Forum: Propositions de logiciels

Topic: kezako les "rootkit"

Subject: Re: kezako les "rootkit"

Publié par: skorpix38

Contribution le : 24/11/2007 08:37:48

Citation :

Le Gaulois a écrit:
(suite) Pour éviter d'attraper des virus, rootkit et autres cochonneries...
...

Toujours de bons conseils bien clairs, Le Gaulois, comme d'hab...
Je rajoute qq grains de sel !
Il commence à y avoir qq petits progs pour détecter les infections par de telles bestioles.
J'entends: situer les différents points d'incrustation, car ils sont tjs mutiples de façon à auto-régénérer le maliciel quand on croit avoir éliminé sa source.
J'ai une fois passé 4 heures à éradiquer un rootkit planté par un site porno ukrainien (d"après l'IP) sur la machine XP d'une grand-mère de 70 ans utilisée imprudemment par qq'un de sa famille.
Cru que je n'y arriverais jamais !

Parmi qq outils pour l'inspection / prévention :
- SEEM (System Eyes & Ears Monitor) en français, par Al et Nunki
- FS BlackLight, de FSecure (oct 2007)
- GMer v1.0.13, petit outil polonais
- RootKit Revealer de Mark Russinovitch (SysInternals)
Après identification certaine, chercher s'il existe un outil de désinfection 'tout fait".
On a aussi très souvent besoin d'un FileKiller qui permettra de tuer le dernier fichier malsain sur le disque dur au moment du reboot : comme il est en mémoire quand Windows est chargé, impossible de faire un delete classique.

Mais tout ça est plutôt axé WinXP.
Mon unique machine Millenium n'est pas connectée Internet, je n'y ai jamais essayé ces outils...
Ca risque plutôt d'être "à la main" dans la base de registre : le casse-pipe assuré pour tout débutant.
Faut chercher une aide qualifiée dans vos relations !