TYPOLOGIE DES LOGICIELS MALVEILLANTS

Spyware :

- Définition : Logiciel espion qui collecte des données personnelles avant de les envoyer à un tiers, comme transmettre les données saisies grâce au clavier par exemple.

- S'en protéger : La plupart des logiciels indésirables infiltrent votre ordinateur suite à une action ou à un manque d'action de votre part. Voici quelques conseils pour éviter les spywares ou adwares non souhaités :

- **Sélectionnez soigneusement ce que vous téléchargez sur votre ordinateur.** Assurez-vous d'avoir besoin d'un programme avant de le télécharger. Si vous n'avez jamais entendu parler du développeur du logiciel, consultez son site Web attentivement de manière à en apprendre plus sur les personnes à l'origine de la technologie en question, ainsi que sur la technologie elle-même. Méfiez-vous des programmes ActiveX, car cet outil est réputé pour installer des spywares sur votre ordinateur à votre insu. Vous avez la possibilité de désactiver l'outil ActiveX via les préférences de votre navigateur et de le réactiver uniquement pour les sites fiables le requérant.
- **Lisez les accords de licence**. La lecture de ces accords est souvent laborieuse, mais évitez de vous contenter de cocher la case "J'accepte" au bas de l'accord sans même en avoir lu le contenu avant d'installer tout logiciel gratuit. Veillez donc à lire attentivement l'intégralité de chaque contrat de licence à la recherche d'indications relatives aux activités de collecte de données, qui pourraient désigner l'installation de spywares et d'adwares en plus du logiciel téléchargé.
- Attention aux faux outils de lutte contre les spywares. Internet regorge d'outils "antispyware" présentant une action très restreinte ou inexistante pour la protection contre les spywares. Certains sont même nuisibles. Les développeurs de ces outils offrent parfois des analyses gratuites de votre système, conduisant invariablement à l'identification de centaines de programmes indésirables sur votre ordinateur. Ils vous proposent alors immédiatement d'investir dans leur produit fictif.
- Méfiez-vous des publicités au clic. Essayez d'éviter les programmes (surtout les gratuits) qui font clignoter des publicités au clic. Leur présence doit vous alerter. Lorsque vous cliquez sur ces publicités, les chances sont grandes que votre réaction soit surveillée

- Exemples : Babylon Translator ; GetRight ; Go!Zilla ; Download Accelerator ; Cute FTP

Adware :

- Définition : ils inspectent les sites visités par leurs utilisateurs afin d'afficher des publicités ciblées, sous la forme de fenêtres pop-up ou de bannières. De nombreux programmes parrainés par de la publicité intègrent des adwares installés souvent à l'insu des utilisateurs.

- S'en protéger :

1. Pensez à décocher les logiciels proposés lorsque vous installez un logiciel (*barres d'outils et autres gadgets inutiles*)
2. Téléchargez vos logiciels depuis les sites des éditeurs, jamais sur un site tiers (comme *01Net, Softonic*...)
3. Ne cliquez pas sur les publicités trop voyantes, à caractères pornographiques ou grossièrement mensongères ("gagner 1 000€ par semaine" par exemple)
4. Activer la protection de votre Antivirus dans les réglages contre les LPIs / PUP.
   PUP : Potential Unwanted Program (*Programme potentiellement indésirable*)
   LPI : Logiciels Potentiellement Indésirables
5. Utilisez WOT (Web-Of-Trusft) sur votre navigateur.
6. Bloquer les publicités intrusives avec AdBlock Plus
7. Bloquer les sites malveillants avec HOSTS Anti-PUPs/Adware

- Exemples : Mirar Toolbar, Oemji Toolbar, Zango Toolbar, Adssite Toolbar

Redirecteur de page :

- Définition : Une redirection consiste à rediriger le visiteur d'une page web vers une nouvelle adresse. Ainsi, si l'utilisateur tape : http://www.adresse-depart.com, il va automatiquement être redirigé vers l'adresse http://www.adresse-arrive.com, et ce sans action particulière de sa part.

- S'en protéger : La seule prévention d'une redirection malveillante est de vérifier durant que l'adresse web chargée dans la barre d'adresse est identique à celle affichée à l'initial

- Exemples : //////

Spam :

- Définition : courriel indésirable est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires.

- S'en protéger : Afin d'éviter les spams dans sa boîte mail, on peut utiliser un filtre anti-spam, et il est préférable de ne pas utiliser son adresse mail sur le net, et de ne pas opter pour une adresse mail trop facile.

C'est aléatoire; ça ne dépend pas du nom de domaine, c'est juste une question de chance. De toute façon, avec les scanners d'adresse email, une adresse finira par être découverte un jour ou l'autre, question de temps !!. Mais statistiquement, on minimise les risques en évitant de laisser son adresse partout...

Si vous avez besoin de communiquer malgré tout votre adresse email pour recevoir des informations, vous pouvez utiliser un service gratuit d'adresse email jetable.

ou bien un service payant "anti-spam Plus" (d'un tiers prestataire) filtrant à partir d'une blacklist commune, qui se greffe sur le portail Webmail existant.

Le filtrage bayesien permet d'éliminer une grande partie des SPAMs grâce à un marquage permanent de votre part.

- Exemples : @wewmail.com ; @air-email.com ; @ais-france.com ; @012.net.il ; @email.fr

Dialer :

- Définition : Composeur (en anglais, *dialer*) est un terme générique qui désigne un logiciel permettant de raccorder un ordinateur à un autre ordinateur, à un appareil électronique, au réseau Internet ou à un autre réseau numérique.

- S'en protéger : Afin de lutter contre les dialers, il est important d'installer un pare-feu et de désactiver ActiveX parce que la majorité des composeurs s'installent par cet intermédiaire

Comme la grande majorité des *composeurs* s'installent par l'intermédiaire d'un contrôle ActiveX, la désactivation de cette technologie dans Internet Explorer réduira grandement le risque. La technologie ActiveX n'a toutefois pas que des applications malicieuses, loin de là. Vous pouvez par exemple effectuer en ligne, gratuitement, une recherche des virus sur votre ordinateur, sur le site web de la firme Symantec, grâce à un contrôle ActiveX. (Pour vous en convaincre: http://security2.norton.com)

ActiveX n'est donc pas une mauvaise technologie en soi. Mais considérant qu'elle est souvent utilisée dans le but de vous piéger, et que les sites web l'utilisant à bon escient sont, dans l'immensité du web, relativement rares, nous vous recommandons de la désactiver. Une procédure simple de désactivation d'ActiveX est expliquée en détails plus bas dans cette page. Soyons clairs, ActiveX est parfois très utile et même nécessaire. (Le meilleur exemple en étant le site de mise à jour de Microsoft, Windows Update, dont nous parlerons plus bas.) Le désactiver complètement vous protège des *composeurs*, mais vous vous rendrez compte qu'il faudra parfois le réactiver temporairement.

L’autre façon de se protéger, qui est probablement la plus sûre, est l’installation d’un logiciel coupe-feu. Un coupe-feu agit comme un filtre entre votre ordinateur et Internet, vous rapportant toute transmission suspecte pour s’assurer que vous voulez l’autoriser. ZoneAlarm est un excellent coupe-feu disponible gratuitement en version d’essai.

- Exemples : 00d Dialer ; 23aw0001 Dialer ; 764 Dialer ; Access ; All-In-One Telcom

Trojan :

- Définition : Un trojan, ou Cheval de Troie, est un programme utilisé comme véhicule pour introduire dans un dispositif un ou plusieurs autres programmes, généralement des parasites, cachés à l'intérieur du premier.

- S’en protéger : Afin de se protéger des trojans, il suffit d'installer un pare-feu (exemple : ZoneAlarm Pro Firewall ; Outpost Firewall Pro ; Jetico Personal Firewall), c'est à dire un programme filtrant les communications entrant et sortant de votre machine.

- Exemples : Socket23 ; Back Orifice ; Vundo ; Darkcomet-RAT ; LANfiltrator ; Blackshades ; Hadès-RAT ; FlashBack

Virus :

- Définition : Programme malveillant destiné à endommager ou freiner le fonctionnement d'un système informatique, il a pour but de se répandre le plus possible

- S’en protéger : Pour se protéger des virus, il est nécessaire de maintenir un ordinateur à jour, utiliser un logiciel anti-virus (exemple : Kaspersky anti-virus ; Eset nod32 anti-virus ; Antivir ; Avast) mais aussi ne pas télécharger des programmes suspects sur des sites douteux

- Exemples : Sirefef ; Reveton ; Dorkbot ; DNSChanger ; W32/Frame

Keylogger :

- Définition : En informatique, un enregistreur de frappe (en anglais, keylogger) est un logiciel espion ou un périphérique qui espionne électroniquement l'utilisateur d'un ordinateur. Le but de cet outil est varié, et peut se présenter sous des airs de légitimité1, mais il ne peut être assuré qu'en espionnant l'intimité informatique de l'utilisateur.

Le terme keylogger est parfois utilisé pour parler de l'espionnage des périphériques d'entrée/sortie, bien que ces espions puissent être nommés spécifiquement en fonction du périphérique visé, comme les mouseloggers pour la souris.

- S’en protéger : Afin de lutter contre les keyloggers, il ne faut pas installer de logiciels dont la provenance est douteuse. Faites attention lorsque vous vous apprêtez à utiliser un ordinateur qui ne vous appartient pas et en cas de douter, n'hésitez pas à utiliser un clavier visuel.

- Exemples : ////////////////////

Vol d'identité :

- Définition : L'usurpation d'identité (improprement qualifiée de vol d'identité) est le fait de prendre délibérément l'identité d'une autre personne vivante, généralement dans le but de réaliser des actions frauduleuses commerciales, civiles ou pénales, comme régulariser sa situation au regard de l'émigration, accéder aux finances de la personne usurpée, ou de commettre en son nom un délit ou un crime, ou d'accéder à des droits de façon indue.

- S'en protéger : Afin de se protéger contre le vol-d'identité, il peut-être utile de changer régulièrement de mots de passe, d'utiliser une adresse mail non évidente et de la diffuser le moins possible sur internet

- Exemples : usurpation d'identité

Réseaux sociaux :

- Définition : les réseaux sociaux sont des applications malveillantes puisqu'il nous demande des informations personnelles et on peut nous même postez des publications (photos, vidéos,…). Les réseaux sociaux sont la cible idéale pour les cybercriminels, les voleurs d'identité, les auteurs de virus, les spammeurs et les pirates informatiques, les arnaqueurs…

- S'en protéger : Afin de se protéger sur les réseaux sociaux, il est important de maintenir un comportement identique à celle de la vie réelle. C'est à dire qu'il faut mesurer la valeur de ses propos, de ne pas poster toutes informations influençant sur votre vie privée ainsi que de bien protéger son compte avec un mot de passe complexe et changer régulièrement

Exemple :

- Pour Facebook, il s'agit de "malware" (logiciels malveillants) et de "phishing" (messages incitant àcommuniquer des informations confidentielles comme des coordonnées bancaires).

- Sur Twitter, le problème majeur est la facilité avec laquelle il est possible de "spammer" (envoyer des messages indésirables). N'importe qui peutcréer un compte Twitter, suivre des milliers de personnes qui le suivront ensuite en retour, et poster des messages contenant des adresses de sites malveillants.

Mobiles :

- Définition : les téléphones mobiles sont porteurs de malveillance. En effet à travers les mobiles les utilisateurs peuvent être la cible d'attaque, de fraude, de vols et de perte de données ainsi que d'attaque par sms(sms frauduleux, arnaque…)

- S'en protéger : Afin de se protéger contre les harcèlements, il est important de limiter la diffusion de son numéro de téléphone portable

- Exemples : arnaques par SMS, harcèlement par téléphone ou moral, publicités mensongères

Cyber harcèlement :

- Définition : c'est une forme d'agression qui se concrétise par la réception répétée de messages par SMS ou sur le Net (MSN, e-mail, réseaux sociaux…).

- Exemples : Liste de cyber harcèlement : l'utilisation de surnoms dévalorisants, moqueries, insultes, menaces, humiliations, chantages, propagations de fausses rumeurs, pratiques de discrimination, exclusion et mise à l'écart.