Gmer Rootkit Killer

Cerca ed elimina i rootkit

▶ Il problema

PROGRAMMA NEL DVD

Proteggersi dai rootkit controllando anche tra gli oggetti meno accessibili di Windows

▶ La soluzione

Gmer Rootkit Killer cerca gli eventuali rootkit presenti nel sistema per evidenziarli in rosso e permetterne l'eliminazione con un clic

I rootkit sono software della categoria malware il cui scopo è l'esecuzione di azioni dannose senza necessità di interventi dell'utente o dell'amministratore. Si installano in punti delicati del sistema, come le chiavi del registro o i servizi, cercando di rendersi invisibili.

Quando giungono ad attivarsi, possono installare backdoor o troiani. Più semplicemente, possono agire per nascondere il funzionamento di altro malware, per esempio spyware che inviano informazioni riservate all'esterno.

Per combatterli, si può lanciare Gmer Rootkit Killer che prova a scovare la presenza di eventuali rootkit eseguendo la scansione di vari componenti del sistema operativo.

Vengono eseguiti controlli nel registro di Windows, tra i processi attivi, nelle librerie e nei servizi installati nel sistema. Viene controllato anche il contenuto degli *Alternate Data Streams*, oggetti software costituiti da flussi (*streams*) di dati associabili ai file nel file system NTFS.

Nel caso in cui venissero rilevati elementi pericolosi, le relative righe verrebbero evidenziate in rosso. A questo punto si può eseguire l'operazione di eliminazione del rootkit, tramite l'apposita voce del menu contestuale che compare facendo clic con il tasto destro del mouse.

Oltre alla ricerca dei rootkit, il programma comprende altre funzioni come la gestione dei processi e dei servizi. I processi vengono elencati in una tabella con il numero (PID), la quantità di memoria impegnata, per quanto tempo è stato impegnato dal kernel e dall'utente. Il clic con il tasto destro su una riga apre un menu contestuale dal quale è possibile visualizzarne le proprietà, chiudere il processo selezionato o tutti quelli in esecuzione con un solo comando.

Nella pagina dei servizi, si può abilitare o disabilitare un servizio e attivarne l'avvio in modalità manuale o automatica. Chi lo desidera può lanciare la cancellazione di uno di essi, selezionandolo e facendo clic su *Delete*.

Va sempre ricordato che interventi come quelli descritti sono da eseguirsi con estrema attenzione, perché possono comportare conseguenze pericolose per il funzionamento di Windows o addirittura il blocco completo del sistema. ■

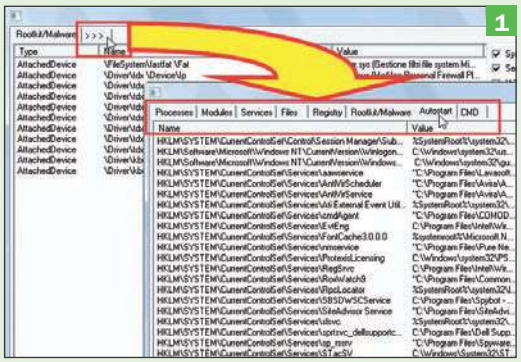
S. R.

Gmer Rootkit Killer 1.0.14
Categoria: utility
Versione: freeware
Download: www.pcopen.it
Richiede installazione: sì
S.O.: Win Vista, XP, NT, 2000

Controlla processi e registro di Windows

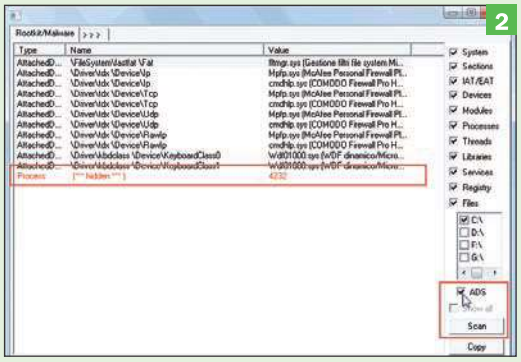
▶ Finestra divisa in schede

All'apertura, il programma esegue subito una scansione, mostrando i risultati nella finestra di lavoro.
Sulla destra si possono attivare le caselle di selezione per scegliere gli elementi in cui deve essere eseguita la ricerca di eventuali componenti pericolosi.



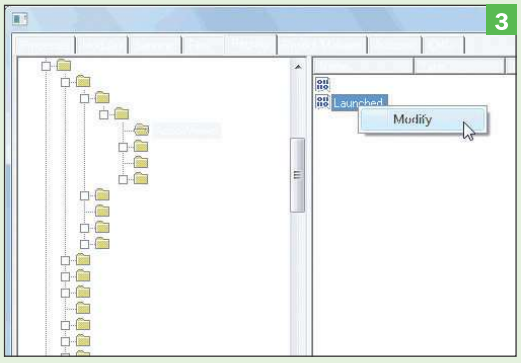
▶ Risultati della scansione

Prima di lanciare la scansione dei dischi selezionati facendo clic su *Scan*, si può scegliere se selezionare anche la casella *ADS*. Al termine, il programma elenca i risultati nella pagina *Rootkit/Malware*. Se una riga è di colore rosso, il relativo elemento è "sospetto". Per eliminarlo, clic con il tasto destro sulla voce e poi su *Kill process*.



▶ Interventi nel registro

Se si fa clic sulla linguetta *Registry*, appare una scheda divisa in due colonne. A sinistra viene visualizzata la struttura del file di sistema, a destra il contenuto della cartella selezionata. Con la dovuta cautela, l'utente può variare una voce del registro facendo clic con il tasto destro sulla riga a destra e poi su *Modify*, nel menu contestuale.



▶ Gestione dei servizi

La linguetta *Services* apre la pagina con la tabella dei servizi installati nel sistema. Oltre al nome, vengono riportate le modalità di avvio, il nome del file e la descrizione. Facendo clic con il tasto destro su una delle righe, si può variare la modalità di avvio, (per esempio impostandola in uno dei valori AUTO, MANUAL o DISABLED) o fare clic su *Delete*.