'opzione **Scansione senza disinfezione**. È inoltre possibile scegliere tra tre livelli di disinfezione selezionando **Configurazione...** > **Pulizia**.

L'esecuzione di controlli del computer attraverso il controllo personalizzato è un'operazione raccomandata per gli utenti avanzati con precedenti esperienze di utilizzo di programmi antivirus.

4.1.2.2 Destinazioni di scansione specifiche

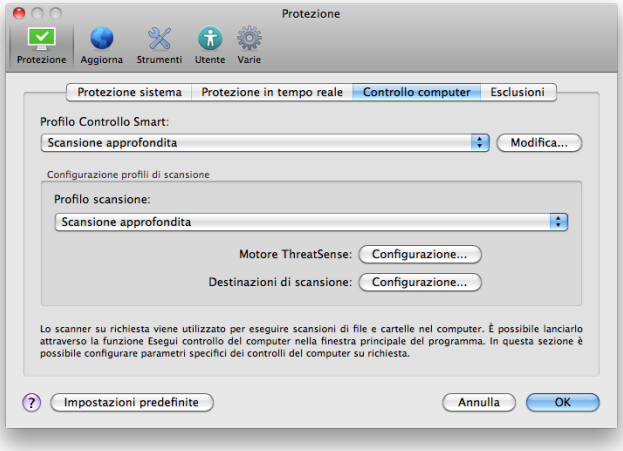
La struttura ad albero delle destinazioni di scansione consente di selezionare i file e le cartelle da sottoporre a scansione anti-virus. È altresì possibile selezionare le cartelle in base alle impostazioni di un determinato profilo.

Una destinazione di scansione può anche essere specificata in modo più preciso, immettendo il percorso alla cartella del/i file che si desidera includere nel controllo. Selezionare le destinazioni dalla struttura ad albero contenente una lista di tutte le cartelle presenti nel computer.

4.1.2.3 Profili di scansione

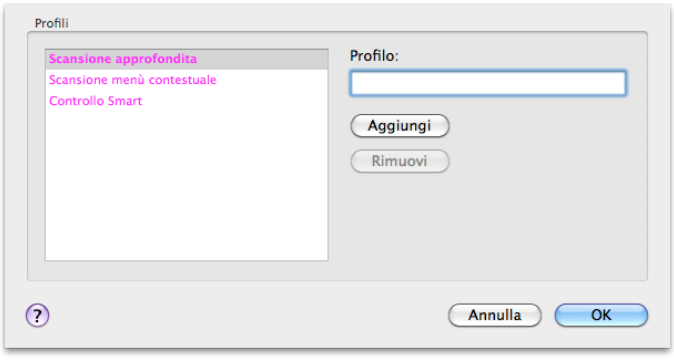
È possibile salvare le impostazioni di scansione preferite per scansioni future. È consigliabile creare un profilo di scansione differente (con diverse destinazioni di scansione, metodi di scansione e altri parametri) per ciascuna scansione utilizzata abitualmente.

Per creare un nuovo profilo, accedere alla sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Protezione** > **Controllo computer** e fare clic su **Modifica...** vicino alla lista dei profili correnti.



Per ricevere assistenza nella creazione di un profilo di scansione adatto alle proprie esigenze, si rimanda alla sezione Configurazione parametri motore ThreatSense 13 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 Smart 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 di Massima pulitura. Nella finestra **Lista profili scanner su richiesta**, digitare il nome del profilo, fare clic sul pulsante **Aggiungi** e confermare facendo clic su **OK**. Specificare quindi i parametri in base alle proprie esigenze impostando **Motore ThreatSense** e **Destinazioni di scansione**.



4.1.3 Configurazione parametri motore ThreatSense

ThreatSense è il nome di una tecnologia che consiste in una serie di complessi metodi di rilevamento delle minacce. Questa tecnologia è proattiva, il che significa che fornisce protezione anche durante le prime ore di diffusione di una nuova minaccia. Essa utilizza una combinazione di diversi metodi (analisi del codice, emulazione del codice, firme generiche, firme antivirali) che operano in modo integrato per potenziare in modo significativo 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 della tecnologia ThreatSense consentono di specificare vari parametri di scansione:

- 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** > **Antivirus e antispyware** > **Configurazione avanzata della protezione antivirus e antispyware** quindi fare clic sul pulsante **Configurazione...** posizionato nei caratteri jolly **Protezione del sistema**, **Protezione in tempo reale** e **Controllo computer**, che utilizzano tutti la tecnologia ThreatSense (vedere sezione sottostante). Scenari di protezione diversi possono richiedere configurazioni diverse. Ciò detto, ThreatSense è configurabile singolarmente per i seguenti moduli di protezione:

- **Protezione del sistema** > Controllo automatico file di avvio
- **Protezione file system in tempo reale** > Protezione file system in tempo reale
- **Controllo computer** > Controllo computer su richiesta

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 delle impostazioni per la scansione degli eseguibili compressi o per l'attivazione della scansione euristica avanzata nel modulo di protezione del file system in tempo reale potrebbe risultare in un rallentamento del sistema. È quindi consigliabile non modificare i parametri predefiniti di ThreatSense per tutti i moduli, con l'eccezione di Controllo computer.

4.1.3.1 Oggetti

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

- **File** - consente di eseguire il controllo di tutti i tipi di file più comuni (programmi, immagini, file audio, file video, database e così via).
- **Link simbolici** - (Solo per scansione su richiesta): consentono di effettuare la scansione di tipologie speciali di file contenenti una stringa di testo interpretata e seguita dal sistema operativo come percorso ad un altro file o directory.
- **File di e-mail** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare la scansione di file speciali contenenti messaggi di posta elettronica.
- **Caselle di posta** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare la scansione delle caselle di posta del sistema. Un uso scorretto di questa opzione potrebbe determinare un conflitto con il client e-mail. Per ulteriori informazioni relative ai vantaggi e svantaggi di tale opzione, vi invitiamo a leggere il seguente articolo relativo alla knowledge base.
- **Archivi** - consente di eseguire il controllo dei file compressi in archivi (.rar, .zip, .arj, .tar e così via).
- **Archivi autoestraenti** - (non disponibile nel caso della protezione in tempo reale): consente di effettuare la scansione dei file contenuti in archivi autoestraenti.
- **Eseguibili compressi** - a differenza dei file di archivio standard, i file eseguibili compressi vengono decompressi in memoria, in aggiunta agli eseguibili statici standard (UPX, yoda, ASPack, FGS e così via).

4.1.3.2 Opzioni

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

- **Database delle firme antivirali** - Le firme consentono di rilevare e identificare in modo esatto e affidabile le infiltrazioni in base al nome, utilizzando il database delle firme antivirali.
- **Euristica** - L'euristica è un algoritmo che analizza le attività (dannose) dei programmi. Il vantaggio principale del rilevamento euristico consiste nella possibilità di rilevare un nuovo software dannoso che in precedenza non esisteva o che non era incluso nell'elenco dei virus conosciuti (database di firme antivirali).
- **Euristica avanzata** - L'euristica avanzata comprende un algoritmo di euristica unico sviluppato da ESET e ottimizzato per il rilevamento di worm e trojan horse scritto in linguaggi di programmazione di alto livello. Grazie all'euristica avanzata, la capacità di rilevamento del programma è decisamente più elevata.
- **Adware/Spyware/Riskware** - Questa categoria comprende software che raccolgono informazioni riservate sugli utenti senza il loro consenso informato. Questa categoria comprende anche il software che consente di visualizzare materiale pubblicitario.
- **Applicazioni potenzialmente indesiderate** - Si tratta di applicazioni non necessariamente dannose. Tuttavia, esse potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. I cambiamenti più significativi comprendono finestre popup indesiderate, attivazione ed esecuzione di processi nascosti, aumento dell'utilizzo delle risorse di sistema, modifiche dei risultati delle ricerche e applicazioni che comunicano con server remoti.
- **Applicazioni potenzialmente pericolose** - tali applicazioni si riferiscono a software commerciali e legali che possono essere sfruttati dagli aggressori informatici se installati all'insaputa dell'utente. Tale classificazione comprende programmi quali strumenti di accesso remoto. Pertanto, questa opzione è disattivata di default.

4.1.3.3 Pulizia

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

- **Nessuna pulitura** - I file infetti non vengono puliti automaticamente. Il programma consentirà di visualizzare una finestra di avviso per consentire all'utente di scegliere un'azione.
- **Pulizia standard** - Il programma tenterà di pulire o eliminare automaticamente un file infetto. Se non è possibile selezionare automaticamente l'azione corretta, il programma proporrà una serie di azioni di follow-up. La scelta tra queste azioni verrà visualizzata anche nel caso in cui non possa essere completata un'azione predefinita.
- **Massima disinfezione** - Il programma pulirà o eliminerà tutti i file infetti (inclusi gli archivi). Le uniche eccezioni sono rappresentate dai file di sistema. Nel caso in cui non fosse possibile pulirli, l'utente potrà intraprendere un'azione all'interno di una finestra di avviso.

Allarme: Nella modalità di pulizia standard, viene eliminato l'intero file di archivio solo se tutti i file contenuti sono infetti. Nel caso in cui fossero presenti anche file non infetti, esso non verrà eliminato. Se nella modalità di Massima pulizia viene rilevato un file di archivio infetto, verrà eliminato l'intero file, anche se sono presenti file puliti.

4.1.3.4 Estensioni

Un'estensione è la parte del nome di un file delimitata da un punto. L'estensione definisce il tipo e il contenuto del file. Questa sezione delle impostazioni dei parametri ThreatSense consente di definire i tipi di file da escludere dalla scansione.

Di default, tutti i file vengono sottoposti a scansione indipendentemente dall'estensione. È possibile aggiungere qualunque estensione all'elenco dei file esclusi dalla scansione. I pulsanti **Aggiungi** e **Rimuovi** consentono di attivare o impedire la scansione delle estensioni desiderate.

L'esclusione di file dalla scansione è utile nel caso in cui il controllo di determinati tipi di file impedisse il corretto funzionamento di un programma che utilizzi le estensioni. Ad esempio, è consigliabile escludere le estensioni *.log*, *.cfg* e *.tmp*.

4.1.3.5 Limiti

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

- **Dimensioni massime:** Consente di definire la dimensione massima degli oggetti da sottoporre a scansione. Il modulo antivirus eseguirà unicamente la scansione degli oggetti di dimensioni inferiori a quelle specificate. Si consiglia di non modificare il valore predefinito, poiché di norma non sussiste alcun motivo per farlo. Questa opzione dovrebbe essere modificata solo da utenti esperti che abbiano ragioni particolari per escludere oggetti di dimensioni maggiori dalla scansione.
- **Durata massima scansione:** 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 di un oggetto una volta raggiunto tale valore temporale, indipendentemente dal fatto che la scansione sia stata completata.
- **Massimo livello di ricerca:** Consente di specificare il livello massimo di scansione degli archivi. Si consiglia di non modificare il valore predefinito di 10; in circostanze normali non sussiste alcun motivo per farlo. Se la scansione termina prima del tempo a causa del numero di archivi nidificati, l'archivio non verrà controllato.
- **Dimensione massima file:**Questa opzione consente di specificare le dimensioni massime dei file contenuti all'interno degli archivi da sottoporre a scansione una volta estratti. Se, a causa di tale limite, la scansione termina prima del tempo, l'archivio non verrà controllato.

4.1.3.6 Altri

Al fine di garantire il miglior livello di scansione, l'attivazione di Smart Optimization 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. L'ottimizzazione smart non è definita in modo rigido all'interno del prodotto. Il team di sviluppo ESET provvede costantemente all'implementazione di nuove modifiche che vengono successivamente integrate in ESET NOD32 Antivirus attraverso aggiornamenti regolari. Se l'opzione Smart Optimization non è attivata, durante la scansione vengono applicate solo le impostazioni definite dall'utente nell'architettura ThreatSense di moduli specifici.

Esegui scansione flussi dati alternativi (Solo per scansione su richiesta)
I flussi di dati alternativi (fork risorsa/dati) utilizzati dal file system consistono in associazioni di file e cartelle invisibili alle tecniche di scansione standard. Numerose infiltrazioni cercano di non essere rilevate presentandosi come flussi di dati alternativi.

4.1.4 Rilevamento di un'infiltrazione

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

Se il computer mostra segnali di infezione da malware (ad esempio appare più lento, si blocca spesso e così via), è consigliabile seguire le seguenti istruzioni:

1. Aprire ESET NOD32 Antivirus e fare clic su **Scansione computer**.
2. Fare clic su **Controllo Smart** (per ulteriori informazioni, vedere la sezione Smart Scan 12).
3. Al termine della scansione, controllare nel registro il numero di file sottoposti a scansione, di file infetti e di file puliti.

Se si desidera effettuare il controllo solo di una parte del disco, scegliere **Controllo personalizzato** e selezionare le destinazioni da controllare alla ricerca di virus.

Per avere un'idea generale di come ESET NOD32 Antivirus gestisce le infiltrazioni, si supponga che il monitoraggio del file system in tempo reale, che utilizza il livello di pulizia predefinito, rilevi un'infiltrazione. Verrà eseguito il tentativo di pulire o eliminare il file. In assenza di azioni predefinite nel modulo di protezione in tempo reale, verrà chiesto all'utente di selezionare un'opzione in una finestra di avviso. Le opzioni generalmente disponibili sono **Pulisci**, **Elimina** e **Nessuna azione**. Non è consigliabile selezionare **Nessuna azione**, perché con tale opzione si lascia(no) i(l) file infetto/i inalterato/i. È opportuno selezionare questa opzione solo quando si è certi che il file non è pericoloso e che si tratta di un errore di rilevamento.

Pulizia ed eliminazione - Applicare la pulizia nel caso in cui un file sia stato attaccato da un virus che ha aggiunto al file pulito un codice dannoso. In tal caso, tentare in primo luogo di pulire il file infetto per ripristinarne lo stato originale. Nel caso in cui il file sia composto esclusivamente da codici dannosi, verrà eliminato.

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 se anche dovessero contenere file puliti non dannosi. È tuttavia consigliabile essere prudenti durante l'esecuzione di una scansione di **Massima pulizia**, poiché in questa modalità l'archivio viene eliminato anche se contiene un solo file infetto, indipendentemente dallo stato degli altri file dell'archivio.

4.2 Aggiornamento del programma

Per garantire il massimo livello di sicurezza sono necessari aggiornamenti regolari di ESET NOD32 Antivirus. Il modulo di aggiornamento garantisce l'aggiornamento costante del programma grazie all'aggiornamento del database delle firme antivirali.

Facendo clic su **Aggiorna** nel menu principale, è possibile visualizzare lo stato corrente degli aggiornamenti, comprese la data e l'ora dell'ultimo aggiornamento riuscito e capire se sia necessario un aggiornamento. Per avviare manualmente il processo di aggiornamento, fare clic su **Aggiorna database delle firme antivirali**.

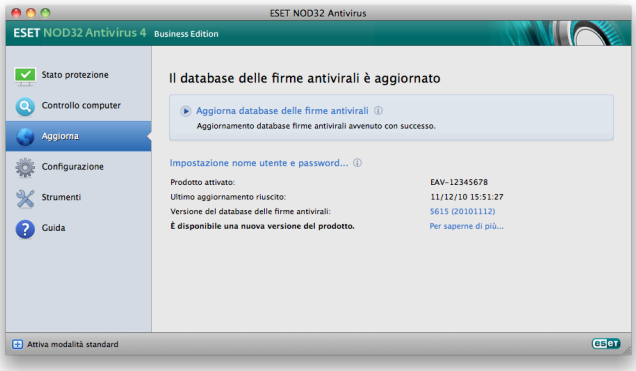
In circostanze normali, quando gli aggiornamenti sono scaricati correttamente, viene visualizzato il messaggio **Il database delle firme antivirali è aggiornato** nella finestra Aggiornamento. Se non è possibile aggiornare il database delle firme antivirali, si raccomanda di verificare le impostazioni di aggiornamento 16 - la causa più frequente per questo errore è l'immissione errata di dati di autenticazione (Nome utente e Password) o la configurazione errata delle impostazioni di connessione 21.

La finestra di aggiornamento contiene anche informazioni relative alla versione del database di 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.

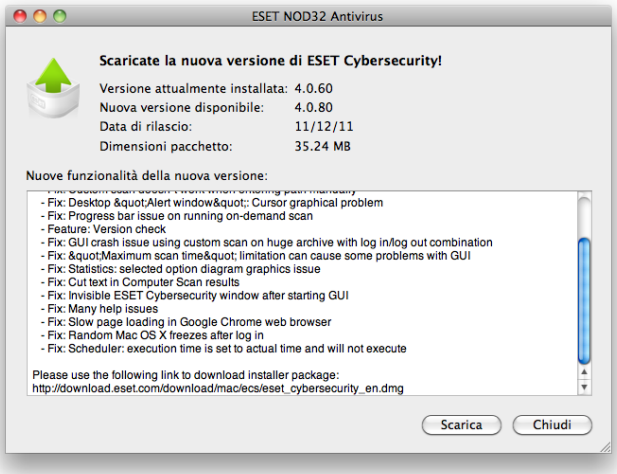
NOTA: Il nome utente e la password vengono forniti da ESET dopo l'acquisto di ESET NOD32 Antivirus.

4.2.1 Aggiornamento a una nuova build

Per assicurare la massima protezione, è importante utilizzare la build più recente di ESET NOD32 Antivirus. Per verificare la disponibilità di una nuova versione, fare clic su **Aggiorna** dal menu principale a sinistra. Se è disponibile una nuova build, sulla parte inferiore della finestra verrà visualizzato il messaggio *È disponibile una nuova versione del prodotto.*. Fare clic su **Per saperne di più...** per visualizzare una nuova finestra contenente il numero di versione della nuova build e il ChangeLog.



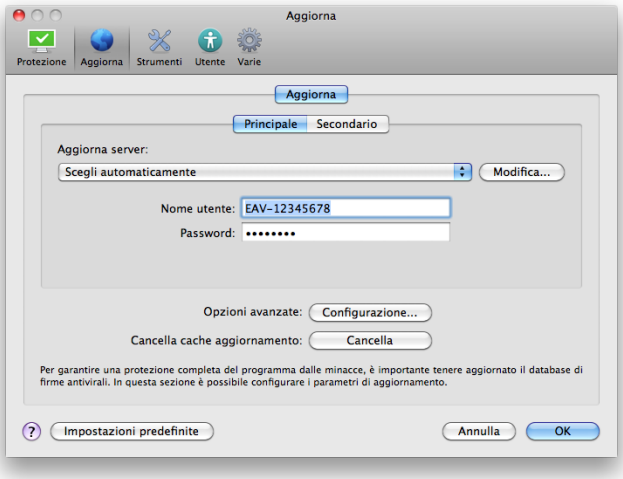
Fare clic su **Download** per scaricare la build più recente. Fare clic su **Chiudi** per chiudere la finestra e scaricare l'aggiornamento in seguito.



Se si seleziona **Download**, il file verrà scaricato nella cartella Download o nella cartella predefinita impostata dal browser in uso. Al termine del download, avviare il file e attenersi alle istruzioni di installazione. Il nome utente e la password verranno trasferiti automaticamente alla nuova installazione. Si consiglia di verificare periodicamente la disponibilità degli aggiornamenti, soprattutto quando si esegue l'installazione di ESET NOD32 Antivirus tramite CD/DVD.

4.2.2 Impostazione dell'aggiornamento

La sezione Impostazione aggiornamento consente di specificare informazioni sull'origine dell'aggiornamento, come i server di aggiornamento e i dati per l'autenticazione per tali server. In base all impostazioni predefinite, il menu a tendina **Server di aggiornamento** è impostato su **Scegli automaticamente** per garantire che i file di aggiornamento verranno scaricati automaticamente dal server ESET con meno traffico di rete.



L'elenco dei server di aggiornamento disponibili è accessibile tramite il menu a tendina **Server di aggiornamento**. Per aggiungere un nuovo server di aggiornamento, fare clic su **Modifica...** Successivamente, inserire l'indirizzo del nuovo server nel campo di inserimento **Server di aggiornamento** e fare clic sul pulsante **Aggiungi**. L'autenticazione per i server di aggiornamento si basa sul **Nome utente** e sulla **Password** generati e inviati dopo l'acquisto del programma.

Per attivare l'utilizzo della modalità test (download degli aggiornamenti pre-rilascio), fare clic sul pulsante **Configura...** accanto a **Opzioni avanzate**, quindi selezionare la casella di controllo **Attiva aggiornamenti pre-rilascio**. Per disattivare la visualizzazione delle notifiche sulla barra delle applicazioni al completamento dell'aggiornamento eseguito con successo, selezionare la casella di controllo **Non visualizzare notifiche relative agli aggiornamenti avvenuti con successo**.

Per eliminare tutti i dati di aggiornamento archiviati temporaneamente, fare clic sul pulsante **Cancella** accanto a **Cancella cache aggiornamento**. Utilizzare questa opzione in caso di problemi relativi all'aggiornamento.

4.2.3 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.

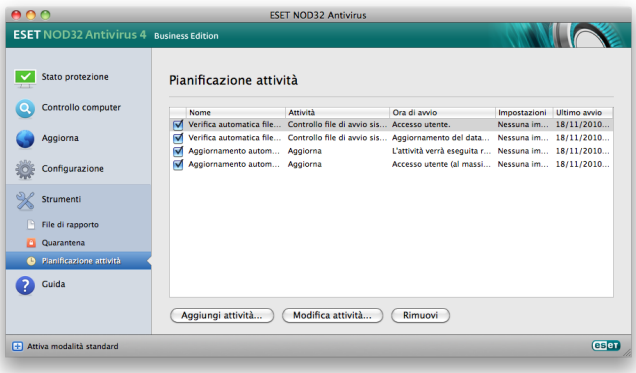
Gli aggiornamenti possono essere eseguiti anche come attività programmate. Per configurare un'attività programmata, fare clic su **Strumenti** > **Pianificazione attività**. Di default, in ESET NOD32 Antivirus sono attivate le seguenti attività:

- **Aggiornamento automatico regolare**
- **Aggiornamento automatico dopo l'accesso dell'utente**

È possibile modificare ciascuna di queste 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, vedere la sezione Pianificazione attività 16.

4.3 Pianificazione attività

La **Pianificazione attività**è disponibile se viene attivata la Modalità avanzata in ESET NOD32 Antivirus. È possibile trovare la Pianificazione attività nel menu principale di ESET NOD32 Antivirus in **Strumenti**. La **Pianificazione attività** contiene un elenco di tutte le attività pianificate e delle relative proprietà di configurazione, come data, ora e profilo di controllo predefiniti utilizzati.



Di default, in Pianificazione attività vengono visualizzate le attività pianificate seguenti:

- Aggiornamento automatico regolare

- Aggiornamento automatico dopo l'accesso dell'utente
- Controllo automatico file di avvio dopo l'accesso dell'utente
- Controllo automatico file di avvio dopo il completamento dell'aggiornamento del database delle firme antivirali
- Manutenzione rapporto (dopo aver attivato l'opzione **Mostra attività di sistema** nella configurazione della pianificazione attività)

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

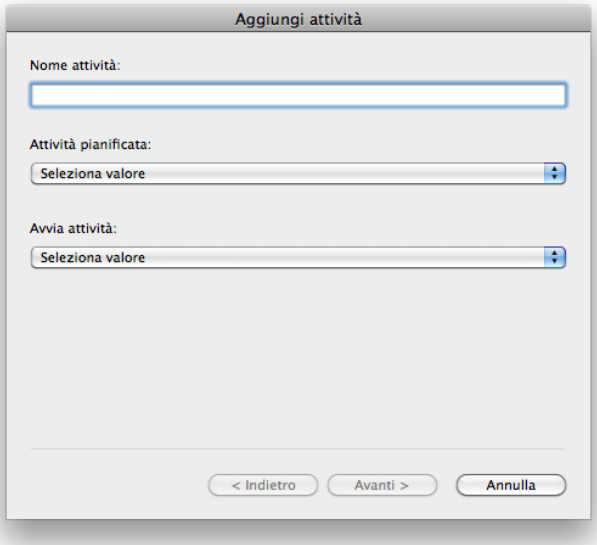
4.3.1 Scopo della pianificazione attività

La Pianificazione attività consente di gestire e avviare attività pianificate con le configurazioni e le proprietà predefinite. La configurazione e le proprietà contengono informazioni quali la data e l'ora, oltre ai profili specificati da utilizzare durante l'esecuzione dell'attività.

4.3.2 Creazione di nuove attività

Per creare una nuova attività in Pianificazione attività, fare clic sul pulsante **Aggiungi attività...** oppure fare clic con il tasto destro del mouse e selezionare **Aggiungi...** dal menu contestuale. Sono disponibili cinque tipi di attività pianificate:

- **Esegui applicazione**
- **Aggiorna**
- **Manutenzione rapporto**
- **Controllo computer su richiesta**
- **Controllo del file di avvio del sistema**



Poiché gli aggiornamenti rappresentano le attività pianificate utilizzate con maggiore frequenza, di seguito verranno illustrate le modalità in cui è possibile aggiungere una nuova attività di aggiornamento.

Dal menu a tendina **Attività pianificata**, selezionare **Aggiorna**. Inserire il nome dell'attività nel campo **Nome attività**. Selezionare la frequenza dell'attività dal menu a tendina **Esegui attività**. Sono disponibili le seguenti opzioni: **Definito dall'utente**, **Una volta**, **Ripetutamente**, **Ogni giorno**, **Ogni settimana** e **Quando si verifica un evento**. In base alla frequenza selezionata, verrà richiesto di specificare i diversi parametri di aggiornamento. È quindi possibile definire l'azione da intraprendere se l'attività non può essere eseguita o completata nei tempi programmati. Sono disponibili le tre opzioni riportate di seguito:

- **Attendi l'ora pianificata successiva**
- **Esegui l'attività appena possibile**
- **Esegui subito l'attività se il periodo trascorso dall'ultima esecuzione supera l'intervallo specificato** (è possibile definire l'intervallo utilizzando la casella di scorrimento **Intervallo minimo di attività**)

Nel passaggio successivo viene visualizzata una finestra contenente un riepilogo delle informazioni relative all'attività corrente pianificata. Fare clic sul pulsante **Fine**.

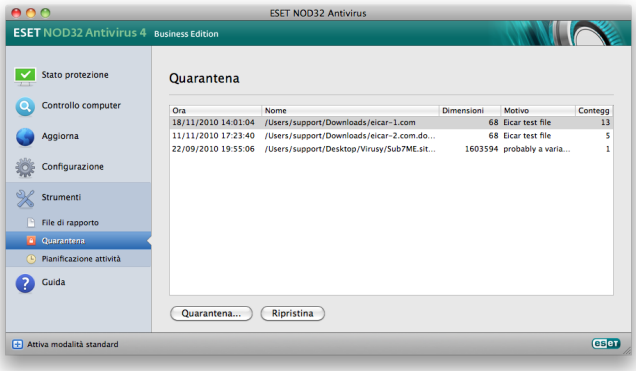
La nuova attività pianificata verrà aggiunta all'elenco delle attività pianificate correnti.

Di default, il sistema contiene attività pianificate essenziali per garantire il corretto funzionamento del sistema. Poiché tali attività non devono essere modificate, sono nascoste di default. Per modificare tale opzione e rendere visibili tali attività, accedere alla sezione **Configurazione** > **Immettere preferenze applicazione ...** > **Strumenti** > **Pianificazione attività** e selezionare l'opzione **Mostra attività di sistema**.

4.4 Quarantena

Lo scopo 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 ai laboratori ESET preposti allo studio delle minacce.



I file salvati nella cartella di 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, aggiunto dall'utente...) e il numero di minacce (ad esempio, se si tratta di un archivio contenente più infiltrazioni). La cartella di quarantena

contenente i file in quarantena (*/Library/Application Support/Eset/cache/esets/quarantine*) rimane all'interno del sistema anche in seguito alla disinstallazione di ESET NOD32 Antivirus. I file in quarantena sono archiviati in un formato sicuro criptato e possono essere ripristinati dopo l'installazione di ESET NOD32 Antivirus.

4.4.1 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 con un clic sul pulsante **Quarantena**. Per questa operazione è possibile utilizzare anche il menu contestuale. Fare clic con il pulsante destro del mouse nella finestra **Quarantena**, scegliere il file che si desidera mettere in quarantena, quindi fare clic sul pulsante **Apri**.

4.4.2 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 tasto destro del mouse sul file desiderato nella finestra di **Quarantena** e facendo clic su **Ripristina**. 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.

4.4.3 Invio di file dalla Quarantena

Se è stato messo in quarantena un file sospetto che non è stato rilevato dal programma, o se un file è stato valutato erroneamente come infetto (ad esempio da un'analisi euristica del codice) e quindi messo in quarantena, inviare il file al laboratorio ESET dedicato allo studio delle minacce. Per inviare un file dalla cartella di quarantena, fare clic con il tasto destro del mouse sul file e selezionare **Invia per analisi** dal menu contestuale.

4.5 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 uno strumento essenziale per l'analisi del sistema, per il rilevamento delle minacce e per la risoluzione dei problemi. La registrazione viene eseguita attivamente in background, senza che sia richiesto l'intervento 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 dal menu principale di ESET NOD32 Antivirus facendo clic su **Strumenti** > **File di rapporto**. Selezionare il tipo di rapporto desiderato dal menu a tendina **Rapporto** nella parte superiore della finestra. Sono disponibili i rapporti seguenti:

1. **Minacce rilevate** - Scegliere questa opzione per visualizzare tutte le informazioni sugli eventi relativi al rilevamento delle infiltrazioni.
2. **Eventi** - Questa opzione è utile agli amministratori del sistema e agli utenti per risolvere i problemi. Tutte le azioni importanti eseguite da ESET NOD32 Antivirus vengono registrate nei rapporti degli eventi.
3. **Controllo computer** - In questa finestra vengono visualizzati i risultati di tutte le scansioni completate. Fare doppio clic su una voce per visualizzare i dettagli del rispettivo controllo del computer su richiesta.

In ciascuna sezione, le informazioni visualizzate possono essere copiate direttamente negli Appunti, selezionando la voce desiderata e facendo clic sul pulsante **Copia**.

4.5.1 Manutenzione rapporto

La configurazione della registrazione di ESET NOD32 Antivirus è accessibile dalla finestra principale del programma. Fare clic su **Configurazione** > **Inserisci preferenze applicazione ...** > **Strumenti** > **File di rapporto**. È possibile specificare le opzioni seguenti per i file di rapporto:

- **Elimina automaticamente i file di rapporto** - le voci del rapporto con data precedente al numero di giorni specificato vengono automaticamente eliminate.
- **Ottimizza automaticamente i file di rapporto** - i file di rapporto vengono automaticamente deframmentati se viene superata la percentuale specificata di record inutilizzati

Per configurare il **Filtro predefinito dei record di rapporto** fare clic sul pulsante **Modifica...** e selezionare/deselezionare i tipi di rapporto come richiesto.

4.5.2 Filtraggio rapporti

I rapporti memorizzano le informazioni relative a eventi importanti di sistema. La funzione di filtro del rapporto consente di visualizzare i record di un determinato tipo di evento.

I tipi di rapporto utilizzati più spesso sono elencati di seguito:

- **Allarmi critici** - errori critici di sistema (es. Impossibile avviare la protezione antivirus)
- **Errori** - messaggi di errore come "*Errore durante il download del file*" ed errori critici
- **Allarmi** - messaggi di allarme
- **Record informativi**- messaggi informativi che includono gli aggiornamenti riusciti, gli avvisi, gli errori e così via.
- **Record diagnostici** - informazioni necessarie per la sincronizzazione ottimale del programma nonché di tutti i record riportati sopra.

4.6 Interfaccia utente

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. È possibile accedere a tali opzioni di configurazione dalla sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Utente** > **Interfaccia**.

In questa sezione, l'opzione relativa alla modalità avanzata consente agli utenti di passare alla Modalità avanzata. La Modalità avanzata consente di visualizzare impostazioni più dettagliate e controlli aggiuntivi per ESET NOD32 Antivirus.

Per avviare la funzionalità relativa alla schermata iniziale, selezionare l'opzione **Mostra schermata iniziale all'avvio**.

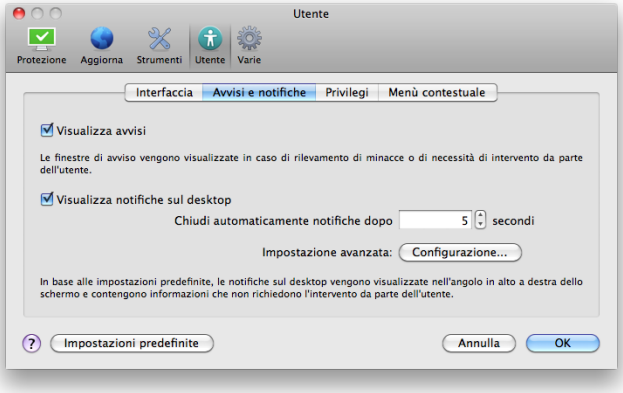
Nella sezione **Utilizza menu standard** è possibile selezionare le opzioni **In modalità standard/In modalità avanzata** per consentire l'utilizzo del menu standard nella finestra principale del programma nella/e rispettiva/e modalità di visualizzazione.

Per attivare l'utilizzo delle descrizioni dei comandi, selezionare l'opzione **Mostra descrizioni comandi**. L'opzione **Mostra file nascosti** consente di visualizzare e selezionare i file nascosti nella configurazione **Destinazioni di scansione** di un **Controllo computer**.

4.6.1 Avvisi e notifiche

La sezione **Avvisi e notifiche** consente di configurare la gestione dei messaggi di avviso e delle notifiche di sistema in ESET NOD32 Antivirus.

La disattivazione dell'opzione **Visualizza avvisi** annullerà tutte le finestre di avviso ed è pertanto adatta solo a situazioni specifiche. Nella maggior parte dei casi, è consigliabile non modificare l'opzione predefinita (attivata).



La selezione dell'opzione **Visualizza notifiche sul desktop** consentirà di attivare le finestre di avviso che non richiedono l'interazione da parte dell'utente per poterle visualizzare sul desktop (di default, l'angolo in alto a destra dello schermo). È possibile definire il periodo durante il quale verrà visualizzata una notifica modificando il valore **Chiudi automaticamente notifiche dopo** X **secondi**.

4.6.1.1 Configurazione avanzata avvisi e notifiche

Consente di visualizzare solo le notifiche che richiedono l'interazione dell'utente
Questa opzione consente di alternare la visualizzazione dei messaggi che richiedono l'interazione dell'utente.

Consente di visualizzare solo le notifiche che richiedono l'interazione dell'utente quando sono in esecuzione applicazioni in modalità a schermo intero
Questa opzione è utile nel caso di presentazioni, giochi o altre attività che richiedono la visualizzazione a schermo intero.

4.6.2 Privilegi

Le impostazioni di ESET NOD32 Antivirus rivestono un ruolo fondamentale dal punto di vista dei criteri di sicurezza dell'organizzazione di appartenenza. Modifiche non autorizzate potrebbero mettere a rischio la stabilità e la protezione del sistema. Di conseguenza, è possibile scegliere quali utenti potranno modificare la configurazione del programma.

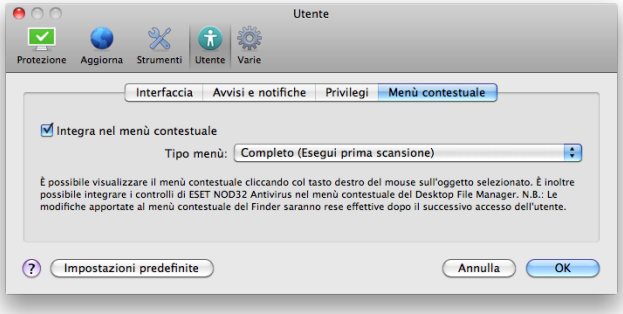
Per specificare gli utenti con privilegi, accedere alla sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Utente** > **Privilegi**.

Per garantire la massima sicurezza del sistema, è necessario configurare correttamente il programma. Qualsiasi modifica non autorizzata può provocare la perdita di dati importanti. Per definire una lista di utenti con privilegi, selezionarli dalla lista **Utenti** sul lato sinistro e fare clic sul pulsante **Aggiungi** . Per rimuovere un utente, selezionarne il nome nella lista **Utenti con privilegi** sulla destra e fare clic su **Rimuovi**.

NOTA: Se la lista di utenti con privilegi è vuota, tutti gli utenti del sistema saranno autorizzati a modificare le impostazioni del programma.

4.6.3 Menù contestuale

È possibile attivare l'integrazione del menu contestuale nella sezione **Configurazione** > **Inserisci preferenze applicazione ...** > **Utente** > **Menù contestuale** attivando la casella di controllo **Integra nel menu contestuale**.



4.7 ThreatSense.Net

Il sistema di allarme immediato ThreatSense.Net invia informazioni tempestive e costanti a ESET relative alle nuove infiltrazioni. Il sistema di allarme immediato bidirezionale ThreatSense.Net ha un unico scopo: migliorare la protezione offerta da ESET. Il modo migliore per assicurarsi che le nuove minacce siano riconosciute da ESET nel momento stesso della loro apparizione è il "collegamento" con il numero maggiore di clienti possibile da utilizzare come "esploratori di minacce". Sono disponibili due opzioni:

1. È possibile decidere di non abilitare il sistema di allarme immediato ThreatSense.Net. Non verranno perse funzionalità del software, che continuerà ad offrire la migliore protezione in assoluto.
2. È possibile configurare il sistema di allarme immediato ThreatSense.Net 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. L'analisi di tali minacce consentirà a ESET di aggiornare il database di minacce e di potenziare le capacità di rilevamento.

Il sistema di allarme immediato ThreatSense.Net 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.

Sebbene esista la possibilità che vengano trasmesse occasionalmente informazioni sull'utente o sul computer (nomi utenti nel percorso di una directory, ecc.) ai laboratori ESET preposti allo studio delle minacce, tali informazioni saranno utilizzate ESCLUSIVAMENTE allo scopo di rispondere in modo immediato alle nuove minacce.

La configurazione di ThreatSense.Net è accessibile dalla finestra di Configurazione avanzata, in **Strumenti** > **ThreatSense.Net**. Selezionare l'opzione **Attiva Sistema di allarme immediato ThreatSense.Net** per attivarla, quindi fare clic sul pulsante **Configura...** vicino alla voce Opzioni avanzate.

4.7.1 File sospetti

L'opzione File sospetti consente di configurare il modo in cui le minacce vengono inviate al laboratorio ESET preposto allo studio delle minacce per sottoporle ad analisi.

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

Invio di file sospetti - È possibile scegliere di inviare tali file **Durante l'aggiornamento**. Ciò significa che essi verranno inviati al Laboratorio ESET preposto allo studio delle minacce durante un aggiornamento del database delle firme antivirali. In alternativa, è possibile scegliere di inviarli **Il prima possibile** - questa impostazione è adatta nel caso in cui si utilizzi una connessione permanente a Internet.

Se non si desidera inviare i file, selezionare l'opzione **Non inviare**. La scelta di non inviare i file per l'analisi non influirà sull'invio di informazioni statistiche, il quale verrà configurato in un'area distinta.

Il sistema di allarme immediato ThreatSense.Net raccoglierà informazioni anonime sul computer degli utenti in relazione alle nuove minacce rilevate. Queste informazioni potrebbero comprendere il nome dell'infiltrazione, la data e l'ora del rilevamento, la versione del prodotto ESET Smart Security, la versione del sistema operativo in uso e le impostazioni di ubicazione. In genere, le statistiche vengono inviate ai server ESET una o due volte al giorno.

Di seguito è riportato un esempio di pacchetto di statistiche inviato:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=9.5.0
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=Users/UserOne/Documents/Incoming/rdgFR1463
[1].zip
```

Invio di dati statistici anonimi- È possibile definire quando inviare le informazioni statistiche. Se si sceglie di eseguire l'invio **Il prima possibile**, le informazioni statistiche verranno inviate subito dopo essere state create. Questa impostazione è adatta nel caso in cui si utilizzi una connessione permanente a Internet. Se viene selezionata l'opzione **Durante l'aggiornamento**, le informazioni statistiche verranno inviate durante l'aggiornamento dopo essere state raccolte.

Se non si desidera inviare informazioni statistiche anonime, è possibile selezionare l'opzione **Non inviare**.

Distribuzione invio - È possibile scegliere in che modo inviare i file e le informazioni statistiche a ESET. Selezionare l'opzione **Server di amministrazione remota o ESET** per inviare i file e le statistiche con tutti gli strumenti a disposizione. Selezionare l'opzione **Server di amministrazione remota** per inviare i file e le statistiche al server di amministrazione remota, che provvederà a inviarli ai laboratori ESET preposti allo studio delle minacce. Se viene selezionata l'opzione **ESET**, tutti i file sospetti e le informazioni statistiche verranno inviati al laboratorio ESET preposto allo studio dei virus direttamente dal programma.

Filtro di esclusione - Questa opzione consente di escludere dall'invio determinati file e/o cartelle. È utile, ad esempio, escludere file che potrebbero contenere informazioni riservate, ovvero documenti o fogli di calcolo. I tipi di file più comuni sono esclusi di default (*.doc*, ecc.). È possibile aggiungere qualunque tipologia di file alla lista degli elementi esclusi dalla scansione.

Indirizzo e-mail del contatto (facoltativo) - Il contatto e-mail viene inviato insieme ai file sospetti e potrebbe essere utilizzato per contattare l'utente qualora fossero richieste ulteriori informazioni ai fini dell'analisi. È importante notare che l'utente non riceverà una risposta da ESET, a meno che non siano richieste ulteriori informazioni.

5. Utente avanzato

5.1 Importa ed esporta impostazioni

Le configurazioni di importazione ed esportazione di ESET NOD32 Antivirus sono disponibili in modalità avanzata in **Configurazione**.

Sia l'importazione che l'esportazione utilizzano i file di archivio per memorizzare la configurazione. Le opzioni di importazione e di esportazione sono utili nel caso in cui si desideri effettuare il backup della configurazione corrente di ESET NOD32 Antivirus per poterlo utilizzare in un secondo momento. L'opzione di esportazione delle impostazioni è utile anche per quegli utenti che desiderino utilizzare la configurazione preferita di ESET NOD32 Antivirus su più sistemi. In tal modo, infatti, sarà possibile importare facilmente il file di configurazione per il trasferimento delle impostazioni desiderate.

5.1.1 Importa impostazioni

L'importazione della configurazione è molto semplice. Nel menu principale, fare clic su **Configurazione** > **Importa ed esporta impostazioni ...** quindi selezionare l'opzione **Importa impostazioni**. Inserire il nome del file di configurazione o fare clic sul pulsante **Sfoglia...** per ricercare il file di configurazione che si desidera importare.

5.1.2 Esporta impostazioni

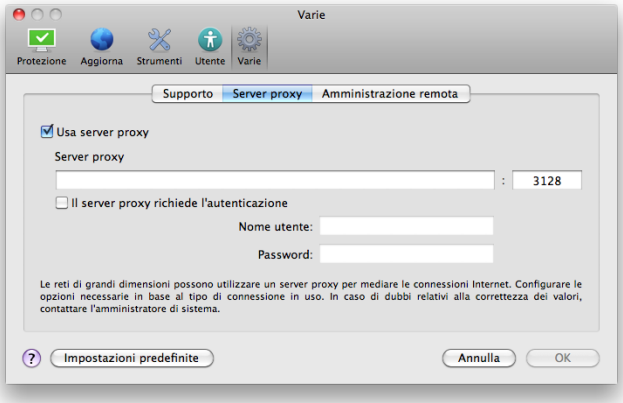
Le operazioni per l'esportazione di una configurazione sono molto simili. Nel menu principale, fare clic su **Configurazione** > **Importa ed esporta impostazioni ...** Selezionare l'opzione **Esporta impostazioni** e immettere il nome del file di configurazione. Utilizzare il browser per selezionare un percorso sul computer in cui salvare il file di configurazione.

5.2 Configurazione del server proxy

È possibile configurare le impostazioni del server proxy in **Varie** > **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 a questo livello, selezionare la casella di controllo **Usa server proxy**, quindi immettere l'indirizzo del server proxy nel campo **Server proxy**, insieme al numero di porta del server proxy.

Se per la comunicazione con il server proxy è necessaria l'autenticazione, selezionare la casella di controllo **Il server proxy richiede l'autenticazione** e immettere **Nome utente** e **Password** validi nei rispettivi campi.



5.3 Blocco supporti rimovibili

I supporti rimovibili (ad esempio, CD o chiavette USB) potrebbero contenere codici dannosi e mettere a rischio il computer. Per bloccare i supporti rimovibili, selezionare l'opzione **Attiva blocco supporti rimovibili**. Per consentire l'accesso a talune tipologie di supporti multimediali, deselezionare i volumi dei supporti desiderati.

5.4 Amministrazione remota

ESET Remote Administrator (ERA) è uno strumento utilizzato per la gestione del sistema di sicurezza e per ottenere una panoramica della sicurezza globale all'interno di una rete. È particolarmente utile quando si applica a reti di una certa dimensione. ERA non determina solo maggiori livelli di sicurezza, ma garantisce anche una facilità di utilizzo nella gestione di ESET NOD32 Antivirus sulle workstation client.

Le opzioni di configurazione dell'amministrazione remota sono disponibili nella schermata principale di ESET NOD32 Antivirus. Fare clic su **Configurazione > Inserisci preferenze applicazione ... > Varie > Amministrazione remota**.

Attivare l'amministrazione remota selezionando l'opzione **Connetti al server di amministrazione remota**. È possibile quindi accedere alle opzioni di seguito descritte:

Intervallo connessioni server - Indica la frequenza con cui ESET NOD32 Antivirus si connetterà a ERA Server. Se il valore impostato è **0**, le informazioni verranno inviate ogni 5 secondi.

Server di amministrazione remota - Indirizzo di rete e numero della porta del server (su cui è installato ERA Server) - questo campo contiene una porta server predefinita utilizzata per la connessione di rete. È consigliabile conservare l'impostazione predefinita della porta su *2222*.

Il server di amministrazione remota richiede l'autenticazione - Password per la connessione a ERA Server, ove richiesta.

Generalmente, è necessario configurare solo il server **Principale**. Se vengono eseguiti più server ERA sulla rete può essere aggiunta un'altra connessione al server **secondario** ERA Server. Esso servirà da soluzione di fallback. Se il server primario diventa inaccessibile, ESET NOD32 Antivirus contatterà automaticamente ERA Server secondario. ESET NOD32 Antivirus cercherà anche di ristabilire la connessione al server principale. Dopo aver riattivato la connessione, ESET NOD32 Antivirus tornerà al server principale. La configurazione di due profili del server di amministrazione remoto è utilizzata in modo più vantaggioso per i client mobili con notebook che si connettono sia dalla rete locale che dall'esterno.

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'infiltrazione che danneggia i file esistenti sul computer. I virus prendono il nome dai virus biologici, poiché utilizzano tecniche simili per diffondersi da un computer all'altro.

I virus attaccano principalmente i file eseguibili, gli script e i documenti. Per replicarsi, un virus allega il suo "corpo" alla fine di un file di destinazione. In breve, un virus funziona nel seguente modo: dopo l'esecuzione del file infetto, il virus si attiva (prima dell'applicazione originale) ed esegue la sua attività predefinita. L'applicazione originale viene eseguita solo dopo questa operazione. Un virus non può infettare un computer a meno che un utente (accidentalmente o deliberatamente) esegua o apra il programma dannoso.

I virus possono essere classificati in base agli scopi e ai diversi livelli di gravità. Alcuni di essi sono estremamente dannosi poiché dispongono della capacità di eliminare di proposito 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.

È importante tenere presente che i virus (se paragonati a trojan o spyware) stanno diventando una rarità, poiché non sono commercialmente allettanti per gli autori di software dannosi. Inoltre, il termine "virus" è spesso utilizzato in modo scorretto per indicare tutti i tipi di infiltrazioni. Attualmente, l'utilizzo di questo termine è stato superato e sostituito dalla nuova e più accurata definizione di "malware" (software dannoso).

Se il computer in uso è infettato da un virus, è necessario ripristinare i file infetti al loro stato originale, ovvero pulirli utilizzando un programma antivirus.

Tra i virus più noti si segnalano: *OneHalf*, *Tenga* e *Yankee Doodle*.

6.1.2 Worm

Un worm è un programma contenente codice dannoso che attacca i computer host e si diffonde tramite una rete. La differenza fondamentale tra un virus e un worm è che i worm hanno la capacità di replicarsi e di viaggiare autonomamente, in quanto non dipendono da file host (o settori di avvio). I worm si diffondono attraverso indirizzi di posta elettronica 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, essi possono espandersi in tutto il mondo entro poche ore dal rilascio e, in taluni casi, perfino entro pochi minuti. 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.

Tra i worm più noti si segnalano: *Lovsan/Blaster*, *Stration/Warezov*, *Bagle* e *Netsky*.

6.1.3 Trojan horse

Storicamente, i trojan horse sono stati definiti come una classe di infiltrazioni che tentano di presentarsi come programmi utili per ingannare gli utenti e indurli a eseguirli. Oggigiorno, tali programmi non hanno più la necessità di camuffarsi. Il loro unico scopo è quello di infiltrarsi il più facilmente possibile e portare a termine i loro obiettivi dannosi. Il termine "Trojan horse" ("cavallo di Troia") ha assunto un'accezione molto generale che indica un'infiltrazione che non rientra in una classe specifica di infiltrazioni.

Poiché si tratta di una categoria molto ampia, è spesso suddivisa in diverse sottocategorie:

- Downloader: un programma dannoso in grado di scaricare altre infiltrazioni da Internet.
- Dropper: un tipo di trojan horse concepito per installare sui computer compromessi altri tipi di malware.
- Backdoor: un'applicazione che comunica con gli aggressori remoti, consentendo loro di ottenere l'accesso a un sistema e prenderne 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 aggressori remoti.
- Dialer - i dialer sono programmi progettati per connettersi a numeri con tariffe telefoniche molto elevate. È quasi impossibile che un utente noti la creazione di una nuova connessione. I dialer possono causare danni solo agli utenti che dispongono di una connessione remota, utilizzata oramai sempre più di rado.
- Solitamente, i Trojan horse assumono la forma di file eseguibili. Se sul computer in uso viene rilevato un file classificato come Trojan horse, si consiglia di eliminarlo, poiché contiene probabilmente codice dannoso.

Tra i trojan più noti si segnalano: *NetBus*, *Trojandownloader.Small.ZL*, *Slapper*.

6.1.4 Adware

Adware è l'abbreviazione di software supportato dalla pubblicità ("advertising-supported software"). Rientrano in questa categoria i programmi che consentono di visualizzare materiale pubblicitario. Le applicazioni adware spesso aprono automaticamente una nuova finestra popup contenente della 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 agli sviluppatori di freeware di coprire i costi di sviluppo delle proprie applicazioni (in genere utili).

L'adware di per sé non è pericoloso, ma gli utenti possono essere infastiditi dai messaggi pubblicitari. Il pericolo sta nel fatto che l'adware può svolgere anche funzioni di rilevamento, allo stesso modo 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.

6.1.5 Spyware

Questa categoria include tutte le applicazioni che inviano informazioni riservate senza il consenso/la 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, di indirizzi e-mail della rubrica dell'utente o un elenco dei tasti digitati.

Gli autori di spyware affermano che queste tecniche hanno l'obiettivo di raccogliere informazioni aggiuntive sulle esigenze e sugli interessi degli utenti per l'invio di pubblicità più mirate. Il problema è 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 spesso sono associati a versioni gratuite di un programma 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 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, l'operazione più appropriata è l'eliminazione dello stesso, in quanto esistono elevate probabilità che il file contenga codice dannoso.

6.1.6 Applicazioni potenzialmente pericolose

Esistono molti programmi legali che servono a 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), si prega di rivolgersi all'amministratore di rete o di rimuovere l'applicazione.

6.1.7 Applicazioni potenzialmente indesiderate

Le applicazioni potenzialmente indesiderate non sono necessariamente dannose. Tuttavia, potrebbero influire negativamente sulle prestazioni del computer in uso. Di norma, tali applicazioni richiedono il consenso per l'installazione. Se sono presenti sul computer, il sistema si comporta in modo diverso rispetto allo stato precedente all'installazione. Le modifiche più significative sono:

- apertura di nuove finestre mai viste in precedenza
- attivazione ed esecuzione di processi nascosti
- maggiore utilizzo delle risorse del sistema
- modifiche dei risultati di ricerca
- applicazioni che comunicano con server remoti.