L'ordinateur bien protégé

Multiples sont les risques auxquels un ordinateur est exposé de nos jours. Des **virus**, des **vers**, des **troyens** (**chevaux de Troie, trojans),** des **dialer** (connexion surtaxée), des **portes dérobées** (**backdoor**) et des arnaques sont présents sur Internet, n'attendant qu'à trouver des ordinateurs non sécurisés pour en faire des **PC zombies**. Les programmeurs de code malicieux (**la mafia informatique**) prennent ces PC zombies comme leurs esclaves, ils peuvent téléguider les PC zombies comme bon leur semble, à votre insu.

Ainsi ils utilisent l'espace de votre disque dur (hard disk) pour stocker du contenu illégal (musique et vidéos piratés, pornos, contenu pédophile, etc.) et/ou pour connecter des dizaines de milliers de **PC zombies** en réseau (**botnet**) pour faire des attaques **„DDOS"** (**distributed denial of service**), ciblant des serveurs de grandes firmes, de banques, des sites Internet des gouvernements, la NASA, le Pentagone et même les serveurs cruciaux qui sont à eux indispensables pour le fonctionnement de l'Internet. Voir ici : **http://www.internetmonitor.lu/Attaque-massive-contre-Internet,-le-reseau-a-tenu_a816.html**

Une autre méthode consiste à faire des attaques du type **„DDOS"** pour rendre inaccessible certains serveurs qui hébergent des sites commerciaux et puis après avertir les propriétaires qu'ils doivent payer une rançon, autrement leur site Internet ne sera plus accessible aux internautes. C'est du chantage informatique à grande échelle.

Pour les firmes qui font du commerce électronique (**eCommerce**) chaque minute de non-présence sur Internet est une perte d'argent considérable ! Et c'est peut être votre ordinateur qui est complice pour faire ces attaques. Est-ce que votre ordinateur est un PC zombie ? Êtes-vous sûr que vous ne participez pas avec dans une attaque pareille ? Posez-vous sérieusement ces questions, parce que lors d'un démantèlement d'un **botnet (réseau de PC zombies)** par la police judiciaire, votre ordinateur pourrait aussi être détecté et vous serez convoqué devant le tribunal. Vous serez coupable d'avoir participé à des actions illégales, voir les lois luxembourgeoises à **l'adresse URL http://www.internetmonitor.lu/download/Pratique_Securite_PC_Internet_27.06.2006.pdf.**

De ce fait il est indispensable d'installer sur l'ordinateur un antivirus, un firewall (pare-feu), une protection antispyware et une protection antitroyen !

L'antidote pour l'ordinateur est l'antivirus, il protège l'ordinateur contre les infections virales. L'antivirus est comparable à la vaccination, le sérum doit être répété afin qu'il puisse être effectif. Avec l'antivirus c'est pareil, il faut faire les mises à jour pour qu'il soit effectif tout le temps !

En dehors de l'antivirus il faut installer un **pare-feu** (**firewall**) d'office ! L'ordinateur dispose de **65.535 (2^{16} -1) ports de communication** qui sont utilisés pour des tâches diverses (imprimer, connexion à Internet, etc.). Ces ports peuvent être visualisés comme des portes. Imaginez-vous un grand immeuble comportant **65.535 bureaux**. Il va de soi, notre sens logique nous le dicte, que ces portes doivent être surveillées afin que personne ne puisse y pénétrer. Dans la vie réelle nous engagerions un portier et nous installerions un système d'alarme afin de surveiller cet immeuble.

En ce qui concerne l'ordinateur, c'est le pare-feu (firewall) qui gère ces ports. Il contrôle le trafic entrant et le trafic sortant de l'ordinateur, et le cas échéant où il y aurait une tentative de pénétration, le pare-feu (firewall) bloque cette activité !

Le firewall (pare-feu) est à voir comme le système anti-intrusion (système d'alarme) !

Ayant installé un antivirus et un firewall (pare-feu) vous êtes déjà assez bien protégés. **Mais notez toutefois que le pare-feu (firewall) de Windows® XP ne contrôle que le trafic entrant et pas le trafic sortant !** Le pare-feu de **Windows® XP** est nul, échangez-le contre un autre pare-feu. Il existe des pare-feux gratuits, tels que **ZoneAlarm™** **http://www.zonelabs.com** par exemple, ou optez pour une protection tout-en-un, une suite de sécurité.

C'est quoi une suite de sécurité ?

Une suite de sécurité est un logiciel incluant différents logiciels de sécurité dans un paquet, à voir, antivirus, pare-feu (firewall), antispyware, filtre parental, antispam, etc.
Actuellement (25.04.2007) les suites de sécurité suivantes sont disponibles, sans rentrer dans les détails laquelle est la meilleure :

- **Norton Internet Security (NIS)**
- **G-DATA**
- **F-Secure**
- **Panda**
- **Kaspersky**
- Etc.

Autres anti-trucs-machins :

Malheureusement il existe encore d'autres sortes d'arnaques et de menaces, telles que :

- **Spyware (mouchards)**
- **Dialer (connexion surtaxée)**
- **Adware**
- **Spoofing (usurpation d'identité)**
- **Browser hijacking (détournement de navigateur)**
- **Phishing**
- **Keylogger**
- **Troyens (trojans, chevaux de Troie)**
- **Rootkits**
- **Etc.**

Les „**spyware**" espionnent vos habitudes de navigation sur Internet et ils renferment assez souvent aussi du malware. Heureusement il existe aussi des logiciels, même gratuits et très performants qui protègent contre ces malware et/ou les éradiquent. En voici deux, gratuits, très réputés et efficaces :

- **Spybot Search&Destroy** **http://www.safer-networking.org**
- **Ad Aware** **http://www.lavasoft.com**

lesquels protègent contre les „**spyware**".

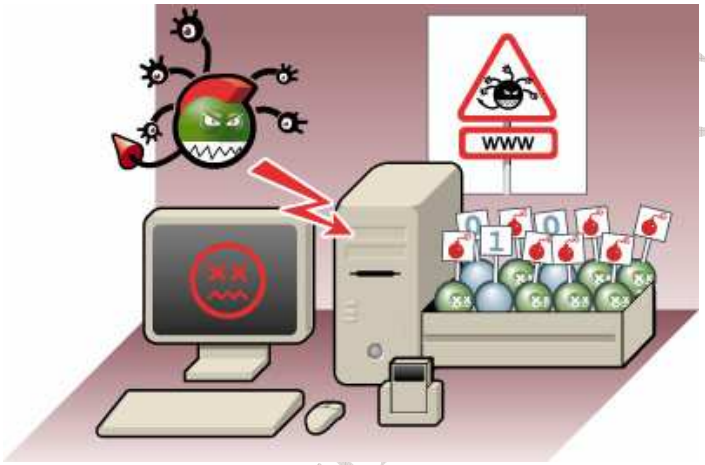
Mais méfiez-vous aussi des **troyens** (**chevaux de Troie, trojans**) ! Comme toute autre sorte de code malicieux ils se camouflent bien, ils volent vos identités informatiques (mots de passe, login, numéros de cartes bancaires, numéros pin et tan, etc.) et les envoient à leur programmeur(s) ! Actuellement (25.04.2007) **il n'existe aucune suite de sécurité au marché qui détecte et éradique efficacement tous les troyens !**

Par contre, un logiciel spécialement conçu pour contrer ces bestioles informatiques (**malware**) au nom de „**a squared**", de chez Emsisoft **http://www.emsisoft.net/fr,** est devenu le cheval de bataille, l'adresse numéro un pour se protéger contre troyens, dialer, keylogger, etc.

„**a squared**" peut être téléchargé à l'adresse URL **http://www.emsisoft.net/fr**. Ce logiciel existe aussi bien en version gratuite qu'en version payante. Remarquez quand même que la version payante (**29 € au 25.04.2007**) vous offre un „**IDS**" (**Intrusion Detection System**) en temps réel, protection incontournable quand vous faites du **P2P** (**peer to peer/échange de fichiers**) et quand vous naviguez comme „power surfer".

L'**IDS** vous offre une sécurité permanente et ceci même contre des codes malicieux qui n'existent pas encore.

Qu'est-ce qu'un IDS ? Comment fonctionne t-il ?



Texte copié du site de „a squared" :

Une protection contre les Malware sans connaitre sa signature ?

Le „**Gardien d'arrière-plan**" de a-squared antimalware examine comme tout autre Gardien d'arrière-plan de logiciels Antivirus, tous les programmes lancés avec le scanneur de signatures. Le scanneur ne peut toutefois reconnaître les nouveaux Malware, que lorsqu'il a déjà la signature pour ce fichier dans sa banque de données. Bien que l'équipe de a-squared s'efforce toujours d'apporter aussi rapidement que possible de nouvelles signatures de Malware par l'intermédiaire des mises à jour en ligne, il se passe un certain temps sans que vous soyez protégé. Cette période critique est entre la première apparition d'un nouveau Ver et le moment de la mise à jour de a-squared sur votre PC.

C'est pour cette raison, que nous avons mis au point a-squared **IDS** (**Intrusion Detection System**). Un système qui est en mesure, de reconnaître et de bloquer les dangereux Malware sans même avoir la signature de celui-ci.

Analyse du comportement

Contrairement aux heuristiques traditionnelles, qui recherchent des fichiers contenant des routines nuisibles sur le disque dur et qui fournissent une analyse approximative si un fichier est dangereux ou non, a-squared lui surveille directement le comportement des programmes actifs dans le système.

Et tout ça fonctionne comme suit :

Chaque type de Malware, peu importe si c'est un Virus, un Trojan, un Ver, un Dialer ou un Spyware, travaille toujours d'après une certaine routine. Chaque type, a par ses propriétés un but principal qui le rend clairement discernable d'un autre. Un Virus contamine, un Ver se propage, un Trojan envoie des données, un Dialer établit une connexion, etc. Un exemple: Les Trojan se différentient toujours dans la manière dont ils envoient ces données. Cependant, cela ne trompe pas sur le fait qu'ils envoient tous des données.

C'est précisément ici que a-squared joue son rôle. Il analyse en direct le comportement de tous les programmes actifs et affiche une alerte aussitôt qu'un programme montre un comportement dangereux. a-squared contient une sorte d'heuristique en temps réel dont le taux de reconnaissance est extraordinairement bon avec tous les types de Malware, pour lequel il a été formé.

Si maintenant, vous pensez que cela est trop beau pour être vrai, vous avez raison d'en douter. Cette technologie a aussi un désavantage: a-squared reconnaît le comportement de Malware. Le comportement d'un type de Malware est toutefois toujours le même. C'est pourquoi a-squared ne peut faire la différence entre deux Malware de même type et les différencier l'un de l'autre. a-squared ne peut pas vous dire si maintenant le ver s'appelle "**NetSky**" ou "**Bagle**", ou si le Trojan s'appelle „**Optix**" ou „**SubSeven**". Il peut simplement reconnaître qu'il s'agit d'un Ver et/ou d'un Trojan. C'est toutefois un risque très faible que l'on prend, si l'on pense à cette protection très puissante.

Contre le **détournement du navigateur** (**browser hijacking**), vous pouvez vous munir du logiciel „**Browser Hijack Retaliator**" qui peut être téléchargé à l'adresse URL **http://www.zamaansoft.com/products/bhr/index.php** et dont voici un didacticiel vous montrant son utilisation : **Hostfile hijacking**.

Voilà, ayant fait un peu le tour des infections et attaques possibles, avec suggestions comment se protéger, faisons-en le résumé.

En bref, connaissant les types d'attaques qui ont été expliqués ci-dessous, il est recommandé d'installer sur un ordinateur les logiciels suivants :

- Antivirus de votre choix, gratuit ou payant
- Firewall (pare-feu), p.ex. : **ZoneAlarm** (gratuit)
- Antispyware (**anti-mouchard**), de préférence deux qui se complètent, **Spybot Search&Destroy** et **Ad Aware**® font bien l'affaire.
- Antimalware, comme suggéré déjà, „**a squared**".

Nom	Adresse de téléchargement
Ad Aware	**www.lavasoft.com**
Spybot Search&Destroy	**http://www.safer-networking.org**
ZoneAlarm	**www.zonelabs.com**
a squared	**www.emsisoft.net/fr**

Avec cette combinaison de logiciels installés et en suivant une politique de sécurité rigoureuse, c'est-à-dire :

- Faire régulièrement les mises à jour (updates) de **Microsoft®**, **Linux®** et **Mac®**
- Faire régulièrement les mises à jour (updates) de **Java™**, **Adobe**, etc.

http://secunia.com/software_inspector

vous serez sécurisés au maximum, pour l'instant (mai 2007) !

Pour plus d'informations, veuillez lire les articles suivants :

Botnet :http://www.emsisoft.fr/fr/kb/articles/tec070503/

Le fichier hôte (hostfile) :http://www.emsisoft.fr/fr/kb/articles/tec061108/

Rootkits :http://www.emsisoft.fr/fr/kb/articles/tec060324/

Spyware :http://www.emsisoft.fr/fr/kb/articles/tec050623/

Chevaux de Troie en détail :http://www.emsisoft.fr/fr/kb/articles/tec040105/

Règles de base de la sécurité :http://www.emsisoft.fr/fr/kb/articles/tec040402/