



Bitdefender[®]

**Bitdefender Endpoint
Security Tools for
Windows**

MANUALE D'USO

Bitdefender Endpoint Security Tools for Windows Manuale d'uso

Data di pubblicazione 2019.11.29

Diritto d'autore© 2019 Bitdefender

Avvertenze legali

Tutti i diritti riservati. Nessuna parte di questo manuale può essere riprodotta o trasmessa in alcuna forma o tramite qualsiasi strumento, elettronico o meccanico, incluse fotocopie, registrazioni, o attraverso qualsiasi informazione di archivio o sistema di recupero dati, senza il consenso scritto di un rappresentante autorizzato di Bitdefender. L'inserimento di brevi citazioni nelle recensioni è possibile solo indicando la fonte citata. Il contenuto non può essere modificato in alcun modo.

Avvertenze e Limiti. Questo prodotto e la sua documentazione sono protetti dal diritto d'autore. Le informazioni su questo documento sono fornite «così come sono» senza alcuna garanzia. Sebbene sia stata adottata ogni precauzione nella preparazione di questo documento, gli autori non hanno alcun obbligo nei confronti di alcuna persona o entità rispetto a qualsiasi perdita o danno causati o che si presume essere stati causati, direttamente o indirettamente, dalle informazioni contenute in questo prodotto.

Questo manuale contiene collegamenti a siti Internet di terze parti, che non sono sotto il controllo di Bitdefender, conseguentemente Bitdefender non è responsabile per il contenuto di qualsiasi sito collegato. Se accedi a siti Internet di terze parti, menzionati in questo manuale, lo farai assumendotene tutti i rischi. Bitdefender fornisce tali collegamenti solo come risorsa, e l'inclusione dei collegamenti non implica che Bitdefender approvi o accetti alcuna responsabilità per il contenuto dei siti di terze parti.

Marchi registrati. In questo manuale potrebbero essere citati nomi e marchi registrati. Tutti i marchi registrati e non in questo documento appartengono ai rispettivi proprietari e vengono rispettosamente riconosciuti.

Indice

Prefazione	iv
1. Finalità e destinatari	iv
2. Come usare questo manuale	iv
3. Convenzioni usate in questo manuale	iv
4. Richiesta di commenti	v
1. Come iniziare	1
1.1. L'icona dell'area di notifica	1
1.2. La finestra principale	2
1.2.1. L'area di stato	3
1.2.2. Cronologia eventi	3
1.3. La finestra Moduli	4
1.4. Menu Azioni	9
2. Eseguire una scansione per i malware	11
2.1. Esaminare un file o una cartella	11
2.2. Eseguire una Scansione veloce	11
2.3. Eseguire una scansione completa	12
2.4. Configurare ed eseguire una scansione personalizzata	13
2.4.1. Tipi di file	14
2.4.2. Che cosa esaminare?	15
2.4.3. Che cosa fare?	16
2.5. Controllare i registri di scansione	17
3. Usare Volume Encryption	18
3.1. Cifrare il tuo sistema	18
3.2. Decriptare il tuo sistema	20
3.3. Verificato lo stato della cifratura	20
3.4. Modificare la password o il PIN di cifratura	20
4. Aggiornamenti	22
4.1. Tipi di aggiornamenti	22
4.2. Verificare se la propria protezione è aggiornata	22
4.3. Eseguire un aggiornamento	23
5. Eventi	24
6. Utilizzare l'interfaccia a linea di comando	25
6.1. Comandi supportati	26
6.2. Codici errore linea di comando	35
7. Ottenere aiuto	37
Glossario	38

Prefazione

1. Finalità e destinatari

Questa documentazione è rivolta agli utenti finali di **Bitdefender Endpoint Security Tools**, il client software Security for Endpoints installato su computer e server per proteggerli da malware e altre minacce Internet, e per applicare policy di controllo degli utenti.

Le informazioni illustrate in questo documento dovrebbero essere facilmente comprensibili da chiunque sia abituato a lavorare in ambiente Windows.

2. Come usare questo manuale

Questa guida è organizzata in modo che sia facile trovare le informazioni richieste.

[«Come iniziare» \(p. 1\)](#)

Ottieni maggiore familiarità con l'interfaccia utente di Bitdefender Endpoint Security Tools.

[«Eseguire una scansione per i malware» \(p. 11\)](#)

Scopri come eseguire le scansioni per i malware.

[«Aggiornamenti» \(p. 22\)](#)

Scopri maggiori informazioni sugli aggiornamenti di Bitdefender Endpoint Security Tools.

[«Eventi» \(p. 24\)](#)

Scopri le attività di Bitdefender Endpoint Security Tools.

[«Ottenere aiuto» \(p. 37\)](#)

Dove cercare e ottenere un aiuto in caso di difficoltà. È inclusa anche una sezione FAQ (Domande frequenti).

3. Convenzioni usate in questo manuale

Convenzioni tipografiche

Nella guida vengono usati diversi stili di testo per una leggibilità migliorata. Il loro aspetto e significato vengono presentati nella tabella sottostante.

Aspetto	Descrizione
business-docs@bitdefender.com	Gli indirizzi e-mail vengono inseriti nel testo come informazioni di contatto.
«Prefazione» (p. iv)	Questo è un link interno, verso una qualche posizione nel documento.
nome file	File e cartelle sono indicati con font monospazio.
opzione	Tutte le opzioni del prodotto sono indicate in grassetto .
parola chiave	Le parole chiave o le frasi importanti sono evidenziate in grassetto .

Avvertenze

Gli avvisi appaiono sotto forma di note di testo, segnalate graficamente, portando alla tua attenzione informazioni aggiuntive relative al paragrafo attuale.



Nota

La nota è una breve osservazione. Anche se la puoi omettere, la nota può fornire informazioni di valore come una caratteristica specifica o un link verso temi collegati.



Importante

Questa richiede attenzione, è sconsigliato saltarla. Solitamente contempla informazioni non critiche ma importanti.

4. Richiesta di commenti

Ti preghiamo di scriverci per indicarci come poter migliorare questa guida e aiutarci a fornire la migliore documentazione possibile.

Puoi contattarci inviando una e-mail a business-docs@bitdefender.com.

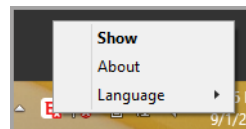
1. COME INIZIARE

Bitdefender Endpoint Security Tools è un programma di sicurezza informatica completamente automatico, gestito in remoto dal proprio amministratore di rete. Una volta installato, ti protegge da ogni tipo di malware (come virus, spyware e trojan), attacchi di rete, phishing e furti di dati. Può anche essere utilizzato per far rispettare le policy di utilizzo di computer e Internet della tua organizzazione. Bitdefender Endpoint Security Tools prenderà la maggior parte delle decisioni relative alla sicurezza per conto tuo, mostrando raramente finestre pop-up di avviso. Maggiori dettagli sulle azioni intraprese e le informazioni sul funzionamento del programma sono disponibili nella cronologia **Eventi**.

1.1. L'icona dell'area di notifica

Al momento dell'installazione, Bitdefender Endpoint Security Tools posiziona un'icona **B** nell'area di notifica. Cliccando due volte su questa icona, si aprirà la finestra principale. Facendo clic con il pulsante destro del mouse sull'icona, un menu contestuale ti fornirà alcune informazioni utili.

- **Mostra** - Apre la finestra principale di Bitdefender Endpoint Security Tools.
- **Informazioni** - Apre una finestra con informazioni su Bitdefender Endpoint Security Tools e indica dove cercare aiuto in caso di problemi inattesi. Questa finestra include anche un link all'Informativa sulla privacy di Bitdefender.
- **Lingua** - Ti consente di modificare la lingua dell'interfaccia utente.
- **Utente esperto** - Ti consente di accedere e modificare le impostazioni di sicurezza, dopo aver fornito la password nella finestra di accesso. Control Center riceve una notifica ogni volta che un endpoint passa in modalità Utente esperto e l'amministratore di Control Center può sempre sovrascrivere le impostazioni di sicurezza locali.



Icona nell'area di notifica





Importante

Questa opzione è disponibile solo se concessa dall'amministratore di rete tramite le impostazioni della policy.

Questa opzione non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

L'icona di Bitdefender Endpoint Security Tools nell'area di notifica ti segnala la presenza di eventuali problemi sul computer, modificando il suo aspetto:

-  Critical issues affect the security of the system.
-  Some issues affect the security of the system.




Nota

L'amministratore di rete può scegliere di nascondere l'icona dell'area di notifica.

1.2. La finestra principale

La finestra principale di Bitdefender Endpoint Security Tools ti consente di verificare lo stato della protezione ed eseguire attività di scansione. Tutto è a pochi clic di distanza. La gestione e la configurazione della protezione vengono eseguite in remoto dall'amministratore di rete.

Per accedere all'interfaccia principale di Bitdefender Endpoint Security Tools, raggiungi il menu Start di Windows, seguendo il percorso **Start** → **Tutti i programmi** → **Bitdefender Endpoint Security Tools** → **Apri console di sicurezza** o, più rapidamente, clicca due volte sull'icona di Bitdefender Endpoint Security Tools  nell'area di notifica.



Finestra principale

La finestra è organizzata in due sezioni principali:

- Stato
- Cronologia eventi

1.2.1. L'area di stato

L'area di **Stato** offre informazioni utili sulla sicurezza del sistema.



Area di stato

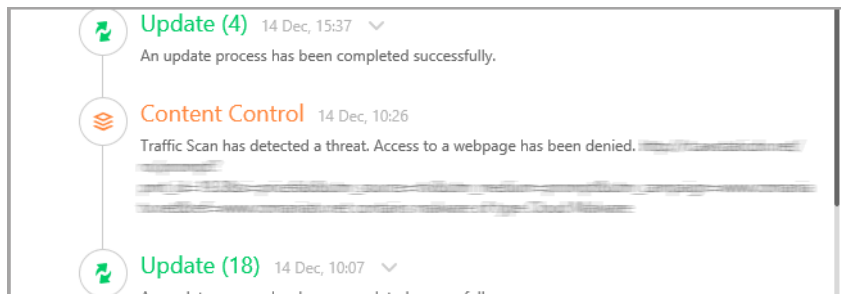
Puoi identificare facilmente lo stato di sicurezza attuale in base al simbolo di stato mostrato alla sinistra dell'area di stato:

- **Segno di spunta verde.** Non ci sono problemi da risolvere. Il computer e i dati sono protetti.
- **Punto esclamativo giallo.** Alcuni problemi non critici influenzano la sicurezza del tuo sistema.
- **Una X rossa.** Alcuni problemi critici influenzano la sicurezza del tuo sistema.

Oltre al simbolo dello stato, un dettagliato messaggio relativo allo stato di sicurezza viene mostrato alla destra dell'area di stato. Puoi visualizzare i problemi alla sicurezza rilevati cliccando nell'area di stato. I problemi esistenti saranno risolti dal tuo amministratore di rete.

1.2.2. Cronologia eventi


Bitdefender Endpoint Security Tools tiene un registro dettagliato degli eventi riguardanti la sua attività sul computer, tra cui le attività monitorate dal Controllo contenuti.

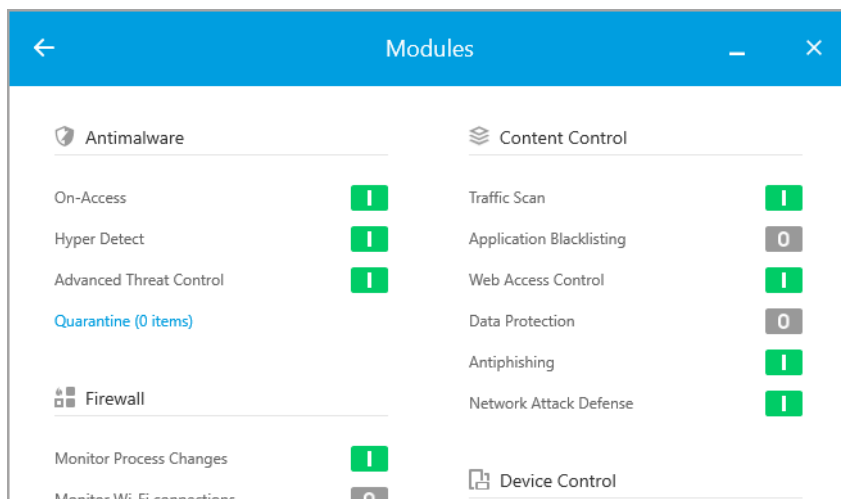


Cronologia eventi

La cronologia **Eventi** è uno strumento importante nel monitorare la tua protezione di Bitdefender. Per esempio, puoi controllare facilmente se un aggiornamento è stato eseguito con successo o se sono stati rilevati malware sul tuo computer.

1.3. La finestra Moduli

La finestra **Moduli** mostra informazioni utili sullo stato e le attività dei moduli di protezione installati. Per aprire la finestra **Moduli**  nella finestra principale di Bitdefender Endpoint Security Tools.

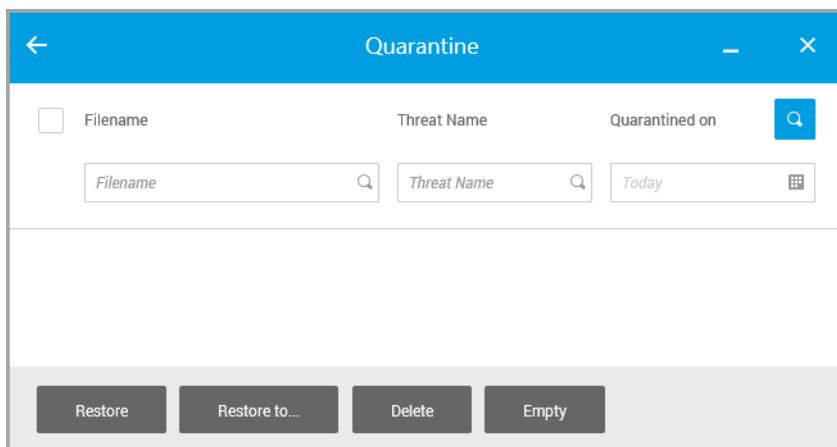


Finestra Moduli

Antimalware

La protezione antimalware è la base della tua sicurezza. Bitdefender Endpoint Security Tools ti protegge in tempo reale e su richiesta da ogni sorta di malware, come virus, trojan, spyware, adware, ecc.

- **All'accesso.** La scansione all'accesso impedisce alle nuove minacce malware di accedere al sistema esaminando i file di rete e locali all'accesso (apertura, spostamento, copiatura o esecuzione), settori di boot e applicazioni potenzialmente indesiderate (PUA).
- **HyperDetect.** HyperDetect rivela gli attacchi avanzati e le attività sospette in fase di pre-esecuzione. Questo livello di sicurezza include modelli di apprendimento automatico e una tecnologia di rilevamento degli attacchi furtivi.
- **Advanced Threat Control.** Monitora costantemente le applicazioni in esecuzione sull'endpoint per rilevare azioni simili a malware. Advanced Threat Control tenterà di disinfettare automaticamente il file rilevato.
- La **Quarantena** mostra l'elenco dei file in quarantena, il loro percorso originale, il tempo di azione e la data della quarantena, e il loro stato di sicurezza. Usa i pulsanti nella parte inferiore per eliminare o ripristinare i file che desideri. Se vuoi eliminare tutti i file dalla quarantena, clicca sul pulsante **Svuota**.



Quarantena

Controllo contenuti

Mentre sei su Internet, il modulo Controllo contenuti ti protegge da attacchi phishing, tentativi di frode, violazioni di dati privati e contenuti web inappropriati. Include anche un set completo di comandi utente che aiuta l'amministratore di rete a far rispettare le policy di utilizzo di computer e Internet.

- **Scansione traffico.** Questo componente impedisce di scaricare contenuti malware sull'endpoint, esaminando le e-mail in arrivo e il traffico web in tempo reale. Le e-mail in uscita sono esaminate per impedire ai malware di infettare gli altri endpoint.
- **Blacklist applicazioni.** Questo componente impedisce di accedere ad applicazioni non autorizzate nella tua azienda. L'amministratore è responsabile della creazione di regole per le applicazioni consentite nell'organizzazione.
- **Controllo accesso web.** Questo componente ti impedisce di accedere a siti web pericolosi in base alle regole definite dall'amministratore.
- **Protezione dei dati.** Questo componente impedisce la divulgazione non autorizzata di dati sensibili in base alle regole definite dall'amministratore.
- **Antiphishing.** Questo componente blocca automaticamente le pagine web phishing note per impedire agli utenti di divulgare inavvertitamente informazioni private o confidenziali a eventuali truffatori online.
- **Network Attack Defense.** Network Attack Defense rileva le tecniche di attacco alla rete usate per ottenere l'accesso su determinati endpoint, come attacchi di forza bruta, exploit di rete e furti di password.



Nota

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

Firewall

Il firewall ti protegge mentre sei connesso alle reti e a Internet filtrando i tentativi di connessione e bloccando connessioni rischiose o sospette.



Nota

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

Controllo dispositivi

Ti consente di prevenire la sottrazione di dati sensibili e le infezioni di malware tramite dispositivi esterni collegati agli endpoint, applicando regole ed eccezioni

di blocco tramite una policy a una vasta gamma di tipi di dispositivi. L'amministratore è responsabile della gestione dei permessi per i seguenti tipi di dispositivi:

- Adattatori di Bluetooth
- Unità CD-ROM
- Unità floppy disk
- IEEE 1284.4
- IEEE 1394
- Unità di imaging
- Modem
- Unità a nastri
- Windows Portable
- Porte COM/LPT
- SCSI Raid
- Stampanti
- Adattatori di rete
- Adattatori di rete wireless
- Dispositivi di acquisizione interni ed esterni

**Nota**

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

Controllo applicazioni

Il modulo Controllo applicazioni blocca l'esecuzione di applicazioni e processi non autorizzati sull'endpoint. Il Controllo applicazioni riduce la frequenza e l'impatto degli incidenti malware, riducendo la superficie di attacco e la vulnerabilità, controllando il numero di applicazioni indesiderate nella tua rete.

**Nota**

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

Sandbox Analyzer

Il modulo Sandbox Analyzer fornisce un potente livello di protezione dalle minacce avanzate, eseguendo un'analisi automatica e approfondita dei file sospetti non ancora firmati dai motori antimalware di Bitdefender. Sandbox Analyzer utilizza una vasta gamma di tecnologie proprietarie per eseguire i payload in un ambiente virtuale contenuto, ospitato da Bitdefender, analizzare

il loro comportamento e segnalare anche il minimo cambiamento del sistema, in genere un chiaro segnale di intenzioni dannose.

**Nota**

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

Volume Encryption

Il modulo Volume Encryption consente di fornire una cifratura completa del disco, gestendo BitLocker su macchine Windows. È possibile cifrare e decifrare i volumi di avvio e non con un solo clic, mentre GravityZone gestisce l'intero processo con un intervento minimo da parte degli utenti. Inoltre, GravityZone memorizza i codici di ripristino necessari per sbloccare i volumi quando gli utenti dimenticano le proprie password.

**Nota**

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

Sensore EDR

Il sensore EDR (Endpoint Detection and Response) ottiene, gestisce e segnala i dati comportamentali di endpoint e applicazioni. Alcune delle informazioni vengono elaborate a livello locale, mentre un set di dati più complesso viene segnalato a un componente di back-end di GravityZone.

Il modulo genera un ingombro minimo in termini di uso della banda di rete e consumo di risorse hardware.

**Nota**

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.


Patch Management

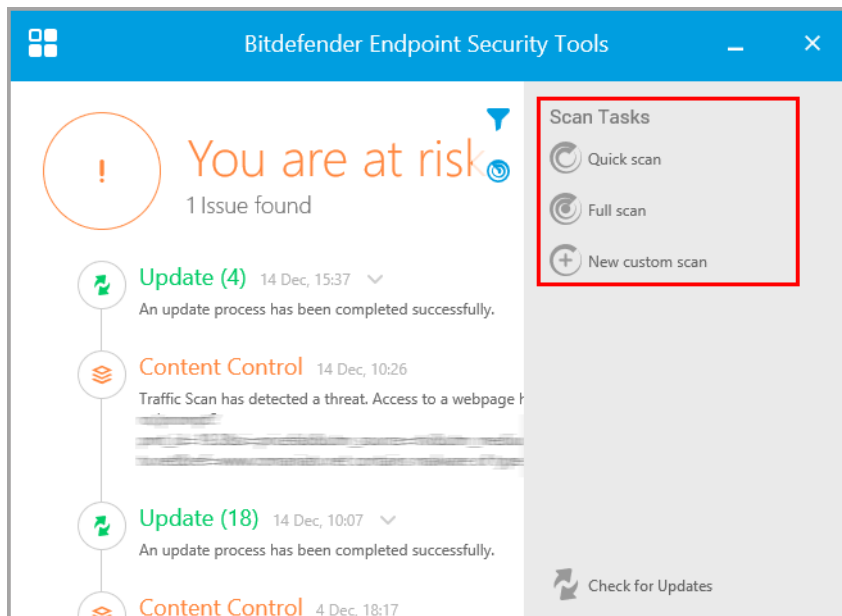
Gestione patch mantiene il sistema operativo e le applicazioni software sempre aggiornati. Questo modulo include diverse funzionalità, come la scansione patch a richiesta / programmata, l'applicazione di patch automatica / manuale o la segnalazione di eventuali patch mancanti.

**Nota**

Questo modulo non è disponibile per Bitdefender Endpoint Security Tools for Windows Legacy.

1.4. Menu Azioni

Per definire o eseguire un'attività di scansione, clicca sul pulsante **Azioni**  per aprire il menu **Azioni**. Da qui puoi anche verificare la presenza di aggiornamenti.



Menu Azioni

Scans. veloce

Utilizza nella scansione in-the-cloud per rilevare malware in esecuzione nel tuo sistema. In genere eseguire una scansione veloce richiede meno di un minuto e usa una frazione delle risorse di sistema di una scansione standard.

Scansione sistema

Esamina l'intero sistema per rilevare tutti i tipi di malware che minacciano la sua sicurezza, come virus, spyware, adware, rootkit e altri.

Scansione personalizzata

Ti consente di scegliere le posizioni da esaminare e configurare le opzioni di scansione.



Controlla disponibilità aggiornamenti

Se viene rilevato un aggiornamento, ti sarà chiesto di confermare l'aggiornamento oppure sarà eseguito automaticamente, secondo le impostazioni di aggiornamento configurate dal tuo amministratore di rete.

2. ESEGUIRE UNA SCANSIONE PER I MALWARE

L'obiettivo principale di Bitdefender Endpoint Security Tools è mantenere il tuo computer privo di malware. Lo fa principalmente esaminando in tempo reale i file a cui si accede, i messaggi e-mail e qualsiasi nuovo file scaricato o copiato nel tuo computer. Oltre alla protezione in tempo reale, ti consente anche di eseguire scansioni per rilevare e rimuovere malware dal tuo computer.

Puoi eseguire la scansione del computer ogni volta che vuoi, avviando le attività predefinite o una tua scansione (attività definite dall'utente). Le impostazioni della scansione specificano le opzioni della scansione e gli elementi da esaminare. Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale.

In qualsiasi momento durante la scansione, puoi visualizzare i progressi nella cronologia **Eventi**.

2.1. Esaminare un file o una cartella

Dovresti controllare i file e le cartelle ogni volta che sospetti che possano essere stati infettati. Clicca con il pulsante destro del mouse sul file o la cartella che desideri controllare e seleziona **Controlla con Bitdefender Endpoint Security Tools**. La scansione inizierà e potrai monitorare i progressi nella cronologia **Eventi**.

Al termine della scansione, visualizzerai i risultati. Per informazioni più dettagliate, clicca su **Vedi rapporto**.

2.2. Eseguire una Scansione veloce

La **Scansione veloce** utilizza una scansione in-the-cloud per elevare eventuali malware in esecuzione sul tuo sistema. Eseguire una scansione veloce richiede meno di un minuto e usa una frazione delle risorse di sistema necessarie per una scansione standard.

La **Scansione veloce** è preconfigurata per consentire la scansione:

- Processi in esecuzione, **settori di avvio** e registro.
- Regioni della memoria critiche
- Solo file nuovi e modificati
- Per **rootkit**, **adware**, **spyware** e applicazioni dialer in percorsi critici del sistema operativo, come: %windir%\system32\, %temp%, /etc, /lib.

- Per applicazioni potenzialmente non desiderate (PUA).

Per eseguire una scansione veloce, segui questi passaggi:

1. Apri la finestra di Bitdefender Endpoint Security Tools.
2. Clicca sul pulsante **Azioni** nell'angolo in alto a destra.
3. Clicca sulla **Scansione veloce**.
4. Attendi il completamento della scansione. Puoi visualizzare i progressi della scansione nella cronologia. Una volta completata, clicca su **Vedi rapporto** per visualizzare i risultati dettagliati.

2.3. Eseguire una scansione completa

L'attività **Scansione completa** esamina l'intero computer per rilevare tutti i tipi di malware che minacciano la sua sicurezza, come virus, spyware, adware, rootkit e altri.



Nota

Poiché la **Scansione completa** esegue una scansione accurata dell'intero sistema, potrebbe richiedere un po' di tempo. Pertanto, si consiglia di eseguire questa operazione quando non si utilizza il computer.

Se desideri controllare ubicazioni particolari sul tuo computer o impostare le opzioni di scansione, configura ed esegui una scansione personale. Per maggiori informazioni, fai riferimento a [«Configurare ed eseguire una scansione personalizzata»](#) (p. 13).

Prima di eseguire una scansione completa, assicurati che Bitdefender Endpoint Security Tools sia aggiornato con le sue firme malware. Eseguire la scansione con un database delle firme obsoleto può impedire a Bitdefender Endpoint Security Tools di rilevare nuovi malware, trovati dopo l'ultimo aggiornamento. Per maggiori informazioni, fai riferimento a [«Aggiornamenti»](#) (p. 22).

La **Scansione completa** è configurata per eseguire la scansione:

- Processi in esecuzione, [settori di avvio](#) e registro.
- Archivi di e-mail e file di rete da tutte le unità, tra cui quelle rimuovibili.
- Per [rootkit](#), [adware](#), [spyware](#), keylogger e applicazioni dialer, su tutte le unità, tra cui quelle rimuovibili.
- Per applicazioni potenzialmente non desiderate (PUA)

- Cookies del browser

Per eseguire una scansione completa, segui questi passaggi:

1. Apri la finestra di Bitdefender Endpoint Security Tools.
2. Clicca sul pulsante **Azioni** nell'angolo in alto a destra.
3. Clicca su **Scansione completa**.
4. Attendi il completamento della scansione. Puoi visualizzare i progressi della scansione nella cronologia. Clicca su **Vedi dettagli** per visualizzare i dettagli della scansione in corso. Puoi anche mettere in pausa, posticipare o fermare la scansione.
5. Bitdefender Endpoint Security Tools intraprenderà automaticamente le azioni consigliate sui file rilevati. Una volta completata, clicca su **Vedi rapporto** per visualizzare i risultati dettagliati.

2.4. Configurare ed eseguire una scansione personalizzata

Per configurare una scansione antimalware in ogni dettaglio e poi eseguirla, segui questi passaggi:

1. Apri la finestra principale di Bitdefender Endpoint Security Tools.
2. Clicca sul pulsante **Azioni** nell'angolo in alto a destra.
3. Clicca su **Nuova scansione personalizzata**. Si aprirà la finestra **Scansione personalizzata**.
4. Configura le opzioni di scansione: **Aggressiva**, **Normale**, **Permissiva**, **Personalizzata**. Usa la descrizione sotto l'opzione per identificare il livello di scansione che si adatta meglio alle tue necessità.
5. Seleziona il bersaglio della scansione nel pannello sulla sinistra.
6. Puoi anche configurare la scansione per eseguire l'attività con bassa priorità, selezionando la casella corrispondente. Ciò diminuisce la priorità del processo di scansione. Consentirai ad altri programmi di essere più veloci, incrementando il tempo necessario per terminare il processo di scansione.

Dopo aver configurato la scansione personalizzata, puoi salvarla come preferita. Per farlo, inserisci un nome e clicca sul pulsante **Preferita** .

Gli utenti avanzati possono trarre vantaggio dalle impostazioni di scansione offerte da Bitdefender Endpoint Security Tools. Per configurare in ogni dettaglio le opzioni della scansione, clicca su **Personalizzata e Impostazioni**.

In alternativa, puoi configurare ed eseguire una scansione personalizzata usando l'utilità linea di comando del prodotto. Per maggiori dettagli, fai riferimento al capitolo «[Utilizzare l'interfaccia a linea di comando](#)» (p. 25).

2.4.1. Tipi di file

Nella scheda **Tipi di file**, puoi specificare quali tipi di file vuoi che siano esaminati. Puoi impostare l'agente di sicurezza in modo che esamini tutti i file (indipendentemente dalla loro estensione), solo i file delle applicazioni o determinate estensioni che ritieni essere pericolose.

Controllare tutti i file ti garantisce una protezione migliore, mentre controllare solo le applicazioni può essere utile per eseguire una scansione più veloce. Le applicazioni (o programmi) sono più vulnerabili agli attacchi dei malware rispetto ad altri tipi di file. Questa categoria include le seguenti estensioni dei file:

386; a6p; ac; accda; accdb; accdc; accde; accdp; accdr; accdt; accdu; acl; acr; action; ade; adp; air; app; as; asd; asp; awk; bas; bat; bin; cgi; chm; cla; class; cmd; cnv; com; cpl; csc; csh; dat; dek; dld; dll; doc; docm; docx; dot; dotm; dotx; drv; ds; ebm; esh; exe; ezs; fky; frs; fxp; gadget; grv; hlp; hms; hta; htm; html; iaf; icd; ini; inx; ipf; isu; jar; js; jse; jsx; kix; laccdb; lnk; maf; mam; maq; mar; mat; mcr; mda; mdb; mde; mdt; mdw; mem; mhtml; mpp; mpt; mpx; ms; msg; msi; msp; mst; msu; oab; obi; obs; ocx; oft; ole; one; onepkg; ost; ovl; pa; paf; pex; pfd; php; pif; pip; pot; potm; potx; ppa; ppam; pps; ppsm; ppsx; ppt; pptm; pptx; prc; prf; prg; pst; pub; puz; pvd; pwc; py; pyc; pyo; qpx; rbx; rgs; rox; rpj; rtf; scar; scr; script; sct; shb; shs; sldm; sldx; smm; snp; spr; svd; sys; thmx; tlb; tms; u3p; udf; url; vb; vbe; vbs; vbscript; vxd; wbk; wcm; wdm; wiz; wll; wpk; ws; wsf; xar; xl; xla; xlam; xlb; xlc; xll; xlm; xls; xlsb; xlsx; xlt; xltm; xltx; xlw; xml; xqt; xsf; xsn; xtp

Opzioni di scansione per archivi

Gli archivi contenenti file infetti non sono una minaccia immediata alla sicurezza del sistema. I malware possono colpire il sistema solo se il file infetto è estratto da un archivio ed eseguito senza aver attivato la protezione in tempo reale. Tuttavia, si consiglia di usare questa opzione per rilevare e rimuovere ogni minaccia potenziale, anche se non è immediata.

Scansiona archivi e-mail

Seleziona questa opzione se desideri attivare la scansione dei file allegati ai messaggi e ai database di e-mail, tra cui formati di file come `.eml`, `.msg`, `.pst`, `.dbx`, `.mbx`, `.tbb` e altri.

2.4.2. Che cosa esaminare?

Nella scheda **Scansione**, seleziona le caselle corrispondenti per attivare le opzioni di scansione desiderate.

Scansiona i settori di avvio

Puoi impostare Bitdefender Endpoint Security Tools per esaminare i settori di boot del tuo disco rigido. Questo settore del disco rigido contiene il codice necessario per inizializzare il processo di avvio del computer. Quando un virus infetta il settore di boot, il disco potrebbe non essere accessibile e potrebbe non essere possibile avviare il sistema e accedere ai dati.

Scansiona alla ricerca di rootkit

Seleziona questa opzione per eseguire una scansione alla ricerca di **rootkit** e altri oggetti nascosti usando tale software.

Scansiona memoria

Seleziona questa opzione per controllare i programmi in esecuzione nella memoria di sistema.

Registro della scansione

Seleziona questa opzione per controllare le chiavi del registro. Il registro di Windows è un database che memorizza le impostazioni e le opzioni di configurazione delle componenti del sistema operativo Windows, oltre a quelle delle applicazioni installate.

Scansiona per keylogger

Seleziona questa opzione per eseguire una scansione alla ricerca di software **keylogger**.

Esamina applicazioni potenzialmente non desiderate (PUA)

Un'applicazione potenzialmente indesiderata (PUA) è un programma che potrebbe essere indesiderato sul PC e a volte viene installato insieme a software freeware. Tali programmi possono essere installati senza il consenso dell'utente (vengono anche chiamati adware) o sono spesso inclusi in modo predefinito nei kit di installazione rapida (ad-supported). Gli effetti potenziali di questi programmi includono la visualizzazione di pop-up, l'installazione di barre degli strumenti non desiderate nel browser predefinito o l'esecuzione di vari processi in background con il conseguente rallentamento delle prestazioni del PC.

Scansiona solo file nuovi e modificati

Controllando solo i file modificati o nuovi, potresti migliorare la prontezza generale del sistema, mantenendo un buon livello di sicurezza.

Scansiona i cookie

Seleziona questa opzione per controllare i cookie memorizzati dai browser sul tuo computer.

2.4.3. Che cosa fare?

Nella scheda **Azioni**, imposta l'azione da intraprendere sui file rilevati, se presenti.

File infetti

File rilevati che corrispondono a firme malware infette nel database di firme malware di Bitdefender.

File sospetti

I file sono stati rilevati come sospetti dall'analisi euristica. I file sospetti non possono essere disinfettati, perché non è disponibile alcuna routine di disinfezione.

Rootkits

I rootkit sono software specializzati che vengono usati per nascondere file al sistema operativo. Anche se non dannosi di natura, i rootkit sono spesso utilizzati per nascondere malware o celare la presenza di un intruso nel sistema.

Esegui azioni appropriate

In base al tipo di file rilevati, saranno disponibili una o più delle seguenti opzioni:

Elimina

Rimuove i file rilevati dal disco.

Se i file infetti sono memorizzati in un archivio con altri file puliti, Bitdefender Endpoint Security Tools tenterà di eliminare i file infetti e riformare l'archivio con i file puliti. Se la ricostruzione dell'archivio non è possibile, sarai informato del fatto che non può essere intrapresa alcuna azione in modo da evitare la perdita di file puliti.

Ignora

Sui file rilevati non sarà eseguita alcuna azione. Dopo che la scansione è stata completata, potrai aprire il registro della scansione per visualizzare le informazioni su questi file.

Sposta i file in quarantena

I file in quarantena non possono essere eseguiti né essere aperti, annullando il rischio d'infezione.

Disinfetta

Rimuove il codice malware dal file infetto e ricostruisce il file originale.

2.5. Controllare i registri di scansione

Ogni volta che esegui una scansione, viene creato un registro di scansione. Il registro di scansione contiene informazioni dettagliate sul processo di scansione registrato, sull'obiettivo della scansione, le minacce individuate e le azioni intraprese su queste minacce.

Puoi aprire il rapporto della scansione direttamente dalla finestra principale, una volta completata la scansione, clicca su **Vedi rapporto**.

Per controllare i registri di scansione in un secondo momento, segui questi passaggi:

1. Apri la finestra principale di Bitdefender Endpoint Security Tools.
2. Clicca sul pulsante **Filtro** per aprire il menu **Filtri**.
3. Clicca sul pulsante **Antimalware**. Qui puoi trovare tutti gli eventi della scansione antimalware, incluso le minacce rilevate dalla scansione all'accesso, le scansioni recenti, le scansioni avviate dall'utente e le variazioni di stato per le scansioni automatiche.
4. Clicca su un evento per visualizzare maggiori dettagli al riguardo.
5. Per aprire il registro della scansione, clicca su **Vedi rapporto**. Sarà visualizzato il rapporto della scansione.

3. USARE VOLUME ENCRYPTION

Il modulo Volume Encryption fornisce una cifratura completa del disco sul sistema Windows tramite le policy applicate dall'amministratore della sicurezza.

3.1. Cifrare il tuo sistema

Quando una policy di cifratura viene applicata al tuo sistema Windows:

1. Una finestra di configurazione ti chiede di inserire:

- Un numero di identificazione personale (PIN), se il sistema ha un chip Trusted Platform Module (TPM) (come nei portatili più moderni).



Nota

Se il tuo sistema ha un TPM efficace, l'amministratore della sicurezza può configurare una policy in grado di cifrare i volumi automaticamente, senza richiedere un PIN.

- Una password se il sistema non ha un chip Trusted Platform Module (TPM). La password è richiesta anche quando il TPM non è efficace o rilevato da Bitdefender Endpoint Security Tools.

2. Clicca sul pulsante **Salva**. Il processo di cifratura inizia immediatamente, prima sul volume di avvio.

Puoi posticipare la cifratura cliccando su **Revoca**. Tuttavia, la finestra ricomparirà dopo un po', chiedendoti di configurare un PIN o una password di cifratura.

Ti serve un solo PIN o una sola password per cifrare tutti i volumi, avvio e non-avvio, su dischi fissi, sistemi desktop e portatili. I dischi rimovibili non sono cifrati. Per dettagli sulla configurazione del PIN o la password di cifratura, fai riferimento a [questo articolo della KB](#).

Dopo la cifratura, devi inserire il PIN o la password ogni volta che Windows si avvia, in una schermata di autenticazione di pre-avvio, in base alla policy di sicurezza applicata al tuo sistema.



Se dimentichi il PIN o la password di cifratura, contatta il tuo amministratore della sicurezza.

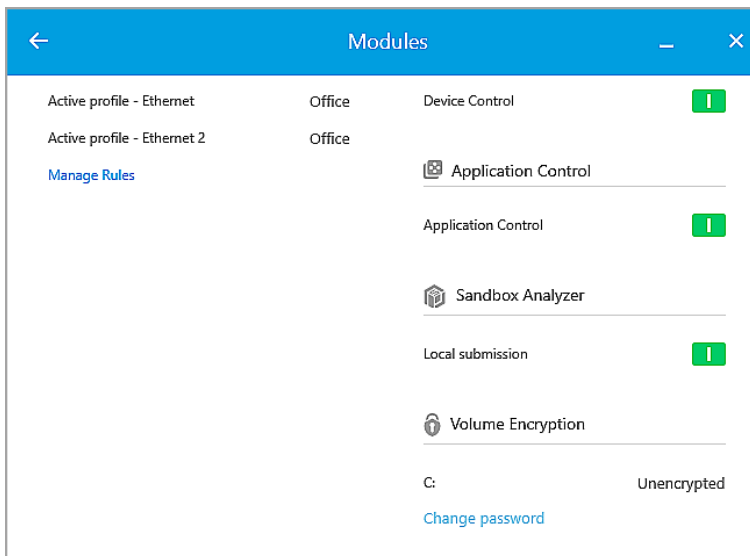
3.2. Decriptare il tuo sistema

Quando viene applicata una policy di decifrazione, i dischi cifrati vengono decriptati automaticamente, senza richiedere alcun intervento da parte tua. Tuttavia, non puoi decriptare il sistema da solo, finché è attiva una policy di cifratura.

3.3. Verificato lo stato della cifratura

Ecco come puoi verificare lo stato della cifratura sul tuo sistema:

1. Nell'area di notifica, clicca due volte sull'icona  per accedere all'interfaccia utente di Bitdefender Endpoint Security Tools.
2. Nell'angolo in alto a destra, clicca sul pulsante  per aprire la finestra **Moduli**.
3. Vai alla sezione **Volume Encryption**, in cui puoi visualizzare quali volumi sono cifrati e quali no.



3.4. Modificare la password o il PIN di cifratura

Ecco come puoi modificare la password o il PIN di cifratura:

1. Clicca sul nome del disco cifrato nella finestra principale dell'interfaccia utente di Bitdefender Endpoint Security Tools.
2. Clicca sull'opzione **Cambia password**.
3. Nella finestra di configurazione, inserisci la nuova password o il nuovo PIN.
4. Clicca sul pulsante **Salva**.

4. AGGIORNAMENTI

In un mondo dove i criminali informatici cercano costantemente di trovare nuovi modi per causare danni, avere un programma di sicurezza aggiornato è essenziale per essere sempre un passo avanti a loro.

Se sei connesso a Internet attraverso una linea a banda larga o ADSL, Bitdefender Endpoint Security Tools si prenderà cura di sé da solo. Di norma, verifica la presenza di aggiornamenti all'accensione del computer e in seguito ad ogni **ora**.

Nota

La frequenza dell'aggiornamento automatico predefinita potrebbe essere modificata dal tuo amministratore di rete.

Il processo di aggiornamento viene eseguito direttamente, ciò significa che i file da aggiornare vengono sostituiti progressivamente. In questo modo, il processo di aggiornamento non interesserà l'operatività del prodotto e, nello stesso tempo, ogni vulnerabilità verrà esclusa.

Se sei connesso a Internet mediante una connessione telefonica, si consiglia di aggiornare regolarmente Bitdefender su richiesta dell'utente. Per maggiori informazioni, fai riferimento a «[Eseguire un aggiornamento](#)» (p. 23).

4.1. Tipi di aggiornamenti

Gli aggiornamenti sono disponibili nelle seguenti forme:

- **Aggiornamenti per le firme malware** - Quando compaiono nuove minacce, i file contenenti le firme malware devono essere aggiornati per garantire una protezione permanente contro di essi.
- **Aggiornamenti prodotto** - quando viene rilasciata la nuova versione di un prodotto, vengono introdotte nuove funzionalità e tecniche di scansione al fine di migliorare l'efficienza del prodotto.

Un upgrade del prodotto è un aggiornamento principale della versione.

4.2. Verificare se la propria protezione è aggiornata

Per verificare se la propria protezione è aggiornata, segui questi passaggi:

1. Clicca con il pulsante destro del mouse sull'icona di Bitdefender Endpoint Security Tools nell'area di notifica e seleziona **Informazioni**.

2. Puoi verificare lo stato dell'aggiornamento e l'ora del controllo di aggiornamento più recente e dell'installazione dell'aggiornamento.

Per maggiori informazioni sugli ultimi aggiornamenti, controlla gli eventi di aggiornamento:

1. Nella finestra principale, clicca sul pulsante **Filtro** per aprire il menu **Filtri**.
2. Clicca sul pulsante **Aggiornamento**. Gli aggiornamenti più recenti saranno mostrati nella cronologia **Eventi**.

Puoi sapere quando gli aggiornamenti sono stati lanciati e avere maggiori informazioni al riguardo - se hanno avuto successo o meno, e se richiedono di riavviare il computer per completare l'installazione. Se necessario, riavvia il sistema al più presto.

4.3. Eseguire un aggiornamento

Per poter eseguire gli aggiornamenti, serve una connessione a Internet.

Per avviare un aggiornamento:

- Clicca due volte sull'icona di Bitdefender Endpoint Security Tools nell'[area di notifica](#).
- Clicca sul pulsante **Azioni** per aprire il menu **Azioni**.
- Clicca su **Controlla disponibilità aggiornamenti**. Il modulo Aggiornamento si conatterà al server di aggiornamento di Bitdefender per cercare eventuali aggiornamenti.
- Se viene rilevato un aggiornamento, ti sarà chiesto di confermare l'aggiornamento oppure sarà eseguito automaticamente, secondo le impostazioni di aggiornamento configurate dal tuo amministratore di rete.



Importante

Se necessario, riavvia il sistema al più presto. Si raccomanda di farlo il prima possibile.

5. EVENTI

Bitdefender Endpoint Security Tools mostra un registro dettagliato di eventi relativi alle sue attività sul tuo computer, incluso le attività del computer monitorate dal Controllo contenuti e le applicazioni bloccate dal Controllo applicazioni. La cronologia **Eventi** è uno strumento importante per monitorare la tua protezione di Bitdefender. Per esempio, puoi controllare facilmente se un aggiornamento è stato eseguito con successo, se sono stati rilevati malware sul tuo computer, ecc. Per verificare il registro degli eventi, segui questi passaggi:

1. Apri la finestra principale di Bitdefender Endpoint Security Tools.
2. Tutti gli eventi vengono mostrati nella cronologia **Eventi**.
3. Clicca sul pulsante **Filtro** per aprire il menu **Filtri**.
4. Seleziona la categoria dell'evento nel menu. Gli eventi sono raggruppati nelle seguenti categorie:
 - **Impostazioni generali**
 - **Antimalware**
 - **Firewall**
 - **Aggiornamento**
 - **Controllo contenuti**
 - **Controllo dispositivi**
 - **Controllo applicazioni**
 - **Sandbox Analyzer**
 - **Volume Encryption**

Ogni evento è fornito delle seguenti informazioni: una breve descrizione, l'azione intrapresa da Bitdefender quando si è verificato e la data e l'ora in cui è avvenuto. Per visualizzare maggiori informazioni su un particolare evento nell'elenco, clicca su **Vedi rapporto**.

Puoi anche filtrare gli eventi in base alla loro importanza per il livello di protezione. Ci sono tre tipi di eventi:



indica le operazioni avvenute con successo.



indica problemi non critici.



indica problemi critici.

Alcuni dei problemi critici e non critici mostrati nella cronologia **Eventi** sono associati ad alcune azioni suggerite per risolverli.

6. UTILIZZARE L'INTERFACCIA A LINEA DI COMANDO

Bitdefender Endpoint Security Tools ti consente di eseguire automaticamente attività di scansioni su richiesta locali e aggiornamenti usando la Console del prodotto, un'interfaccia a linea di comando presente nella cartella di installazione del prodotto sulle tue macchine Windows.

L'interfaccia a linea di comando di BEST ha due modalità di funzionamento:

- **Comandi multipli contemporaneamente.** Questa modalità utilizza la propria interfaccia a linea di comando e ti consente di inserire comandi e ottenere risultati finché non esci.

Per accedere a questa modalità:

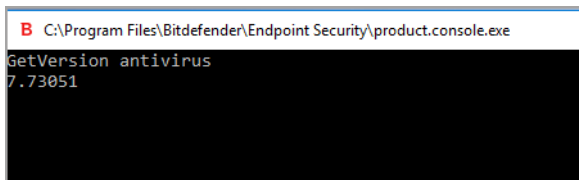
1. Vai in `c:\Program Files\Bitdefender\Endpoint Security` o alla cartella in cui è stato installato BEST.
2. Trova e clicca due volte sull'eseguibile **product.console**. Si apre l'interfaccia a linea di comando.
3. Esegui il comando desiderato.

Esempio:

```
GetVersion antivirus
```

Il risultato ottenuto rappresenta il numero della versione delle firme antimalware.

4. Esegui `exit` per chiudere l'interfaccia a linea di comando.



```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion antivirus
7.73051
```

- **Un comando alla volta.** Questa modalità utilizza il prompt dei comandi e torna al prompt del sistema una volta eseguito il comando.

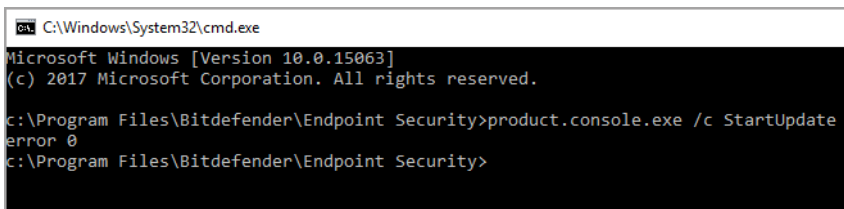
Per accedere a questa modalità:

1. Apri il prompt dei comandi (`cmd.exe`).
2. Usa il comando `cd` per raggiungere la cartella di installazione di Bitdefender Endpoint Security Tools.
3. Esegui il comando desiderato.

Esempio:

```
C:\Program Files\Bitdefender\Endpoint Security>
product.console.exe /c StartUpdate
```

4. Se il comando viene eseguito con successo, il risultato ottenuto è `error 0`.



```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

c:\Program Files\Bitdefender\Endpoint Security>product.console.exe /c StartUpdate
error 0
c:\Program Files\Bitdefender\Endpoint Security>
```

6.1. Comandi supportati

L'interfaccia a linea di comando supporta diversi comandi, alcuni dei quali richiedono determinati parametri per dare risultati validi.

Tutti gli esempi in questa sezione vengono assegnati usando la console del prodotto dalla cartella di installazione di BEST.

GetUpdateStatus `product|antivirus`

Recupera informazioni sui nuovi aggiornamenti.

Questo comando richiede uno dei seguenti parametri:

- `prodotto` – si riferisce alla versione di BEST.
- `antivirus` – si riferisce alla versione delle firme antimalware.

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetUpdateStatus product
lastSucceededTime: 1504513705
lastAttemptedTime: 1504513705
lastError: 0
GetUpdateStatus antivirus
lastSucceededTime: 1505739144
lastAttemptedTime: 1505739144
lastError: 0
```

GetVersion product|antivirus

Recupera informazioni sulla versione attuale del prodotto.

Questo comando richiede uno dei seguenti parametri:

- `prodotto` – si riferisce alla versione di BEST.
- `antivirus` – si riferisce alla versione delle firme antimalware.

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
GetVersion product
6.2.24.938
GetVersion antivirus
7.73205
```

IsUpdateInProgress

Verifica se è in corso un aggiornamento del prodotto.

Valori di uscita:

- `true` - un aggiornamento del prodotto è in corso.
- `false` - non è in corso alcun aggiornamento del prodotto.

Esempio:


```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateInProgress
false
```

IsUpdateRestartNeeded

Verifica se una macchina richiede un riavvio del sistema dopo l'aggiornamento.

Valori di uscita:

- `true` - la macchina richiede un riavvio del sistema dopo l'aggiornamento.
- `false` - la macchina non richiede un riavvio del sistema dopo l'aggiornamento.

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
IsUpdateRestartNeeded
false
```

StartUpdate

Avvia un aggiornamento e ottieni il risultato senza attendere il completamento dell'attività.

Esempio:

```
StartUpdate
```

Formato di uscita: `error 0` (il comando è stato eseguito con successo)

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
StartUpdate
error 0
```

FileScan.OnDemand.RunScanTask custom [option]

Avvia una scansione a richiesta e mostra il percorso per il rapporto e il sommario della scansione.

Questo comando richiede il parametro `custom`, seguito, se necessario, da una o più opzioni. Per esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505742554_1_01.xml
Scanned items: 990886
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

Con le opzioni, puoi personalizzare un'attività di scansione. Tali opzioni non sono obbligatorie.

Ogni opzione ha due o più valori disponibili, ma puoi usare un solo valore.

Quando il comando `FileScan.OnDemand.RunScanTask` non specifica un'opzione, la scansione personalizzata prende in considerazione il valore predefinito di tale opzione. Per esempio, eseguendo questo comando senza menzionare l'opzione `scanKeyloggers`, significa che Bitdefender Endpoint Security Tools effettuerà comunque la scansione per i keylogger, in base al valore predefinito `scanKeyloggers (true)`.



Nota

Non ci sono comandi specifici per la **Scansione veloce** o la **Scansione completa**. Tuttavia, puoi configurare `FileScan.OnDemand.RunScanTask` per esaminare solo la posizione del sistema operativo o l'intero sistema, con le tutte le opzioni attivate, in base alle necessità.

Opzioni

path="<path>"

Inserisci il percorso della posizione bersaglio della scansione. Per più percorsi, usa path="<path1>" path="<path2>".

Esempio:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
```

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505746495_1_01.xml
Scanned items: 74074
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

infectedAction1=ignore|disinfect|disinfectOnly|delete|quarantine

Seleziona la prima azione da intraprendere quando viene rilevato un file infetto: ignora, disinfetta, elimina o metti in quarantena. Puoi usare questa azione insieme a infectedAction2.

Valore predefinito: disinfect

Esempio:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" infectedAction1=ignore
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505813252_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

infectedAction2=ignore|disinfect|disinfectOnly|delete|quarantine

Seleziona la seconda azione da intraprendere quando viene rilevato un file infetto, se la prima dovesse fallire.

Valore predefinito: quarantine

Esempio:

```
FileScan.OnDemand.RunScanTask custom infectedAction1=disinfect infectedAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824102_1_01.xml
Scanned items: 500139
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction1=ignore|delete|quarantine

Seleziona la prima azione da intraprendere quando viene rilevato un file sospetto. Puoi usare questa azione insieme a suspiciousAction2.

Valore predefinito: ignore

Esempio:

```
FileScan.OnDemand.RunScanTask custom path="C:\Program Files\Common Files" suspiciousAction1=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505824920_1_01.xml
Scanned items: 5542
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

suspiciousAction2=ignore|delete|quarantine

Seleziona la seconda azione da intraprendere quando viene rilevato un file sospetto, se la prima dovesse fallire.

Valore predefinito: ignore

Esempio:

```
FileScan.OnDemand.RunScanTask custom path="C:\Users" suspiciousAction1=delete suspiciousAction2=quarantine
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1505825170_1_01.xml
Scanned items: 54455
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanBootSectors=true|false

Esamina i settori di boot del tuo disco rigido.

Valore predefinito: false

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanBootSectors=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073447_1_01.xml
Scanned items: 416206
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRegistry=true|false

Esamina le chiavi del registro sulla tua macchina.

Valore predefinito: false

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRegistry=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506073099_1_01.xml
Scanned items: 419060
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanMemory=true|false

Esamina i programmi in esecuzione nella memoria del tuo sistema.

Valore predefinito: false

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanMemory=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506072517_1_01.xml
Scanned items: 427016
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom scanMemory=true
```

smartScan=true|false

Esamina solo i file nuovi e modificati.

Valore predefinito: true

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom smartScan=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070911_1_01.xml
Scanned items: 1614889
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanRootKits=true|false

Esamina alla ricerca di rootkit e oggetti nascosti usando tale software.

Valore predefinito: false

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanRootKits=true
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506070601_1_01.xml
Scanned items: 416548
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanKeyloggers=true|false

Esamina alla ricerca di keylogger.

Valore predefinito: true

Esempio:

```
FileScan.OnDemand.RunScanTask custom scanKeyloggers=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

scanPUA=true|false

Esamina alla ricerca di applicazioni potenzialmente non desiderate (PUA).

Valore predefinito: false

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom scanPUA=true
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`scanArchives=true|false`

Esamina alla ricerca di file infetti negli archivi.

Valore predefinito: `true`

Esempio:

```
FileScan.OnDemand.RunScanTask custom scanArchives=false
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506069462_1_01.xml
Scanned items: 416845
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`extensionType=all|application|custom|none`

Esamina i file in base alla loro estensione: tutti i file, solo i file eseguibili, solo i file con le estensioni desiderate o non esaminare alcun file.

Valore predefinito: `all`

Esempio:

```
B C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom extensionType=application
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506068866_1_01.xml
Scanned items: 165522
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`customExt="<string>"`

Questa opzione ti aiuta a esaminare solo i file con le estensioni che desideri. Richiede una stringa con ogni estensione tra le barre verticali (come

"|exe|ini|txt|"). Questa opzione è valida solo insieme all'opzione `extensionType=custom`.

Esempio:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506351027_1_01.xml
Scanned items: 6
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0

FileScan.OnDemand.RunScanTask custom path="c:\Program Files\WinRAR" extensionType=custom customExt="|dll|dat|"
Status: finished
Log path: C:\Program Files\Bitdefender\Endpoint Security\Logs\system\0-0-0-0\1506351335_1_01.xml
Scanned items: 0
Remaining issues: 0
Resolved issues: 0
Objects that were not scanned: 0
```

`lowPriority=true|false`

Esegui l'attività con bassa priorità.

Valore predefinito: `false`

Esempio:

```
C:\Program Files\Bitdefender\Endpoint Security\product.console.exe
FileScan.OnDemand.RunScanTask custom lowPriority=true
```

Queste opzioni sono un'alternativa alle opzioni disponibili nella console di BEST. Per maggiori informazioni fai riferimento a [«Configurare ed eseguire una scansione personalizzata»](#) (p. 13).

6.2. Codici errore linea di comando

L'utilità della linea di comando potrebbe restituire i seguenti codici di errore:

Codice errore	Descrizione
0	Comando eseguito con successo.



Codice errore	Descrizione
87	Parametro non valido.
160	Argomenti errati.
1627	Funzione fallita - Durante l'esecuzione del comando si è verificato un errore.



7. OTTENERE AIUTO

Pr eventuali problemi o domande relative a Bitdefender Endpoint Security Tools, contatta il tuo amministratore di rete.

Per trovare informazioni di contatto e sul prodotto, clicca con il pulsante destro del mouse sull'icona di Bitdefender Endpoint Security Tools nell'area di notifica e seleziona **Informazioni** per aprire la finestra **Informazioni**.

Glossario

Adware

La modalità adware è spesso combinata con un'applicazione che viene fornita gratuitamente se l'utente accetta l'adware. Considerando che le applicazioni adware vengono di solito installate dopo che l'utente ha accettato l'accordo di licenza, dove viene spiegato il proposito dell'applicazione, non viene commessa alcuna infrazione.

Comunque, le finestre pop-up di avvertimento possono essere fastidiose e in alcuni casi ridurre le prestazioni del sistema. Inoltre, le informazioni che vengono raccolte da alcune di queste applicazioni possono causare inconvenienti riguardo la privacy degli utenti, non sempre completamente informati sui termini dell'accordo di licenza.

Aggiornamento

Una nuova versione di un prodotto software o hardware creato per sostituire la versione precedente. In aggiunta, le routine di installazione degli aggiornamenti spesso verificano e si assicurano che sia già installata una versione precedente sul computer, diversamente non sarà possibile installare l'aggiornamento.

Bitdefender ha un proprio modulo di aggiornamento che consente la verifica manuale degli aggiornamenti oppure l'aggiornamento automatico del prodotto.

Archivio

Un Disco, un nastro o una cartella che contiene file memorizzati.

Un file che contiene uno o più file in forma compressa.

Area di notifica

Introdotta con Windows 95, l'area di notifica è situata nella barra delle applicazioni di Windows (in genere in basso vicino all'orologio) e contiene icone miniaturizzate per un accesso veloce a funzioni di sistema come fax, stampante, modem, volume e molto altro. Clicca due volte o clicca con il pulsante destro su un'icona per visualizzare e accedere ai dettagli e i controlli.

Attacchi mirati

Gli attacchi informatici che puntano principalmente a guadagni finanziari o a rovinare una reputazione. Il bersaglio può essere un individuo, un'azienda, un

software o un sistema, ben studiato prima che l'attacco avvenga. Questi attacchi vengono eseguiti per un lungo periodo di tempo e per fasi, usando uno o più punti d'infiltrazione. Vengono notati difficilmente, e la maggior parte delle volte quando il danno è già stato fatto.

Backdoor

Una breccia nella sicurezza di un sistema deliberatamente lasciata dal programmatore o dal manutentore. La presenza di tali "brecce" non sempre è dolosa: su alcuni sistemi operativi, ad esempio, vengono utilizzate per l'accesso con utenze privilegiate per servizi tecnici o per i programmatori del produttore a scopo di manutenzione.

Bootkit

Un bootkit è un programma dannoso che ha la capacità di infettare il master boot record (MBR), il volume boot record (VBR) o il settore di boot. Il bootkit resta attivo anche dopo un riavvio del sistema.

Browser

Abbreviazione di browser web, un'applicazione software utilizzata per localizzare e visualizzare pagine web.

Cookie

Nell'industria di Internet, i cookie vengono descritti come piccoli file contenenti informazioni relative ai computer individuali che possono essere analizzate e utilizzate dai pubblicitari per tenere traccia di interessi e gusti online degli utenti. In questo settore, la tecnologia dei cookie è ancora in fase di sviluppo e l'intenzione è quella di fornire offerte pubblicitarie personalizzate in base agli interessi degli utenti. Per molte persone è una lama a doppio taglio, poiché da una parte è efficace e consente di far vedere solo ciò che viene dichiarato interessante. Ma dall'altra, implica in effetti un "tracciamento" di dove si va e di cosa si seleziona. In considerazione di questo è in atto un dibattito relativo alla riservatezza e molte persone si sentono offese all'idea di essere visti come un "codice SKU" (il codice a barre sul retro delle confezioni che viene letto dalle casse). Se questo punto di vista può essere considerato estremo, in alcuni casi può essere corretto.

Estensione del nome di un file

Porzione del nome di un file che segue il punto finale e che indica il tipo di dati inclusi nel file.

Molti sistemi operativi utilizzano estensioni di file, come Unix, VMS e MS-DOS. Sono normalmente composti da una a tre lettere (alcuni vecchi sistemi operativi non ne supportano più di tre). Esempi: "c" per codici sorgente C, "ps" per PostScript, "txt" per testi semplici.

Euristico

Un metodo basato su regole per l'identificazione di nuovi virus. Questo metodo di scansione non si basa su specifiche firme dei virus. Il vantaggio della scansione euristica è di non essere ingannata dalle nuove varianti dei virus esistenti. Tuttavia, può occasionalmente segnalare una parte di codice sospetto in programmi normali, generando i cosiddetti "falsi positivi".

Eventi

Un'azione oppure un evento segnalato da un programma. Gli eventi possono essere azioni dell'utente, come cliccare con il mouse o premere un tasto sulla tastiera, oppure del sistema, come l'esaurimento della memoria.

Exploit

In genere, un exploit è un qualsiasi metodo usato per ottenere accesso non autorizzato ai computer o una vulnerabilità nella sicurezza di un sistema che rende vulnerabile il sistema a un attacco.

Falso positivo

Appare quando un prodotto di analisi antivirus individua un documento come infettato quando di fatto non lo è.

File di rapporto

Un file che elenca le azioni avvenute. Bitdefender crea un rapporto che elenca i percorsi controllati, le cartelle, il numero di archivi e file esaminati, oltre a quanti file infetti e sospetti sono stati trovati.

File sospetti e traffico di rete

I file sospetti sono quelli con una reputazione piuttosto dubbia. Questa classifica è data da molti fattori, tra cui: l'esistenza della firma digitale, il numero di occorrenze nelle reti di computer, il packer usato, ecc. Il traffico di rete viene considerato sospetto quando si discosta dal modello. Per esempio, una sorgente inaffidabile, richieste di connessione a porte insolite, un maggiore uso della banda, tempi di connessione casuali, ecc.

Firma malware

Le firme malware sono frammenti di codice estratti da campioni attuali di malware. Sono usate dai programmi antivirus per eseguire confronti di esempi e rilevare i malware. Le firme vengono usate anche per rimuovere il codice malware dai file infetti.

Il database di firme malware di Bitdefender è una raccolta di firme malware aggiornato continuamente dai ricercatori malware di Bitdefender.

Grayware

Una classe di applicazioni software tra software legittimi e malware. Anche se non sono dannosi come i malware che possono influenzare l'integrità del sistema, il loro comportamento è comunque fastidioso, portando a situazioni non desiderate, come furto di dati, uso non autorizzato e pubblicità non gradita. Le applicazioni grayware più comuni sono [spyware](#) e [adware](#).

IP

Internet Protocol – protocollo di instradamento nella suite di protocollo TCP/IP, responsabile dell'indirizzamento IP, dell'instradamento, della frammentazione e della ricomposizione dei pacchetti IP.

Keylogger

Un keylogger è un'applicazione che registra ogni informazione digitata.

I keylogger non sono dannosi di natura. Possono essere usati anche per scopi legittimi, come monitorare le attività di dipendenti o bambini. Tuttavia, sono utilizzati anche dai criminali informatici per scopi dannosi (per esempio, ottenere dati personali, come credenziali o codici di accesso).

Linea di comando

In un'interfaccia a linea di comando, l'utente digita i comandi nello spazio previsto direttamente sullo schermo, utilizzando il linguaggio di comando.

Macro virus

Un tipo di virus informatico, codificato come macro all'interno di un documento. Molte applicazioni, come ad esempio Microsoft Word ed Excel, supportano potenti linguaggi macro.

Queste applicazioni consentono di codificare una macro in un documento e di eseguire la macro ogni volta che il documento viene aperto.

Malware

Malware è un termine generico per software progettati appositamente per essere dannosi, un'abbreviazione di "software dannoso" (in inglese "malicious software"). Non è ancora usato in maniera universale, ma la sua popolarità come termine generale per indicare virus, Trojan, worm e codice mobile dannoso sta aumentando.

Non euristico

Questo metodo di scansione si basa su specifiche firme di virus. Il vantaggio della scansione non-euristica è di non essere ingannata da ciò che potrebbe sembrare un virus, e quindi non genera falsi allarmi.

Phishing

L'atto d'inviare un'e-mail a un utente fingendo di essere una società legittima e affermata, nel tentativo di truffarlo, facendogli cedere informazioni private che saranno usate per furti d'identità. L'e-mail invita gli utenti a visitare un sito web, dove gli sarà chiesto di aggiornare determinate informazioni personali, come password e numero di carta di credito, codice fiscale o coordinate bancarie, che l'azienda legittima ovviamente possiede già. In ogni caso, la pagina web è falsa e creata solo per rubare i dati personali dell'utente.

Porta

Un'interfaccia su un computer dalla quale è possibile connettere un dispositivo. I personal computer hanno vari tipi di porte. Internamente ci sono varie porte per la connessione di unità disco, monitor e tastiere. Esternamente i personal computer hanno porte per la connessione di modem, stampanti, mouse e altre periferiche.

Nelle reti TCP/IP e UDP, un endpoint per una connessione logica. Il numero della porta ne identifica il tipo. Ad esempio, la porta 80 viene usata per il traffico HTTP.

Programma di download Windows

È il nome generico di un programma che ha come funzionalità principale quella di scaricare contenuti a scopi indesiderati o dannosi.

Ransomware

Un malware che ti isola dal tuo computer o blocca l'accesso ai tuoi file e applicazioni. Un ransomware ti chiederà di pagare un determinato costo

(riscatto), in cambio di una chiave di decifrazione che ti consente di riottenere l'accesso al tuo computer o ai tuoi file.

Rootkit

Un rootkit è una serie di strumenti software che consente di accedere a un sistema come amministratore. Il termine fu usato per la prima volta per i sistemi operativi UNIX e faceva riferimento a strumenti ricompilati che fornivano agli intrusi i diritti di amministratore, consentendo loro di celare la propria presenza, in modo da non essere visti dagli amministratori del sistema.

Il ruolo principale dei rootkit è nascondere i processi, i file, gli accessi e i registri. Se incorporano il software adeguato, possono anche intercettare dati dai terminali, dalle connessioni di rete o dalle periferiche.

I rootkit non sono dannosi per natura. Ad esempio, i sistemi e persino alcune applicazioni nascondono file critici utilizzando i rootkit. Comunque, vengono principalmente utilizzati per nascondere malware o per celare la presenza di un intruso nel sistema. Se combinati ai malware, i rootkit rappresentano una grave minaccia per l'integrità e la sicurezza di un sistema. Possono monitorare il traffico, creare backdoor nel sistema, alterare file e registri, ed evitare il rilevamento.

Script

Altro termine per macro o file batch, uno script è una lista di comandi che possono essere eseguiti senza interazione con l'utente.

Settore di avvio:

Un settore all'inizio di ogni disco che ne identifica l'architettura (dimensione del settore, dimensione del cluster, ecc.). Nei dischi di avvio, il settore di boot contiene anche un programma che carica il sistema operativo.

Sottrazione di password

Un password stealer raccoglie parti di dati che possono essere nomi di account e le relative password. Tali credenziali rubate vengono poi usate per scopi dannosi, come il furto di account.

Spam

Messaggi di posta elettronica o newsgroup indesiderati. Generalmente conosciuto come e-mail non desiderate.

Spyware

Qualsiasi software che raccoglie segretamente informazioni dell'utente tramite la sua connessione a Internet, senza che questo se ne accorga, di solito per scopi pubblicitari. Le applicazioni spyware in genere sono incluse come componente nascosta di programmi freeware o shareware, che possono essere scaricati da Internet. Tuttavia, occorre segnalare che la maggioranza delle applicazioni shareware o freeware non includono alcun programma spyware. Una volta installato, uno spyware monitora le attività dell'utente su Internet e trasmette di nascosto tali informazioni a qualcun altro. Gli spyware possono anche raccogliere informazioni su indirizzi e-mail o addirittura password e numeri di carta di credito.

Gli spyware sono simili a un cavallo di Troia che gli utenti installano inconsapevolmente con altre applicazioni. Un modo comune per diventare vittima degli spyware è utilizzare i programmi peer-to-peer attuali per condividere e scaricare file.

Oltre a questioni di etica e privacy, gli spyware sottraggono risorse di memoria al computer, "mangiandosi" larghezza di banda poiché inviano informazioni alla propria "base" usando la connessione internet dell'utente. Poiché gli spyware utilizzano memoria e risorse del sistema, le applicazioni eseguite in background possono provocare instabilità o blocchi del sistema.

Storm di scansione antimalware

Un intenso uso delle risorse del sistema che si verifica quando un software antivirus esamina contemporaneamente più virtual machine su un solo host fisico.

TCP/IP

Transmission Control Protocol/Internet Protocol – Insieme di protocolli di rete largamente utilizzati su Internet, che consentono le comunicazioni attraverso le reti interconnesse di computer con diverse architetture hardware e vari sistemi operativi. TCP/IP include gli standard su come comunicano i computer e le convenzioni per connettere le reti e il relativo traffico.

Trojan

Un programma distruttivo che si maschera da applicazione benevola. Diversamente dai virus, i cavalli di Troia non si replicano ma possono comunque essere altrettanto distruttivi. Un tipo di cavallo di Troia

particolarmente insidioso è un programma che dichiara di pulire i virus dal computer, ma al contrario li introduce.

Il termine deriva da una storia dell'Iliade di Omero, in cui i Greci mandarono un gigantesco cavallo di legno ai loro avversari, i Troiani, apparentemente come offerta di pace. Ma dopo che i Troiani portarono il cavallo all'interno delle mura della loro città, i soldati Greci uscirono dal ventre cavo del cavallo e aprirono le porte della città, consentendo ai loro compatrioti di entrare e conquistare Troia.

Virus

Un programma o parte di codice caricato sul computer a propria insaputa e che viene eseguito contro la propria volontà. La maggior parte dei virus è anche in grado di auto replicarsi. Tutti i virus informatici sono creati dall'uomo. È relativamente facile produrre un semplice virus in grado di copiare se stesso innumerevoli volte. Persino un virus così semplice è pericoloso in quanto utilizzerà velocemente tutta la memoria disponibile e porterà il sistema allo stallo. Un tipo di virus ancora più pericoloso è quello in grado di trasmettere se stesso attraverso le reti superando i sistemi di sicurezza.

Virus di boot

Un virus che infetta il settore di avvio di un disco rigido oppure di un'unità floppy. Qualsiasi tentativo di effettuare il boot da un disco floppy infettato con un virus di boot, farà sì che il virus venga attivato in memoria. Da quel momento in poi, ogni volta che si esegue il boot del sistema, il virus sarà attivo in memoria.

Virus polimorfico

Un virus che modifica la propria forma con ogni file che infetta. Non avendo caratteristiche binarie costanti, questi virus sono difficili da identificare.

Worm

Un programma che si propaga in una rete, riproducendosi durante lo spostamento. Non si può attaccare ad altri programmi.