13. Nouvelles menaces, les “rootkits”

Le monde virtuel (Internet) n’arrête pas de nous étonner, pour le meilleur et pour le pire. Surtout les malware (virus, ver, troyen, etc.) poussent comme des champignons. La créativité des programmeurs de ces codes malicieux semble illimitée.
Une nouvelle sorte de ces malware est apparue : les “rootkits” !

C’EST QUOI LES “ROOTKITS“ ?

Les “rootkits” sont bien connus depuis des années dans le monde de “Unix®” et de “Linux®” et font leur apparition officielle dans le monde de “Windows®” depuis mi-février 2005, selon un communiqué officiel de Microsoft® et de la “RSA Security”.

Ils s’intègrent en principe directement dans le cœur de Windows®, dans le “kernel” [1] et ils se font passer comme étant des processus et services de Windows®. Même les scanneurs de malware (antivirus, antitroyen, etc.), ainsi que les “firewall” [2] (pare-feu) n’arrivent pas à détecter ces bestioles informatiques, dû au fait qu’ils ont développé une certaine intelligence.

Ils sont capables de se faire passer pour un service légitime de Windows® et de cette façon ils échappent au scan des anti-virus et des firewall !

Ils s’activent automatiquement dès démarrage de votre ordinateur.

Leur rôle principal consiste à ne pas se faire révéler !

Ils se camouflent comme “drivers”, processus et services légitimes de Windows®, se cachent dans des endroits de la base des registres sans se faire remarquer ! Même étant détectés et éradiqués, ils ressuscitent et se reproduisent à nouveau !

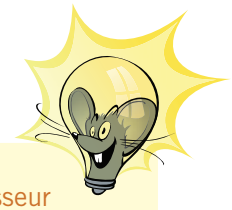
QUEL EST LE BUT DE CES “ROOTKITS” ?

Leur but est bien de nature lucrative ! Cette nouvelle sorte de malware ne veut rien d’autre que les autres malware aussi, profiter de la naïveté (non connaissance des risques de sécurité) des internautes !

En principe les “rootkits” peuvent être classés dans la catégorie “blended threats” [3], une combinaison de “troyens” plus “backdoor” [4] et “keylogger” [5].

Seule différence avec les autres malware, ils ont été programmés soigneusement pour ne pas être détectés !

Ceci nous montre bel et bien, qu’il y a des professionnels cachés derrière cette nouvelle menace, la mafia informatique, des groupes de criminels bien organisés !



[1] Coeur du processeur
[2] Portier qui contrôle le trafic informatique entrant et sortant
[3] Un mixage de troyens, backdoor, keylogger, etc.
[4] Logiciel ouvrant des ports de communication
[5] Logiciel enregistrant les frappes de clavier
[6] A squared est un anti-troyen, anti-dialer et anti-malware http://www.emsisoft.net
[7] I.D.S. = Intrusion Detection System

La priorité des programmeurs des "rootkits" est de ne pas se faire repérer, une sorte de code éthique !

Ces programmes (logiciels et scripts) peuvent "dormir" et attendre jusqu'à ce qu'ils soient "réveillés" par leur programmeur pour envoyer toutes vos données secrètes à leur (s) programmeur (s) !

De cette façon, ces malfaiteurs auront accès à vos comptes bancaires et à toutes vos transactions faites par Internet !

COMMENT NOUS PROTÉGER ET AVEC QUOI ?

La seule chose que nous pouvons faire est de nous munir d'un anti-virus, d'un firewall et d'être à jour avec les updates (patches / mises à jour) de notre système d'exploitation (Windows®, Mac® OS, Linux®) !

Un logiciel (programme) anti-troyen comme "a²" de chez "Emsisoft" http://www.emsisoft.net est fortement à recommander !

Ce logiciel en version payante de 39,95 € est pourvu d'un "IDS". Un "IDS" surveille tous les processus dans le système d'exploitation. Le gardien d'arrière-plan de a-squared empêche et bloque les fichiers dangereux d'arriver sur votre ordinateur bien avant qu'ils ne deviennent actifs. Pour cela, il utilise une nouvelle technique et unique dans le monde entier qui s'appelle "analyse du comportement des programmes" (IDS) qui vous donne immédiatement une alarme, aussitôt qu'un programme démarré fait quelque chose de dangereux.

Selon le magazine informatique professionnel allemand "COM!", édition 06 / 2005, page 8, http://www.com-magazin.de, il existe des logiciels (programmes) qui détectent ces "rootkits". Il s'agit de deux logiciels":

1. Strider Ghostbuster de Microsoft®

http://research.microsoft.com/rootkit/

2. Rootkit-revealer de Sysinternals™

http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml

Malheureusement ces deux logiciels arrivent à détecter ces "rootkits", mais sont incapables de les éradiquer !

COMPORTEMENT DE L'ANALYSE

Contrairement aux heuristiques traditionnelles, qui recherchent des fichiers contenant des routines nuisibles sur le disque dur et qui fournissent une analyse approximative, si un fichier est dangereux ou non, a² lui surveille directement le comportement des programmes actifs dans le système.

Que détecte-t-il?

a-squared est actuellement entraîné pour trouver les types de malwares suivants:

- Vers, Emails
- Backdoors (Porte dérobée)
- Backdoors avec Reversed Connection Logic (LAN Bypass)
- Spywares / Adwares
- HiJackers
- Dialers
- Rootkits

Fonctionnement de l' "IDS" à l'adresse suivante :
http://www.emsisoft.net/fr/software/ids/

Pour l'instant (04.05.2005) il n'existe pas de programmes (logiciels) qui puissent être capables de détecter et d'éradiquer ces bestioles informatiques.

Si jamais vous avez attrapé un de ces "rootkits" il ne vous reste rien d'autre à faire que de réinstaller votre système d'exploitation !

MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA FORMATION PROFESSIONNELLE
Centre de technologie de l'éducation