Prevx Proteggere il computer da rootkit e da altro malware

▶ Il problema

Aumentare il livello di protezione del computer da rootkit e malware

PROGRAMMA NEL DVD

▶ La soluzione

Prevx attiva un meccanismo di controllo della presenza di malware che lavora in modo euristico, affiancandosi agli altri programmi di protezione

Prevx è un programma da utilizzare per proteggere il computer da malware e da rootkit, pur non essendo un antivirus propriamente detto. Lo si può installare contemporaneamente ad altre applicazioni che intervengono per la protezione del sistema operativo, senza che sorgano conflitti. Tra l'altro, l'eseguibile ha dimensioni estremamente contenute, inferiori a 1 MB. Anche l'attività di verifica della presenza di eventuali elementi pericolosi è piuttosto veloce. Un controllo completo, infatti, avviene nel giro di qualche minuto, occupando pochissime risorse del sistema operativo.

Modalità di funzionamento

Il funzionamento del programma si basa sul controllo delle applicazioni installate in Windows e del comportamento dei processi attivi. I dati rilevati vengono confrontati con quelli del database *Online Prevx Community Database*, letti in tempo reale dal sito del produttore. Il programma, quindi, funziona correttamente solo in presenza di una connessione attiva in Internet.

PrevX
Categoria: Sicurezza
Versione: freeware
Sito: www.pcopen.it
Richiede installazione: sì
S.O.: Windows

Chi ha il computer in una rete protetta da un *proxy*, può inserirne i dati per riuscire ad accedere a Internet.

Protezione e prevenzione

Subito dopo l'installazione, viene lanciata una scansione del sistema. Il risultato appare in una tabella le cui righe mostrano gli eventuali file portatori di malware.

Nel caso di rilevamento di infezioni o di pericoli, il programma non interviene immediatamente per rimuovere gli elementi nocivi, ma chiede all'utente come comportarsi. La versione freeware, tra l'altro, può intervenire solo su parte delle minacce trovate, destinando alle versioni a pagamento o ad altri prodotti la loro rimozione.

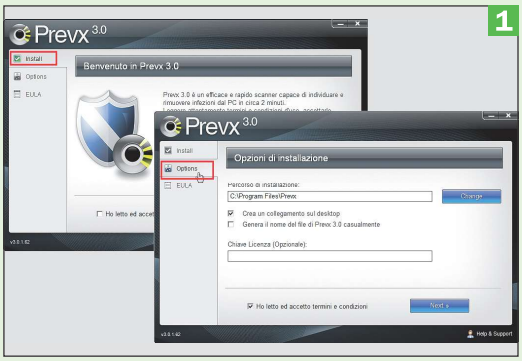
Nella tabella con i file infetti rilevati durante la scansione, accanto a ogni riga appare un'icona. Nella versione freeware di Prevx il suo colore cambia per indicare se il programma è in grado di intervenire per rimuovere la minaccia oppure no.

Per esempio, un'icona di colore scuro con una F significa che il programma è in grado di eliminare il malware (F= *Free to cleanup*), portando l'elemento in quarantena. Quando l'icona è di colore rosso, invece, significa che la versione gratui-

Annotazioni sempre e ovunque

Finestra di lavoro

La finestra di lavoro del programma ha dimensioni fisse. Sulla sinistra ha una barra di navigazione verticale con le aree in cui si può intervenire e, a destra, l'area di lavoro vera e propria. Nella fase iniziale si può fare clic su *Options* per visualizzare la pagina in cui scegliere la cartella di installazione del programma.

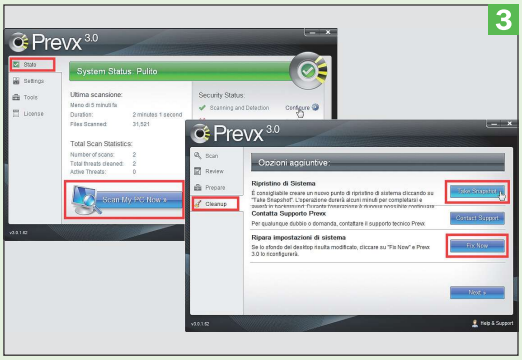


Scansione iniziale

Appena installato, Prevx lancia subito la scansione dei dischi del computer. L'utente può fermarla con un clic su *Cancel Scan*. Perché si possano leggere i dati del malware dal database online, il computer deve essere connesso in Internet. Nel caso di minacce, l'azzurro della finestra diventa rosso e un clic su *Cleanup Now* ne avvia la rimozione.

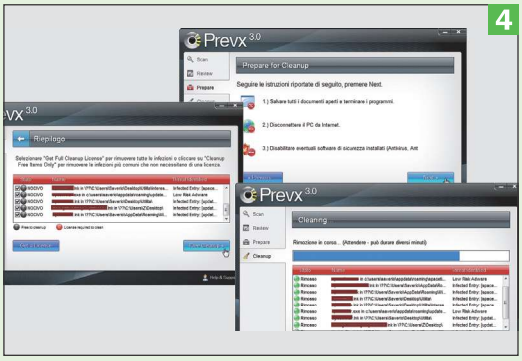
Scansione e recupero da anomalie

Con *Stato*, *Scan My PC Now* si lancia la scansione dei dischi e le voci della barra laterale cambiano in *Scan*, *Review*, *Prepare* e *Cleanup*. Nella pagina *Cleanup*, un clic su *Take Snapshot* crea un punto di ripristino del sistema operativo, mentre un clic su *Fix Now* corregge eventuali anomalie nella visualizzazione dello sfondo del *Desktop*.



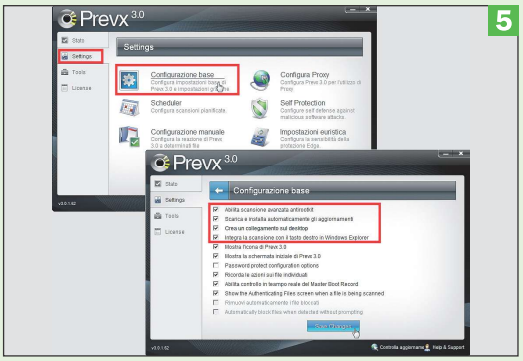
Segnalazione presenza malware

Quando viene rilevata la presenza di malware, ogni elemento viene riportato nel rigo di una tabella con accanto un'icona. La versione freeware di Prevx elimina gli elementi indicati da un'icona con la F (= *Free to cleanup*) facendo clic su *Cleanup Now*, *Free Cleanup*, *Next*. Al termine appare l'elenco degli elementi maligni che sono stati rimossi.



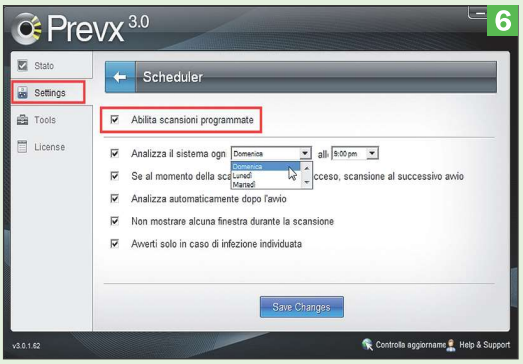
ta non riesce a intervenire. L'utente, allora, deve dirigersi su una delle versioni di Prevx a pagamento o fornirsi di altri strumenti software per liberarsi del pericolo.

Completata la prima scansione degli archivi, nel momento in cui si chiude il programma, questo si trasferisce sotto forma di icona nel vassoio di Windows. Lì appare anche durante le successive sessioni di lavoro, perché il programma parte automaticamente ogni volta che si avvia il sistema operativo.



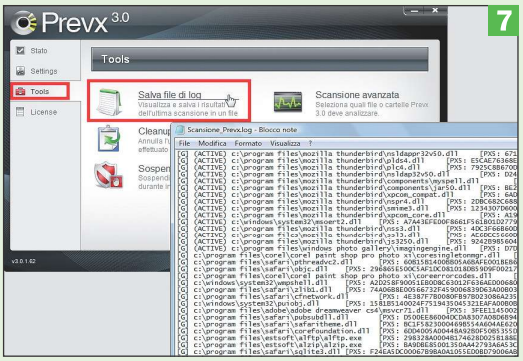
5

Impostazioni di base
Con *Settings*, *Configurazione Base* si apre la pagina in cui si possono modificare varie modalità di funzionamento di Prevx, tramite una serie di caselle di selezione. Per esempio, si possono impostare la scansione avanzata rootkit, l'aggiornamento automatico da Internet e l'integrazione dei comandi nel menu contestuale di Explorer.



6

Scansioni programmate
Per far partire le scansioni automaticamente, si attiva la casella *Abilita scansioni programmate* nella pagina *Settings*, *Scheduler*. In *Analizza il sistema ogni...* si sceglie se lanciarla quotidianamente o in quale giorno della settimana e a che ora. Altre opzioni indicano come comportarsi se il PC non è acceso e cosa fare in caso di infezioni.



7

Creazione file di log
Ogni volta che esegue una scansione, Prevx crea un file di testo con righe che riportano l'esito del controllo sui vari file. L'utente può salvare l'ultimo con *Tools*, *Salva file di log*, indicando nome e cartella di destinazione nella finestra *Salva con nome*. Successivamente, lo si può aprire con *Blocco Note* per verificarne il contenuto.

8

Nel sito, informazioni sulle minacce
Nel proprio sito Internet, Prevx fornisce numerose informazioni sui vari tipi di malware, documentandoli in modalità dettagliata dividendo la pagina Web in sezioni. Per ogni elemento vengono elencati: comportamento (*Behavior*), nazione di origine, altri nomi con cui può presentarsi (*Aliases*), dimensioni e tipo del file e, se noto, da chi proviene.

Dal menu contestuale che appare facendo clic sull'icona, si può lanciare la scansione degli archivi o aprire la finestra di lavoro del programma. La dotazione di base dell'applicazione viene integrata con un gruppo di funzioni di utilità, elencate nella pagina degli strumenti *Tools*.

La prima di esse permette di eseguire il salvataggio dei risultati dell'ultima scansione in un file di testo, consultabile anche con *Blocco Note*. Dall'elenco delle voci si possono vedere in dettaglio quali programmi e librerie sono stati controllati e con quale risultato.

L'esito del controllo viene riportato con una o due lettere tra parentesi quadre all'inizio della riga. Le iniziali possono essere [B] per *Bad* (in italiano: "cattivo"), [G] per *Good* ("buono"), [U] per *Undefined* ("indefinibile"), indicazioni facilmente interpretabili da chiunque.

Altre funzioni di utilità permettono di ripristinare lo stato a una situazione precedente a uno degli ultimi interventi eseguiti dal programma e di avviare la scansione in modalità rapida o in quella avanzata. Nella versione freeware, non sono attive tutte le funzionalità.

Opzioni di funzionamento e aiuto

Tra le opzioni di configurazione disponibili, si può impostare la scansione avanzata contro i *rootkit*, chiedere di prelevare automaticamente gli aggiornamenti da Internet e di attivare il controllo dal menu contestuale di Explorer. Gli eventuali aggiornamenti, comunque, riguardano l'applicazione in senso stretto e non un file di firme del malware, perché i dati raccolti da Prevx vengono confrontati con quelli di un database in Internet.

Per evitare di doversi ricordare di lanciare in esecuzione il programma, si possono pianificare scansioni periodiche dei dischi che partono automaticamente.

Tutte le impostazioni possono essere protette da variazioni indesiderate tramite una password.

Nella parte inferiore della finestra, Prevx mostra due collegamenti. Il primo, *Controlla aggiornamenti*, avvia la ricerca di eventuali nuove versioni nel sito del produttore.

Il secondo, *Help & Support*, apre la pagina del sito *prevx.com* in cui si possono chiedere aiuto e spiegazioni alla struttura di supporto tecnico. Le risposte ai quesiti vengono inviate all'indirizzo di posta elettronica fornito dall'utente.

Nella pagina Web *Prevx 3.0 Help* raggiungibile all'indirizzo Internet http://info.prevx.com/edgehelp.asp, è disponibile una dettagliata guida utente sul programma in inglese. Nelle varie sezioni del documento sono presenti anche le immagini utili alla comprensione delle diverse fasi operative.

Prevx viene fornito in tre versioni, di cui una freeware e due commerciali.

Quella freeware rileva la presenza di malware e lo segnala. Può eliminare solo parte degli elementi trovati, però, corrispondenti ai rootkit che infettano il record di boot del disco di avvio (MBR: *Master Boot Record*) e all'adware. Indica, comunque, esplicitamente per quali di essi non può intervenire.

Una seconda versione elimina tutti i componenti maligni trovati, ma non lavora in tempo reale. La terza versione, infine, lavora in tempo reale e interviene nel modo più completo per proteggere il sistema operativo. ■

Saverio Rubini