TEGAM International
www.tegam.fr
Tel : 01.64.66.15.97

Les virus impuissants et les virus de laboratoire :

Qui fait les virus ? Et qui fait les virus impuissants ?

Contrairement aux légendes répandues, aujourd'hui, créer un virus est une chose simple et non pas réservée aux petits génies. Un codeur de virus n'a qu'à utiliser des parties de virus, et des informations pour le fabriquer, généralement disponibles sur l'Internet, et en faire une nouvelle variante de l'une des quatre familles : BOOT, EXE, MACRO ou VER. Créer et diffuser un nouveau virus relève d'une agressivité aveugle et non d'un exploit technique. Rien à voir avec l'effort de création nécessaire pour développer un logiciel utile. La création et la propagation d'un virus informatique sont eux des actes de vandalisme, commis pour nuire, par des individus malveillants, pervers, ou psychopathes. Ces actes ne sont plus considérés comme bénins, mais assimilés à du cyber-crime. Aux Etats-Unis le cyber-crime est officiellement considéré comme du terrorisme. Il existe des milliers de virus qui ne vont jamais se propager, et donc ne constitueront jamais un danger. Ces virus sont et resteront des virus impuissants.

Les virus impuissants :

Comme les virus biologiques, les virus informatiques se propagent, d'un ordinateur à l'autre, et d'un réseau à l'autre. Pour qu'un virus se propage, il ne suffit pas qu'il fonctionne sur un PC. Un programme viral doit être capable de se déplacer sur d'autres PC, **dans des conditions d'utilisation réelles.** Passons en revue les différentes règles qui font qu'un virus est susceptible d'être dangereux, en se propagent et d'arriver jusqu'à votre ordinateur pour le contaminer. Nous tenons compte des conditions de « survie » pour les virus infecteurs de fichiers (ceci est différent pour les vers) :

- **Première règle de survie pour un virus infecteur de fichiers :** rester inaperçu et ne pas gêner l'utilisation de l'ordinateur. Un virus qui détruirait systématiquement tout sur son passage ou qui tuerait son hôte, n'arriverait pas à passer à un autre ordinateur. D'une part il serait rapidement détecté, et d'autre part en détruisant le système il se détruirait aussi lui-même et arrêterait ainsi sa propre propagation. S'il déclenche une charge destructive, le virus doit veiller à le faire à certaines dates seulement, mais certainement pas souvent. Un virus infecteur de fichiers qui détruirait tout sur son passage s'auto détruirait et ne se propagerait pas au delà d'un ou deux ordinateurs.

- **Deuxième règle :** pour « réussir », un virus doit pouvoir fonctionner sur les systèmes d'exploitation et plates-formes les plus courantes. Par exemple, un virus tel que Win95.Zerg fonctionnant seulement en tant que VxD sur plate-forme Windows 95 a très peu de chances d'infecter une quantité de PCs aujourd'hui : étant trop dépendant de ce type de plate-forme, son infection s'arrête en effet chaque fois qu'il atteint un poste Windows NT / 2000 / XP, voire même d'autres plates-formes Win 9x incorrectement supportées. D'ailleurs, la preuve en est qu'il est quasiment impossible de trouver de l'information sur ce virus tant il est rare (à ne pas confondre avec le macro-virus Zerg). Comme pour tout autre programme, un virus qui a été programmé sur une ancienne plate-forme, ou un virus qui est trop dépendant d'une certaine configuration comporte aussi plus de bugs, plus de problèmes de stabilité et potentiellement plus de conflits avec d'autres drivers sur les machines rencontrées, et ne pourra pas se propager correctement. Inutile de dire que dans le cas d'un virus, il est impossible « d'organiser » un bêta-test pour « stabiliser son virus »...

- **Troisième règle:** un virus infecteur de fichiers doit obligatoirement infecter des fichiers qui sont souvent échangés. Cela paraît une évidence, mais certains analystes ou pseudo-experts (*) l'oublient souvent dans leurs tests et simulent manuellement des situations et opérations qui sont

en réalité improbables. Un virus dont l'infection repose sur la modification d'autres fichiers BAT, par exemple, n'a aucune chance de survivre. Combien de fois avez vous échangé des fichiers .BAT ces derniers mois ? De tels virus ont déjà été essayés (la technique pour les créer existe depuis longtemps), mais aucun de ceux-là n'a jamais réussi à se propager. Ceci à l'opposé des « macro-virus » qui, malgré leur simplicité technique, avaient réussi à se propager très vite à cause du fait qu'ils se propagent par fichiers documents, qui sont échangés beaucoup plus souvent que tout autre type de fichier. Donc les techniques les plus sophistiquées ne sont pas toujours les plus réussies dans le domaine des virus.

- Le mode d'infection peut lui aussi être une barrière pour la propagation d'un virus. Les virus "compagnons", par exemple, sont une ancienne idée (plus de dix ans) qui n'a pourtant jamais réussi à infecter en réalité. Le concept consiste non pas à ajouter le virus aux fichiers hôtes, mais à s'y substituer. Par exemple, plutôt qu'infecter un fichier WINWORD.EXE, le virus renommerait celui-ci en WINWORD.CLEAN et mettrait sa propre copie virale à la place de WINWORD.EXE. Deux problèmes : d'abord, le virus qui est dupliqué partout sur le disque devient extrêmement visible. De plus, pour le propager, l'utilisateur devrait procurer aux utilisateurs avec lequel il est en contact le fichier infecté, ce qui en réalité demande presque que l'utilisateur le fasse exprès. La preuve est, une fois de plus, que ces virus existent mais ne sont pas dans la « nature ».

A qui profitent les virus impuissants ?

La très grande majorité des virus impuissants sont écrits avec de grandes ambitions, par des individus peu compétents et pas suffisamment connaisseurs. Ces virus ne se propageront jamais. Trop souvent, des médias ou éditeurs d'antivirus tendent à créer un climat de panique autour de nouveaux « virus-catastrophes », en exagérant largement le danger. Certains éditeurs d'antivirus maintiennent des relations étroites avec les auteurs de ces virus, pour pouvoir être les premiers à annoncer le virus. Combien d'alertes au loup a-t-on vu autour de virus qui n'ont quasiment pas infecté des ordinateurs dans le monde ? Ce genre de virus ne sont pas des virus dangereux car ils ne se propageront jamais dans la nature. On se souvient des alertes catastrophes pour « W2K.Stream NTFS », « Java Black Widow », les prétendus virus de JPG, virus compagnons, virus BAT, infecteurs de fichiers .PAS….

(*) Pour plus d'informations sur les faux experts, les faux virus et les « hypes » (exagérations ou quasi-inventions) sur les virus, nous vous conseillons l'article de du spécialiste Américain Rob Rosenberger : http://www.vmyths.com/fas/fas1.cfm ainsi que les autres ressources disponibles sur ce site.

Les virus et études de laboratoire

Il ne faut pas confondre les virus impuissants avec les virus de laboratoire pour simuler une « démonstration de concept ». Les virus de laboratoire "proof of concept" ont la réelle capacité de se propager, mais ils sont volontairement conçus par leurs auteurs pour ne pas le faire. Ceux-là sont très rares ; ce sont les seuls réellement écrits (et non propagés) non pas pour nuire, mais pour faire avancer la recherche et démontrer aux institutions de sécurité informatique de nouvelles menaces, avant que celles-ci ne prennent forme sur le terrain. On notera dans cette catégorie le premier virus macro « DMV », écrit par un chercheur de façon non anonyme et jamais propagé (ni directement ni indirectement) par son auteur. Ce virus, écrit plusieurs mois avant le premier virus macro propagé à grande échelle, a permis aux développeurs de la sécurité de devancer le danger.

Autre catégorie, les études de laboratoire à des fins préventives : c'est le cas du rapport « GoodLuck » sur les futures méthodes de chevaux de Troie. Il s'agit d'un assemblage théorique de méthodes existantes, qui ne peut être programmé par un individu seul, mais par une équipe (donc, plutôt dans un contexte de terrorisme). Le rapport a été adressé par TEGAM International dans un but préventif aux institutions de défense nationale et à des experts internationaux. Ses idées ont été gardées confidentielles.

TEGAM International a toujours écarté les virus impuissants qui ne posent pas de risque pour l'utilisateur final. Les vrais risques ne sont pas ces virus impuissants comme certains pseudo-experts peuvent le

prétendre pour détourner l'attention sur eux et se « valoriser » et gratifier leur égo...
Le danger réel, ce sont les virus, vers, chevaux de Troie et bombes logiques qui se propagent et qui pourront réellement arriver sur vos ordinateurs. Contre cela, nous offrons la protection la plus fiable. En sécurité, on protège les disques durs de ce qui est susceptible de vous attaquer. Nous le faisons sans avoir à connaître chaque programme malveillant spécifiquement, et nos résultats sur de nombreuses années et nombreux clients font preuve de la fiabilité de notre concept de protection et nos technologies.