LES LOGICIELS MALVEILLANTS

Les virus

Au sens strict, un virus informatique est un programme informatique écrit dans le but de se propager à d'autres ordinateurs en s'insérant dans des programmes légitimes appelés « hôtes ». Il peut aussi avoir comme effet, recherché ou non, de nuire en perturbant plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme l'Internet, mais aussi les disquettes, les cédéroms, les clefs USB, etc. Les virus informatiques ne doivent pas être confondus avec les vers qui sont des programmes capables de se propager et de se dupliquer par leurs propres moyens sans contaminer de programme hôte.

Les vers (*worm*)

Ils se répandent dans le courrier électronique en profitant des failles des différents logiciels de messagerie (notamment Microsoft Outlook). Dès qu'ils ont infecté un ordinateur, ils s'envoient eux-mêmes à des adresses contenues dans tout le carnet d'adresses, ce qui fait que l'on reçoit ce virus de personnes connues. Certains d'entre eux ont connu une expansion fulgurante (comme le ver I Love You). Les experts n'arrivent pas à se mettre d'accord sur l'appartenance ou non des vers à la classe des virus informatiques.

Les wabbits

C'est un autre type de logiciels malveillants se reproduisant très rapidement. Contrairement aux virus, ils n'infectent pas les programmes ni les documents. Contrairement aux vers, ils ne se propagent pas par les réseaux. Ils interviennent dans le code source de Windows Explorer, en particulier la saisie semi automatique, en incorporant des termes censés amener l'internaute sur des sites payants. C'est le nom générique regroupant plusieurs hijackers (voir (en) hijacking) : piratage de la page de démarrage Internet, pour une redirection vers un site choisi. Un hijacker modifie les réglages du navigateur en utilisant une page Web contenant un contrôle ActiveX ou du JavaScript.

Les chevaux de Troie (*Trojan horses*)

Ce nom vient de la célèbre ruse imaginée par Ulysse. Ces programmes prétendent être légitimes (souvent de petits jeux ou utilitaires), mais comportent des routines nuisibles exécutées sans l'autorisation de l'utilisateur. On confond souvent les chevaux de Troie avec les backdoors. Ces derniers sont en effet **une** catégorie de chevaux de Troie, mais pas la seule. Les backdoors prennent le contrôle de l'ordinateur et permettent à quelqu'un de l'extérieur de le contrôler par le biais d'Internet. Les chevaux de Troie ne sont pas des virus car ils leur manquent la fonction de reproduction, essentielle pour qu'un programme puisse être considéré comme un virus.

Les portes dérobées (*backdoor*)

Une porte dérobée peut être introduite soit par le développeur du logiciel, soit par un tiers, typiquement un pirate informatique. La personne connaissant la porte dérobée peut l'utiliser pour surveiller les activités du logiciel, voire en prendre le contrôle (par contournement de l'authentification).
Parmi les motivations amenant les développeurs de logiciel à créer des portes dérobées, il y a :
- L'intérêt pratique d'un accès facile et toujours ouvert au logiciel pour pouvoir mener efficacement les actions de maintenance.

- La possibilité de désactiver subrepticement le logiciel en cas de désaccord avec son client (non-paiement de licence).

Parmi les motivations amenant les pirates informatiques à installer une porte dérobée :
- La possibilité de surveiller ce que fait l'utilisateur légitime et de copier ou détruire des données ayant une valeur (mots de passe, clé privée pour déchiffrer des messages privés, coordonnées bancaires, secrets commerciaux).
- La possibilité de prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malfaisantes (envoi de pourriels notamment pour l'hameçonnage, de virus informatiques, déni de service).
- Le contrôle d'un vaste réseau d'ordinateurs (voir botnet), qui peut être utilisé pour du chantage au déni de service distribué (DDoS), ou revendu à des criminels.

Les logiciels espion (*spyware*)

Ils peuvent accompagner certains graticiels (mais pas les logiciels libres), partagiciels et pilotes de périphériques, s'installant discrètement sur l'ordinateur, sans prévenir l'utilisateur, et collectant et envoyant des informations personnelles à des organismes tiers. Les spywares sont permis par la loi mais seulement dans certaines conditions très précises (si elles ne sont pas respectées, les créateurs du logiciel peuvent être attaqués par la justice).

Les exploits

Dans le domaine de la sécurité informatique, un exploit est un programme permettant à un individu d'exploiter une faille de sécurité informatique dans un système d'exploitation ou un logiciel que ce soit à distance (remote exploit) ou sur la machine sur laquelle cet exploit est exécuté (local exploit), ceci, afin de prendre le contrôle d'un ordinateur

Les rootkits

On nomme rootkit un programme ou ensemble de programmes permettant à un tiers (un pirate informatique, par exemple, mais pas nécessairement) de maintenir dans le temps un accès frauduleux à un système informatique. Les « rootkit » opèrent une suite de modifications, notamment au niveau des commandes système, voire du noyau (kernel). À la différence d'un virus informatique ou un ver de nouvelle génération, un « rootkit » ne se réplique pas. L'installation d'un « rootkit » nécessite des droits administrateur (root) sur la machine, notamment à cause des modifications profondes du système qu'il engendre. Cela signifie que le pirate doit initialement disposer d'un accès frauduleux, avec les droits du « root »

Les composeurs (*dialers*)

Le composeur (aussi appelé composeur d'attaque ou war dialer en anglais) est un logiciel qui balaie une série de numéros de téléphone fournis par l'utilisateur à la recherche d'un autre appareil électronique ou d'un réseau de communications. C'est un logiciel malveillant, installé sur un ordinateur à l'insu de l'utilisateur de l'ordinateur, qui branche un ordinateur à un numéro de téléphone dont les frais d'utilisation sont très élevés. Les numéros de téléphone visés sont typiquement des numéros 1-900 ou des numéros de pays étrangers.

Les publiciels (*adwares*)

Les publiciels ne sont logiquement pas considérés comme des malwares par la loi lorsqu'ils sont indiqué lors de l'installation (la barre Googles pour les navigateurs Internet sont une sorte de publiciels), mais ne sont pas considerés comme des malwares

Les canulars (*hoax* en anglais)

Classé régulièrement à tort de virus ou de logiciel malveillant. Ce sont des courriers électroniques dont le contenu est souvent une alerte sur un faux-virus et qui n'ont pour conséquence indirecte que de saturer les serveurs de courriels de messages inutiles. Dans cette fausse alerte, le message peut aussi vous inviter à supprimer un fichier système important ; ce message utilise alors la naïveté du destinataire comme vecteur de malveillance.

Hameçonnage (*phishing* en anglais)

L'hameçonnage, est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance — banque, administration, etc. — afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. C'est une forme d'attaque informatique reposant sur l'ingénierie sociale. L'hameçonnage peut se faire par courrier électronique, par des sites Web falsifiés ou autres moyens électroniques.