Rootkits 2ème partie

Comme déjà décrit dans mon tutorial du 05.05.2005. « **Nouvelles menaces, les rootkits** », une nouvelle menace, les « **rootkits** » sont en train d'envahir les **PC-WINDOWS**.
Link : **http://www.internetmonitor.lu/Nouvelles-menaces,-les-rootkits-_a539.html**

C'est quoi un « rootkit » ?

Le mot « **rootkit** » vient bien évidemment de l'anglais et il est composé de deux mots : « **root**[1] » et « **kit**[2] ».
« **Root** » veut dire la racine et « **kit** » est représentatif pour un assemblage de pièces diverses.
Les deux mots assemblés « **rootkits** » veulent dire : assemblage de scripts qui attaquent la racine du processeur, le « **Kernel**[3] ».
Le mot « **Kernel** » vient bien entendu aussi de l'anglais et signifie « **noyau** ».

Et c'est exactement ce que font ces nouvelles bestioles informatiques (nouveau pour le **PC-WINDOWS**, mais pas pour le **MAC OS**, ni **LINUX**, ni **UNIX**).
Ils s'incrustent dans la racine du processeur, dans le « **Kernel** ». Ces scripts malicieux sont nommés presque égaux que les services **WINDOWS**, seulement ils seront changés légèrement.

Exemple pratique :

Imaginons qu'un attaquant a développé un script nommé « netstat.exe » (ce service existe vraiment sur le PC) et que le script malicieux a déjà été infiltré au PC.
L'attaquant n'éradique pas le service original (netstat.exe), mais par contre le renomme en « netstast_alt.exe ». De cette façon il pourra utiliser le service original lui-même ultérieurement.

Si maintenant, le service « netstat.exe » est activé, **le script malicieux** active le service original, dévie ce service, cache ses vraies intentions et présente son propre service modifié. **L'utilisateur (même averti et expert) ne remarquera rien du tout, car tout fonctionne normalement !**

Seul différence, ce scripte malicieux a installé et caché un « **Troyen**[4] », qui lui cache un « **Keylogger**[5] » et un « **Backdoor**[6] ». ***En plus, ce « Rootkit » installe plusieurs scriptes en cascade !***

Si on arriverait à détecter un d'eux et qu'ils seraient éradiqués, les autres scriptes s'activeraient automatiquement ; très astucieuse cette méthode et très dangereuse !

Impossible de détecter les « **Rootkits** » (juin 2005) avec des anti-virus. Si on attrape ces sales bestioles informatiques, il ne reste rien d'autre à faire que de réinstaller **WINDOWS** !

Qui est visé ?

Contrairement à ce que croient la plupart des gens, ce n'est pas seulement les firmes et grandes firmes qui sont visées, **mais surtout les privés** ! Étonné(e)s ? Eh bien oui, les **privés** sont même **privilégiés par** la « **mafia informatique** », parce qu'ils sont plus naïfs, dû à **la non connaissance et/ou ignorance aux risques de sécurité !**
Rien de plus simple que de leurs (vous) refiler une de ces bestioles informatiques et de téléguider leurs (votre) PC !

[1] Root = racine
[2] Kit = assemblage de pièces diverses
[3] Kernel = noyau, le coeur du processeur
[4] Troyen = programme (script) qui en cache minimum un autre programme
[5] Keylogger = programme (scripte) qui enregistre les frappes de clavier et qui les envoie à son programmeur
[6] Backdoor = programme (scripte) qui ouvre les ports du PC pour permettre au Keylogger et Troyen d'expédier leurs messages.

Pourquoi téléguider le PC ?

L'intérêt de cette « **mafia informatique** » est d'espionner votre PC pour récupérer vos mots de passe, numéros **PIN** et **TAN (e-banking, ebay, etc.)**, d'autres codes d'accès et **d'utiliser entre autre votre espace de disque dur (hard disk) pour y stocker du contenu illégal** et/ou de l'employer comme base pour envoyer du « **Spam**[7] », du courrier non sollicité !
En plus votre disque dur (hard disk) sera employé comme relais pour faire des **attaques du type DDOS**[8]. Votre PC sera transformé en **PC-ZOMBIE**[9] !
Lire aussi l'article suivant :

Votre PC est-il un «zombie» à louer?

http://www.internetmonitor.lu/index.php?action=article&id_article=67428

Le pire, vous ne vous en apercevrez pas de l'utilisation clandestine de votre disque dur !

Mais passons en maintenant à notre trousse de secours.

Comment détecter les « Rootkits » ?

Comme les menaces des « **Rootkits** » sont encore relativement récentes sur les **PC WINDOWS**, les logiciels (programmes) sont encore très rares. Néanmoins il en existent quelques un :

Rootkit Hunter : **http://.rootkit.nl/projects/rootkit_hunter.html**

Blacklight : **http://www.f-secure.com/blacklight**

Strider Ghostbuster : **http://research.microsoft.com/rootkit**

Rootkit Revealer : **http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml**

Process Guard : **http://www.diamonds.com.au**

Et puis il existe encore « **A squared** » (a2) de chez Emsisoft.
Toutes ses fonctions ont déjà été décrites dans la première partie de « **Rootkits** » à l'adresse suivante :

http://www.internetmonitor.lu/Nouvelles-menaces,-les-rootkits-_a539.html

« A squared » est un programme que je vous recommande fortement et que j'utilise déjà depuis plus d'une année. C'est un programme anti-malware qui est en développement constant.

Conclusion :

Attention aux „**Rootkits**"! C'est une nouvelle menace qui est très performante et qui seulement est en développement. Je ne veux pas prédire les choses (je ne suis pas prophète), mais il me semble bien que cette menace **deviendra un nouveau fléau à ne pas sous estimer du tout**.
Son potentiel est énorme, de telle façon que même des experts en ont des problèmes à les détecter (les éradiquer est impossible de toute façon, pour l'instant [14.06.2005.]!) !

[7] **SPAM** : Courrier non sollicité
[8] **Attaques DDOS** : Attaques massives d'un serveur avec des données jusqu'à ce qu'il est surchargé et ne fonctionne plus

[9] **PC ZOMBIE** : PC non protégé et téléguidé pour faire des actions illégales

Résumé :

Les « **Rootkits** » sont des « **Super Troyens** », ont pourrait même les nommer des « **Troyens camouflés** », qui s'incrustent dans l'A.P.I. (**Application Program Interface**) du PC WINDOWS. L'« **API** » est une interface qui gère entre autre les services **WINDOWS** et la base de registre du système, ainsi que le bon fonctionnement de tous les modules du système d'exploitation entre eux.

Une fois ces services demandés, les « **Rootkits** » les interceptent et les exécutent, mais en même temps **ils exécutent leur code malicieux et le camouflent de telle manière qu'il ne sera plus détecté.** En plus, s'il y a un programme (logiciel) anti-virus qui scanne le PC et qui aurait détecté cette application, aucune chance. ***Les « Rootkits » filtrent cette requête et renvoient un statut normal à l'anti-virus. Ils deviennent ainsi invisibles (très dangereux et très ingénieux) !***

Même en examinant le PC avec le « **TASK MANAGER** », le « **gestionnaire des tâches** », vous ne les verrez pas, ils sont cachés !

Des signes éventuels que vous ayez des « **Rootkits** » installés sur votre Pc sont :

- Des ports ouverts
- Puissance utilisée de votre PC a augmenté
- La mémoire virtuelle de votre disque dur a diminué

« **Bonjour les dégâts** »

NORTON INTERNET SECURITY contient un « **Anti-virus** », un « **Firewall** », un « **Anti-Spam** » et un « **Filtre parental** ».

Dans des tests de magazines PC professionnels, « **NORTON INTERNET SECURITY** », ainsi que « **ZONEALARM** » ont été sélectionnés aux premiers rangs.

Norton Internet Security : http://www.symantec.com/region/fr/product/

Zonealarm : http://fr.zonelabs.com