Source de cet article : http://forum.malekal.com/pourquoi-comment-fais-infecter-t3259.html

Pourquoi et comment je me fais infecter sur internet

Cet article explique comment les infections se propagent via internet.
Après avoir lu cet article, vous connaîtrez les mécanismes utilisés pour installer les infections sur votre ordinateur ainsi que des conseils afin de mieux le protéger.

NOTE : La connaissance de certaines notions et expressions est nécessaire pour appréhender cet article... Reportez-vous au Glossaire : Notions et Expressions pour suivre cet article.

L'installation d'application/virus

Pour installer une application.. vous devez donc exécuter le programme d'installation.
L'installation est seulement possible si vous avez les droits administrateur.

Le schéma ci-dessous illustre ceci :

Les infections sont des programmes elles aussi, pour s'installer sur un système elles ont donc besoin "d'un programme d'installation".
Il existe donc un fichier contenant l'application, qui, une fois exécuté sur l'ordinateur, va installer l'infection sur le système.
Le fichier contenant l'application se nomme le dropper (voir la page : Dropper & Payload : Explications.. une fois exécuté, il "drop" (du verbe to drop --> déposer) l'infection dans le système.

Le schéma ci-dessous montre un dropper téléchargé depuis internet.. S'il est exécuté avec les droits "Administrateur" et si l'antivirus ne détecte rien, l'ordinateur est infecté.

Ceci montre plusieurs choses :
On voit tout de suite que le maillon faible est le dropper. Si le programme d'installation d'une application est endommagé ou s'il ne fonctionne pas, l'installation de l'application est impossible. Pour le dropper, c'est la même chose, s'il est détecté par l'antivirus, c'est gagné puisque l'infection ne pourra pas s'installer.. malheureusement ce n'est pas aussi facile.
Si le dropper n'est pas exécuté avec les droits "Administrateur".. l'installation dans le système est impossible. Malheureusement par défaut sous Windows, l'utilisateur est "Administrateur", par manque de connaissances et par facilité.. l'utilisateur tourne et surfe tout le temps avec les droits administrateurs.

Ceci montre aussi qu'ouvrir n'importe quel fichier qui vous tombe sous la main, sans vérifier la source, rend l'infection de votre ordinateur très facile. Certains diront "pas grave mon antivirus me protège" : oui et non... ! Les droppers utilisent de nombreuses méthodes pour que les antivirus ne détectent pas l'infection (cryptage, package etc..), plusieurs milliers de nouveaux droppers (et donc d'infections) sortent par jour afin de noyer les éditeurs de logiciels de sécurité et s'assurer de l'infection des ordinateurs. Pour plus d'informations sur les Antivirus VS droppers, je vous invite à suivre cet article un point sur les antivirus

L'antivirus reste le dernier rempart, compte tenu du fait que les utilisateurs ne font généralement pas attention à ce qu'ils téléchargent et ont souvent de mauvaises habitudes (utiliser des cracks, sites pornographiques), on peut voir que l'antivirus reste le dernier maillon dans le système pour prévenir l'installation d'une infection. Malheureusement, les éditeurs de logiciels de sécurité ont de plus en plus de mal à contenir les auteurs de malwares ce qui vous rend de plus en plus vulnérable.

Les failles de sécurité à la rescousse des hackers

Les exploits sur les sites WEB
Vous allez voir aussi que même en faisant très attention.. la simple visite d'un site ou la visualisation d'une vidéo même sur des sites reconnus (Youtube, daylymotion etc..) peuvent mener à l'infection.

Imaginez que le téléchargement et l'installation de l'infection soit automatique sans

intervention humaine. Cela fait peur non ? et bien c'est possible via les failles de sécurité!

Lorsque vous surfez ou visualisez des vidéos, écoutez des mp3 etc.. vous utilisez des logiciels (navigateur WEB, lecteur audio/vidéo etc..).
Régulièrement des failles de sécurité sont publiées sur ces logiciels.. les auteurs de malwares sautent alors sur l'occasion pour exploiter ces failles et tendre des pièges aux internautes afin d'infecter leurs ordinateurs.

Dans le cas d'une faille sur le navigateur WEB (ou un de ses composants Java, Flash, Adobe Reader etc..), le piège est très facile à tendre :
1/ L'internaute se connecte via un site piégé.. pour attirer l'utilisateur.. l'auteur de malwares va bien sûr créer un site sur un thème à la mode pour attirer un maximum de monde afin d'infecter un maximum d'ordinateurs (cracks, site pornographique, émoticons, jeux etc..).
L'auteur de malware peut aussi hacker des sites WEB existants qui ont déjà une bonne audience. Ce dernier insère une iframe qui va faire télécharger le contenu néfaste lors de la visite de la page (voir : Les Exploits sur les sites WEB piégés, exemple contret: IE6 VS IE 7 : Pourquoi maintenir son navigateur à jour ?)

2/ L'internaute avec son navigateur non à jour se connecte sur le site, et ce faisant télécharge la page piégée, l'exécution du dropper se fait alors automatiquement en exploitant la faille du navigateur WEB.
Dans le cas où l'antivirus détecte le dropper (ou le fichier exploit).. l'internaute recevra une simple alerte de son antivirus ne se doutant pas que son navigateur WEB n'est pas à jour et qu'il est vulnérable.
Dans le cas où l'antivirus ne voit rien, la machine est infectée.

Le schéma ci-dessous illustre ceci. La page du forum Le danger des cracks ! montre aussi une infection depuis un site de cracks exploitant une faille de sécurité.. vous pouvez voir comment l'infection du système est fulgurante.

L'exploitation de failles de sécurité ne s'arrête pas au niveau des navigateurs WEB.. à l'heure où les sites de vidéos en ligne sont à la mode.. les failles sur les lecteurs vidéos/audios sont une aubaine pour les auteurs de malwares.
La visualisation d'une vidéo piégée sur un logiciel vidéo/audio vulnérable peut aussi permettre l'infection d'un ordinateur.

Ces failles sont intéressantes pour les auteurs de malwares car il leur suffit de "pondre" des sites piégés (Ce qu'ils font très bien) pour infecter des ordinateurs.

Les vulnérabilités ne se trouvent pas que sur le navigateur WEB mais aussi sur les composants additionnels comme java ou flash que les utilisateurs ne mettent que rarement à jour.
Encore une fois et toujours, maintenez Windows et TOUS vos logiciels à jour (voir la page :

Tester la vulnérabilité de votre PC

Les failles sur le système d'exploitation
D'autres failles plus dangereuses sont aussi très attendues par les auteurs de malwares, ce sont les failles de sécurité à distance sur le système d'exploitation. Celles-ci permettent la création de vers qui se propagent automatiquement d'un ordinateur à l'autre sur la toile.

Pour cela, la faille doit être exploitable à distance, c'est à dire par simple connexion sur l'ordinateur.
L'ordinateur doit bien sûr ne pas être à jour (sinon la faille est corrigée) et ne doit pas posséder de pare-feu (firewall)... puisque le pare-feu filtre les connexions entrantes non désirées.. ce dernier stopperait alors les connexions tentant d'exploiter la faille.

Les ordinateurs infectés envoient alors des requêtes régulières sur internet vers de nouveaux ordinateurs afin de les infecter.
L'infection se propage alors rapidement et automatiquement.
Il est important de comprendre que la simple connexion d'un ordinateur, même durant quelques secondes, sans pare-feu et non à jour permet l'infection

C'est par exemple le cas des vers Blaster/Sasser qui ont à leur époque fait beaucoup parler d'eux.
Blaster
Sasser

Il faut savoir que ces infections sont encore actives puisque beaucoup d'internautes qui se connectent avec des Windows non à jour (Windows 2000 et Windows XP SP1) sans protection.
D'où le fait qu'il faut, si vous réinstallez ces versions de Windows, effectuer quelques préparations afin de se connecter à internet après l'installation de Windows munis d'un pare-feu, pour plus d'informations, vous pouvez vous reporter à l'article Préparer le formatage de son ordinateur

Ce schéma montre la propagation des vers sur internet.

et si on vous faisait exécuter les infections ?

Une autre solution consiste à vous faire télécharger les programmes infectieux.
Vous allez me dire "haha je suis aussi bête pour me faire avoir" ... et bien ça reste à voir!

Les auteurs de malwares font appel au le social engineering pour vous faire télécharger les programmes piégés et croyez moi, ça fonctionne...

Prenons l'infection Magic.Control/Navipromo, comme expliqué sur la page du le social engineering.
Cette infection ouvre des popups de publicités qui rémunèrent les auteurs. Cette infection s'installe via des programmes gratuits... notez qu'il vaut mieux proposer des programmes gratuits que payants, les internautes vont se ruer dessus.
Des thèmes qui plaisent (surtout aux ados) : émoticons pour MSN ou mail, sudoku, jeux en ligne...
Les internautes naifs qui vont voir les pubs vont se dire "wow un super programme d'émoticons pour mes mails/msn ou jeux...." clicquent et se retrouvent sur un joli site... qui semble faire sérieux... et oui l'important est de donner l'impression que le site est sérieux...
On écrit en gros que c'est gratuit, une petite bannière "NO SPYWARE", plusieurs bannières de publicités pour faire connaître et les internautes se font avoir à tour de bras.

On a aussi Les faux codecs qui sont proposés en téléchargement pour visualiser des vidéos pornographiques..
pour les crakeurs des cracks piégés sur des sites WEB ou via des infections qui créent de faux cracks sur P2P, voir Le danger des cracks.

En général, ce sont les ados qui sont ciblés et ça marche très bien... puisqu'ils téléchargent "tout et n'importe quoi" sans faire un minimum attention... et faisant une confiance aveugle à leur antivirus.

Ceci ne sont que des exemples... Vous pouvez parcourir le site et le forum pour découvrir d'autres pièges tendus par les auteurs de malwares.

Conclusion et conseils

Cette page démontre trois choses :

- Surfer sur des sites non recommandés, télécharger des cracks sur des sites ou des réseaux P2P vous conduira tôt ou tard à l'infection. Voir l'article Prévention : Logiciels et sources de téléchargements
- Surfer avec les droits administrateurs vous rend très vulnérable sur internet. Pour pallier à ceci, vous pouvez :
    - lire l'article Pourquoi ne pas surfer avec les droits administrateurs? et la La gestion des utilisateurs - lire l'article Surfer de manière sécurisée! qui vous permet de surfer depuis un système d'exploitation autre que Windows afin de ne pas l'infecter.
    - utiliser le logiciel DropMyRights qui permet de surfer sans les droits administrateurs sans toucher à la configuration Windows. Pour plus d'informations, voir le tutorial DropMyRights
    - Sécuriser un peu plus Firefox de mégataupe sur Zebulon.fr

- Maintenir vos logiciels et votre système d'exploitation à jour, afin de corriger les failles de sécurité, est très important :
    - Pour maintenir Windows à jour, vous pouvez lire Maintenir Windows à jour avec Windows Update
    - Maintenir l'ensemble de vos logiciels à jour (voir Logiciels pour maintenir ses programmes à jour : Scanner votre ordinateur afin de vérifier si vos logiciels comportent des failles de sécurité, pour plus d'informations : effectuer un scan de vulnérabilités

Multiplier les logiciels de protection antispywares etc... ne sert à rien ! voir : Phénomène de sur-multiplication des logiciels de protection, faire trop confiance à son antivirus est aussi une erreur.
Ne partez pas du principe que si vous avez un antivirus, vous pouvez télécharger "n'importe quoi" en pensant qu'il va vous détecter les menaces!
La discipline et un minimum de connaissances quant aux pièges tendus par les auteurs de malwares font la différence.

Plus globalement, vous pouvez lire les pages :

- Infections VS Antivirus
- La sécurité de son PC, c'est quoi ?
- Sécuriser son ordinateur et connaître les menaces qui vous liste les moyens de propagation et menaces sur internet et vous donne des conseils pour sécuriser votre ordinateur.

Pour aller plus loin, ou si la sécurité vous interresse, voici des documents/reportages sous forme de vidéos :

- 25 ans de malwares et mise à jour du Projet AntiMalwares
- Envoyé Spécial : Cybercriminalité
- Vidéo : La guerre invisible (Arte) - (botnet, cyberguerre etc)

Dernière édition par Malekal_morte le 03 Juin 2007 14:20, édité 3 fois.

Première régle élémentaire de sécurité : on réfléchit puis on clic et pas l'inverse - Les fichiers/programmes c'est comme les bonbons, quand ça vient d'un inconnu, on n'accepte pas