PC Tools ThreatFire Free

Combattere i virus del "giorno zero"

▶ Il problema

PROGRAMMA NEL DVD

Aumentare la protezione dal malware, migliorando quella garantita dal solo antivirus

▶ La soluzione

ThreatFire analizza il comportamento del software in transito nel sistema per intercettare e bloccare eventuali comportamenti anomali

Un antivirus combatte il malware in transito nel computer, tentando di identificarlo attraverso l'individuazione di una stringa di byte detta "firma". ThreatFire è un programma da affiancare all'antivirus per intercettare le minacce nel loro "giorno zero" (*zero day threats*). Con questa dizione ci si riferisce al nuovo malware appena rilasciato in Rete, del quale non è già disponibile la firma per riconoscerne la presenza e cancellarlo.

Nuovi trojan, rootkit, worm e altri codici con finalità maligne, infatti, continuano a diffondersi a getto continuo grazie a posta elettronica, chat, scambi di file in peer to peer. I produttori di antivirus hanno bisogno di un minimo di tempo per disporre del codice infetto e aggiornare il file delle firme. Peraltro, non tutti gli utenti aggiornano con frequenza il proprio antivirus, anche se spesso sono i programmi stessi a farlo in tempo reale quando ci si connette in Internet.

ThreatFire, invece, svolge un'azione tanto utile quanto discreta: rimane residente in memoria per "accorgersi" di eventuali comportamenti sospetti, tipici del malware. In questo modo è in grado di intervenire per bloccarlo immediatamente, senza necessità di disporre della firma specifica.

Un'altra funzione è il controllo del contenuto dei dischi per verificare l'eventuale presenza di minacce già in atto. La scansione può avvenire in modalità di base, più veloce, o piena (full scan). Nel secondo caso il controllo del sistema è più accurato, anche se si impiega più tempo per portarlo a termine.

Il programma è ampiamente personalizzabile. Si possono creare proprie regole di comportamento su determinati tipi di file, per chiedere di intervenire o di disabilitare l'attività di controllo. Si può attivare o meno la verifica di alcuni processi del sistema operativo. Si può anche escludere dal controllo il traffico relativo a specifici client di posta elettronica e browser.

Il livello di protezione può variare da uno (solo su minacce di tipo già conosciuto) a cinque (su tutte le attività) .

Un grafico pubblicato nel sito del produttore riporta che la capacità di intercettare il malware dell'accoppiata antivirus più ThreatFire aumenta dal 15 al 230 per cento, a seconda del tipo di antivirus utilizzato. ■

S. R.

PC Tools ThreatFire Free 3.0.14
Categoria: sicurezza
Versione: freeware
Download: www.pcopen.it
Richiede installazione: sì
S.O.: Win Vista, 2003, 2000, XP

Ricco di opzioni

▶ Stato della protezione

Il primo pulsante della barra di navigazione è *Security Status*. Apre la pagina con i dati dello stato della protezione del sistema, aggiornati in tempo reale. Due colonne mostrano il numero di eventi, di programmi, di attività sospette e di malware bloccati. I valori vengono ripartiti per periodo temporale: oggi, ultimi 7, 30 e 90 giorni e totale.

▶ Scansione del sistema

Un clic su *Start Scan* lancia il controllo del contenuto dei supporti di memoria del sistema. Attivando il pulsante di opzione *Basic Scan* sotto *Select Scan Type*, si chiede di eseguire un controllo veloce, oppure *Full Scan*, (scansione più approfondita). Si può chiedere di cercare eventuali rootkit attivando la casella sottostante *Scan for rootkits*.

▶ Lingua e altre opzioni di configurazione

Il pulsante *Settings* apre la pagina delle impostazioni, divisa in tre schede. In *General* si gestiscono l'attivazione del programma, il livello di protezione, la richiesta di aggiornamenti, la lingua dell'interfaccia (pulsante Program Language). Nella scheda *Quarantine* appare il malware messo in quarantena.

▶ Impostazione del livello di protezione

Con la sequenza *Settings*, *Protection level*, *General* a destra appare un cursore orizzontale. Spostando il cursore si imposta il livello di intervento desiderato, dal più basso 1 al più alto 5. Attivando il livello uno, il programma verifica solo la presenza di minacce già note. Il livello cinque è il più completo, anche se consuma più risorse.