Forum: Propositions de logiciels

Topic: recherche des rootkits

Subject:

Publié par: Lotesdelere

Contribution le : 12/05/2006 00:47:40

[quote:3779615938="sylvie"]Pour moi Rootkit revealer est très compliqué.
Je ne comprends pas comment il fonctionne.[/quote:3779615938]
Il n'est pas si compliqué et il fonctionne tout seul :P
Il s'est bien amélioré dans les versions récentes. Il se contente de rapporter ce qui est "invisible" par les API de Windows et qui donc peut fonctionner "à l'insu de notre plein gré", pour reprendre une expression célèbre :)

Rootkit Revealer scanne la base de registres ce que BlackLight ne semble pas faire :?
Les deux outils sont donc complémentaires, BlackLight est toutefois un peu dangereux car il peut proposer d'effacer des choses qui ne devraient pas l'être.

Pour info il y a de nombreux logiciels tout à fait légitimes qui utilisent le système de rootkit pour pouvoir fonctionner et/ou qui agissent au niveau Ring0, c'est-à-dire au plus près du kernel.
Par exemple: Daemon Tools, Alcohol 120%, NOD32, Kaspersky AV, Process Guard, BitDefender, PestPatrol, Look'n'Stop, Tiny Personal Firewall, Kerio Personal Firewall, Sygate Personal Firewall, Symantec/Norton Firewall, OutPost Firewall, Norton Ghost, pour ne parler que des plus connus/répandus.

Et en bonus voici un freeware de protection qui va se charger de surveiller les accès au clavier, à l'écran et aux fenêtres de Windows qui pourraient être faits par d'autres logiciels: SnoopFree Privacy Shield.
Par contre, n'utilisez pas le lien Download.com pour télécharger SnoopFree car c'est une ancienne version (1.05). Utilisez ce lien pour télécharger la dernière version 1.07:
http://www.snoopfree.com/download.htm
Disponible en anglais uniquement et ne fonctionne que sous Windows XP.