Forum: Propositions de logiciels

Topic: recherche des rootkits

Subject: Re: re

Publié par: Lotesdelere

Contribution le : 12/05/2006 22:25:44

[quote:555a79ca9e="pakalou94"]il me trouve un spy nommé Médiaplex cookie !
apparament livré avec snoopfree[/quote:555a79ca9e]
Les apparences sont parfois trompeuses...

Mais comme on n'est jamais trop prudent, et pour en avoir le cœur net, j'ai installé cet après-midi un Windows XP SP2 tout neuf dans une machine virtuelle de Microsoft Virtual PC 2004 (qui, soit dit en passant, est un logiciel absolument génial de Microsoft, car oui, il leur arrive de faire des choses bien. Payant, c'est du Microsoft hein, mais génial. Bref...).
Virtual PC émule un ordinateur et vous permet donc d'installer et de faire tourner quasiment n'importe quel OS, ce qui permet de faire des tests tout en limitant les risques d'une "vraie" installation mais avec un comportement strictement identique. Parce-que bon, répétons le, on n'est jamais trop prudent.

A peine l'OS installé et mis à jour, je m'empresse de copier l'image disque pour avoir un XP tout propre pour chaque test que je veux effectuer.
Logiciels mis en œuvre: Kaspersky AV, Avast, NOD32, Kerio PF, OutPost Firewall, Process Guard, Ghost Security Suite (AppDefend et RegDefend), RegMon, FileMon, InCtrl5, Process Explorer, Rootkit Revealer, IceSword, BlackLight, Dependency Walker, FAR Manager, Port Explorer, Registry File Viewer, Registry Crawler, ERUNT, WinHex, Spybot, Ad-Aware, M$ AntiSpyware, HiJackThis, et je dois en oublier quelques uns.

Bon, je ne vais pas entrer dans les détails de toutes les manips effectuées seulement voilà, j'ai beau chercher dans tous les coins du disque dur, de la base de registres et même d'éventuels rootkits, je ne trouve rien de rien, n'obtiens pas d'alarmes au sujet de processus suspects qui se lanceraient ou qui seraient modifiés (DLL injection) et autres modifications douteuses, pas de spyware / malware /adware ni même de tentatives de connexion vers internet (LSP non modifiés).

SnoopFree a installé un service et une interface utilisateur, ajouté quelques clefs dans la base de registres, rien d'autre semble-t-il.

Je tâche donc d'en savoir plus sur Mediaplex cookie et là surprise! Il s'agit d'un cookie. Un fichier texte donc.
Très mal noté il est vrai car Mediaplex semble incorporer à ce cookie des informations de traçage que la netiquette réprouve. Ce qui lui vaut la mention "Spy" et non pas Spyware car ce n'est pas un logiciel.
Rappelons au passage qu'un cookie n'est généré par un site qu'au travers d'un navigateur ou de certains media players.

Bon, ça m'apprendra, la prochaine fois je chercherai d'abord sur Scroogle avant de me lancer dans deux heures de tests.
Je ne cherche plus avec Google car c'est des vilains, ils mettent plein de cookies traceurs sur mon

ordi et je n'ai pas envie de réinstaller Windows après chaque recherche (voir http://www.google-watch.org/gmail.html).

Bien, il est temps que j'aille manger, je me sens si las...