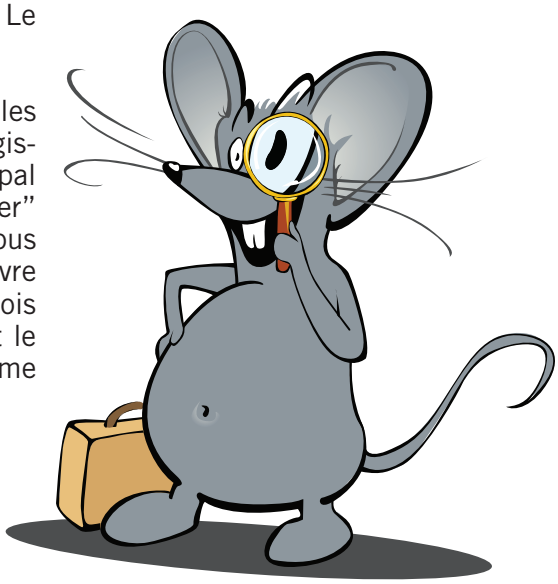
04. Troyens, Trojans, chevaux de Troie

C'EST QUOI UN "TROYEN" ?

L'expression "troyen", "trojan horse", "trojan" ou encore "cheval de Troie", est dérivée de la mythologie grecque.
Comme les Grecs cachaient des soldats dans le ventre d'un cheval en bois lors de la guerre contre Troie, cette malware (troyen) en fait de même.
Le "troyen" est un programme malicieux qui en cache un autre. Le programme caché est en principe un "keylogger".



Le "keylogger" lui-même est un programme qui enregistre toutes les frappes de clavier et qui envoie ensuite toutes ces données enregistrées à son programmeur par l'intermédiaire du programme principal qui l'héberge. Le programme principal, qui héberge le "keylogger" s'intègre dans la base des registres à votre insu (sans que vous vous en apercevrez) et prépare l'envoi vers son programmeur. Il ouvre certains ports de communication vers l'extérieur. Ces ports une fois ouverts, son programmeur peut avoir accès à votre ordinateur et le téléguider ! Cette sorte de "troyen" est appelée aussi un programme "backdoor".

Téléguider mon ordinateur ?

Eh bien oui, c'est possible !

Le premier programme malicieux (principal) ouvre les ports de communication (c'est comme une maison avec les portes principales grandes ouvertes).

Lire aussi :
Firewalls http://www.webwizardbiz.com/tutorials/firewalls/

Le deuxième programme malicieux, le "keylogger" a copié toutes vos frappes de clavier, tels que vos mots de passe, numéros de carte de crédit, vos données d'accès à vos comptes de sites internet etc. Toutes ces données seront envoyées et connues par le programmeur de ce code malicieux.

Ces deux combinaisons dans un programme malicieux sont très dangereuses.

Comment attraper un “troyen” ?

On peut attraper un “troyen“ :

1. En ouvrant un courrier électronique (e-mail) d’une personne inconnue. En principe ils sont cachés dans les pièces jointes (attachments).

2. Par l’intermédiaire des portails P2P (peer to peer), les portails d’échange de fichiers.

Kazaa : 45 % des fichiers exécutables seraient infectés.
Si vous téléchargez des logiciels ou des jeux vidéo de Kazaa, vous pourriez obtenir plus que vous n’en demandiez puisque près de la moitié des fichiers exécutables seraient infectés par des virus, vers informatiques ou chevaux de Troie.

Lien de cet article :
Kazaa : http://www.internetmonitor.lu/Kazaa-45-des-fichiers-executables-seraient-infectes_a155.html

Pour voir à quel point ces actions illégales sont déjà nombreuses, veuillez suivre les liens suivants :
PC ZOMBIES: http://www.internetmonitor.lu/index.php?action=article&id_article=67428
PC ZOMBIES 2 : http://www.internetmonitor.lu/index.php?action=article&id_article=74448

Quel but poursuivent les programmeurs de ces codes malicieux ?

Le but est bien évidemment commercial.

Commercial, comment ?

Si votre ordinateur peut être téléguidé comme énoncé ci-dessus, cela veut dire que le programmeur du code malicieux (troyen) est en mesure de faire avec votre ordinateur ce qu’il veut !

Votre ordinateur peut être téléguidé et vous ne vous en apercevrez même pas !

Dès connexion à Internet, sans protections de sécurité sur votre ordinateur, votre ordinateur est exposé à des intrusions. À voir comme une maison sans système d’alarme et ayant toutes les portes et fenêtres grandes ouvertes ! Un intrus (cambrioleur) peut entrer et sortir à votre insu !
Mais revenons maintenant au but commercial. Ces programmeurs travaillent dans des groupes bien organisés (sorte de mafia informatique) et ils louent votre ordinateur à des polluposteurs (envoyeurs de pourriels), ils gagnent bien leur pain avec cette méthode.

Votre ordinateur sera transformé en “PC zombie”, un ordinateur téléguidé et employé pour des actions illégales !

Une autre variante de se servir de votre ordinateur, consiste à déposer du contenu illégal sur votre disque dur et dès que vous êtes connectés à Internet, de permettre aux autres internautes de faire des téléchargements illégaux de ces contenus. En principe il s’agit de contenu pornographique et / ou pédophile !
Vous hébergerez du contenu illégal sur votre disque dur sans le savoir !

Imaginez-vous votre maison avec toutes les portes et fenêtres ouvertes et que des masses de personnes inconnues circulent à l’intérieur. Du va-et-vient qui échappe à votre contrôle !

Mais l'exemple de réflexion ci-dessus vous montre bel et bien ce qui se passe "visiblement" quand votre ordinateur n'est pas équipé de firewall (pare-feu) ! Dès connexion à Internet, votre ordinateur est visible par des millions d'internautes sur Internet et les brigands n'attendent que ça pour vous prendre comme prochaine victime !

En installant un firewall (pare-feu) votre ordinateur devient invisible sur Internet et les risques seront réduits à un minimum.

Comment tester si mon ordinateur est bien protégé ?

Faites un test online gratuit à l'adresse suivante :
Portscan gratuit : http://www.securitymetrics.com/portscan.adp

Maintenant que nous savons ce qu'est un "troyen" et quels dégâts il peut provoquer, nous nous poserons certainement la question :

Comment nous protéger?

1. D'abord il faut installer un firewall (pare-feu). C'est un portier qui contrôle le trafic entrant et sortant.

2. Comme protection supplémentaire, qui nous protège contre les "troyens" et qui éradique aussi les "troyens" installés sur notre ordinateur, il nous faut installer un logiciel (programme) antitroyen.

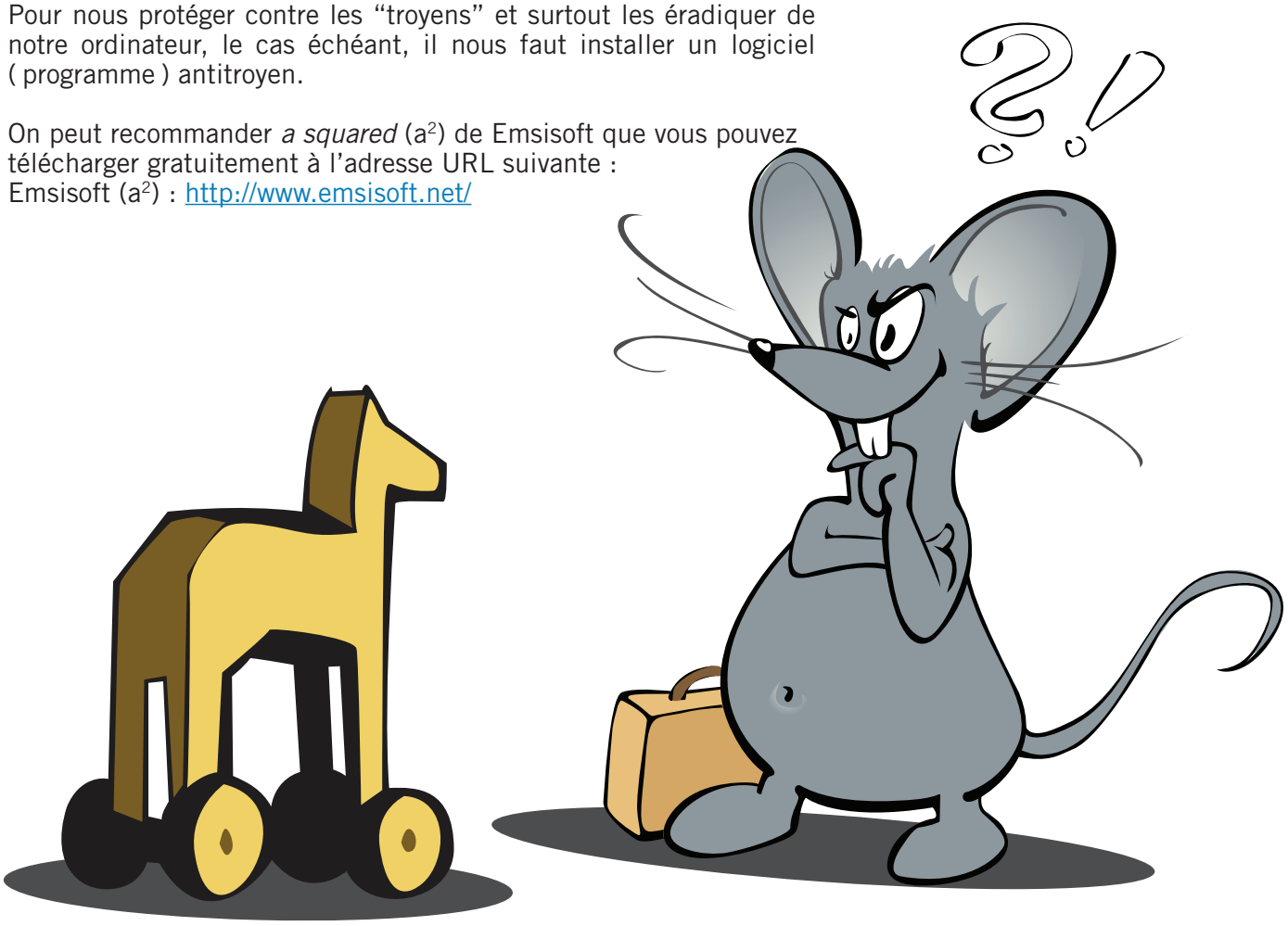
Le firewall (pare-feu) nous protège contre les données entrantes et sortantes non désirées. C'est-à-dire : si jamais il y avait un "troyen" installé sur notre ordinateur, il bloquerait sa connexion vers l'extérieur, mais le "troyen" serait toujours résident sur notre ordinateur !

Pour nous protéger contre les "troyens" et surtout les éradiquer de notre ordinateur, le cas échéant, il nous faut installer un logiciel (programme) antitroyen.

On peut recommander *a squared* (a^2) de Emsisoft que vous pouvez télécharger gratuitement à l'adresse URL suivante :
Emsisoft (a^2) : http://www.emsisoft.net/

Emsisoft (a^2) : C'est un logiciel anti-malware (antitroyen, anti-dialer, etc.) et multilingue qui nous protège et qui éradique aussi les malware.

Explication détaillée et technique d'un "troyen" de a^2 : http://www.emsisoft.net/fr/kb/articles/tec040105/



Un didacticiel concernant le téléchargement et l'utilisation de *a squared* (a^2) peut être trouvé à l'adresse suivante :
Didacticiel *a squared* (a^2) : http://www.internetmonitor.lu/download/Tutoriel_12.11.2004..pdf

Nous vous conseillons aussi de lire les didacticiels suivants :
Visual PC & Internet

Figure 1 : L'antivirus Norton Internet Security™, *a squared* (a^2) scannent l'ordinateur et le firewall "zone-alarm®" a bloqué une intrusion.

GLOSSAIRE :

Troyen, Trojan, Trojan horse :	Cheval de Troie
Backdoor :	Cheval de Troie réputé et très dangereux
Port :	Port de communication de l'ordinateur. Il en existe 65535 (2^{16}) -1
P2P ou "Peer to Peer" : . . .	Échange de fichiers
Kazaa, Emule, eDonkey : . .	Portail d'échange de fichiers
PC zombie :	Ordinateur téléguidé et non sécurisé
Firewall (pare-feu) :	Protection des données. Portier électronique.
Malware :	Toute sorte de code malicieux (ver, virus, troyen, etc.)

MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA FORMATION PROFESSIONNELLE
Centre de technologie de l'éducation