Comment se protéger des programmes malveillants ?

Bien que de nouveaux programmes malveillants voient sans cesse le jour, quelques grands types de ces « malicious software », ou « malwares », peuvent être répertoriés. La connaissance étant mère de sureté, voici donc un tour d'horizon des principales techniques d'intrusion, d'exploitation et de diffusion malveillantes.

LES PROGRAMMES **MALVEILLANTS**

Adware : programme affichant d'autorité des bandeaux publicitaires, en vue de rediriger l'utilisateur vers certains sites web ou de générer directement des revenus au coût par click pour les partenaires des sociétés concernées.

Backdoor : programme caché qui offre une porte d'entrée à un attaquant et lui permet d'installer et d'exécuter d'autres programmes. Plusieurs ordinateurs, voire des milliers, peuvent ainsi être contrôlés à distance par une personne malveillante dans ce que l'on appelle un « Botnet » (contraction de « robot » et « internet »), un réseau d'ordinateurs détournés. L'attaquant utilise les ressources des machines infectées de diverses façons et notamment pour envoyer massivement du spam.

Cheval de Troie : programme d'apparence ordinaire, tel qu'un économiseur d'écran, un générateur de numéro de série pour logiciel payant ou un (faux) anti-virus, qui sert à cacher un autre programme, malicieux celui-là.

Exploit : programme exécuté directement par l'attaquant ou par un « ver », en général à distance, utilisant un trou de sécurité ou un ***bug*** connu dans un système d'exploitation ou un logiciel, pour ensuite installer et exécuter un programme malicieux.

Keylogger : programme qui enregistre automatiquement les frappes au clavier et permet donc de récupérer identifiants, mots de passe, numéros de cartes de crédit, etc.

Spyware : programme qui collecte des informations privées sans le consentement des intéressés, souvent dans le but d'affiner le ciblage publicitaire.

Ver (« Worm ») : c'est un peu la version « réseau » du virus, à ceci près qu'il n'a pas besoin d'un programme hôte pour être hébergé. Il utilise une faille de sécurité connue pour se propager ou se diffuse par e-mail en utilisant le carnet d'adresses de l'utilisateur.

Virus : programme qui s'exécute en tâche de fond et est capable de se reproduire et de se diffuser de manière autonome en infectant des programmes hôtes et des supports de données (disques durs, clés USB…). Classiquement, il s'agit de détruire ou de corrompre les données des ordinateurs infectés.

GLOSSAIRE

Bug
Anomalie de fonctionnement d'un programme informatique.

Crédit photo Masterfile France / Big Cheese Photo - Donna Day

PRATIQUES **INTRUSIVES OU MENSONGÈRES**

Hoax (canular) : les appels à la sympathie pour des situations tragiques sont souvent des hoax. En invitant leur destinataire à transmettre un e-mail à toutes ses connaissances, l'objectif réel est de saturer le réseau par une diffusion exponentielle du message. On peut facilement se reporter à un site internet de « hoaxbuster » pour vérifier l'information.

Pages web malveillantes : il en existe de plusieurs sortes. Certains sites utilisent des fonctionnalités agressives pour ouvrir des « pop-up », le plus souvent publicitaires, ou forcer des téléchargements. Autre forme de publicité intempestive : le succès du réseau social Facebook engendre la création de pages internet postant, à l'insu de leurs visiteurs, des liens « J'aime » vers les pages concernées sur le « mur » Facebook de ces derniers. Certaines pages web, enfin, simulent un scan de l'ordinateur à la recherche d'antivirus dans le seul but de vendre leur propre produit…

SE PROTÉGER

Voici quelques règles de bon sens applicables par tous :

- maintenir à jour en permanence votre système d'exploitation et votre antivirus ;
- ne jamais ouvrir les pièces jointes à un e-mail dont vous ne pouvez pas identifier l'expéditeur ;
- ne télécharger que des programmes connus ou, à défaut, des programmes distribués par des sites connus ;
- stopper aussitôt l'activité en cours lorsqu'une alerte se déclenche dans le navigateur ou bien directement dans une page web ;
- privilégier les programmes « open source » qui, du fait que leur code source, la programmation originelle, est lisible par tous les programmeurs qui souhaitent l'améliorer, contiennent très rarement des programmes malicieux.

(Voir la fiche *Pratiques d'internet // je navigue sur internet)*

GLOSSAIRE

Navigateur internet

Programme permettant de « naviguer » sur internet. Il en existe plusieurs, les plus connus étant actuellement Internet Explorer (Microsoft), Google Chrome, Firefox (Fondation Mozilla), et Safari (Apple).