Courtesy of Gabriele Del Giovine, Microsoft MVP

Com'è noto, nelle ultime settimane si è notevolmente diffusa questa piaga endemica chiamata **LinkOptimizer/Gromozon.**

In primo luogo è necessario mettersi in mente che NON ESISTE UN TOOL IN GRADO DI RIMUOVERE IL PROBLEMA ma che occorre procedere caso per caso dato l'elevato numero di varianti e di rootkit che vengono installati. Inoltre tools come Hijackthis non sono sempre utili allo scopo.

Prima di iniziare munitevi di questi strumenti:
- Il removal di PrevX1: http://www.prevx.com/gromozon.asp
- Il Rootkit removal tool di Sophos:
http://www.sophos.com/products/free-tools/sophos-anti-rootkit.html
Download Removal Tool Symantec (NDR)
- Il Rootkit removal tool di Fprot:
http://www.f-secure.com/blacklight/try_blacklight.html
- L'antiSpyware Ewido: http://www.ewido.net/en/
- Un antivirus decente

Quella che segue è la procedura base, che ho seguito con successo in diversi casi.

0) accedere alla macchina come amministratore.

1) iniziare con il removal tool fornito da Prevx1

2) Non è detto che la cosa si esaurisca con il removal tool di Prevx1. Molte varianti di LinkOptimizer installano rootkit aggiuntivi che tolgono alcuni diritti avanzati agli utenti amministrativi, come ad esempio quello di debug e di accesso ad alcuni rami di Registry. Grazie a questo bloccano l'installazione di quasi tutti i tools antivirus, antispyware e di rimozione dei rootkit.
Verificate che tra gli account di Windows non ci siano account con nomi strani (senza senso) e che fra i servizi di windows non ci siano servizi che usano questi account creati dal rootkit. Ci saranno sicuramente.
Il servizio normalmente si chiama **WebLck** ma potrebbero essercene diversi con nomi similari.

Per prima cosa DISATTIVATE o CANCELLATE l'Account usato dai servizi che costituiscono parte di LinkOptimizer. Quindi fate ripartire il PC.

Nelle proprietà dei servizi vedrete anche quali sono i file interessati ma purtroppo non sarete in grado di eliminarli.
I file sono posizionati di norma in c:\programmi\file comuni\System
Li riconoscete perche sono gli unici due eseguibili exe. Inoltre sono crittografati.

Come detto prima occorre riottenere il possesso dei files (*Ownership*) accedendo alle impostazioni avanzate di sicurezza di ogni singolo file.
Indicate come proprietario dei files il gruppo locale degli amministratori.
Fatto questo potete reimpostare le autorizzazioni per i file.
Date full control al gruppo degli administrators locali. Quindi DISTRUGGETE i files.

Utile: LinkOptimizer: come rimuoverlo ed altri suggerimenti by MVP Ester Memoli

Riavviate la macchina.

Ora installate Ewido, fate l'aggiornamento e quindi una scansione.
Troverà altro materiale (probabilmente in c:\windows\system).
Rimuovete il tutto e riavviate.

Ora potete passare ai rootkit removal.
Il tool di **Sophos** è particolarmente utile dato che mostra chiaramente quali sono i problemi ed i file che ospitano i vari rootkit.
Se il tool di **Fprot** si installa significa che non ci sono più processi attivi relativamente a LinkOptimizer.
Il servizio che ospitava LinkOptimizer può essere rimosso eliminando dal registry la relativa entrata. Anche qui occorre reimpostare il proprietario di ogni singolo ramo di configurazione.
Una volta reimpostato il proprietario potete reimpostare le autorizzazioni e quindi dare full control al gruppo

degli amministratori locali. Fatto ciò potete cancellare la parte di Registry relativa ai servizi usati da LinkOptimizer.