

Teamlog - Les virus

par Loïc Hennequin ([Teamlog](#))

Date de publication : 06/05/2002

Dernière mise à jour : 16/07/2004

Cet article décrit les virus et leur principe de fonctionnement par Loïc Hennequin : consultant Teamlog. 06/05/2002

Principes de base

Principes de fonctionnement

Scanner

Moniteurs de comportement

Contrôleurs d'intégrité

Analyseurs spectraux

Analyseurs heuristiques

Terminologie

Les virus canulars ou Hoaxes

Les virus du secteur de boot

Les virus de fichiers exécutables

Les virus macro

Les virus polymorphes

Les virus furtifs

Les virus résidents

Les chevaux de Troie

Les virus compagnons

Les vers

Les bombes logiques

Les virus défensifs

Les virus mailers et mass-mailers

Autres articles et liens

Autres articles

Liens

Principes de base

Principes de fonctionnement

Généralités

Mécanisme de réplication

Ce mécanisme permet au virus de se répliquer.

Il y a plusieurs méthodes pour y arriver :

- * soit en infectant davantage de fichiers
- * soit en utilisant un service réseau pour infecter d'autres ordinateurs

Charge utile

La charge utile est le coeur même du virus, c'est elle qui contient sa capacité de nuisance réelle. Elle peut être l'une de celles-ci :

- * Affichage d'un message,
- * Altérations mineures de fichiers,
- * Destruction du contenu d'un disque dur,
- * Détérioration lente du contenu des fichiers avec ou sans possibilité de restauration,
- * Vol ou diffusion d'informations confidentielles.

Déclencheur

Le déclencheur peut être réglé pour

- * Une action immédiate
- * Une action ponctuelle (un jour particulier)

* Une action répétitive (à chaque démarrage du système, pour un anniversaire)

Mécanisme de protection

Compression

La compression est faite pour limiter la taille du code du virus, pour offrir un plus petit motif pour les anti-virus et pour ne pas attirer l'attention par des pertes de taille de disque.

Polymorphisme

Le polymorphisme permet de limiter la reconnaissance du code par les scanners anti-virus.

Furtivité

Il s'agit ici de rendre plus difficile la détection par l'anti-virus en détournant tous les appels au disque.

Multiplés phases

C'est une méthode exotique de création de virus qui consiste à le faire passer par plusieurs mode d'infection. Le virus peut agir comme un virus macro puis comme un virus résident infectant les fichiers par des macros...

Scanner

C'est la méthode la plus ancienne et aujourd'hui encore la plus utilisée.

Cette méthode présente l'avantage de détecter un virus avant qu'il ne s'exécute sur une machine.

Son principe est de rechercher sur le disque dur toute chaîne de caractères identifiée comme appartenant à un virus. Cependant comme chaque virus a sa propre signature, il faut, pour le détecter avec un scanner que le concepteur de l'anti-virus ait déjà été confronté au virus en question et l'ait intégré à une base de données.

Un scanner n'est donc pas en mesure de détecter les nouveaux virus ou (les virus polymorphes lien vers autre P) (car ceux-ci changent de signature à chaque répllication.)

Dans les années 80, seuls quelques virus existaient, et l'écriture d'un scanner était une chose relativement simple.

Actuellement, avec plusieurs milliers de virus et l'apparition quotidienne de nouveaux modèles, la mise à jour d'un scanner n'est pas évidente car elle représente une somme de travail considérable, et même, quasi-impossible à réaliser.

C'est pourquoi les concepteurs d'anti-virus proposent des mises à jour de la base de donnée tous les jours sur leur site WEB, c'est le seul moyen pour le scanneur de détecter les nouveaux virus.

En général, un scanner contient des champs associés à chaque chaîne de recherche qui lui indiquent où rechercher une chaîne particulière. Cette sélectivité permet de réduire la charge de travail et de rendre plus rapide sa recherche.

Certains possèdent également différents modes de recherche qui orientent celle-ci en fonction de ce que l'utilisateur souhaite. Ils peuvent alors s'intéresser uniquement aux exécutables ou vérifier l'ensemble des fichiers.

Moniteurs de comportement

Les moniteurs de comportement observent l'ordinateur à la recherche de toute activité de type virale et alertent l'utilisateur. En général, un moniteur de comportement est un programme résidant en mémoire que l'utilisateur charge au démarrage du système (AUTOEXEC.BAT) et qui reste actif en arrière-plan en surveillant tout comportement inhabituel.

Ces "comportements inhabituels" concernent :

- * les tentatives d'ouverture de fichiers COM/EXE en lecture/écriture ;
- * les tentatives d'écriture sur les secteurs de partition et de boot ;
- * les tentatives de mise en résidant.

Pour repérer ces tentatives, les anti-virus détournent les principales interruptions de l'ordinateur et les remplacent par l'adresse de leur code.

Les interruptions détournées sont l'int 13H (disque dur), l'int 21H (DOS). Ainsi dès qu'un virus tente d'écrire sur le secteur de Boot, c'est l'anti-virus qui est d'abord appelé, et qui peut ainsi prévenir l'utilisateur qu'un virus tente de modifier le secteur de Boot.

L'anti-virus peut alors éliminer le virus de la mémoire, enregistrer une partie de son code dans la base de donnée et lancer un scanning pour repérer la/les souche(s) sur le disque dur et les détruire.

Contrôleurs d'intégrité

Un contrôleur d'intégrité va construire un fichier contenant les noms de tous les fichiers présents sur le disque auxquels sont associées quelques caractéristiques. Ceci peut simplement être la taille, la date et l'heure de dernière modification ou encore un checksum (somme de contrôle).

Par un checksum ou un code de redondance cyclique (CRC), le contrôleur pourra détecter si une altération s'est produite et alertera l'utilisateur afin que ce dernier puisse prendre des mesures.

Le problème de cette méthode est qu'il peut y avoir des milliers de virus sur une machine, l'utilisateur n'en sera informé que lorsque le virus s'exécutera ou modifiera un fichier.

Les scanners restent actuellement la méthode la plus populaire car elle donne une indication claire et précise sur la situation, et répond aux attentes d'un utilisateur novice en lui indiquant la conduite à tenir : "le fichier 'FICHIER.COM' est infecté par le virus 'TRUC'. Voulez-vous l'effacer ?"

Les anti-virus à base de moniteurs de comportements ont en général moins de succès et sont souvent critiqués par des non-techniciens. En effet les messages du genre : "Tentative d'ouverture en lecture/écriture du fichier 'FICHIER.EXE'. (A)rrêter ou (P)oursuivre ?" peuvent laisser perplexe.

De même, les contrôleurs d'intégrités non pas plus de succès avec des messages comme : "Attention ! Le fichier 'FICHIER.COM' a été modifié !". Un utilisateur novice ne saura certainement pas comment réagir à un tel message.

Pourtant, un scanner idéal est une impossibilité mathématique. En effet, on peut prouver mathématiquement qu'il est impossible de concevoir un scanner parfait qui serait en mesure de déterminer systématiquement s'il y a ou non, un virus présent dans un programme.

Pour ceux qui ont certaines notions de logiques mathématiques, ce problème est identique au problème d'arrêt pour une machine de Turing.

Un scanner réel manque donc de détecter certains virus ou bien de signaler des programmes comme dangereux, quitte à émettre une alarme faussement positive. Ce sont les limitations inhérentes à tout scanner.

Analyseurs spectraux

Tout code généré automatiquement est supposé contenir des signes révélateurs qui pourront être détectés par un algorithme reconnaissant ces modèles.

Une façon très simple d'analyser du code en employant cette technique consiste à rechercher les instructions atypiques générées par un virus polymorphe, mais qui ne sont pas utilisées par des programmes ordinaires.

Ainsi les moteurs de mutations DAME ou TPE génèrent régulièrement des accès mémoire au niveau des limites de segments. Ce n'est pas une programmation très élégante, et la plupart des programmes conventionnels s'en abstiennent.

Techniquement, on peut parler du spectre des instructions machines présentes dans un programme.

Il faut imaginer un espace abstrait dans lequel toutes les instructions possibles et tous les états possibles d'un processeur soient représentés par un point ou un groupe de points.

Il existe un nombre fini de ces points qui peuvent être numérotés. Un programme peut donc être représenté par une série de points ou de nombres.

L'analyse spectrale concerne l'étude de la fréquence d'apparition et des interrelations liées à ces nombres.

Ainsi, le nombre associé à un accès mémoire généré par un moteur de mutation, correspond à un nombre qui ne peut être généré par aucun compilateur normal.

Tout programme générant du code machine, que ce soit un compilateur C, un assembleur ou un virus polymorphe, va n'exploiter qu'une partie de l'ensemble des points de cette espace.

Un compilateur C peut ne jamais utiliser telle instruction. De même un assembleur, pourtant très souple, n'utilisera qu'un jeu restreint d'instructions.

Si on étudie alors l'intégralité des différents jeux de codes machines générés par tous les programmes à même de produire du code machine, on trouve des zones de concordance.

On peut alors écrire un programme qui effectue une analyse spectrale du code machine présent à l'intérieur des programmes pour déterminer les sous-ensembles d'appartenance s'ils existent.

On peut alors déterminer l'origine de ces programmes, savoir que le code a été assemblé par tel assembleur, tel compilateur C ou tel virus polymorphe.

Une autre technique utilisée en analyse spectrale consiste simplement à analyser un bloc de code et à observer si la fréquence des instructions présentes correspond à du code machine normal.

La forme la plus rustique d'une telle analyse consiste à prendre en compte les octets pour décider s'il s'agit réellement de code. Un code chiffré présente un spectre différent d'un code en clair.

En prolongeant cette idée un peu plus loin, si on diagnostique la présence d'une routine de cryptage, on peut utiliser la boucle de décryptage pour décrypter le code et ensuite le réexaminer pour s'assurer qu'il s'agit effectivement de code machine.

Analyseurs heuristiques

L'analyse heuristique concerne la recherche de code correspondant à des fonctions virales.

Elle est différente, dans son principe, d'un moniteur de comportement qui surveille les programmes ayant une action de type viral.

L'analyse heuristique est passive. Elle considère le code comme une simple donnée et n'autorise jamais son exécution.

Un analyseur de ce type va donc rechercher du code dont l'action est suspecte ou malveillante s'il vient à être exécuté.

L'analyse heuristique permet, par exemple, pour les virus polymorphes, de chercher une routine de déchiffrement. En effet une routine de déchiffrement consiste à parcourir le code pour ensuite la modifier.

Ainsi lors de l'analyse heuristique, l'anti-virus essaie de rechercher, non pas des séquences fixes d'instructions spécifiques au virus, mais un type d'instruction présent sous quelque forme que ce soit.

Pour en revenir à notre exemple de virus polymorphes, l'anti-virus cherche une suite d'instructions de lecture suivie d'une suite d'instructions d'écritures.

Cette méthode est donc un peu plus intelligente que les autres, car elle vise à analyser les fonctions et instructions les plus souvent présentes et que l'on retrouve dans la majorité des virus.

Cette méthode permet ainsi, contrairement au scanning, de détecter des nouveaux virus dont la signature n'a pas été ajoutée à la base de données.

L'analyse heuristique peut se réaliser conjointement avec l'analyse spectrale de sorte que si la première indique l'absence de virus, les paramètres issus de l'autre peuvent néanmoins permettre d'émettre un avertissement.

Terminologie

Les virus canulars ou Hoaxes

Généralités

Les virus canulars ne sont pas des virus en tant que tels. Il n'y a aucune technique sous-jacente. Un virus canular consiste simplement à envoyer un message électronique à des personnes, leur demandant d'envoyer ce message au plus grand nombre de personnes.

Ils peuvent donc avoir une capacité de nuisance réelle : saturation des messageries, saturation d'un numéro de téléphone cité dans le message, voire saturation de services administratifs ou hospitaliers évoqués dans le message.

Ces canulars sont toujours construits de la même manière. Une introduction très alarmiste, des éléments pseudo-techniques qui peuvent être démontés rapidement pour peu qu'on prenne la peine d'y réfléchir, des sources officielles citées à leur dépend, et la sempiternelle conclusion qui demande, pour sauver l'humanité toute entière de faire suivre le message au plus grand nombre de personnes.

Certains de ces canulars sont d'ordre technique et évoquent le danger d'un hypothétique virus qu'il est facile d'éradiquer en détruisant certains fichiers sur l'ordinateur de l'internaute (fichiers nécessaires bien entendu au bon fonctionnement de l'ordinateur et qui l'empêcheront de démarrer ou de fonctionner s'ils sont détruits).

Certains de ces canulars sont d'ordre littéraire. Ils racontent des histoires abracadabrantes particulièrement alarmistes et participent en plus à la création de rumeurs.

Ces virus n'ont pas de capacité de nuisance au sein d'eux-mêmes. Ils ont besoin de la crédulité des utilisateurs pour se répandre.

Le bon réflexe à avoir si vous recevez un message électronique de ce genre est de l'effacer et de ne pas en tenir compte. Si toutefois l'histoire racontée vous interpelle, avant de faire suivre le message à tout votre carnet d'adresses, prenez quelques minutes pour rechercher sur les sites ci-après si l'histoire en question n'est pas déjà répertoriée. Souvent, les canulars lorsqu'ils arrivent en France ont déjà sévi dans d'autres pays voire d'autres continents, même si au passage les sources ou les lieux évoqués sont francisés.

Et si le message électronique vous demande d'effacer des fichiers de votre ordinateur, n'en faites rien et faites confiance à votre administrateur si vous en avez un.

Liens

[La liste des virus blagues du Virus Bulletin](#)

[La liste des virus blagues de Rob Rosenberger](#)

[La liste des virus blagues de Stiller Research](#)

[La liste des virus blagues de Network Associates](#)

[La liste des virus blagues de Sophos](#)

[La liste des virus blagues de Trend Micro](#)

[La liste des virus blagues du CIAC](#)

[La liste des virus blagues du NCSA](#)

Les virus du secteur de boot

Généralités

Les virus du secteur de boot s'installent dans le premier secteur d'un disque dur ou d'une disquette.

Ils remplacent le secteur de boot par une copie d'eux même et décalent les données préexistantes immédiatement après ou sur des secteurs libres du disque.

La position sur le secteur de boot leur permet de se charger en mémoire dès le lancement de l'ordinateur et d'ainsi continuer l'infection.

Ils chercheront à infecter toutes les disquettes introduites dans l'ordinateur.

Les virus de fichiers exécutables

Généralités

Ces virus disposent d'une fonction d'altération des fichiers exécutables présents sur les disques de la machine infectée.

Ces virus utilisent plusieurs techniques d'infection :

* **Virus par recouvrement** : Ces virus écrasent le début des programmes cibles avec leur propre code machine. Le programme cible est alors inutilisable. Le seul avantage de cette technique est que la taille du code n'est pas modifiée.

* **Virus par ajout** : Ces virus altèrent le début du programme infecté pour faire exécuter le code viral en premier. Ce code est ajouté à la fin du fichier. La taille du fichier est modifiée.

* **Virus par entrelacement** : Cette technique est plus fine que les deux précédentes. Il s'agit alors d'insérer le code malicieux dans des zones non-utilisées du programme. Ces zones sont typiquement entre les blocs du programme (code, données et pile).

Les virus macro

Généralités

Les virus macro sont des virus visant un langage de macro d'un produit particulier.

L'exemple le plus connu est celui de la suite Office de Microsoft.

Les virus sont écrits dans le langage de macro de l'application visée (exemple: Visual Basic) et s'exécutent sur une action particulière (ouverture, fermeture, impression,...)

Ces virus se répandent très facilement entre documents en utilisant comme vecteur d'infection le fichier modèle de base de tout document.

La diffusion inter-utilisateur est effectuée par l'échange de documents infectés.

Les virus polymorphes

Généralités

Les virus polymorphes sont des virus capables de s'automodifier. A chaque fois qu'ils infectent un nouveau fichier, le code du virus est modifié.

Les anti-virus utilisent souvent des fichiers de signatures contenant un certain motif qui identifie précisément un virus donné.

Le virus polymorphe essaie par divers moyens de limiter la taille du motif, ce qui le rend plus difficile à détecter avec certitude.

En effet, plus le motif est court, plus il peut être retrouvé dans un grand nombre de programmes.

Le principe le plus couramment utilisé est le chiffrement du virus en générant une nouvelle clé à chaque nouvelle infection. La routine de chiffrement est également perturbée pour qu'elle ne soit pas elle-même une partie fixe.

Les virus furtifs

Généralités

Ces virus sont capables de détourner les interruptions pour devenir invisibles ; ils peuvent également avoir des capacités pour tromper les débogueurs.

Dans le cas où ils détournent les interruptions, ils masquent leurs présences en retournant des images des fichiers ou secteurs de boot tels qu'avant l'infection.

Les virus résidents

Généralités

Les virus résidents sont des virus qui se chargent en RAM et qui infectent les fichiers au fil du temps lors de leur ouverture ou exécution.

Les plus récents de ces virus prennent souvent la forme d'un pilote virtuel sous Windows (.vxd). Ils sont alors chargés par le système d'exploitation lui même et avant les anti-virus.

Ceci les rend plus difficiles à détruire.

Les chevaux de Troie

Généralités

Les chevaux de Troie sont des virus requérant une action de l'utilisateur pour s'exécuter. Ils utilisent un nom propre à tromper l'utilisateur.

On les trouve en particulier sur certains sites pirates qui offrent la dernière version d'un utilitaire qui, bien sûr, n'est qu'un virus n'ayant rien à voir avec le véritable programme.

Il ne se déclenche que si l'utilisateur les exécute. Le risque d'infection n'est donc pas spontané.

Une autre classe de chevaux de Troie est apparue avec l'avènement d'Internet. Ce sont des programmes qui ouvrent des canaux de communication sur le réseau et qui sont prêts à recevoir des ordres de la part d'un intrus.

Ces nouveaux virus utilisent de plus en plus des techniques intrusives des crackers en utilisant des vulnérabilités de produits répandus tel Internet Information Server de Microsoft.

Les virus compagnons

Généralités

Les virus compagnons sont des virus portant le même nom qu'un autre programme et qui utilisent la précedence des extensions.

En effet, si l'on veut utiliser un programme prg.exe, qu'il existe dans le chemin un programme prg.com et que l'on appelle prg sans extension, c'est prg.com qui s'exécutera.

Le virus compagne utilise donc un nom de fichier du système ou courant en substituant l'extension .com à .exe.

Il s'exécutera donc à la place de l'exécutable réel en .exe lors d'un appel sous précision de l'extension.

Le virus compagne peut, ou non, être dans le même répertoire que sa cible. Il suffit qu'il soit dans un répertoire situé avant dans la variable PATH.

Ces virus sont apparentés aux chevaux de Troie.

Les vers

Généralités

Les vers sont des virus particuliers qui peuvent se répliquer par eux-même entre ordinateurs

Les vers sont des programmes autonomes même si certains d'entre eux utilisent des documents pour mieux se répandre (typiquement un message électronique).

Les vers sont de plus en plus courants et prennent de multiples formes. Ils peuvent viser soit des serveurs Internet particuliers (comme IIS avec code-rouge) ou bien les documents d'entreprise.

Les derniers virus sont quasiment tous des vers.

Les bombes logiques

Généralités

Ce ne sont pas à proprement parler des virus. Ce sont des éléments de programmes créés dans une optique particulière qui affectent de manière destructrice le système dans lequel ils sont implantés.

Les bombes logiques n'ont pas de capacité de réplication.

Les virus défensifs

Généralités

Ces virus sont capables de désactiver ou détruire certains anti-virus. Ils sont donc capables de se propager sans être détectés.

Les virus mailers et mass-mailers

Généralités

Ces virus sont capables d'utiliser la messagerie électronique pour se propager.

- * Les virus mailers envoient un mail à chaque activation.
- * Les virus mass-mailers envoient plusieurs mails à chaque activation (par exemple à tous les contacts outlook)

Les éditeurs anti-virus indiquent cette capacité par @m pour mailer et @mm pour mass-mailers

Autres articles et liens

Autres articles

Open Anti-virus

Nimda : une nouvelle étape dans la course au virus

Liens

Les virus célèbres de l'an 2001

Site d'Aladdin

Site d'Alwil

Site de Command Software

Site de Computer Associates

Site de F-Secure

Site de Kaspersky Lab

Site de McAfee

Site de Network Associates

Site de Norman

Site de Panda

Site de Sophos

Site de Symantec Antivirus

Site de Tegam

Site de Trendmicro

Site de Trendmicro France

Site du Virus Bulletin

Cet article décrit les virus et leur principe de fonctionnement. Il a été écrit par un consultant Teamlog, l'original est consultable sur le site **Teamlog**

Loïc Hennequin 06/05/2002

