Forum: Propositions de logiciels

Topic: re : Sophos Anti-Rootkit

Subject: re : Sophos Anti-Rootkit

Publié par: Lotesdelere

Contribution le : 24/08/2006 23:37:45

Bonjour Monsieur Phelps,

[quote:cecb504af4="vinyz"]Il m'a trouvé un fichier appelé "akgelnjrvw.exe" à plusieurs endroits différents et dans différentes variantes

E:WINDOWSsystem32akgelnjrvw.exe
E:WINDOWSsystem32akgelnjrvw.dat
E:WINDOWSsystem32akgelnjrvw_nav.dat
E:WINDOWSsystem32akgelnjrvw_navps.dat
E:WINDOWSPrefetchAKGELNJRVW.EXE-07BB45F8.pf

et dans la registry :
HKEY_USERSS-1-5-21-1935655697-839522115-682003330-1007SOFTWAREMicrosoftWindowsCurrentVersionRunakgelnjrvw

cependant il n'y a rien sur le disque dur à l'endroit désigné.
Il est vrai que c'est soit disant un fichier caché mais même en caché ... y'a rien.[/quote:cecb504af4]

Ca sent mauvais.
A éliminer d'urgence.
C'est bien le problème avec les rootkits, à supposer que ça en soit un, ils se planquent !

Un peu d'aide ici:
http://forum.telecharger.01net.com/te ... ve-403484/messages-1.html

Et là:
http://forum.telecharger.01net.com/te ... nt-403575/messages-1.html

Télécharger également Autoruns:
http://www.sysinternals.com/Utilities/Autoruns.html
qui pourra t'aider à détecter les saletés qui se chargent au démarrage de ton ordinateur. Attention! A utiliser avec grandes précautions!
Au préalable, sauvegarde de la base de registres (avec ERUNT bien sûr) indispensable!
Ne pas oublier de désactiver la restauration système puis de la réactiver quand tout sera à nouveau propre.

Bonne chance Jim !