SECURITY MONITOR

Numéro 3/2009

Une publication de l'Internet Monitor
http://www.internetmonitor.lu

PC Sécurité

La cybercriminalité ou l'économie souterraine

Entre temps presque tout le monde sait maintenant ce que c'est un virus informatique et qu'il existe aussi des troyens (trojan, chevaux de Troie), même que certains avaient déjà infecté leur ordinateur avec ces bestioles informatiques.

Mais qui crée ces malwares et pourquoi ?

Ce ne sont plus les scriptkiddies (mais ils existent toujours) qui s'amusent à programmer des virus pour la gloire, mais ce sont des criminels financièrement motivés qui créent et répandent de nouveaux programmes à une cadence accélérée.

Les SophosLabsTM, réseau international de chercheurs et d'analystes de Sophos, reçoivent chaque jour environ 20 000 nouveaux échantillons de logiciels suspects. La plupart de ces échantillons sont des chevaux de Troie, conçus pour voler silencieusement les données personnelles des utilisateurs ou pour pirater leur ordinateur et en prendre le contrôle.

Ces criminels ont développé des modèles économiques autour de la fraude aux moyens de payement, du spam, de la contrefaçon, de codes malicieux… On parle maintenant de la « **cybercriminalité » organisée** !

L'appât du gain

Symantec estime à plus de 276 millions de dollars la valeur de tous les produits proposés sur les serveurs de l'économie souterraine entre le 1er juillet 2007 et le 30 juin 2008.

Dans ce numéro

Points de vue

- La sécurité ne se discute pas, on l'applique.
- Il est impératif d'installer les mises à jour (Windows, Mac et Linux).
- Il est impératif d'installer les mises à jour des applications tierces (Adobe Acrobat Reader, Flash, Java, Open Office, VLC Media Player, Firefox, Opera, IE, etc.)

La cybercriminalité aujourd'hui (janvier 2009)

www.miscmag.com

Les cybercriminels ont développé des modèles économiques autour de la fraude aux moyens de payement :

- **Du spam (courrier non sollicité)**
- **De la contrefaçon (piratage de logiciels/copies et vente illégales)**
- **De codes malicieux**
- **Chantage au déni de service**
- **Phishing**
- **Pharming**
- **Carding**

Plus d'informations ici : http://tinyurl.com/5mvs53

Etude Webroot : 85% des malwares seraient disséminés par le Web

http://www.globalsecuritymag.fr/Etude-Webroot-85-des-malwares,20080924,5176

Les cybercriminels ne veulent qu'une seule chose, infecter un maximum d'ordinateurs pour gagner un maximum d'argent. L'appât du gain ne connaît ni gênes, ni frontières.

L'appât du gain

Extrait de GLOBAL SECURITY MAG :

Webroot vient de dévoiler une étude révélant l'impact du **Web 2.0** sur l'entreprise. Pas moins de **85% des malwares sont désormais disséminés par le Web**, selon les recherches de Webroot, et les entreprises ne sont pas correctement protégées contre les virus, les logiciels espions issus du Web et le **comportement des employés qui conduit à des failles dans la sécurité**, la perte de la propriété intellectuelle et la diffusion de données confidentielles.

Source de l'extrait :

http://www.globalsecuritymag.fr/Etude-Webroot-85-des-malwares,20080924,5176

Microsoft constate que l'utilisation des logiciels malveillants est le fait de **criminels de plus en plus organisés** et de plus en plus **motivés par l'appât du gain**.

http://www.mag-securs.com/spip.php?article10400

Les conseils d'utilisation de l'ordinateur et de l'Internet

- **Installez un antivirus (gratuit ou payant) et un pare-feu (firewall) Installez un antimalware, http://www.emsisoft.net/fr qui lui est un complément à l'antivirus et au firewall**

- **Installez régulièrement les mises à jour de Windows, Mac et Linux**
- **Installez l'application gratuite de McAfee, le SiteAdvisor, qui lors de votre navigation sur Internet vous montre les sites douteux**

- **Si votre antivirus ne dispose pas de protection antiphishing, installez la barre d'outils de Spoofstick ou de Netcraft. De cette façon vous disposerez d'une protection contre le Phishing .**

- **N'ouvrez jamais de courrier électronique (email) de personnes inconnues, surtout pas les pièces jointes.**

- **Ne répondez jamais à du courrier électronique (email) provenant de banques, poste et télécommunications, eBay, PayPal, etc. vous incitant à donner vos données confidentielles (pin, tan, email, mot de passe, login...). Il y a danger de phishing (hameçonnage par courrier électronique). Ces institutions ne vous adresseront jamais des demandes pareilles par courrier électronique. Veuillez lire aussi notre didacticiel : Phishing, le nouveau fléau sur Internet**

- **Avant d'utiliser un support de sauvegarde (CD, DVD, Memory stick, clé USB, appareil photo digital, disquette, caméscope, MP3player, baladeur, iPod, etc.) scannez-le avec votre antivirus sur une contamination éventuelle !!!**

Contrairement à ce que la plupart des gens croient, en dehors d'une infection (virus, troyen, trojan, cheval de Troie et autre malware) par connexion Internet, votre ordinateur peut aussi être infecté par un support de sauvegarde. Dès qu'un ordinateur est infecté et que l'on enregistre des données sur un médium de sauvegarde, il y a de très fortes chances que ce médium de sauvegarde devient aussi infecté. Alors, soyez sur vos gardes quand vous recevez des médiums de sauvegarde de vos amis, proches, etc. et que vous deviez les insérer dans votre ordinateur.

Les logiciels utiles :

- **McAfee SiteAdvisor**

www.siteadvisor.com

- **A squared antimalware**

www.emsisoft.net/fr

- **Netcraft toolbar**

http://toolbar.netcraft.com/

- **Threatfire**

www.threatfire.com

- **KNOL (pendant Wikipédia) sur la sécurité PC et Internet**

http://tinyurl.com/5mvs53

Une petite aide, les 10 commandements de l'éthique informatique :

01. Tu n'utiliseras point ton ordinateur pour nuire à autrui.

02. Tu n'entraveras point le travail d'autrui sur ordinateur.

03. Tu ne fouineras pas dans les fichiers d'autrui.

04. Tu n'utiliseras point ton ordinateur pour voler.

05. Tu n'utiliseras point ton ordinateur pour tromper.

06. Tu n'utiliseras point les logiciels dont les droits d'auteur ne sont pas régularisés.

07. Tu n'utiliseras point les ressources d'autrui sans en avoir la permission explicite.

08. Tu ne commettras jamais de plagiat.

09. Tu es conscient des conséquences sociales et morales de tes programmes.

10. Tu utiliseras ton ordinateur de façon responsable et respectueuse.

Le meilleur exemple pratique : Les malware (virus, ver, troyen et co) présents dans la station spatiale ISS (27.08.2008) à cause d'une "flash card" emporté par les astronautes qui était infectée...

- **Surtout les baladeurs, iPod, MP3 Player et clés USB qui contiennent des fichiers musicaux, fichiers vidéos et présentations Flash et Power Point, ainsi que des jeux, sont à haut risque parce que les fichiers stockés ont été certainement téléchargés sur des réseaux P2P (peer to peer [EN]) appelés aussi réseaux d'échange de fichiers. Or il s'est avéré qu'il y a grand risque de contamination sur les réseaux P2P. Ayez le réflexe de sécurité et scannez ces supports avec votre antivirus avant de les utiliser.**

- **Évitez de télécharger sur les réseaux d'échange de fichiers, appelés aussi le P2P (peer to peer), ou disons plutôt "de pire en pire". La plupart de ces fichiers sont contaminés avec des chevaux de Troie (trojan, trojan horse) et autres malware. Votre antivirus ne détecte pas toute sorte de troyens, il n'est pas conçu pour ça. Son rôle initial, comme son nom l'indique, est de protéger contre des virus. Si vous continuez quand même à utiliser le P2P, alors installez svp un antimalware (antitroyen, antikeylogger, antibackdoor, etc.) qui lui détectera ces malware. Nous vous conseillons "a squared", dont voici aussi une vidéo de démonstration.**

- **Évitez de télécharger sur des sites Internet se terminant avec un "z", tels que "crackz", "warez", "serialz", etc. Ces sites Internet n'ont qu'un seul but; vous inviter à télécharger des choses soi-disant gratuites, mais illégaux, et finalement infecter votre ordinateur pour en faire un PC zombie, un ordinateur pris en otage et téléguidé par les cybercriminels (mafia informatique) pour faire des actions illégales (à l'insu de leurs propriétaires) !!!**

- **Quand vous êtes invité(e)s par courrier électronique, Messenger, ou sur YouTube et autres portails pour télécharger un "codec" pour qu'une vidéo vous intéressant peut être visionnée, soyez vigilants !!! La plupart du temps il s'agit d'une invitation pour vous inciter à télécharger un logiciel malveillant qui vous infecte avec un troyen (trojan, cheval de Troie).**

- **Téléchargez régulièrement les mises à jour de tout logiciel installé sur votre ordinateur, surtout les plug-ins ou les logiciels dits "indispensables", tels que : Acrobat Reader, Java, Flash, ITunes, QuickTime, VLC qui présentent parfois des vulnérabilités critiques lesquelles un malfaiteur peut exploiter pour prendre le contrôle de votre ordinateur. Il existe des nouvelles variantes d'attaques qui exploitent ces vulnérabilités, appelées le "cross-site-scripting" (XSS), code injection, et quand vous visitez un site Internet (même légitime), cela peut être n'importe quel site, votre ordinateur sera infecté à votre insu. Ni l'antivirus, ni le pare-feu vous épargnerons de cette attaque!!! Peut être que les nouvelles versions auront intégré cette protection, mais actuellement (2008) non ? Vous deviendrez victime du "drive-by-download".**

- **Il existe entre temps des logiciels spéciaux gratuits qui scannent l'ordinateur pour trouver les logiciels "out of date" (où il n'y aura plus de support, ni mises à jour) et les logiciels "non mis à jour" dont il existe des mises à jour qu'il faut absolument télécharger, tels que le Secunia Software Inspector, Personal Software Inspector (PSI), Update Star, SUMO, pour ne nommer que ceux-ci...**

- **Pour les amateurs de jeux en ligne (online games), ne désactivez pas votre pare-feu ou essayez de désactiver certains ports du PC pour que vous puissiez jouer sans que le firewall (pare-feu) vous bloque l'accès à ces jeux. Il existe des suites de sécurité qui ont des options avancées pour les joueurs en ligne, comme par exemple GDATA à des prix avantageux de 35,95 € (août 2008) pour une licence d'une année, ainsi que Norton Internet Security 2009 et qui permettent ainsi de jouer en ligne en toute sécurité.**

- **Installez deux navigateurs (browsers), Internet Explorer (version 7 pour août 2008) pour pouvoir télécharger manuellement les mises à jour de Microsoft (Windows) et Mozilla Firefox pour naviguer sur Internet. Mozilla Firefox est plus sécuritaire que l'Internet Explorer pour l'instant (août 2008).**

- **Protégez-vous contre le cross-site-scripting (XSS) en installant "NoScript" sur Firefox.**

- **Vérifiez les logiciels installés sur votre (vos) ordinateur (s) pour contrôler s'il n'y en pas de logiciels malveillants, dont des faux antispywares (rogue antispyware [EN]) et/ou des logiciels à risque haut.**

Pourquoi existe-t-il des vulnérabilités ?

Les vulnérabilités, ou failles de sécurité, correspondent à des erreurs de conception ou de programmation des logiciels.

Ces "bugs" peuvent être exploités par des hackers ou pirates pour endommager une machine, en prendre le contrôle, lire des données, voire les modifier. Les failles concernent tous les logiciels : les systèmes d'exploitation comme les familles Windows, Unix, Linux, MacOS, les applications, mais aussi les logiciels des routeurs, switchs ou Firewalls.

Les failles de sécurité se corrigent soit par une reconfiguration du système, soit par l'ajout d'un correctif de sécurité, ou patch de sécurité.

Les administrateurs systèmes et réseaux doivent donc suivre la publication des nouvelles failles pour mettre à jour leurs systèmes et s'assurer que "leurs portes sont bien fermées".

Le « **Cross-Site Scripting** » (**XSS**) est une infection d'un site Internet, qui en fait de celui-ci un **site Internet frauduleux**. Ce site Internet infectera tous les visiteurs qui disposent d'un ordinateur non sécurisé ou mal sécurisé !!! Récemment le «**Cross-Site-Scripting** » a fait aussi son apparition au Luxembourg, dont même le ministère de l'économie Luxembourgeois a cru étant nécessaire de publier un communiqué de presse.

Les gens qui travaillent avec un ordinateur sans avoir installé des mesures de protection adéquates prêtent leur ordinateur (à leur insu) aux cybercriminels pour que ceux-ci gagnent de l'argent facile avec le matériel d'autrui, et ceci avec des actions illégales !!!

- **Installez aussi un "antirootkit" et faites-en minimum un scan par mois avec cet outil. Il existe différents outils "antirootkit" gratuits, tels que (liste non exhaustive) :**

AVG antirootkit gratuit, Sophos antirootkit, F-Secure BlackLight Beta, Panda Anti-Rootkit,
Veuillez lire aussi mon didacticiel sur F-Secure BlackLight Détecter et éradiquer les rootkits.

- **Veillez à télécharger des logiciels gratuits que sur des sites de confiance, tels que (liste non exhaustive) : Télécharger.com, Clubic.com, Libellules.ch, Computer Bild (DE), PC Welt (DE), PC Magazin (DE), COM Magazin (DE), CNET Donload.com (EN), ZDNET (FR), etc.**

- **Dès que vous avez terminé votre session Internet, débranchez votre routeur.**

- **Quand vous partagez l'ordinateur à la maison en famille, veillez à ce que l'emplacement de celui-ci soit dans une pièce bien visible par tout le monde (surtout par les parents). De cette façon les enfants pourront à tout moment vous demander (et qui sait aussi donner) conseil. Le risque d'actions illégales est aussi réduit, mais jamais zéro !**

- **Introduisez une charte d'utilisation de la place informatique à la maison, responsabilisez vos enfants et vous même, les mêmes droits et obligations pour tout le monde. Veuillez lire aussi mon didacticiel "La sécurité à la maison (et ailleurs) bien appliquée".**

- **Quand vous partagez l'ordinateur à la maison en famille, veillez à bien configurer votre ordinateur. Créez un seul compte "administrateur" (tous les droits) et un compte unique "limité" (guest [EN]) pour chaque utilisateur avec mot de passe obligatoire. Par exemple : Jean (père) comme administrateur (le chef), Pauline, Christophe avec des comptes utilisateurs limités montrant leurs noms et avec des mots de passe différents. De cette façon les enfants n'auront pas le privilège de tout pouvoir télécharger, ce sera vous (parents, responsables) qui devront autoriser le téléchargement sur votre session "administrateur" et puis le répartir en réseau (si présent) afin que les autres utilisateurs puissent l'utiliser.**

Qu'est-ce qu'un réseau de zombies (botnet)?

Le réseau de zombies est un réseau d'ordinateurs infectés par un programme malveillant de type Backdoor qui permet au cybercriminel de prendre à distance les commandes des machines infectées (séparément, d'un groupe d'ordinateurs du réseau ou de l'ensemble du réseau).

Les programmes malveillants de type Backdoor développés spécialement pour bâtir des réseaux de zombies sont des bots. Ces programmes exploitent les failles présentes sur les ordinateurs.

Les réseaux de zombies possèdent des ressources de traitement considérables, ils sont une arme cybernétique terrible et constituent une source de revenus illégitimes pour les individus mal intentionnés. Qui plus est, le maître du réseau de zombies peut administrer les ordinateurs infectés depuis n'importe où, qu'il s'agisse d'une autre ville, d'un autre pays ou d'un autre continent. Via Internet et grâce à son organisation, il peut « gérer » en préservant l'anonymat.

Le propriétaire de l'ordinateur infecté ne soupçonne même pas que sa machine est utilisée par des individus mal intentionnés. C'est la raison pour laquelle les ordinateurs infectés par un bot qui sont placés sous le contrôle secret des cybercriminels sont appelés des zombies et le réseau qu'ils forment devient un réseau de zombies.

Dans la majorité des cas, les ordinateurs qui figurent dans les réseaux de zombies sont des ordinateurs de particuliers.

http://www.viruslist.com/fr/analysis?pubid=200676152#l11

- **Ordinateur personnel : créez aussi un compte limité, intitulé "Internet" que vous utilisez pour surfer sur Internet. Ceci limite les dangers de se faire attaquer.**

- **Faites des "backup", des sauvegardes de vos fichiers sur un médium de sauvegarde extérieur (disque dur externe). En cas d'un crash du disque dur vous pouvez alors toujours récupérer vos données. Remarque : un disque dur a une durée de vie de +/- 5 années seulement. Un crash peut être fatal, pertes de données, peut être des photos et documents uniques non reproductibles. Au cas où cela vous arrive (ou est arrivé), vous avez quand même une petite chance pour récupérer vos données perdues en utilisant un logiciel gratuit de récupération de données, tels que PC Inspector File Recovery, Recuva, Undelete Plus, TestDisk & PhotoRec**

- **Changez les paramètres par défaut de votre routeur. Changez absolument le mot de passe de votre routeur, car les données du mot de passe par défaut sont connues par les cybercriminels et en scannant le web ils pourraient trouver chaque routeur "type" et de cette façon manipuler toute action et se l'approprier pour...**

- **Vos outils de protection (antivirus, firewall et suites de protection) sont munis d'une fonction de protection par mot de passe. Utilisez cette fonction en l'activant et en intégrant un mot de passe personnalisé (rappelez-vous de choisir un mot avec plus de 8…). Si jamais un intrus essayait de "bypasser" (court-circuiter) votre protection il devrait d'abord savoir le mot de passe pour le faire, chose pas impossible pour lui de le trouver, mais vous ne lui facilitez pas la vie...**

Conseil :

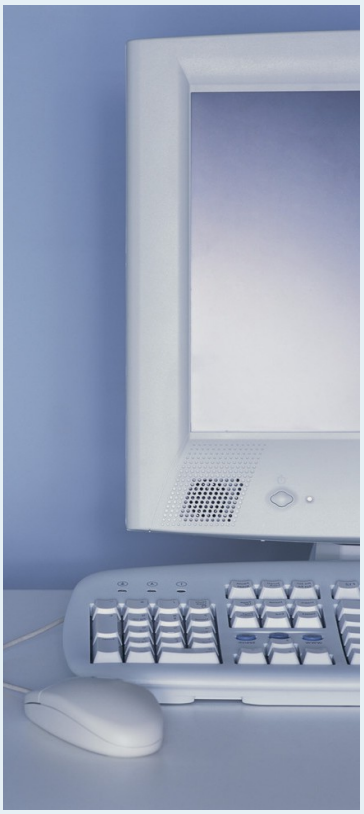
Visitez le site Internet de VODECLIC http://www.vodeclic.com/parcourir/accueil, où vous trouverez beaucoup de tutoriels, des vidéo-formations gratuites lesquelles vous expliquent en détail comment travailler avec certains programmes et logiciels.

Logiciels de sécurité :

http://www.vodeclic.com/parcourir/categorie/6-securite

Il existe aussi une rubrique pour les Mac !!!

http://www.viruslist.com/fr/analysis?pubid=200676152#l11



La vigilance et l'information sont le premier pas envers la sécurité

Actuellement il y a tellement de vulnérabilités, arnaques et attaques que les internautes (nous, ceux qui surfent sur Internet) n'arrivent presque plus à suivre et que nous ne savons plus quoi faire pour nous protéger.

De ce fait **il est devenu nécessaire de rester informé sur ce qui se passe sur Internet, de savoir qu'elles sont les nouvelles menaces qui nous guettent.**

Internet Monitor
http://www.internetmonitor.lu
vous donne cette possibilité

Internet Monitor www.internetmonitor.lu est un magazine qui se consacre à la **sécurité informatique domestique** des ordinateurs et à la **protection des enfants**. **Internet Monitor offre des didacticiels pédagogiques** qui peuvent être téléchargés **gratuitement**, des **outils gratuits de contrôle de la sécurité** et un **newsletter**, ainsi que des **vidéos pédagogiques**.

Internet Monitor offre aussi la syndication de contenu, appelé aussi des « **Fils RSS** », simple à intégrer dans chaque site Internet et à lire avec un « **RSS Reader** » au format « **RSS** » et « **Atom** ». L'abonnement gratuit peut se faire ici www.internetmonitor.lu/xml/syndication.rss.Il vous est aussi possible de **lire les « Fils RSS » (nouveautés de la sécurité) sur votre cellulaire (Handy, GSM, Bluetooth) à l'adresse suivante :**

http://www.internetmonitor.lu/m.

Toolbar gratuite :

http://internetmonitorlu.ourtoolbar.com

Veuillez aussi vous abonner à nos cours pédagogiques gratuits au site Internet du Ministère de l'Éducation nationale « MySecureIT » : http://www.mysecureit.lu.

Mieux vaut prévoir que guérir !!!

Apprentissage à la « Sécurité PC et Internet » :

http://tinyurl.com/5mvs53