Se protéger « Faire la guerre à un Troyen »

Vous venez de télécharger des données et depuis, votre ordinateur a un comportement bizarre : des logiciels s'ouvrent sans que vous ne les ayez lancés, votre disque dur mouline alors que vous ne faites rien, votre souris a des réactions curieuses… Il y a des chances pour que vous hébergiez un Troyen. Rassurez-vous, l'éradiquer ne prend pas vingt ans, comme l'Odyssée.

Connaître l'ennemi

On l'appelle cheval de Troie, Trojan, ou encore Troyen parce qu'il s'introduit en douce subrepticement sur votre machine. A la manière des soldats grecs qui sont entrés dans la ville de Troie cachés dans un cheval, le Troyen se dissimule dans un programme valide pour envahir votre machine. Comme le virus, c'est un code nuisible placé dans un programme sain ou dans la pièce jointe d'un mail. Sauf que ce n'est pas un virus, car bien qu'il utilise le même mode de déploiement, il ne poursuit pas les mêmes objectifs.

Pour vous tourmenter, le Troyen doit d'abord s'installer sur votre disque dur. Le plus souvent, ils se camouflent dans les fichiers à la provenance douteuse (sites warez, pages personnelles d'internautes, pièces jointes de mails…). Pour vous inciter à le télécharger, il se présente comme LE programme qu'il faut posséder : un lecteur de format divx révolutionnaire, un antivirus puissant, un programme de hack… Méfiance dès que la proposition est trop alléchante ou que les données proviennent d'un site de pair à pair.

Savoir +

Comment un Troyen peut-il vous nuire ?

Le cheval de Troie peut entre autres :
inventorier le contenu de vos disques durs, détruire ou modifier vos fichiers ;
effectuer des opérations de téléchargement (upload et download) sur votre machine ;
rebooter, installer des virus, prendre la main sur votre ordinateur ;
voler des mots de passe ;
en clair, il peut faire tout ce qui VOUS est possible, à votre insu.

Se protéger « Faire la guerre à un Troyen »

Ensuite, le Troyen ouvre un des ports de communication de votre machine. Au nombre de 65 536, ces ports sont les accès par lesquels transitent les informations qui vont ou viennent d'Internet. A chaque port correspond un service précis identifié par un numéro. Potentiellement tous ces ports constituent une faille pour la sécurité de votre système, comme les portes et les fenêtres de votre maison pour un cambrioleur.

En ouvrant un port, le Troyen permet à son concepteur, en général un pirate, de s 'introduire sur votre machine par le réseau en ouvrant une porte dérobée (backdoor en anglais). Par cette porte, il accède à toutes les données de votre disque dur.

▷▷▷ Le débusquer

Lorsque vous récupérez un Troyen, il se dissimule sur votre disque dur, de préférence dans un fichier que vous n'allez jamais consulter, et se lance, à votre insu, chaque fois que vous démarrez votre machine. Si vous ne constatez rien au moment de son installation, vous le détecterez tôt ou tard. Par exemple, votre disque dur mouline, ou les diodes de votre modem clignotent alors que vous êtes connecté à Internet mais que vous ne faites rien : ni navigation, ni téléchargement… Cette activité est peut-être due à la présence d'un Troyen.

Savoir +

Les symptômes d'une infection par un Troyen

Un comportement inhabituel de votre ordinateur peut trahir la présence d'un Troyen. Interrogez-vous si vous constatez :

. une activité anormale du modem, de la carte réseau, ou du disque dur ;
. l'ouverture inopinée de programmes ;
. des réactions insolites de la souris ;
. des plantages à répétition.

Détecter ce type de programmes malicieux est difficile car il faut parvenir à déterminer si l'action du programme est voulue ou non par le cheval de Troie. Sans compter que chaque Troyen qui envahit votre disque dur s'attaque à un port en particulier, ils ont chacun leur spécialité : JammerKillah tentera de passer par le port 121 tandis que Telecommando s'attaquera au 61466… Pour les repérer, commencez par scanner votre disque dur avec votre antivirus.

S'il s'agit réellement d'un cheval de Troie, vous pouvez utiliser ce que l'on appelle communément un bouffe-troyen, capable de détecter et de détruire les chevaux de Troie. Vous pouvez faire confiance à des logiciels tels que : BoDetect, Back orifice eliminator, The Cleaner 3.0 (surpuissant, il élimine à peu près toutes les sortes de Troyens connus), Anti-Socket de Troie, DMCleanup, NetBuster… Mais téléchargez-les plutôt sur le site de l'éditeur ou sur un site miroir officiel plutôt que sur un site personnel. On ne sait jamais, le programme a pu être modifié…

Pensez aussi à mettre ces logiciels à jour, sans quoi vous risquez de ne rien détecter.

Se protéger « Faire la guerre à un Troyen »

▷▷▷Blinder les portes

Le plus simple pour ne pas être envahi par un cheval de Troie, c'est encore de rester maître des ports, c'est-à-dire de ne pas laisser n'importe quel port ouvert : il faut l'empêcher d'aller sur Internet et d'effectuer une connexion entre le pirate et la machine. L'arme de prévention la plus efficace reste le pare-feu (firewall). Il fait office de filtre entre votre ordinateur et Internet. Il sécurise les ports de communication : toutes les données qui entrent et qui sortent sont bloquées et soumises à votre approbation. Il est impératif de refuser la connexion aux programmes que vous ne connaissez pas. Et si ce programme récidive, il faut vérifier que votre ordinateur n'est pas contaminé.
Si vous cherchez un pare-feu efficace, vous pouvez faire confiance à ZoneAlarm, Kerio, Look'n'Stop, Sygate BlackIce, PCCillin, McAfee Personal Firewall et Norton Firewall.

Attention, les pare-feux ne vérifient pas le contenu des données envoyées ou reçues. Et donc l'invasion de virus… Ils servent seulement à repérer s'il y a un Troyen ou non et à bloquer la connexion.

Enfin, si vous espérez gagner vos galons de pirates en utilisant un Troyen, prenez garde… Cette communauté vous considérera comme un « lamer », un cyber-idiot comme on dit courtoisement et si on vous repère, vous pouvez être poursuivi pénalement, toute intrusion non désirée étant considérée comme criminelle…

Savoir +

Les fichiers dont il faut se méfier

Jusqu'à présent tous les Troyens identifiés étaient des fichiers exécutables (.exe). Donc, si vous avez téléchargé une image en .jpeg, une chanson en .wav ou en .mid, ou encore un fichier texte (.txt), vous avez peu de chances d'y trouver un Troyen. Exécutable signifie aussi que le programme n'est pas capable de se lancer de lui-même. Si vous n'y touchez pas, vous resterez à l'abri d'une contamination. Si, en plus, vous avez configuré votre antivirus de manière à ce qu'il scanne tout ce que vous enregistrez, vous n'aurez pas de virus non plus.

◁◁◁