14. Les “rootkits”, 2ième partie

Comme déjà décrit dans notre didacticiel “Nouvelles menaces, les rootkits”, une nouvelle menace, les “rootkits” sont en train d’envahir les PC-Windows®.
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 de la même façon que les services Windows®, seulement ils seront changés légèrement.

Exemple pratique :

Imaginons qu’un attaquant ait développé un script nommé “netstat.exe” (ce service existe vraiment sur l’ordinateur) et que le script malicieux ait déjà été infiltré dans l’ordinateur. Le script malicieux n’éradique pas le service original (netstat.exe), mais par contre le renomme en “netstat_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 !

Seule différence, ce script 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 arrivait à détecter l’un d’eux et qu’ils étaient éradiqués, les autres scripts s’activeraient automatiquement. Cette méthode est très astucieuse et très dangereuse !

Impossible de détecter les “rootkits” (juin 2005) avec des antivirus. 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 ne sont 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 des risques de sécurité !
Rien de plus simple que de leur (vous) refiler une de ces bestioles informatiques et de téléguider leur (votre) ordinateur !

Pourquoi téléguider le PC ?

L'intérêt de cette "mafia informatique" est d'espionner votre ordinateur pour récupérer vos mots de passe, numéros PIN et TAN (eBanking, 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 (relais) pour envoyer du "spam"[7], du courrier non sollicité !
En plus votre disque dur sera employé comme relais pour faire des attaques du type DDOS[8]. Votre ordinateur 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

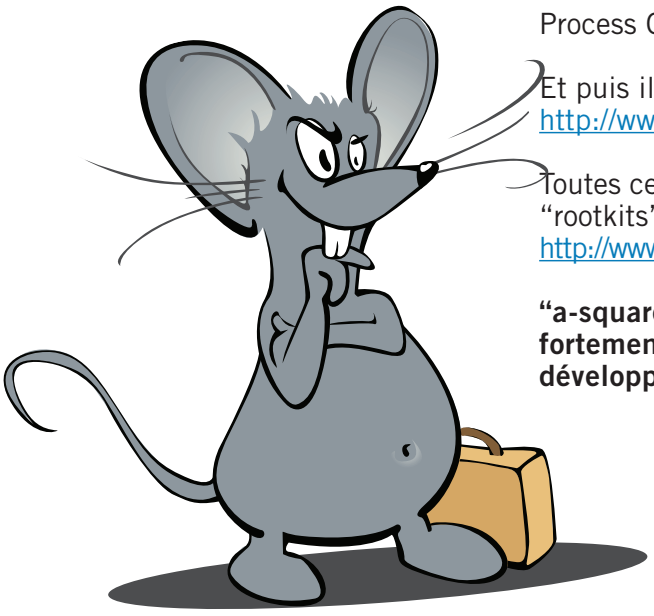
Le pire, vous ne vous apercevrez pas de l'utilisation clandestine de votre disque dur !

Mais passons 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 existe quelques-uns :

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 : www.diamondcs.com.au/processguard



Et puis il existe encore "a-squared" (a^2) de chez Emsisoft.
http://www.emsisoft.net/fr/

Toutes ces 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" (a^2) est un programme qu'on vous recommande fortement. C'est un programme antimalware qui est en constant développement.

CONCLUSION :

Attention aux “rootkits” ! C’est une nouvelle menace qui est très dangereuse et qui est encore en développement. Cette menace deviendra un nouveau fléau à ne pas sous-estimer.
Son potentiel est énorme, de telle façon que même des experts en informatique ont des problèmes à les détecter (les éradiquer est impossible de toute façon, pour l’instant [14.06.2005] !) !

RÉSUMÉ :

Les “rootkits” sont des “Super Troyens”, on 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 l’ordinateur et qui aurait détecté cette application, aucune chance. Les “rootkits” filtrent cette requête et renvoient un statut normal à l’antivirus. Ils deviennent ainsi invisibles !

Même en examinant l’ordinateur 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 ordinateur sont :

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

“Bonjour les dégâts”

Norton Internet Security™ contient un “antivirus”, un “firewall”, un “antispam” 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

[1] root : racine

[2] kit : assemblage de pièces diverses

[3] kernel : noyau, le coeur du processeur

[4] troyen : programme (script) qui 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 de l’ordinateur pour permettre au Keylogger et Troyen d’expédier leurs messages.

[7] SPAM : Courrier non sollicité

[8] Attaques DDOS : Distributed Denial Of Service / 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

Installez toujours un :
antivirus (p.ex. : Norton Internet Security™)
firewall / pare feu (p.ex.: ZONEALARM®)
antimalware (p.ex.: a-squared)
Rootkit Revealer.
Faire régulièrement les updates de chez Microsoft® !