Les rootkits sur Windows : le fonctionnement, détection et suppression

Cet article traite des logiciels malveillants de type rootkit. En effet, beaucoup de mythes et d'idées reçues sur ce type de malwares certainement dû au fait qu'ils sont capables de se cacher au sein du système d'exploitation.
Souvent sur les forums, on peut voir des personnes qui parlent de piratage de leurs connexions Wifi par le voisin pour implanter un rootkit.

Vous trouverez des explications générales sur le fonctionnement des rootkits mais aussi un historique de ces menaces informatiques.

Qu’est-ce qu’un rootkit et le fonctionnement

Les rootkits sont des menaces informatiques particulières.

Initialement, les rootkits sont des malwares qui ont la capacité de se rendre invisible.
C’est à dire qu’en utilisant les applications classiques pour lister les fichiers ou processus comme le gestionnaire de tâches de Windows, vous ne verrez pas ce dernier.
En fait, c’est un peu plus complexe que cela pour bien comprendre les possibilités qu’offre un rootkit sur Windows, il faut comprendre le fonctionnement général.

Les rootkits sont donc les logiciels malveillants les plus sophistiqués.
Il faut voir le rootkit comme une fonctionnalité et pas la fonction du logiciel malveillant. Un rootkit peut-être un au final, Adware, un Trojan.Clicker ou encore un spambot.
En général, il permet aussi le contrôle de l’ordinateur infecté.

Pour plus d’informations sur le type de menaces informatiques, voici une liste des type de logiciels malveillants sur la page : Liste des menaces informatiques : Virus, Trojan, Backdoor, Adware, Spywares, etc

Le fonctionnement des rootkits

Un rootkit est en réalité un logiciel malveillant qui est capable de détourner les appels systèmes (API).
Tous les applications et processus de Windows utilisent les API et appels systèmes pour faciliter la programmation des applications.
En effet, lorsqu’un programme a besoin d’effectuer une action système comme lister les processus, accéder à des fichiers,

utiliser le réseau… Ils utilisent des fonctions de Windows toutes faites et disponibles.
Cela évite aux concepteurs de logiciels de devoir réécrire toutes ces routines générales et ainsi gagner du temps.

Le rootkit tire partie de ces mécanismes pour détourner ces appels systèmes vers lui même et fausser les résultats.

Ainsi, lorsque le gestionnaire de tâches demande à Windows de lister les processus, cette demande passe par le rootkit qui va alors retourner une liste en retirant son processus.
De ce fait, pour pouvoir détecter un rootkit, il faut utiliser des applications spéciales comme les scanner rootkit qui n'utilisent pas directement les appels systèmes ou de manière différentes.
On parle alors de crochet ou hook en anglais pour désigner ces aptitudes de détournement.

La page suivante, un peu ancienne, explique le fonctionnement technique générale : Le danger et fonctionnement des rootkits

Les rootkits ne sont pas qu'invisible

La définition donnée au départ n'est pas tout à fait exacte et on désigne plutôt en rootkit, les logiciels malveillants capables de détourner les appels systèmes.
Si certains rootkits ont utilisé ce fonctionnement pour se rendre invisible, d'autres ont détournés les appels systèmes liés aux systèmes de fichiers pour rendre leur suppression plus difficile voire impossible.
En clair, lorsque vous tentez avec l'explorateur de fichiers ou une application de supprimer le fichier de rootkit, l'action était refusée.
Ce dernier écoutait tous les appels systèmes de suppression de fichiers et si le fichier du rootkit en était la cible, la tentative de suppression se voyait refusée.

Parfois, c'était tellement compliqué, qu'il fallait passer par un Live CD pour supprimer le rootkit.

La vidéo suivante montre comment un rootkit parvient à cacher le fichier dans le dossier démarrage :

Les types de rootkit

Sur Windows, il existe plusieurs types de rootkits, voici quelques exemples :

- **rootkit userland** : ce dernier fonctionne au niveau de l'utilisateur et se lance au démarrage de Windows de manière classique pour un logiciel malveillant. Par exemple par une clé Run ou un raccourci dans les startup. Le rootkit détourne les appels systèmes lors du lancement d'une application de l'utilisateur. La limite étant que les applications qui tournent au niveau du kernel ne sont pas affectés par ce dernier.
- **rootkit kernel-mode ou Ring-0** : il fonctionne dans un niveau plus bas que les rootkit userland. Pour fonctionner, il faut un pilote (fichier .sys) et un service Windows pour lancer ce dernier. Ce sont les rootkits les plus coriaces et difficile à détecter et supprimer.

- **Les bootkits** : Enfin les bootkits sont des rootkits qui modifient le démarrage de Windows (dans le MBR) d'où le nom boot et rootkit. Le but est se charger avant le système d'exploitation et ainsi prendre la main très tôt. Cela leur confère un avantage, car ils sont actifs avant l'antivirus.

Les rootkits kernel-mode sont les plus complexes à développer et peuvent dans certains cas générer des écrans bleus BSOD.

Quelques rootkits sur Windows

Voici la genèse des rootkits sur Windows ce qui va permettre de voir les évolutions techniques.
Il y a bien entendu eu beaucoup de rootkits donc nous évoquerons les plus importants.
Une partie de ces rootkits sont évoqués sur la page des botnets étant donnés qu'ils ont permis de constituer des botnet de plusieurs milliers ou millions de machines : Les botnets : réseau de machines infectées

Mais certains Trojan Banker ont utilisé des fonctions de rootkit, comme SpyEye – Trojan.Pincav ou Trojan.Carberp : Stealer et rootkit.
Une liste en vrac de quelques rootkits :

- Alureon (Trojan.Clicker)
- Cutwail (SpamBot)
- Detrahere aka Zacinlo – lié à des PUPs et adwares.
- Rustock (SpamBot)
- Sinowal (Trojan Banker) – Le premier Bootkit que j'ai croisé =)
- Sirefef
- Necurs qui sert depuis 2015 à des campagnes de mails malveillants

~ 2005 – MagicControl

Magic.Control était un adware qui sévissait en France autour de 2005.
Le but était de charger des popups de publicités.
Il s'agit d'un rootkit userland qui se composait de fichiers .exe et .dat dans le dossier %APPDATA%

A l'époque l'utilitaire HijackThis et le gestionnaire de tâches n'étaient pas capables de lister les processus de ce rootkit.
Les antivirus ne détectaient pas non plus le malware et on pouvait utiliser le scanner anti-rootkit de F-Secure pour voir les fichiers.
Par la suite, l'utilitaire navilog1 fut développé pour détecter et supprimer cette infection de manière plus automatisée.

Quelques cas sur le forum mais il y a en plein d'autres.

- Magic.Control : Rootkit
- malware Magic control agent pub intempestive
- Magic.Control : epaas-key et fenêtre intempestives porno

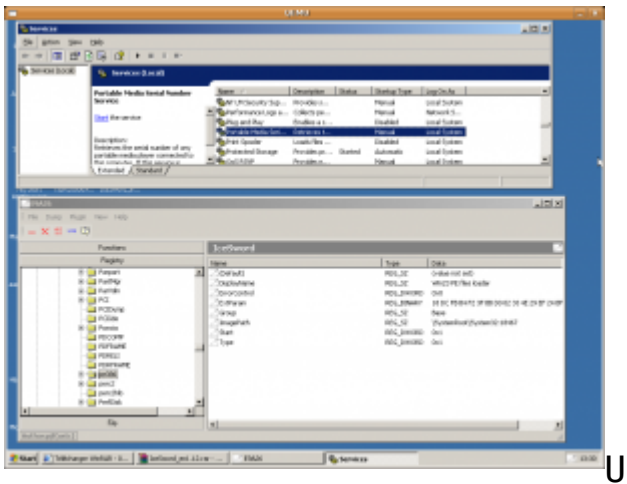
Le dernier sujet est assez intéressant, car un rapport HijackThis est présent avec le scanner anti-rootkit de F-Secure.
On voit clairement qu'HijackThis ne montre pas le processus de Magic.Control détecté par F-Secure.

La page suivante donne toutes les détails de la diffusion à la suppression : Supprimer Magic.Control / egdaccess / Adaware.NaviPromo

2006 : Rustock / PE386

Le nom de P386 provient du nom du premier service Windows utilisait par ce rootkit kernel-mode : pe386.sys.

Par la suite des ADS ont été utilisés comme pilote.
Rustock est un malware de type Spammer (spambot) qui a pu infecter des milliers de machines pour s'en émetteur de SPAM.
Une page sur le forum est consacré à ce dernier : Rootkit Pe386 / Rustock



Une opération de démantèlement de ce botnet en mars 2011 où celui a cela, le volume de spam a chuté de 800 000 mails par jour.

2007 : Storm aka Peacomm / Nuwar / Zhelatin/Storm worm

Storm est un malware qui a sévit pendant plusieurs années et qui n'a pas toujours été sous la forme d'un rootkit.
C'est surtout à ses débuts que des méthodes de rootkit ont été utilisées.
Le nom du malware vient du fait que la première campagne de mail malveillant pour se diffuser à tirer partie de la tempête de Janvier 2017.

La page de la propagation de Storm du forum : Zhelatin/Storm/Waledac Worm
Quelques informations techniques : Win32.Packed.Tibs / Win32.Email-Worm.Zhelatin

Notamment cette partie nous apprends qu'il s'agit d'un rootkit kernel-mode puisqu'un driver et son service Windows étaient présents :

C:\WINDOWS\system32\windev-xxxy-xxy.sys - où x sont des chiffres et y des lettres.
ex :
C:\WINDOWS\system32\windev-peers.ini
C:\WINDOWS\system32\windev-784b-489a.sys
C:\WINDOWS\system32\windev-peers.ini
Nom : Win32.Packed.Tibs.R / Win32.Email-Worm.Zhelatin.CX

Par la suite d'autres variantes de Storm on vu le jour qui n'ont pas utilisés de fonctionnalités de rootkit.

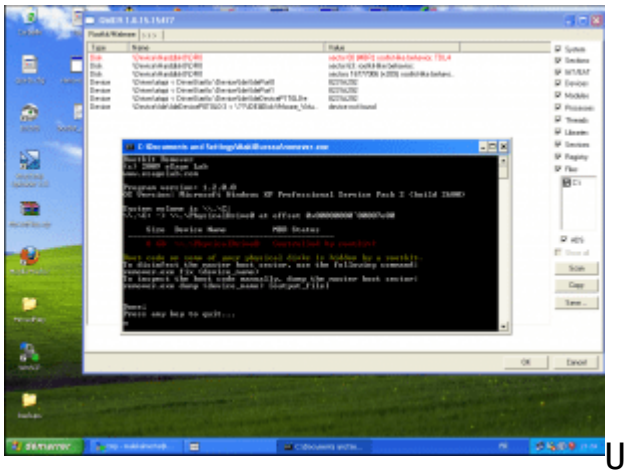
2008/2009 : Trojan.Win32.Alureon/Trojan.TDSS

Par la suite, un autre rootkit a aussi tapé très fort : Trojan.TDSS ou Trojan.Win32.Alureon.
Il s'agit d'un malware qui existait avant mais qui à partir de ces dates à commencer à utiliser des fonctions de rootkit.

Le nom TDSS provient du fait que la première version utilisait un driver : *C:WINDOWS\System32\\drivers\tdssserv.sys*
Il s'agit d'un Trojan.Clicker, c'est à dire qu'il utilisait l'ordinateur pour charger des pubs et simuler des clics.
Cela permettait aux auteurs de gagner de l'argent à travers ces pubs (Click Fraud).
Des redirections lors des recherches Google avaient aussi lieux vers des publicités, de fausses pages d'alertes de virus faisant la promotion de rogues.

Par la suite, les pilotes on pris des noms aléatoires.
En effet plusieurs versions ce sont succédées TDSS-3, TDSS-4.
Ci-dessous une vidéo avec l'utilitaire TDSSKiller qui détecte TDSS.

La version 4 est un bootkit, la page suivante présente ce dernier : Rootkit.TDSS TDL 4 (Trojan.Alureon)

 Une opération en 2011 a permis l'arrestation de certains acteurs de ce malware pour affaiblir ce dernier jusqu'à sa disparition.

2011 : ZeroAccess

Ce dernier a pris la relève de TDSS et comme son prédécesseur un Trojan.Clicker.
Le nom provient du fait que ZeroAccess empêché totalement l'accès aux fichiers qui le compose.
Sa désinfection était donc relativement difficile.
La page suivante donne un aperçu de ce malware : [ZeroAccess / Sirefef.B / Rootkit.Win32.ZAccess / MAX++]
Initialement, des drivers ont été utilisés puis par la suite des fichiers.

Une opération de démantèlement partielle du botnet ZeroAccess a eu lieu fin 2013 mais tous les serveurs utilisés n'ont pas été saisies.
Le botnet a donc pu survivre.

Après 2011

Par la suite, les rootkits ont été moins utilisés du fait des contre mesures qui ont été ajoutés par les antivirus et Windows.
Des PUPs et adwares ont toutefois pu utiliser des fonctions de rootkit.
Notamment :

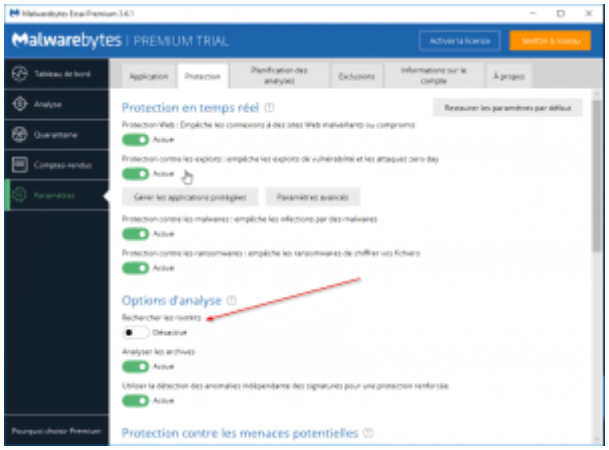
- Pilotes « bsdriver.sys » & « cherimoya.sys » : abengine
- NetUtils

La détection et suppression des rootkits

Initialement, il fallait utiliser des outils annexes pour pouvoir détecter ce type de menaces.
Par exemple, Kaspersky a developpé un outil gratuit du nom de TDSSKiller capable de détecter les rootkits et les bootkits.
Par la suite, la plupart des antivirus intègre un scan anti-rootkit.

Gmer était aussi un utilitaire gratuit très populaire mais son développement a cessé.
Une partie de l'application a été intégrée dans Avast!.

Très souvent les fonctions de recherche de rootkit ne sont pas activées par défaut.
Par exemple, chez MBAM, il faut aller dans les options pour activer la recherche de rootkit.
Cela s'explique par le fait que ces fonctions sont très instables et provoquent très souvent des BSOD.



Windows 10 et les rootkits

Les protections contre les rootkits ont été ajoutées dans les différentes versions de Windows.
Mais c'est surtout Windows 10 qui possède les plus de protections.
Premièrement, il faut savoir que les ordinateurs ont évolués et depuis quelques années les BIOS UEFI ont vu le jour.
Cela a deux conséquences :

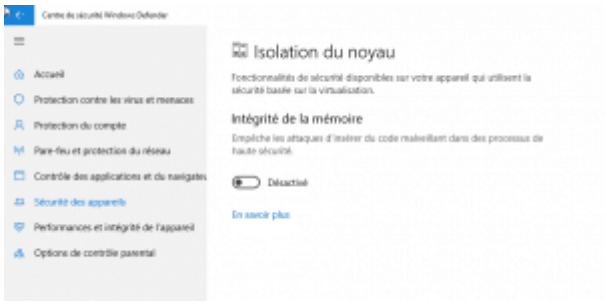
- L'ajout du Secure Boot qui vérifie et interdit de démarrer l'ordinateur, si le code du démarrage n'est pas signé.
- Les disques sont passés en GPT et le démarrage MBR a disparu.

Ainsi, cela a provoqué la mort des bootkits MBR car modifier le démarrage pour ajouter du code malveillant avec le Secure Boot est plus compliqué.
De plus, il aurait fallu recoder au complet les bootkits pour fonctionner sur les systèmes UEFI.
Toutefois, le premier rootkit UEFI utilisait dans des campagnes de compromissions a été découvert par ESET fin septembre 2018. Plus d'informations : Lojax : le premier rootkit UEFI

Du côté de Windows 10, beaucoup d'élément ont été ajoutés avec :

- L'interdiction ou plus de difficultés pour installer et charger des pilotes non signés. Cette mesure est apparue avec Windows 8.1. En clair donc installer un rootkit kernel-mode est devenu plus complexe.
- Patchguard protège le noyau de Windows et rend les hook plus difficiles. Plus d'informations sur la page : Rootkit et PatchGuard sur Windows 64 Bits
- Des fonctions d'isolation du noyau de Windows qui rend

les hook plus difficiles à réaliser.



Ainsi, il y a eu une grosse chute de l'utilisation des rootkits pour revenir à des menaces plus classiques.
Bien entendu, cela ne veut pas dire qu'ils feront leurs retours mais cela risque d'être un peu plus complexe.

Plus d'informations sur les protections ajoutées dans Windows 10, suivre notre article : Windows 10 et la protection contre les virus et attaques

Autres liens

Quelques autres liens autour des rootkits :

- Le danger et fonctionnement des rootkits
- Supprimer les rootkits sur Windows