



Forum: Propositions de logiciels

Topic: AVG Anti-Rootkit 1.0.0.13 Beta

Subject: Re: AVG Anti-Rootkit 1.0.0.13 Beta

Publié par: Lotesdelere

Contribution le : 28/08/2006 13:55:13

[quote:eae6f96a44="sylvie"]et encore un anti rootkit...c'est la mode

[/quote:eae6f96a44]

La "mode", disons plutôt la tendance, est surtout d'installer des saletés sur votre ordinateur en utilisant le système de rootkits puisqu'ils sont invisibles par les API de Windows et donc indétectables par les anti-virus et les anti-spywares classiques.

Merci à Sony pour avoir montré cette méthode à x milliers de script kiddies

Le seul moyen connu d'empêcher l'installation des rootkits est un surveillant de processus comme [Process Guard](#) ou AppDefend de [Ghost Security Suite](#).

Je crois que Sylvie a posté un freeware qui semble offrir des fonctions similaires mais dont je ne me souviens plus du nom et que je n'ai pas testé, étant l'heureux propriétaire d'une licence Process Guard.

Par ailleurs ces utilitaires sont à manier avec d'extrêmes précautions car en utilisant un paramétrage incorrect vous pouvez aboutir à un blocage total ou partiel de votre OS. A ne pas mettre entre toutes les mains donc, et la protection du paramétrage par mot de passe est indispensable surtout si vous utilisez un PC partagé entre plusieurs personnes et/ou en réseau.