*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 pareil.

Le ***Troyen*** est un programme malicieux qui en cache un autre. Le programme caché est en principe un ***Keylogge**r**.

Le ***Keylogge**r** lui-même est un programme qui enregistre toutes les frappes de clavier et qui ensuite envoie toutes ces données enregistrées à son programmeur vers 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 apercevez) 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 PC et le téléguider !

Cette sorte de ***Troyen*** est appelé aussi un programme ***backdoor*.**

Téléguider mon PC ?

Eh bien oui, c'est possible !

Le premier programme malicieux (principal) ouvre les ports de communication (à voir comme une maison avec les portes principales grandement ouvertes).

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

Le deuxième programme malicieux, le ***Keylogge**r** 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, 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 :

http://www.internetmonitor.lu/index.php?action=article&id_article=67306&id_rubrique=9834

Quel but poursuivent les programmeurs de ces codes malicieux ?

Le but en est bien évidemment commercial.

Commercial, comment ?

Si votre PC peut être téléguidé comme énoncé ci-dessus, cela veut dire que le programmeur du code malicieux (**Troyen**) est en mesure de faire avec votre PC ce qu'il veut !
Surpris ? Eh bien oui, **Votre PC peut être téléguidé et vous ne vous en apercevrez même pas** !

Dès connexion à Internet, sans protections de sécurité sur votre PC, votre PC est exposé à des intrusions. À voir comme un maison sans système d'alarme et ayant toutes les portes et fenêtres grandement ouvertes ! Un intrus (cambrioleur) peut entrer et sortir à votre insu (sans que vous vous en apercevrez) !

Mais revenons maintenant au but commercial. Ces programmeurs travaillent dans des groupes bien organisés (sorte de mafia informatique) et ils louent votre PC à des polluposteurs (envoyeurs de **Spam**) ! Et ils gagnent bien leur pain **(£, $, €)** avec cette méthode.
Là vous êtes certainement encore beaucoup plus étonnés, n'est-ce pas ?

Mais c'est la réalité, malheureusement !

Votre PC sera transformé en **PC ZOMBIE, un PC téléguidé et employé pour des actions illégales !**

Pour voir à quel point ces actions illégales sont déjà présentes, veuillez cliquer les liens suivants :

http://www.internetmonitor.lu/index.php?action=article&id_article=67428

http://www.internetmonitor.lu/index.php?action=article&id_article=74448

Une autre variante de se servir de votre PC, consiste à déposer du contenu illégal sur votre disque dur (Hard Disk) et dès que vous êtes connectés à Internet, de faire profiter les autres internautes à 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. Du va et vient sans votre contrôle ! Est-ce que ce serait normal pour vous ? Sincèrement, je ne crois pas.

Mais l'exemple de réflexion ci-dessus vous montre bel et bien ce qui se passe *visiblement* quand votre PC n'est pas équipé de **Firewall** (**pare-feu**) !

Dès connexion à Internet, votre PC 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 PC devient invisible sur Internet et les risques seront réduits à un minimum.

Comment tester si mon PC est bien protégé ?

Faites en un test online, ceci gratuit à l'adresse suivante :

Portscan GRATUIT : http://www.securitymetrics.com/portscan.adp

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

Comment nous protéger ?

1. ***D'abord il faut installer un Firewall (pare-feu).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 PC, il nous faut installer un logiciel (programme) anti-troyen.***

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

Pour nous protéger contre les ***Troyens*** et surtout les éradiquer de notre PC, le cas échéant, il nous faut installer un logiciel (programme) anti-troyen.

Je vous conseille **a2 de Emsisoft** que vous pouvez télécharger gratuitement à l'adresse URL suivante :

http://www.emsisoft.fr

C'est un logiciel anti-malware (anti-troyen, anti-dialer etc,.) et multi langues qui nous protège et qui éradique aussi les malware.

Explication détaillée et technique d'un *Troyen* de a2 :

http://www.emsisoft.net/fr/kb/articles/tec040105/

Un tutoriel concernant le téléchargement et l'utilisation de ****a squared (a2)**** peut être trouvé à l'adresse suivante :

http://www.internetmonitor.lu/download/Tutoriel_12.11.2004..pdf

Je vous conseille aussi de lire mon tutoriel suivant :

http://www.internetmonitor.lu/index.php?action=article&id_article=70793

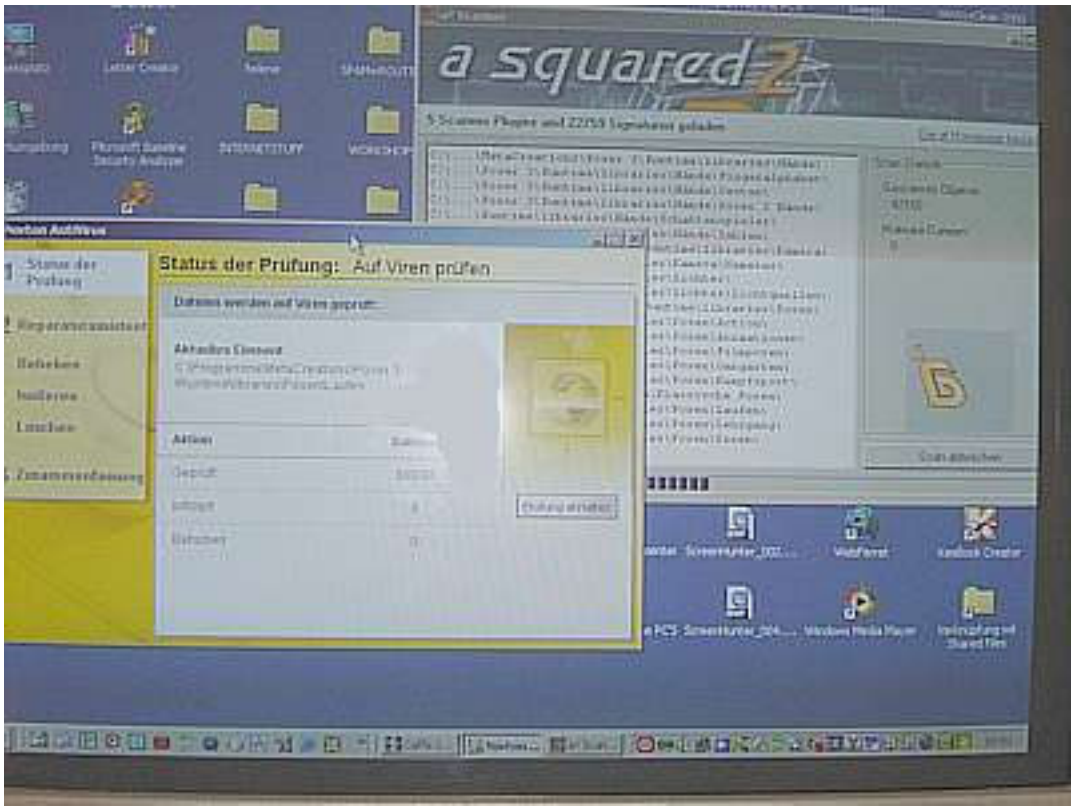

Figure 1 : L'Anti-virus NORTON INTERNET SECURITY et A2 scannent le PC

Glossaire :

Troyen, Trojan, Trojan horse	**: Cheval de Troie**
Backdoor	**: Cheval de Troie réputé et très dangereux**
Port	**: Port de communication du PC. Il en existent 65535**
P2P ou *Peer to Peer*	**: Échange de fichiers**
Kazaa, Emule, Edonkey	**: Portail d'échange de fichiers**
PC Zombie	**: PC téléguidé et non sécurisé**
Firewall (pare-feu)	**: Protection des données. Portier électronique.**
Malware	**: Toute sorte de code malicieux (ver, virus, troyen, etc.)**