Les malwares - Généralités

- Objet : Les malwares - généralités
- Suivi :
  à-compléter
  - Création par milou le 14/10/2015
  - Tatouillé par paskal le 18/10/2015
- Commentaires sur le forum : c'est ici [1)]

- Voir aussi les logiciels malveillants (malwares) sous Linux

Introduction

Un logiciel malveillant ou maliciel (en anglais malware) est un programme développé dans le but de nuire à un système informatique sans le consentement de l'utilisateur dont l'ordinateur est infecté, et dont certains ont la propriété de se propager d'une machine à une autre.

De nos jours, le terme « virus » est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les maliciels englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.

Les différents logiciels malveillants

(Source : logiciel malveillant, sur Wikipedia)

Les virus

Les virus sont capables de se répliquer, puis de se propager à d'autres ordinateurs en s'insérant dans des programmes ou des documents légitimes appelés «hôtes».

Ils se répartissent ainsi :

- les virus de secteur d'amorçage (virus de boot) ;
- les virus de fichier qui exploitent le système de fichiers d'un système d'exploitation particulier (ou de plusieurs) afin de se propager ;
- les virus de macro (ou macrovirus) qui utilisent le langage de programmation d'un logiciel pour en altérer le fonctionnement ; ils s'attaquent principalement aux fichiers des utilisateurs ;
- les virus de script : ils forment un sous-groupe des virus de fichier ; ils sont programmés dans une grande variété de langages (VBS, JavaScript, BAT, PHP, etc.).
  Soit ils infectent d'autres scripts (ex. : les fichiers de commande et de service Windows ou Linux), soit ils font partie d'un virus à plusieurs composants.
  Les virus de script peuvent infecter d'autres formats tels que HTML si ce format permet l'exécution de scripts.

Certains intègrent des rootkits (outil de dissimulation d'activité). Pour l' attaquant, l'utilité d'un rootkit

est soit de mettre à disposition des ressources système (temps processeur, connexions réseaux, etc.) sur une, voire plusieurs machines, parfois en utilisant la cible comme intermédiaire pour une autre attaque, soit d'espionner, d'accéder aux données stockées ou en transit sur la machine cible.

Les virus peuvent s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées.

Les vers

Les vers (worm) sont capables d'envoyer une copie d'eux-mêmes à d'autres machines. Contrairement à un virus informatique, un ver n'a pas besoin d'un programme hôte pour se reproduire. Il exploite les différentes ressources de l'ordinateur qui l'héberge pour assurer sa reproduction.

Son objectif :

- espionner l'ordinateur où il se trouve ;
- offrir une porte dérobée à des pirates informatiques ;
- détruire des données sur l'ordinateur où il se trouve ou y faire d'autres dégâts ;
- envoyer de multiples requêtes vers un serveur Internet dans le but de le saturer (déni de service).

Ils peuvent être classés selon leur technique de propagation :

- les vers de courrier électronique ;
- les vers Internet ;
- les vers IRC ;
- les vers de réseau ;
- les vers de partage de fichiers.

Les chevaux de Troie

Les chevaux de Troie (Trojanhorse) sont divisés en plusieurs sous-catégories ; ils comprennent notamment :

- les portes dérobées : dans un logiciel, une porte dérobée (de l'anglais backdoor, littéralement “porte de derrière”) est une fonctionnalité inconnue de l'utilisateur légitime, qui donne un accès secret au logiciel ;
- les droppers : fichiers exécutables qui contiennent d’autres virus afin de les installer sur les ordinateurs ;
- les notificateurs : ces chevaux de Troie envoient au «maître» des renseignements relatifs à la machine infectée ; ils confirment la réussite de l'infection et envoient des informations relatives à l'adresse IP, aux numéros de ports ouverts, aux adresses de courrier électronique, etc. de l'ordinateur attaqué. Ces informations sont envoyées via courrier électronique au site du maître ou via ICQ ;
- les logiciels espions (dont les keyloggers) : programmes qui recueillent et enregistrent une liste de toutes les touches entrées au clavier par l’utilisateur. Le programme peut ensuite rendre cette liste publique et permettre à des tierces personnes d’accéder à ces données (c'est à dire aux informations entrées par l’utilisateur via son clavier : mots de passe, documents textes, emails, combinaisons de touches, etc.).

Ils ont chacun des objectifs spécifiques.
Certains chevaux de Troie utilisent également des rootkits pour dissimuler leur activité.

Autres menaces

D'autres menaces existent, elles ne sont pas dangereuses en elles-mêmes pour la machine mais servent à installer des infections ou à réaliser des attaques DNS.

Il s'agit :

- des outils de déni de service :
    - DDoS : attaque par déni de service (DoS) dans laquelle plusieurs ordinateurs sont impliqués et attaquent en même temps le même serveur. Les ordinateurs compromis (infectés) peuvent être vulnérables et utilisés par des pirates pour mener ce genre d’action malveillante,
    - DoS : type d’attaque causée parfois par des virus, qui empêche les utilisateurs d’accéder à certains services (du système d’exploitation, de serveurs web, etc.) ;
- des exploits : programmes malveillants qui profitent d’une vulnérabilité ou faille de sécurité existante dans un protocole de communication, un système d’exploitation, une application ou un utilitaire donné de l’ordinateur ;
- des inondeurs : ces malwares ont pour objectif de rendre inaccessible un service web délivré par un site, en démultipliant le nombre de connexions à ce site, à l'aide de “machines-zombies” (ou soldats). On parle alors de DDoS (distributed denial of service attack) ;
- des nukers, programmes qui lancent une attaque “nuke” : attaque conçue pour empêcher les connexions réseau d'aboutir, entraînant le blocage d'un ordinateur ou de sa connexion réseau ;
- du pharming : technique de piratage informatique exploitant des vulnérabilités DNS. Cette technique ouvre de manière que, pour une requête DNS pour un nom de domaine, ce ne soit pas l'IP réelle du nom de domaine qui soit donnée mais celle d'un site frauduleux.
- des publiciels (adwares) et des rogues (rançongiciels ou riskwares) ; ils ne sont pas non plus directement dommageables pour la machine. Il s'agit de programmes utilisant des techniques de mise en marche (ouverture de fenêtres intempestives, enregistrement automatique dans la barre URL, modification des liens référencés) bien souvent contraires à l'éthique.
  Les adwares font la promotion des rogues via des popups de publicité.
  Les rogues sont de faux anti-spywares ou antivirus ; dès que vous êtes infecté, ils se mettent en route automatiquement et vous détectent des menaces imaginaires. Seulement, pour “nettoyer” ces infections imaginaires, la version commerciale doit être achetée ;
- des programmes qui servent à créer des logiciels malveillants, en particulier les virtools, les générateurs polymorphes, ou les crypteurs de fichiers.

Certains éléments, qui ne sont pas à l'origine conçus pour être malveillants, sont parfois utilisés à des fins illégales et/ou compromettantes.
Il s'agit notamment des composeurs (en anglais, “dialers” : c'est un terme générique qui désigne un logiciel permettant de raccorder un ordinateur à un autre ordinateur, à un appareil électronique, au réseau Internet ou à un autre réseau numérique), téléchargeurs, serveurs FTP, mandataires (proxy),Telnet et Web, clients IRC, canulars, utilitaires de récupération de mots de passe, outils d'administration à distance, décortiqueurs et moniteurs.

[1)]
N'hésitez pas à y faire part de vos remarques, succès, améliorations ou échecs !

From:
http://debian-facile.org/ - **Documentation - Wiki**

Permanent link:
http://debian-facile.org/doc:systeme:securite:les-malwares

Last update: **21/10/2015 21:51**