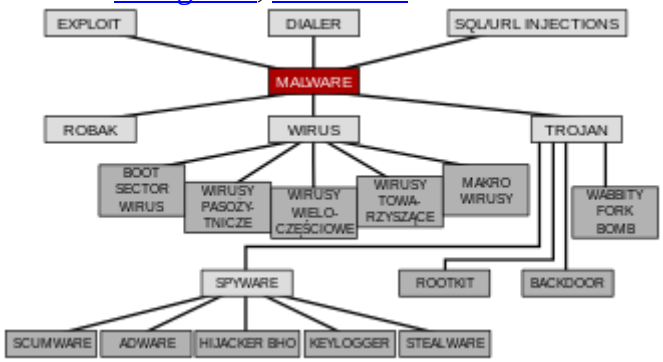
Logiciel malveillant

Un article de Wikipédia, l'encyclopédie libre.
Aller à : Navigation, rechercher



Différents types de logiciels malveillants

Un **logiciel malveillant** (en anglais, ***malware***) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur infecté. De nos jours, le terme *virus* est souvent employé, à tort, pour désigner toutes sortes de logiciels malveillants. En effet, les malwares englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces. La catégorie des virus informatiques, qui a longtemps été la plus répandue, a cédé sa place aux chevaux de Troie en 2005.

Le terme *Logiciel malveillant*, dont l'usage est préconisé par la commission générale de terminologie et de néologie en France, est une traduction du mot anglais *malware*, qui est une contraction de *malicious* (qui signifie *malveillant*, et non *malicieux*) et *software* (*logiciel*). Dans les pays francophones, l'utilisation de l'anglicisme *malware* est le plus répandu ; le mot **maliciel** est bien souvent utilisé au Québec[1], mais il n'est pas reconnu par le GDT[2].

Classification[modifier | modifier le code]

Les logiciels malveillants peuvent être classés en fonction des trois mécanismes suivants :

- le **mécanisme de propagation** (par exemple, un *ver* se propage sur un réseau informatique en exploitant une faille applicative ou humaine) ;
- le **mécanisme de déclenchement** (par exemple, la *bombe logique* — comme la bombe logique surnommée *vendredi 13* — se déclenche lorsqu'un évènement survient) ;
- la **charge utile** (par exemple, le *virus* Tchernobyl tente de supprimer des parties importantes du BIOS, ce qui bloque le démarrage de l'ordinateur infecté).

La classification n'est pas parfaite, et la différence entre les classes n'est pas toujours évidente. Cependant, c'est aujourd'hui la classification standard la plus couramment adoptée dans les milieux internationaux de la sécurité informatique.

Dans une publication[3], J. Rutkowska propose une taxonomie qui distingue les malwares suivant leur mode de corruption du noyau du système d'exploitation : ne touche pas au noyau (*ie*, applications, micrologiciel), corruption d'éléments fixes (code), corruption d'éléments dynamiques (données) et au-dessus du noyau (hyperviseurs).

Les virus[modifier | modifier le code]

Les **virus** sont capables de se répliquer, puis de se propager à d'autres ordinateurs en s'insérant dans d'autres programmes ou des documents légitimes appelés « hôtes ». Ils se répartissent ainsi : virus de secteur d'amorçage ; de fichier ; de macro ; et de script. Certains intègrent des rootkits. Les virus peuvent s'avérer particulièrement dangereux et endommager plus ou moins gravement les machines infectées.

Les vers[modifier | modifier le code]

Les **vers** (*worm*) sont capables d'envoyer une copie d'eux-mêmes à d'autres machines. Ils peuvent être classés selon leur technique de propagation : les vers de courrier électronique ; Internet ; IRC ; les vers de réseau ; et ceux de partage de fichiers. Certains, comme le ver *I Love You*, ont connu une expansion fulgurante.

Les chevaux de Troie[modifier | modifier le code]

Les **chevaux de Troie** (*Trojan horse*) sont divisés en plusieurs sous-catégories, et comprennent notamment les portes dérobées, les droppers, les notificateurs, les logiciels espions (dont les keyloggers) etc. Ils ont chacun des objectifs spécifiques. Certains chevaux de Troie utilisent également des rootkits pour dissimuler leur activité.

Autres menaces[modifier | modifier le code]

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 (DoS et DDoS), des exploits, inondeurs, *nukers*, du *pharming*, et des programmes qui servent à créer des logiciels malveillants, en particulier les *virtools*, les générateurs polymorphes, ou les crypteurs de fichiers. Les publiciels (*adware*) et les rogues (rançongiciels ou riskwares) ne sont pas non plus directement dommageables pour la machine. Il s'agit de programmes utilisant des techniques de mise en marché (ouverture de fenêtres intempestives, enregistrement automatique dans la barre URL, modification des liens référencés) bien souvent contraires à l'éthique.

Certains éléments, qui ne sont pas à l'origine conçus pour être malveillants, sont parfois utilisées à des fins illégales et/ ou compromettantes. Il s'agit notamment des composeurs, téléchargeurs, enregistreurs de frappes, 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.

Logiciels malveillants et menaces		
Virus	de boot · de fichier · macrovirus · de script	
Vers	de réseau · de courrier électronique · Internet · IRC	
Chevaux de Troie	porte dérobée · dropper · notificateur · logiciel espion	
Autres menaces	exploit · Rançongiciel · publiciel · rogue · composeur · enregistreur de frappe · rootkit · canular · pharming	

Sommaire

[masquer]