ASSOCIATION APLDI

www.apldi.fr.st

SUPPORT DE COURS D'INFORMATIQUES

CHAPITRE VIRUS

Virus informatiques et autres bestioles !

En raison de l'importance du sujet, ce dossier se décomposera en deux parties.

Il existe divers types de programmes nuisibles qui sont parfois regroupés sous le nom de malwares (par opposition à software). Le public appelle généralement virus deux types de malwares : les virus proprement dits et les vers. C'est à eux que ce dossier est essentiellement consacré, mais nous croiserons sur notre chemin les bombes logiques, les chevaux de Troie et les backdoors que divers virus ou vers installent à l'insu de l'utilisateur.

Ce dossier fera le tour des principaux types de virus et de vers, de la manière dont ils s'introduisent dans l'ordinateur, des dégâts qu'ils peuvent causer sur les fichiers ainsi que diverses autres nuisances. Ces connaissances sont indispensables pour apprendre à se protéger, ce qui fera l'objet d'un deuxième dossier.

Sommaire

1°) Généralités

Les deux fonctions fondamentales de l'informatique sont de traiter de l'information et donc, par voie de nécessité, de la stocker. **Tout dysfonctionnement dans le traitement, le stockage ou l'accès à l'information constituera donc un dommage.** Dans de nombreux cas, ce dommage peut être considérable.

De tout temps la destruction, l'altération, la modification, accidentelles ou délibérées, ou encore le détournement frauduleux de l'information, ont existé, mais le traitement automatisé des informations (qui fonctionne généralement comme une boîte noire pour le propriétaire ou l'utilisateur final) et la puissance (à certains égards difficilement contrôlable) conférée aux spécialistes par la connaissance des méthodes de programmation, ont donné naissance à un nouveau type de délinquance. Certains de ces délits sont la version moderne, mais plus difficile à détecter, des fraudes en écriture. D'autres se proposent d'altérer ou détruire l'information, ou de perturber le fonctionnement du système informatique.

La grosse informatique connaît depuis longtemps de telles agressions perpétrées dans un but de détournement d'information, de sabotage, de vengeance, voire de chantage.

La micro-informatique a vu le développement d'un type nouveau d'agression, qui n'a pas à ce jour d'équivalent dans les autres domaines de l'informatique : les virus.

2°) Définitions

Il existe divers types de programmes nuisibles qui sont parfois regroupés sous le nom de malwares. Tous ne sont pas recensés dans ce dossier. Voir par exemple le dossier
« Spywares : ces espions qui nous surveillent ».

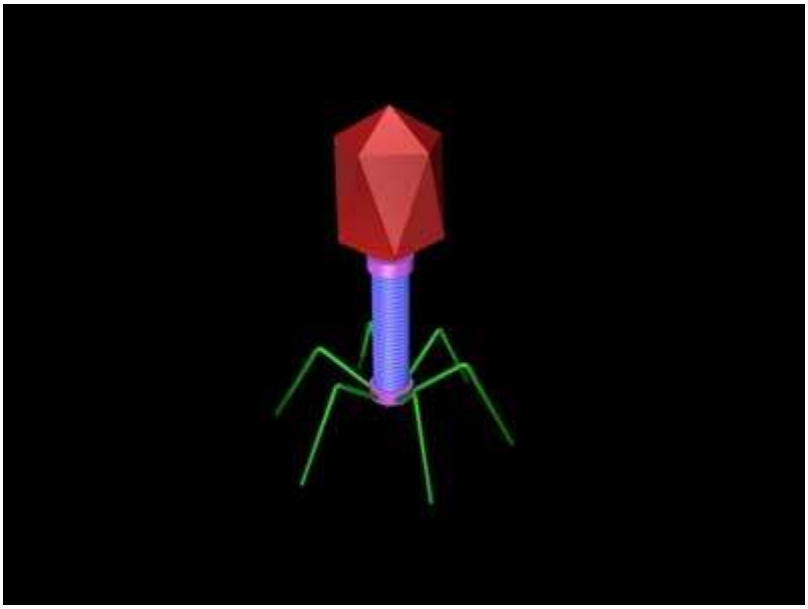
Pour débuter voici deux définitions importantes parce que le public appelle généralement virus des programmes qui n'en sont pas.

- **a) Virus**

On appelle virus informatique un petit programme doté des fonctions suivantes :

- **auto reproduction**
- **infection** (contamination)
- **activation**
- **altération du fonctionnement du système ou de l'information stockée.**

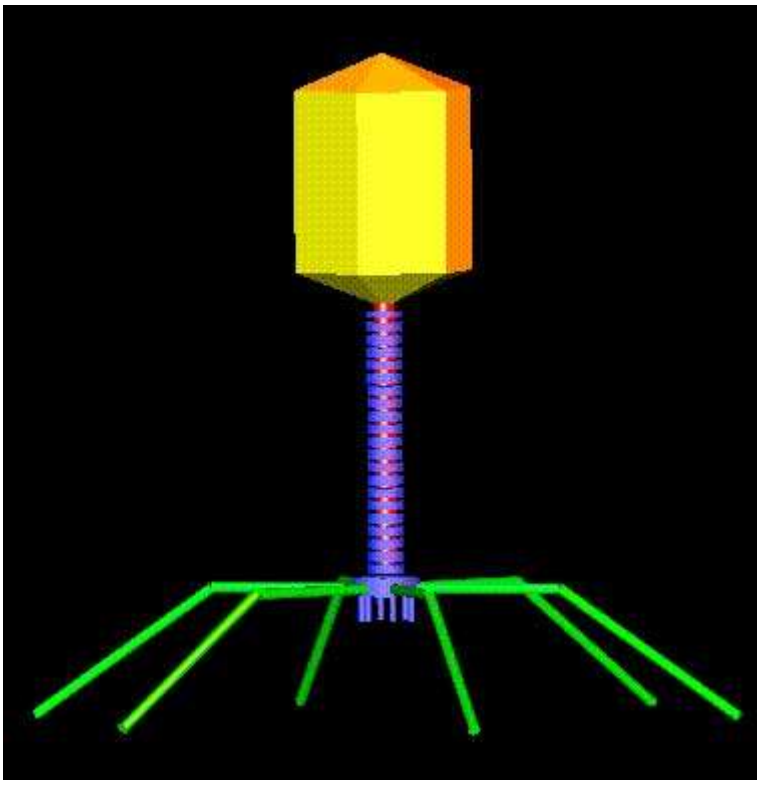
La faculté d'autoreproduction ne nécessite provisoirement que peu d'explications complémentaires : tout programme peut être dupliqué (copié à l'identique) sur un support magnétique par un programme de copie spécialisé (programme COPY du DOS ou autre) ; un programme doté d'une fonction d'auto reproduction possède, au contraire, la faculté de **se recopier lui-même** soit de façon systématique, soit si certaines circonstances sont remplies.



L'infection signifie que le programme dupliqué va se loger de manière illégitime dans certaines parties du système informatique. Les cibles privilégiées sont **la mémoire centrale** (ce ne peut être la seule cible car le virus ne se propagerait pas d'un ordinateur à l'autre, sauf à travers des réseaux, et disparaîtrait à l'extinction de l'ordinateur) et **les zones d'informations exécutables** contenues sur les disques ou les disquettes (on pense immédiatement aux programmes enregistrés sur ces supports, mais ce n'est pas le seul cas possible). Lorsque l'ordinateur tentera d'exécuter ces instructions, le programme viral qu'elles contiennent s'exécutera également.

L'activation du virus, ou plus exactement celle de sa (ou de ses) fonction(s) pathogène(s) se produira uniquement si certaines conditions sont réunies : par exemple lors du nième lancement du virus, tous les vendredis 13, ou toute autre conjonction arbitraire de conditions.

La conséquence de cette particularité de la plupart des virus est qu'ils ont une « vie » composée de deux phases : dans la première le virus se multiplie et propage son infection sans qu'aucun, ou presque aucun signe ne le signale ; dans la deuxième phase les dommages apparaissent, mais la situation est alors généralement bien plus grave que les premiers signes ne le laissent penser.



Lorsque les conditions d'activation sont remplies le virus déclenche en effet une fonction d'agression (payload en anglais) restée en sommeil : il prend au moins partiellement le contrôle du fonctionnement de l'ordinateur pour lui faire accomplir des actions diverses. Par exemple certains virus anciens pouvaient afficher un message inattendu, jouer le beau Danube bleu, la marche funèbre, faire tomber les lettres en cascade de leur position normale sur l'écran vers les lignes du bas, ralentir fortement le fonctionnement de l'ordinateur... Mais les virus se limitent rarement à ces gags agaçants ou fortement gênants.**Très vite les virus sont devenus beaucoup plus pervers :** en particulier la plupart d'entre eux altèrent de façon plus ou moins étendue (voire complète) les fichiers enregistrés sur les mémoires de masse contaminées.

- **b) Vers**

  Contrairement aux virus qui doivent se loger dans des programmes (ou autres informations exécutables) pour agir, **un ver est un programme malveillant qui a une existence autonome (ce n'est pas un parasite).** "En général les concepteurs de virus s'efforcent de faire des programmes de petite taille pour rendre l'infection discrète. Au contraire, bien qu'on connaisse des vers très courts, beaucoup sont d'une taille nettement plus importante car ils ne cherchent pas à se cacher, mais à se faire passer pour un fichier normal."

Certains résident uniquement en mémoire et disparaissent donc lorsqu'on éteint la machine ; plus fréquemment ils sont enregistrés sur le disque et utilisent divers moyens pour se lancer à l'insu de l'utilisateur (dans Windows le solution généralement utilisée consiste à introduire de façon clandestine le nom du ver dans la clé RUN de la base de registre).

D'autres définitions sont données à la fin du paragraphe suivant.

3°) Un peu d'histoire

Dès 1949 Von Neumann, auteur du principe sur lequel reposent les ordinateurs actuels, démontre théoriquement la possibilité de programmes autocopiables.

Dans le début des années 60, quelques informaticiens des laboratoires Bell inventent le jeu Core War. Le principe consiste à implanter dans la mémoire d'un ordinateur deux programmes qui vont alors, sans aucune intervention humaine, lutter l'un contre l'autre en cherchant à se localiser et à se détruire mutuellement. Chaque programme peut en outre se défendre en s'autoréparant en cas de dommage causé par l'adversaire, et en se dupliquant dans la mémoire. La partie est terminée lorsque l'un des joueurs a perdu tous ses programmes ou si ceux-ci ont été modifiés au point d'être rendus inactifs.

Le gagnant est celui qui possède le plus grand nombre de copies actives du programme.

En 1972 apparaissent deux dérivés de Core War : Darwin et Worm. La première mention publique de Core War est faite en 1983. En 1984 la revue à grande diffusion Scientific American publie un article qui suscite un intérêt énorme, exposant une méthode complète pour créer un programme de ce type. Ces programmes ne se développaient et n'agissaient que dans la mémoire vive de l'ordinateur. Il suffisait donc d'éteindre celui-ci pour que tout rentre dans l'ordre. Toutefois, le problème peut devenir grave pour les systèmes reliés en réseau comme en témoigne ce qui est arrivé en 1988 au réseau Internet.

À l'époque, ce réseau n'avait ni le développement ni la célébrité qu'il a acquis maintenant. L'essentiel des ordinateurs qu'il reliait appartenaient à des universités, des ministères, quelques entreprises et des agences gouvernementales (NASA par ex.) des USA. Un jeune mordu d'informatique (Robert Morris Jr) crée un ver, c'est-à-dire un programme capable de s'autodupliquer indéfiniment. Il lance son ver sur le réseau Internet, mais en raison d'une imperfection de programmation, le ver échappe complètement à son contrôle.

A partir du 2 novembre 1988 au soir tous les ordinateurs américains reliés au réseau Internet sont progressivement contaminés et, bien que le ver soit dépourvu de toute fonction offensive, ils entament un processus d'activité spontané qui s'amplifie et paralyse rapidement le réseau.

En moins de 24 h. plus de 6000 ordinateurs (2000 selon d'autres estimations) répartis sur l'ensemble du territoire des États-Unis voient leur mémoire encombrée et leur vitesse de fonctionnement s'effondrer, tandis que les lignes du réseau sont presque saturées.

En théorie, la solution est simple puisqu'il suffit d'éteindre simultanément tous les ordinateurs puis de les relancer, mais ceci est impossible pour un réseau comprenant des milliers d'ordinateurs appartenant à des organisations différentes

très dispersées géographiquement. Il suffit en effet qu'un seul ordinateur reste sous tension pour que cette parade soit inefficace.
Il a fallu plusieurs semaines pour résoudre complètement le problème et le coût des dommages a été estimé à 150 000 dollars, voire 1 million si on prenait en compte le « manque à gagner » lié au temps perdu (des chiffres s'élevant à 96 millions de dollars ont même été avancés, mais ils ont été critiqués par la suite).

Revenons en 1983-1984. À cette époque F. Cohen démontra théoriquement la possibilité de créer de véritables virus (capables de se reproduire sur mémoire de masse et de se propager en causant des dommages irréversibles). Il réalisa quelques expériences bien contrôlées pour attirer sans grand succès l'attention des responsables de sécurité informatique.

Tout ceci se limitait alors aux ordinateurs classiques (moyens et grands systèmes) et, si l'on excepte le cas du ver Internet et un ou deux autres cas non cités ici, ne paraît pas avoir eu d'incidence notable.

D'autres moyens d'agression informatiques étaient en outre bien connus, certains depuis longtemps.

- **Une bombe logique** est **une fonction illicite ajoutée par un informaticien à un programme normal hébergé par un ordinateur.**

  Cette fonction est généralement conçue pour se déclencher si certaines

conditions particulières sont réalisées, de façon à constituer un moyen de vengeance ou de pression sur une entreprise. Un exemple bien connu est celui d'une bombe logique qui devait entrer en action si le nom de l'informaticien disparaissait du fichier du personnel.

Lorsque l'informaticien fut licencié, la bombe logique commença à effacer progressivement des noms de clients du fichier de l'entreprise. Lorsque celle-ci s'en aperçut, longtemps après, les dommages étaient considérables et l'entreprise était au bord de la faillite. Compte tenu de la complexité des programmes, il est très facile de dissimuler de telles bombes. C'est toujours une agression commise par un informaticien au service de l'entreprise ou un prestataire de services. Il est vraisemblable qu'on ne sait pas tout dans ce domaine et bien d'autres cas ont dû être affrontés, ou négociés, avec un maximum de discrétion. On imagine toute l'importance que cette arme pourrait avoir pour des logiciels « sensibles », par exemple en terme de défense nationale.

- **Le cheval de Troie**, au contraire, est **un programme entièrement conçu pour provoquer des dommages, mais en empruntant le nom et l'apparence d'un programme ayant une autre fonction.**

  Ainsi, en 1989 de nombreux médecins reçurent pour essai un logiciel se présentant comme un logiciel d'information sur le SIDA. En réalité, après un certain temps de fonctionnement en apparence correct, ce logiciel renommait de façon fantaisiste tous les fichiers contenus sur le disque dur de telle sorte que

plus rien n'était identifiable. Un exemple encore plus pervers a été celui d'un cheval de Troie qui avait pris le nom et l'apparence de l'antivirus SCAN qui était distribué librement en shareware. En réalité, son action véritable était de détruire la table d'allocation du disque dur, ce qui entraînait la perte de tout le contenu de celui-ci. Les chevaux de Troie existent toujours et sont souvent désignés par l'appellation anglaise « trojan horse », ou plus brièvement « trojan » (ce qui est stupide puisque le cheval de Troie d'Homère n'était pas troyen, mais grec).

- **Les backdoors**: ce terme peut être traduit par « porte dérobée ». **C'est un moyen pour contourner la manière normale d'entrer dans un programme.**

  A l'origine il s'agit d'une pratique informatique tout à fait normale : au cours de la mise au point d'un programme le programmeur peut souhaiter entrer dans le programme ou dans certains modules de celui-ci par une voie plus directe que celle offerte par l'exécution normale. Ces points d'entrée peuvent court-circuiter les procédures d'accès et les sécurités du programme. Normalement ces backdoors doivent être supprimées lorsque le programme a fini d'être testé.

  Mais il peut être nécessaire d'en maintenir à des fins de dépannage en cas de problème majeur empêchant d'utiliser le programme dans des conditions normales. Parfois aussi certains programmeurs laissent délibérément une backdoor pour des raisons plus équivoques. Ces backdoors sont généralement dissimulées par des combinaisons de touches ou d'opérations très exotiques et ne sont connues que du programmeur.

  L'idée peut être généralisée à des fins malveillantes. **Divers virus, vers ou chevaux de Troie peuvent installer des backdoors sur un ordinateur, ce qui permet à un pirate de prendre le contrôle de la machine, en général avec des privilèges d'administrateur.** A partir de ce moment là il est possible de faire n'importe quoi : pirater le contenu de l'ordinateur, récupérer le mot de passe vers un compte bancaire, et surtout se servir de cet ordinateur pour lancer, de façon masquée, une attaque vers d'autres ordinateurs bien plus intéressants du point de vue du pirate.

  Chevaux de Troie et backdoors sont souvent introduits subrepticement par des vers ou la visite de pages Web piégées.

4°) Importance du problème des virus

Les premiers virus ont été des virus fonctionnant sous DOS. Leur progression a été d'abord modérée : 1 en 1986, 225 en 1990, mais 2350 en 1993.

Dès mars 93 deux virus conçus pour fonctionner dans l'environnement Windows 3 étaient signalés et il existe maintenant un nombre considérable de virus fonctionnant avec les diverses versions de Windows. Il faut signaler que les Windows de la série NT (NT 4, 2000, XP) sont beaucoup plus résistants aux virus classiques que les versions 95, 98 et Millenium qui sont basées sur le DOS. Malheureusement il existe de plus en plus de virus et vers conçus pour les versions NT.

L'étape ultérieure a été la création de virus utilisant le langage de script de Microsoft : ce sont les virus spécifiques à Word ou Excel. Enfin, les premiers virus de mail sont apparus plus récemment. Certains détournent également ce langage de script.

En 2002 plusieurs antivirus proclamaient qu'il étaient capables de détecter plus de 61000 virus (en comptant leurs variantes) et beaucoup proposent des mises à jour hebdomadaires ou même quotidiennes. Actuellement ce nombre doit être nettement plus élevé, mais il est difficile de trouver des informations. Un antivirus connu annonce actuellement qu'il a une base de l'ordre de 60000 critères de détection différents. Sachant qu'un critère peut assez souvent servir à détecter plusieurs virus (ou autres programmes malveillants) proches, une estimation de l'ordre de 100000 virus, vers et chevaux de Troie (ou plus) est vraisemblable.

Les causes de cette inflation incroyable du nombre de virus et programmes apparentés sont multiples. Tout d'abord, il faut savoir qu'il est bien plus facile de modifier un virus existant que d'en créer un de toutes pièces. C'est pourquoi de nombreux virus ont donné naissance à des variantes multiples qui constituent des familles de virus. Les changements peuvent être mineurs et viser à empêcher (au moins temporairement) la reconnaissance du virus par un programme comparant son code à une liste de référence des virus connus ; ils peuvent aussi modifier la fonction d'agression ou en introduire de nouvelles.

L'ampleur du problème résulte de la conjonction de plusieurs facteurs :

- **l'énorme diffusion des micro-ordinateurs,** spécialement ceux fonctionnant sous MS-DOS puis maintenant sous Windows ;
- **la structure même du DOS et dans une certaine mesure de Windows,** ainsi que l'introduction par Microsoft dans diverses applications d'un langage de script (Vbscript) destiné à automatiser des opérations très utiles, mais qui peut être détourné de sa fonction initiale pour exécuter des virus ou vers ;
- **le reproche récurrent fait à Windows, Internet Explorer et Outlook Express de contenir de nombreuses failles** trop tardivement corrigées ;
- **la diffusion de l'outil micro-informatique s'est faite largement en dehors du domaine d'influence de l'informatique classique,** c'est-à-dire sans aucune prise en considération des problèmes de sécurité : les usages professionnels, privés... et ludiques s'interpénètrent largement ;
- en d'autres termes, **la micro-informatique est une proie tentante et fragile**, car toutes les conditions sont réunies pour qu'un virus lâché quelque part se répande de façon totalement incontrôlable.

5°) Où le virus se loge-t-il ?

On distingue classiquement trois types de virus : les virus de programmes, les virus du système et les virus de document (essentiellement Word et Excel).

A cette liste se rajoute depuis quelques années une quatrième catégorie : les virus de mail qui sont en réalité des vers pour la plupart d'entre eux. Enfin quelques virus/vers/chevaux de Troie peuvent être transmis par des pages Web et tout récemment on a vu certains de ces programmes malveillants s'introduire directement dans les ordinateurs par l'intermédiaire de l'Internet. La distinction nette entre virus, vers et cheval de Troie s'est beaucoup estompée, certains de ces programmes empruntant des caractéristiques appartenant aux autres catégories. Le public a donc tendance à confondre tous ces programmes malveillants sous le nom de virus.

- **Virus de programmes**

  Ces virus ajoutent leur code à celui d'un programme présent sur le disque dur (ou autre support). Lorsque ce programme est lancé, c'est le code du virus qui est exécuté en premier. Le virus passe alors dans la mémoire de l'ordinateur et recherche sur le disque un (des) nouveau(x) programme(s) à contaminer. **La contamination se fait donc de proche en proche.** Tant que la fonction d'agression du virus n'est pas activée aucune manifestation de la présence du virus n'est perceptible pour un utilisateur non averti.
  Certains virus ajoutent leur code au programme en recouvrant (=remplaçant) une partie du code du programme. La taille du fichier contaminé ne change pas mais on observera probablement assez vite des dysfonctionnements ou des blocages correspondant aux parties du programme remplacées (toutefois s'il s'agit d'une partie du programme qui est rarement utilisée le problème tardera à se manifester).

  La plupart des virus de programmes insèrent leur code dans celui du programme sans le recouvrir : la longueur du programme est augmentée de la longueur de celle du virus. Un simple examen avec la commande DIR du DOS ou sont équivalent Windows devrait permettre en théorie de vérifier que le programme présent est plus long que le programme d'origine. **Toutefois, beaucoup de virus « furtifs » détournent ces instructions pour afficher non pas la longueur exacte du programme contaminé,** mais la longueur diminuée de celle du virus (le programme semblera avoir gardé sa longueur initiale et on ne

pourra pas vérifier la contamination par cette méthode).
Afin d'éviter la contamination d'un programme par plusieurs exemplaires du même virus (ce qui nuirait à la discrétion de la contamination), la plupart de ceux-ci vérifient que le fichier n'a pas déjà été contaminé avant d'ajouter leur propre code. Les méthodes utilisées dans ce but sont variables et n'empêchent nullement un programme d'être contaminé par plusieurs virus différents.

De toutes façons, au début l'infection est toujours discrète car la longueur du code des virus est faible (le plus petit virus dont j'ai trouvé mention a une longueur de 135 octets, mais c'est assez exceptionnel quand même).

- **Virus du système**

Il n'y a pas que les fichiers de programmes qui peuvent contenir du code exécutable. En raison de la manière dont le système d'exploitation démarre et prend le contrôle des disques et disquettes, **le premier secteur de la disquette (secteur d'amorçage = secteur de boot) ou les premiers secteurs du disque dur (secteur de la table de partition et secteur d'amorçage) peuvent contenir un bout de code exécutable**.

C'est bien entendu un endroit rêvé pour installer un virus. S'il s'agit du disque à partir duquel le système d'exploitation est chargé, ce procédé est d'autant plus redoutable que le code du virus s'exécutera et se chargera en mémoire au démarrage, avant le chargement du système d'exploitation et à plus forte raison avant celui d'un éventuel logiciel antivirus.

Pour qu'un virus du système (= virus de boot) s'installe dans un ordinateur il faut généralement démarrer celui-ci avec une disquette contaminée présente dans le lecteur A: (que cette disquette contienne ou non le DOS) car le BIOS tente normalement de lire le contenu du secteur d'amorçage de A: avant celui de C:. C'est la raison pour laquelle il est préférable de rendre le disque C: prioritaire en modifiant un réglage du BIOS. Toutefois certains virus de programme sont également conçus pour aller infecter secondairement le secteur de boot.

En conclusion, les virus classiques (voir toutefois ci-dessous virus Word ou Excel) ne pouvaient pas être transmis par un fichier de données (= document). Mais contrairement à ce que l'on croit parfois un virus peut parfaitement être présent (dans le secteur de boot) sur une disquette qui ne contient pas de programme, et les disquettes ont été pendant longtemps le moyen le plus efficace de

propager les virus. Pendant plusieurs années les virus les plus répandus en France ont été les virus de boot.

- **Virus Word et Excel (virus de macro)**

  Les applications sophistiquées, telles que le traitement de texte Word ou le tableur Excel, contiennent un langage de programmation qui permet d'automatiser des opérations complexes grâce à l'écriture de macro-instructions (connues sous le nom de macros) exécutées par l'application.

  Ces macros sont enregistrées dans les documents. Autrement dit, tout document renfermant des macros contient du code exécutable. Cette particularité a ouvert la porte à l'apparition de virus écrits en langage de macros et incorporés par des mécanismes d'infection spécifiques dans ces documents. **Ce sont des virus pour les documents Word qui sont apparus les premiers (en 1995), puis des virus pour Excel ont été signalés.** A partir de 1997 les virus Word ont été les virus les plus répandus.

- **Virus/vers de mail**

L'apparition de ce type de programme a été rendue possible par le fait qu'on peut attacher à des mails des fichiers divers. S'il s'agit de fichiers exécutables, ils s'exécutent immédiatement dès qu'on clique dessus. Bien entendu ce sont les systèmes les plus répandus qui sont les premiers visés, en particulier le lecteur de mails Outlook Express de Microsoft. **Certains de ces virus/vers tirent parti du fait que les ordinateurs équipés de Windows disposent d'un langage de programmation incorporé appelé vbscript.**

Il faut se méfier du fait que le titre du fichier attaché (c'est lui qui est dangereux) peut paraître intéressant car il peut être prélevé par le virus parmi les titres présents sur le disque dur de l'expéditeur. De plus plusieurs virus peuvent prélever du texte sur le disque dur pour l'envoyer comme un mail normal. C'est ainsi que j'ai reçu un exemplaire de virus avec un texte de message qui était un dossier médical nominatif prélevé sur un ordinateur d'un organisme de santé. Cet exemple montre que certains virus peuvent causer la **diffusion d'informations confidentielles,** problème qui n'a pas été assez souligné.

Lorsque **les correctifs d'Outlook Express n'ont pas été installés certains virus/vers de mail peuvent se déclencher dès l'affichage du mail, même si on n'a pas cliqué sur le document attaché.**

Certains de ces vers peuvent même infecter des pages Web qui contamineront ensuite les ordinateurs des visiteurs.

Quand on reçoit un virus par mail, dans la plupart des cas :

- **l'expéditeur ne sait pas que son ordinateur envoie des mails contaminés** (c'est le virus qui a expédié le mail à l'insu de l'expéditeur, ou qui attache le virus à un mail rédigé par l'expéditeur ;)

- **l'expéditeur n'est probablement pas celui qui figure dans les en-têtes du mail :** beaucoup de virus prélèvent en effet une adresse au hasard dans le carnet d'adresse (ou dans d'autres documents) de l'ordinateur infecté et s'envoient dans un message en se faisant passer pour cet expéditeur (par exemple l'ordinateur de Dupont a dans son carnet d'adresses l'adresse de Durand et celle de Duval… le virus peut envoyer un mail contaminé à Duval en se faisant passer pour Durand, alors que le virus s'est expédié depuis l'ordinateur de Dupont).

Les vers de mails peuvent en effet utiliser la fonction d'envoi des messages d'Outlook Express à l'insu de l'utilisateur, mais les plus « efficaces » intègrent leur propre serveur de mail (serveur SMTP) qui travaille de façon totalement autonome et bombarde de mails contaminés toutes les adresses trouvées sur l'ordinateur.

- **Les hoaxes**

  Un hoax (canular en français) est un message que vous recevez d'une personne inconnue ou d'un correspondant qui vous l'a fait suivre.

En règle très générale le message signale l'arrivée du virus le plus dangereux qu'on ait jamais vu, affirmation confirmée par Microsoft, le FBI, ou tout autre organisme important. **Ce virus va détruire le disque dur, peut-être vider votre compte bancaire, et aucun antivirus ne peut le détecter et encore moins réparer ses dégâts.** Enfin le texte se termine par une forte incitation à diffuser cette information à tous les membres de votre carnet d'adresse.

Vous avez là les caractéristiques types d'un hoax, car les vrais virus ne sont jamais annoncés ainsi et le seul but de ces messages est de provoquer un phénomène de boule de neige par la diffusion pyramidale d'une fausse information. Ne relayez jamais ce type de message.

En cas de doute consultez http://www.hoaxbuster.com

Deux hoaxes plus pervers font toujours des victimes. Leur principe est de dire que si vous avez sur votre disque dur un fichier dont le nom est indiqué, il faut l'effacer parce que c'est un virus. Et bien entendu le message vous demande de diffuser l'information à tous vos correspondants, parce que vous les avez infectés.

L'un des hoax parle du fichier SULFNBK.EXE et l'autre de JDBGMGR.EXE dont l'icône est un petit ourson. Dans les deux cas n'effacez pas ces fichiers : ils font partie du système d'exploitation. Par chance leur rôle est habituellement mineur et cela n'entraîne la plupart du temps que peu de perturbations. Malheureusement les choses se compliquent parce qu'un autre message peut vous arriver qui propose de réinstaller SULFNBK.EXE en cliquant sur une pièce jointe. **Mais là il s'agit d'un vrai virus : Magistr**

6°) Dommages causés par les virus

Les premiers virus provoquaient seulement l'affichage de messages fantaisistes ou d'effets graphiques divers perturbant l'utilisateur. C'est plus grave lorsque l'ordinateur voit sa vitesse réduite d'un facteur 10.

Mais ceci n'est rien comparé aux dommages plus sévères et aussi plus fréquents dont la liste suivante donne une idée très incomplète :

effacement ou altération de nombreux fichiers, formatage intempestif du disque dur, altération du secteur d'amorçage du disque, de la table d'allocation des secteurs (donc impossibilité de lire les fichiers du disque), remplacement des noms des fichiers par des suites aléatoires de caractères...

Parfois un symptôme anodin peut cacher un danger beaucoup plus important. Par exemple si les icônes du bureau s'enfuient à l'approche du pointeur de la souris, c'est le signe d'une infection par le virus de mail Magister. Ce virus provoque au bout d'un certain temps une panne pratiquement irréparable de la carte mère. C'est pourquoi il doit être éradiqué dès qu'il est identifié.

À ces caractéristiques agressives délibérées, il faut ajouter d'autres dommages de type indirect. Par exemple lorsqu'un virus met son code à la place d'une partie de celui d'un programme, le fonctionnement de ce dernier sera altéré. Cette perturbation n'est généralement pas le but réellement recherché, mais la conséquence indirecte d'un mode de contamination peu perfectionné. De même la présence d'un virus dans la mémoire de l'ordinateur peut perturber, pour

des raisons d'incompatibilité imprévues, le fonctionnement de certains programmes.

Divers virus placent leur code dans des parties rarement utilisées du disque ou de la disquette (fin de la table d'allocation, fin de l'espace réservé au répertoire racine, derniers secteurs du support). Si par malchance des informations s'y trouvent il en résultera des dommages plus ou moins étendus. Enfin certains dommages résultent tout simplement d'une faute de programmation faite par l'auteur du virus !

On a parfois affirmé que des virus pourraient provoquer des pannes matérielles en altérant des circuits électroniques ou d'autres organes (disque dur par exemple). Aucun virus de ce type n'est actuellement connu et rien ne permet d'affirmer que ceci soit techniquement faisable. **En revanche, un virus tel que Magistr (alias Magister) peut altérer sans difficulté le contenu de la mémoire C-MOS qui contient les informations sur la configuration de l'ordinateur (taille de la mémoire, types de lecteurs, de carte vidéo installés...) ou le BIOS, et empêcher complètement ou presque le fonctionnement de celui-ci.** Cela peut nécessiter dans certains cas le changement de la carte mère de l'ordinateur.

De même, la modification de la table de partition du disque dur peut faire croire à une panne matérielle alors qu'un nouveau partitionnement suivi d'un formatage complet permettrait de récupérer le disque.

Enfin ajoutons que beaucoup de virus/vers récents sont capables d'inactiver les antivirus les plus connus lorsqu'ils se sont installés.

7°) Pourquoi crée-t-on des virus ? Le crime profite-t-il à quelqu'un ?

Certains ont fait observer il y a quelques années que ceux à qui l'existence des virus profite le plus sont les concepteurs de logiciels antivirus. Cette remarque a été à la base de théories sur la création intentionnelle de virus à des fins commerciales. Rien ne permet d'accréditer cette hypothèse qui est du domaine de la rumeur non fondée, voire malveillante. D'autres interrogations (très probablement non motivées) sur l'intervention de services secrets avaient été suscitées jadis par l'abondance des virus d'origine bulgare.

En fait la production de virus informatiques n'est qu'un aspect d'une longue tradition d'activités pirates dans le domaine des télécommunications et de l'informatique.

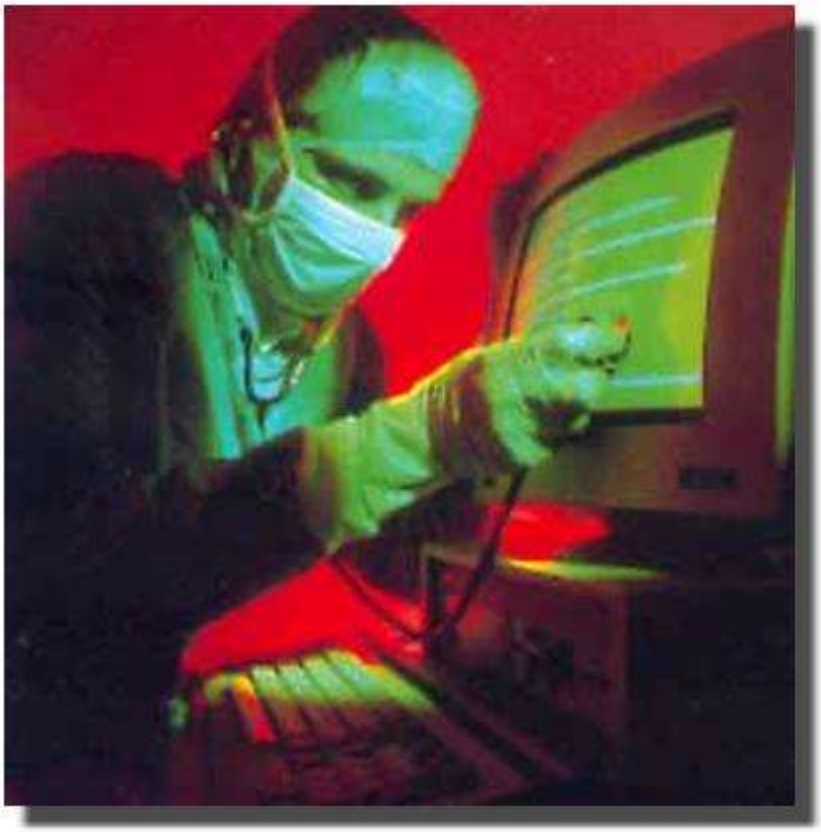
L'origine de ces pratiques remonte à plusieurs dizaines d'années aux États-unis lorsque certains individus, plus ou moins organisés en réseaux clandestins, ont découvert qu'il était possible d'effectuer des opérations illicites sur les réseaux téléphoniques (comme téléphoner n'importe où gratuitement) en envoyant sur les lignes des signaux destinés à inhiber les moyens de contrôle normaux.

Très logiquement, ces pirates étendirent ensuite leur activité en cherchant à pénétrer dans des réseaux informatiques : en effet la quasi totalité de ceux-ci étaient connectés au réseau téléphonique pour effectuer des transactions à longue distance. La recherche des numéros d'accès téléphonique de ces systèmes informatiques (qui bien entendu, ne sont pas publics), le déploiement de trésors d'ingéniosité pour contourner les mécanismes de protection des systèmes d'exploitation, la recherche des mots de passe permettant de se substituer à un utilisateur habilité, constituent des activités passionnantes, bien que parfaitement illicites, pour ces pirates.

Ceci étant fait il est possible de consulter des informations éventuellement secrètes, d'utiliser un ordinateur puissant pour son usage personnel, de placer des bombes logiques ou simplement un message pour montrer aux responsables du système informatique qu'on a pu contourner les mesures de protection et qu'on est plus fort qu'eux.

Dans un autre domaine le piratage des logiciels de micro-informatique par recopie illicite est toujours une activité florissante. L'apparition de mécanismes

protégeant les logiciels contre la copie n'a constitué qu'un frein relatif, car ces protections ont été considérées comme un défi intéressant à relever par les pirates.



L'identification des mécanismes (parfois très astucieusement dissimulés) de protection et le «déplombage» du logiciel protégé sont alors devenus un « sport ». C'est la raison pour laquelle les grands éditeurs de logiciels ont généralement abandonné la protection de leurs programmes par ces procédés.
Dans ce contexte où la fraude est considérée comme un exploit intellectuel ludique il ne faut pas s'étonner de l'existence des virus informatiques. Leur création procède du même état d'esprit et il s'y rajoute certainement la fascination, qui a un côté pathologique, de voir proliférer un être informatique qu'on a créé, de savoir qu'il mène une « vie » autonome et peut se répandre, avec un peu de « chance » dans le monde entier.

Ce qui précède était ce qu'on pouvait dire il y a peu de temps encore. Mais une nouvelle tendance apparaît : l'utilisation de vers comme outils pour **des délits informatiques graves.** En effet certains vers récents ont pour objectif délibéré d'introduire dans les ordinateurs des chevaux de Troie permettant de faire du

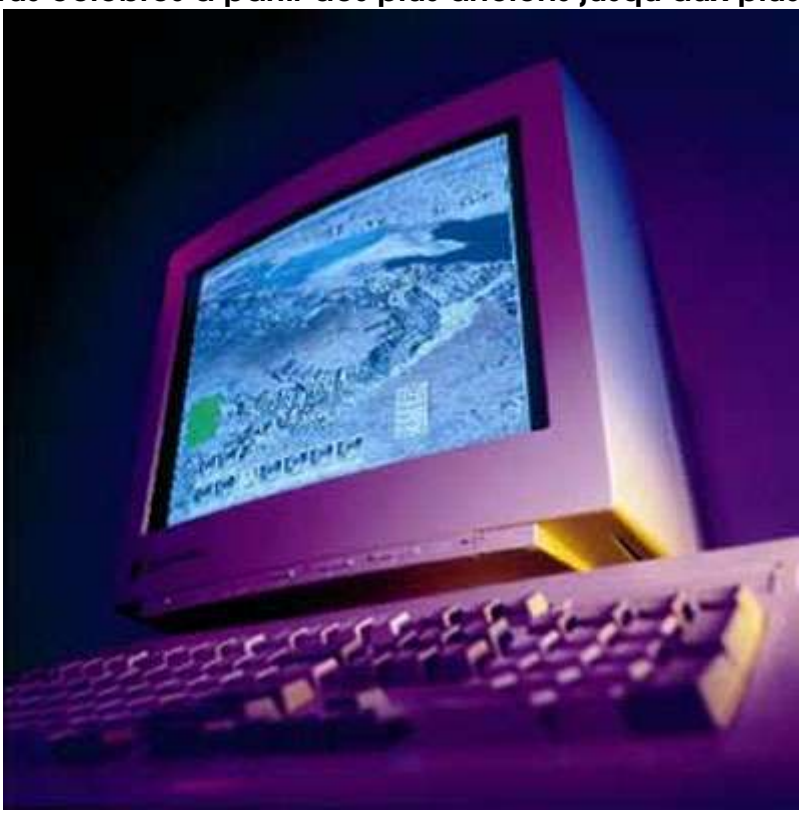
spam massif, masquant ainsi son origine exacte puisque les destinataires penseront que c'est **votre ordinateur** qui a émis les messages. Certains chevaux de Troie pourront servir de relais pour attaquer de façon masquée d'autres ordinateurs. Enfin d'autres vers sont conçus pour espionner les mots de passe, recueillir des informations bancaires précieuses, etc.

Il faut donc savoir que si vous avez sur Internet des pratiques à risque, si vous ne mettez pas régulièrement à jour votre système pour corriger ses failles, si vous n'utilisez pas d'antivirus et de pare-feu, vous pouvez vous rendre involontairement complice d'actes délictueux graves, dont certains relèvent de l'escroquerie pure et simple. On est pour le moment dans une situation de vide juridique complet, mais rien n'exclut qu'à l'avenir la responsabilité d'un utilisateur puisse être invoquée pour cause de négligence grave ayant causé des dommages à autrui.

Ces points seront illustrés dans la deuxième partie du dossier.

Deuxième partie du dossier : "Virus informatiques et autres bestioles "!

Dans une première partie nous avons vu ce que sont les virus et autres programmes malveillants qui peuvent s'attaquer à nos ordinateurs. Pour apprendre à s'en protéger il faut voir de plus près comment ces programmes peuvent pénétrer dans l'ordinateur et par voie de conséquence quels sont les comportements à respecter pour les éviter. L'aide que peuvent apporter les antivirus et pare-feux sera ensuite envisagée. Pour terminer nous verrons un petit inventaire de virus célèbres à partir des plus anciens jusqu'aux plus récents.



Sommaire

1°) Les protections contre les virus

1 - Voie d'entrée des virus

Les ordinateurs sont isolés ou regroupés en réseaux locaux ou reliés à l'Internet. **Un virus ne peut s'introduire que par une disquette, un CD-ROM ou par le réseau.**

Pendant longtemps la contamination d'un ordinateur par un virus signifiait qu'à un moment **une disquette (ayant été utilisée sur un ordinateur étranger) avait été employée.** C'est le cas lorsque des disquettes passent d'un ordinateur personnel à l'autre, puis à des ordinateurs professionnels. Il faut se souvenir que des virus peuvent être transmis par des fichiers Word ou Excel. Même si ce type de contamination est en nette perte de vitesse il ne faut pas le négliger car Word est sans doute le programme le plus employé au monde, suivi par Excel. Bien entendu un CD-ROM gravé sur un ordinateur contaminé peut également véhiculer des virus.

Avec le développement des réseaux, les disquettes constituent maintenant une source mineure de virus, comme le prouve l'envahissement **actuel par les virus ou vers de mail, mais aussi le cas moins connu du public de virus véhiculés par des pages Web, par IRC, par les échanges P2P comme Kazaa, ou ceux qui attaquent directement à travers l'Internet** en l'absence de toute action de l'utilisateur. Un ordinateur en **réseau local** peut aussi être contaminé sans qu'aucune manipulation imprudente n'ait été effectuée à son niveau, tout simplement parce qu'un virus résidant initialement sur un autre ordinateur s'est propagé à travers le réseau. Ceci se produit par exemple avec divers vers lorsqu'il existe des disques partagés dans un réseau Windows.

2 - Comportements à respecter

De ces affirmations découlent quelques règles simples qu'il n'est malheureusement pas facile de faire respecter. Ces règles sont pourtant essentielles car le meilleur programme antivirus ne peut pas protéger contre un virus totalement nouveau, tandis que le respect de ces précautions permet d'éviter la plupart des problèmes.

- **Ne pas utiliser une disquette qui a servi (ou un CD-ROM qui a été gravé) sur un ordinateur dont on n'a pas le contrôle total.** En particulier éviter à tout prix les programmes piratés qui ont fait l'objet d'un tel nombre de copies qu'on ne sait plus quelle en est l'origine (en outre cette pratique ne respecte pas les droits des auteurs des logiciels ; **c'est un délit très sévèrement puni par la loi)**. De plus en plus rarement la nécessité du fonctionnement normal de certains services implique le passage de disquettes ou de CD-ROM sur des ordinateurs extérieurs. On limitera alors les risques en vérifiant systématiquement ces supports avec un antivirus, en veillant à ce que les supports servant à l'échange de données ne contiennent aucun programme (ceci évite la transmission des virus de programmes), et en utilisant la fenêtre permettant d'interdire l'écriture sur la disquette chaque fois qu'il suffit de la lire (évite seulement la contamination de la disquette par un éventuel virus de boot présent sur l'ordinateur chargé de la lecture).

<u>Recommandation très importante</u>

La prévention contre les virus ou vers de mail implique quelques précautions de base. La manière la plus simple de s'en prémunir est **de ne jamais cliquer sur un document attaché, même s'il a été envoyé par une personne de confiance,** car ce type de virus est joint au message à l'insu de l'expéditeur. Une bonne règle est de préciser dans le texte du message le nom et la nature du fichier joint. **Si le message provient d'une personne de confiance ET si le fichier attaché est clairement annoncé dans le texte** par l'expéditeur du message, on peut

considérer que sa consultation est probablement peu risquée. **Dans tous les autres cas il faut considérer que le fichier est suspect** (même si vous connaissez l'expéditeur). En particulier les pièces attachées ayant les extensions suivantes sont pratiquement à coup sûr des fichiers de virus : **COM, EXE, BAT, PIF, VBS, LNK, SCR** ainsi que les fichiers ayant une double extension (par exemple le célèbre **LOVE-LETTER-FOR-YOU.TXT.VBS**).

- **Les versions actuelles de Windows sont configurées par défaut** pour ne pas afficher l'extension de la plupart des fichiers : par exemple **DOCUMENT.DOC sera affiché DOCUMENT.** Dans ce cas **LOVE-LETTER-FOR-YOU.TXT.VBS sera affiché LOVE-LETTER-FOR-YOU.TXT,** ce qui n'attire pas l'attention sur le caractère anormal du nom. Il est donc fortement conseillé de rétablir l'option d'affichage des extensions.
- **On conseille souvent d'éviter le téléchargement de logiciels** sauf si on est en mesure de contrôler l'intégrité de ceux-ci (mais aucun logiciel antivirus n'offre une garantie absolue de détection). En fait les sites Internet de téléchargement les plus connus contrôlent sérieusement l'intégrité des programmes qu'ils proposent, mais il faudra proscrire les autres sources, **en particulier les sites spécialisés dans la distribution de logiciels piratés (dits sites Warez) et se méfier des échanges entre particuliers (P2P comme Kazaa, eDonkey, Gnutella, eMule**...)
- **Une recommandation particulière doit être faite aux utilisateurs de Windows, Microsoft Internet Explorer, et Outlook Express** : **utilisez toujours les dernières mises à jour** qui peuvent être chargées à partir du site de Microsoft (dans Internet Explorer, **menu Outils, Windows update)** car divers virus récents exploitent des trous de sécurité existant dans Windows ou ces programmes. Par exemple avec des versions non mises à jour d'Outlook Express certains virus de mail peuvent infecter l'ordinateur même si l'on n'a pas cliqué sur la pièce jointe. De même les quelques virus pouvant se transmettre par des pages Web ont utilisé des failles de sécurité d'Internet Explorer qui n'avaient pas été détectées à temps. Les mises à jour incorporent des protections nouvelles au fur et à mesure que des problèmes sont signalés. **Divers virus/vers dangereux se sont propagés grâce à des ordinateurs non mis à jour, alors que les correctifs avaient été diffusés par Microsoft plusieurs mois auparavant.** Une ultime recommandation concernant Outlook Express : dans les options de lecture, cochez « Lire tous les messages en texte clair » (l'intitulé peut changer légèrement selon les versions). Cela supprime l'affichage HTML pour afficher uniquement le texte brut : c'est beaucoup moins joli, mais on évite ainsi les

risques liés aux virus exploitant des failles de ce mode d'affichage.

- **Faire des sauvegardes régulières des fichiers importants sur des supports extractibles (disquettes, CD-ROM R/W).** En cas d'attaque par un virus, on pourra revenir à une copie intacte. Il faut toutefois être sûr que la copie de sauvegarde est saine, ce qui n'est pas toujours évident ; c'est pourquoi il faut faire des générations de sauvegarde successives (par exemple un jeu de sauvegardes renouvelé journellement, un autre jeu qui sera renouvelé toutes les semaines, un autre tous les mois... tout dépend de l'importance des fichiers et de la fréquence de leur modification.) : si la dernière est défectueuse, il faut revenir à l'avant-dernière, ou même plus en arrière encore. C'est pourquoi dans le cas d'un réseau ces opérations de sauvegarde sont automatisées et sont faite au niveau du ou des serveurs sur des bandes magnétiques.

3 - Les antivirus

De toute façon, il faudra envisager l'utilisation systématique d'un **programme antivirus**. Disons d'emblée qu'**aucun programme ne peut garantir une efficacité absolue, même s'il le prétend**. On peut comparer un antivirus à un gilet pare-balles : celui-ci n'empêche pas la possibilité de blessures à la tête ou aux membres, mais il réduit fortement les risques. Il existe divers programmes commerciaux tout à fait sérieux. Ils permettent de contrôler et, lorsque c'est possible, de décontaminer les fichiers, disquettes ou disques infectés. Des versions sont adaptées à la protection des réseaux et certaines prennent en charge les risques nouveaux liés à l'utilisation d'Internet.

- **On peut identifier dans le code de la plupart des virus des séquences d'octets caractéristiques de ce virus.** Si cette séquence est bien choisie, elle a de fortes chances de se retrouver également dans la plupart des virus obtenus par modification d'un même virus souche. **On appelle signature de détection une telle séquence d'octets.** Beaucoup d'antivirus détectent les virus en recherchant systématiquement ces signatures dans le secteur d'amorçage et les fichiers. Il est évident que chaque virus (ou famille de virus) possède sa propre signature. En conséquence, on doit fournir une liste de signatures aux antivirus utilisant cette méthode. Bien entendu on ne peut détecter que des virus déjà connus ; c'est pourquoi la liste des signatures doit être complétée périodiquement.

  Posséder un antivirus a peu d'intérêt si on ne dispose pas de mises à jour fréquentes. Les antivirus doivent en effet être mis à jour régulièrement (au moins toutes les semaines, tous les jours si possible) en téléchargeant sur Internet les nouveaux fichiers de définitions virales. Cette opération peut être automatisée sur la plupart des antivirus actuels. Ceci montre l'aspect illusoire des antivirus piratés.

  Divers virus posent de gros problèmes à cette méthode de détection, car ils sont cryptés et auto-mutants. On les appelle généralement **virus polymorphes**. À chaque réplication le virus se crypte lui-même avec une clé aléatoire. On ne peut donc définir aucune signature stable qui permette de le reconnaître. Pour être efficace l'antivirus doit faire une analyse du contenu pour rechercher d'éventuels mécanismes de cryptage.
- **L'idéal serait de pouvoir identifier dans le code des structures logiques caractéristiques des mécanismes viraux en général.** Ceci rendrait possible la détection de virus encore inconnus. Malheureusement, rien ne permet d'identifier avec certitude un virus par cette méthode. Certains détails de structure sont fortement suspects car ils sont souvent employés dans les virus, mais l'exploration systématique des programmes montre qu'on peut parfaitement les rencontrer dans des logiciels tout à fait normaux, et même dans des fichiers du système d'exploitation.
- **La plupart des antivirus actuels utilisent des fichiers de signatures mais incorporent aussi d'autres méthodes de détection** dites heuristiques qui reposent par exemple sur l'analyse empirique de certains détails de structure des fichiers, comme indiqué ci-dessus. Ceci leur permet parfois de détecter un nouveau

virus avant que sa signature soit connue.

- **Un autre groupe de méthodes consiste à prendre une « empreinte » de chaque fichier de programme et à contrôler** périodiquement que ce fichier n'a subi aucune modification. Cette méthode ne permet que la détermination a posteriori d'une contamination, mais elle offre théoriquement l'avantage de détecter la présence de virus encore inconnus. **L'empreinte du fichier comprend généralement son nom, ses date et heure de création ou modification, sa longueur et une « somme de contrôle » (checksum) obtenue en faisant la somme (en utilisant l'opération modulo) de tous les octets du code du logiciel, ou de certaines zones sensibles de celui-ci.** Le logiciel antivirus enregistre ces données lors d'un premier examen du disque et, lors des examens ultérieurs, compare ces données initiales avec celles que lui fournit l'examen en cours. En théorie, toute modification, même minime, d'un fichier doit pouvoir être détectée ainsi. En réalité, certains virus utilisent des méthodes sophistiquées pour leurrer ces logiciels de contrôle.
- **Il y a deux stratégies fondamentales d'utilisation des antivirus.** La première est d'utiliser ces outils pour scanner tout fichier nouveau avant installation, et les disquettes ou CD-ROM avant utilisation. Par précaution il est également recommandé de scanner périodiquement son disque dur.
- **La deuxième technique consiste à installer en mémoire au démarrage de l'ordinateur un module antivirus spécial, appelé généralement moniteur.** Tous les antivirus actuels possèdent un moniteur. Celui-ci peut **rechercher automatiquement la signature de virus connus dans tout fichier devant être exécuté ou recopié.** Il peut aussi **surveiller en permanence l'activité de l'ordinateur, détecter et empêcher tout comportement suspect :** tentative d'écriture sur le secteur d'amorçage, modification de la table d'allocation en dehors des procédures normales, effacement inopiné de fichier, formatage du disque, écriture directe sur le disque (en particulier dans un fichier de programme), contournement des fonctions du système d'exploitation ou détournement de celles-ci de leur rôle normal. Cette stratégie permet, en théorie, d'intercepter à la source les tentatives de contamination ou d'agression des virus même inconnus.

  Contrairement aux moniteurs fondés essentiellement sur la recherche des signatures, ceux (plus rares) qui reposent essentiellement sur la surveillance d'opérations suspectes affichent souvent des messages d'avertissement lors du fonctionnement de divers programmes sains. En effet certains de ces

comportements suspects sont également utilisés par des programmes normaux. Si ces antivirus sont mal conçus les messages seront trop nombreux et finalement l'utilisateur n'en tiendra aucun compte ou abandonnera l'usage de ce dispositif de protection. Si les messages ne sont pas assez nombreux, une agression assez habile pourra passer inaperçue. Cette méthode n'a pas non plus une efficacité absolue, car certains virus sont capables de masquer leur action.

Il faut savoir que les moniteurs fonctionnant en temps réel peuvent être moins efficaces que les programmes d'analyse lancés à la demande (pour des questions d'encombrement en mémoire ou de charge du microprocesseur) : ils ne dispensent donc pas de faire une analyse systématique du disque de façon périodique.

- **On distingue les virus actuellement en circulation (virus in the wild, dans le jargon des spécialistes) et les virus in the zoo, qui ne se rencontrent que dans les collections des spécialistes et des éditeurs d'antivirus**. Ce dernier groupe comprend des virus qui n'ont jamais vraiment réussi à percer, des virus expérimentaux et des virus très anciens qui ne se rencontrent plus actuellement. Cette distinction est importante : en raison de l'inflation du nombre des virus les éditeurs ont tendance à retirer de la base de signatures les virus les plus anciens, afin d'éviter d'avoir une base de taille excessive qui ralentirait fortement l'analyse. On peut donc avoir de mauvaises surprises en réutilisant des fichiers se trouvant sur de vieilles disquettes.
- **Si l'antivirus est paralysé par un virus ou ver on peut avoir recours à un antivirus en ligne,** tel ceux qui sont disponibles sur les sites suivants :

  http://fr.trendmicro-europe.com/consumer/products/housecall_pre.php

  http://www.mcafee.com/myapps/mfs/default.asp

  http://www.pandasoftware.com/activescan/fr/activescan_principal.htm

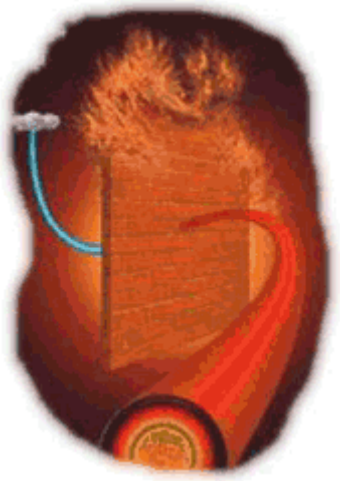
  http://www.bitdefender.com/scan/licence.php

  http://www.secuser.com/antivirus/index.htm

  Ces antivirus en ligne nécessitent généralement l'utilisation d'Internet Explorer pour fonctionner.

4 - Les pare-feux (firewalls)

Lorsqu'un ordinateur est connecté à l'Internet il est susceptible de subir des agressions variées en provenance du réseau. Ces tentatives d'intrusion utilisent des portes d'entrées (terme technique = ports) par lesquels les divers protocoles communiquent avec d'autres ordinateurs (par exemple les serveurs Web communiquent à travers le port 80).



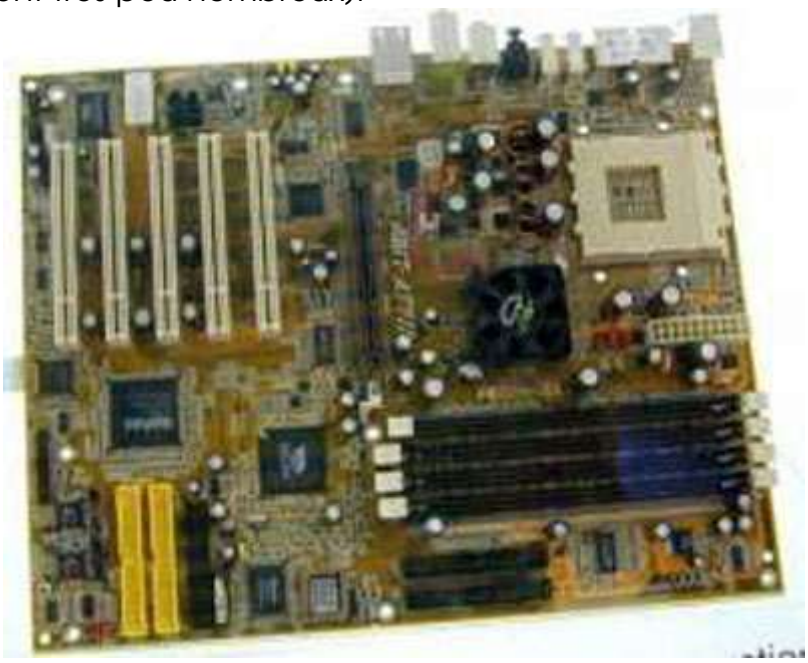
Le rôle d'un programme pare-feu est de fermer tous les ports inutilisés et d'ouvrir les ports nécessaires sur la base de critères bien précis. On trouve des programmes pare-feux facilement utilisables pour un usage personnel. Ils sont gratuits ou peu coûteux. Windows XP possède un petit firewall incorporé, mais il bloque uniquement ce qui pourrait venir de l'extérieur et ne permet pas de limiter ce qui sort de l'ordinateur, de telle sorte qu'un cheval de Troie ou spyware qui serait installé sur l'ordinateur pourrait communiquer en toute impunité avec l'extérieur (par exemple si vous êtes contaminé avec un ver de mail, il peut envoyer à l'extérieur à votre insu des milliers de mails infectés). Il est question que ce défaut soit corrigé dans le Service Pack 2 pour Windows XP.

L'utilisation des pare-feux dépasse largement le problème des virus/vers qui peuvent attaquer les ordinateurs directement à travers le réseau, **mais il faut retenir que ce type de protection est absolument indispensable** (même si là non plus l'efficacité absolue n'est pas garantie) le risque étant proportionnel à la durée de la connexion (les utilisateurs de l'ADSL restent en général connectés en permanence).

2°) Réparation en cas d'infection

Il faut distinguer deux types d'interventions. **Dans certains cas, le virus ou vers sera détecté avant le déclenchement de sa fonction de dommage.** S'il s'agit d'un **virus du système**, il suffit de remplacer le secteur d'amorçage par une copie saine de celui-ci (idem si le virus est dans la table de partition, mais c'est plus délicat). S'il s'agit **d'un virus de programme**, la solution la plus simple est de détruire les programmes infectés et de les remplacer par une copie de réserve saine. Ceci peut prendre beaucoup de temps, car il suffit d'oublier un seul programme contaminé pour que le virus se propage de nouveau. Il n'est pas toujours possible de remplacer le programme contaminé, par exemple parce qu'on n'en a pas de copie saine.

Dans un certain nombre de cas **il est possible de réparer le fichier en supprimant le code du virus.** Bien entendu, il ne faut pas que le virus ait détruit une partie du code du programme. Divers antivirus proposent la réparation automatique des programmes (pour certains virus uniquement). **Tous les antivirus n'ont pas la même efficacité quant au nombre de virus qu'ils peuvent traiter ou l'état (plus ou moins fonctionnel) dans lequel ils restaurent les programmes. Les contaminations simultanées par plusieurs virus peuvent être redoutables car les tentatives de réparation risquent d'entraîner des dommages irréparables.** Si la contamination touche des ordinateurs professionnels dont l'usage est critique, il vaut mieux payer le prix et utiliser **les services d'un vrai spécialiste en sécurité** (ils sont malheureusement très peu nombreux).



Les vers sont autonomes puisqu'ils ne se greffent pas sur des programmes. Leur élimination est donc plus facile. Comme la quasi-totalité des « virus » de mail sont en fait des vers, cela explique pourquoi les éditeurs d'antivirus peuvent fournir très rapidement en téléchargement gratuit de petits utilitaires spécialisés dans l'élimination de chacun des vers susceptibles de contaminer un ordinateur. Face à un fichier contenant un virus qui ne peut être désinfecté, l'antivirus propose généralement l'effacement complet ou la mise en quarantaine (en gros, mise à l'abri dans un répertoire spécial). On rencontre toutefois de plus en plus de cas où l'élimination d'un ver (ainsi que des chevaux de Troie ou des backdoors qu'il installe) semble impossible. Cela peut être dû à deux problèmes. Le premier est qu'on ne peut généralement pas effacer le fichier d'un programme actif. Le deuxième est que de plus en plus de vers désactivent les antivirus connus. Cette difficulté est généralement réglée en démarrant l'ordinateur en mode sans échec avant de pratiquer la désinfection.

Il faut savoir que divers antivirus ne détectent pas les virus/vers des messages stockés dans Outlook ou Outlook Express en raison du format d'enregistrement ; d'autres possèdent une option pour scanner la messagerie, mais cette option est inutile voire nuisible. En effet ces virus ou vers ne peuvent pas s'activer lorsqu'ils sont archivés. En outre chaque dossier (par exemple Boîte de réception) correspond à un fichier unique qui peut être de taille importante si on a l'habitude d'archiver ses mails. Comme souvent la seule solution en cas d'infection serait de détruire le fichier (ce qui est fait parfois automatiquement), on perdrait alors tous les mails archivés. **Le bon réflexe, si on veut consulter le document attaché à un mail, consiste à l'enregistrer sur le disque dur et à le scanner avant ouverture** (beaucoup d'antivirus, mais pas tous, détecteront d'ailleurs un éventuel virus dès la phase d'enregistrement).

Le deuxième type d'intervention correspond aux cas où le virus a déjà causé des dommages. Dans ce cas, il faudra détruire toute trace du virus mais également essayer de réparer ce qui peut l'être, car toutes les situations peuvent se rencontrer, depuis l'altération d'un petit nombre de fichiers jusqu'au formatage du disque dur. La règle de base est que tous les fichiers présents sur un disque dur doivent être régulièrement sauvegardés sur un support extractible, comme cela a déjà été expliqué. Il faut cependant savoir que certains dégâts qui semblent importants sont parfois plus facilement réparables qu'on ne le pense. Un fichier entièrement effacé peut souvent être récupéré grâce à des programmes spécialisés. Il en est de même pour un disque reformaté si certaines précautions

ont été prises au préalable. De même une atteinte de la table de partition du disque peut faire croire que celui-ci est hors d'usage alors qu'il peut être récupéré assez facilement.

En règle générale toutefois la plupart des opérations de réparation portant sur les fichiers ou le disque dur ne sont pas à la portée de n'importe qui, même en ayant des connaissances de base en informatique. Certaines tentatives maladroites causent plus de dommages que le virus lui-même et **contrairement à ce qu'on pense un formatage complet du disque (dans l'espoir d'effacer toute trace de contamination) est inutile et même ne détruit pas les virus de système contenus dans le premier secteur du disque (table de partition ou MBR).**

Il ne suffit pas de désinfecter le disque dur. Il faut aussi examiner toutes les disquettes utilisées et les CD-ROM gravés sur les ordinateurs contaminés ainsi, si nécessaire, que les autres ordinateurs du réseau.

3°) Les virus et les micro-ordinateurs, quelques dates mémorables

Il ne s'agit là que de quelques exemples ; on aurait pu faire d'autres choix dans une liste malheureusement trop longue.

1 - Les débuts

- **Le premier virus fut un virus pour Apple II,** Elk Cloner en 1983 créé pour son amusement par Rich Skrenta qui avait alors 16 ans. C'était un virus non destructif mais qui finissait par devenir gênant.
- **Le premier virus pour PC disséminé,** fut le virus Brain (1986) créé par les frères Alvi, de Lahore (Pakistan). Il s'agissait d'un virus destiné à limiter la copie illicite des logiciels vendus par les deux frères dans leur magasin Brain Computer Services. Le paradoxe est qu'il a été diffusé par l'intermédiaire de copies pirates de MS-DOS vendues par ce magasin aux touristes ! Ce virus modifiait le label de la disquette, et affichait un message invitant à prendre contact avec les auteurs pour obtenir l'antivirus.
- **Début 1988 une revue canadienne décida de lancer une campagne de sensibilisation aux virus.** Elle fit réaliser un virus sans danger présentant les caractéristiques suivantes : le virus ne possédait aucune fonction offensive ; il devait se déclencher le 2/3/88 (date anniversaire de la commercialisation du micro-ordinateur MacIntosh II), afficher un message de paix universelle et se détruire. Malheureusement, ce virus contamina accidentellement une disquette utilisée pour la duplication de la version de démonstration d'un logiciel commercial connu et, bien que non dangereux, il se répandit dans plusieurs pays.
- **Le virus Datacrime ou virus du vendredi 13 (13 octobre 1989)** a fait l'objet d'une campagne d'alerte de la part d'un organisme de sécurité informatique des Pays-Bas début octobre 1989. Ce virus avait en effet été annoncé avant son déclenchement. Il a donné lieu, en France en particulier, à une campagne de presse hors de proportion avec l'importance de l'infection. Cette campagne a abouti en définitive à discréditer dans une certaine mesure ceux qui attiraient l'attention sur les risques présentés par les virus informatiques.
- **La revue Soft et Micro distribue avec son numéro de mai 1991** une disquette de démonstration accidentellement contaminée dans des circonstances mal élucidées par **le virus Frodo.** Le virus devait se déclencher le 22 septembre, date de l'anniversaire de Frodo (en français Frodon, héros du Seigneur des Anneaux de J.R.R. Tolkien). Rapidement avertie, la revue retire la plupart des disquettes

des points de vente et distribue gratuitement sur demande un antivirus spécifique. On estime toutefois que plus de 20 000 disquettes contaminées ont été diffusées et le virus Frodo a été très répandu en France dans les mois et années suivants. Il est considéré comme un modèle de virus furtif et a été un des plus perfectionné à son époque.

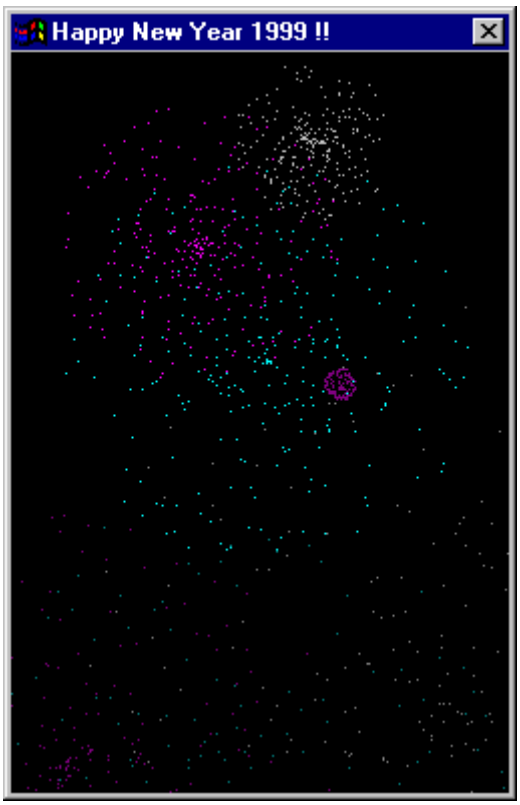
- **En 1991 on découvre un nouveau virus qui devait effacer le disque dur des ordinateurs le 6 mars 1992** (date anniversaire de la naissance de Michel-Ange, d'où son nom : **Michaelangelo**). Une campagne de presse hystérique, stimulée par certains experts (pas toujours désintéressés) prédit que 5 millions d'ordinateurs vont perdre leurs données. En fait seuls 10 000 à 20 000 cas ont été dénombrés, et là encore la presse s'est couverte de ridicule.

2 - Des virus récents

- **1998 est l'année d'apparition de Tchernobyl** (alias **CIH**) un virus se déclenchant le 26 avril de chaque année (anniversaire de la catastrophe de la centrale nucléaire). Il efface alors le premier Mo du disque dur, mais surtout il modifie le contenu du BIOS. Dans beaucoup de cas cela implique le changement de la carte mère.

Les « virus » les plus nombreux actuellement sont des vers de mail. Rappelons qu'il faut généralement cliquer sur une pièce jointe pour que le ver/virus s'installe dans l'ordinateur. Toutefois certains d'entre eux peuvent s'exécuter spontanément dès qu'on lit le message si on utilise une version non mise à jour d'Outlook Express.

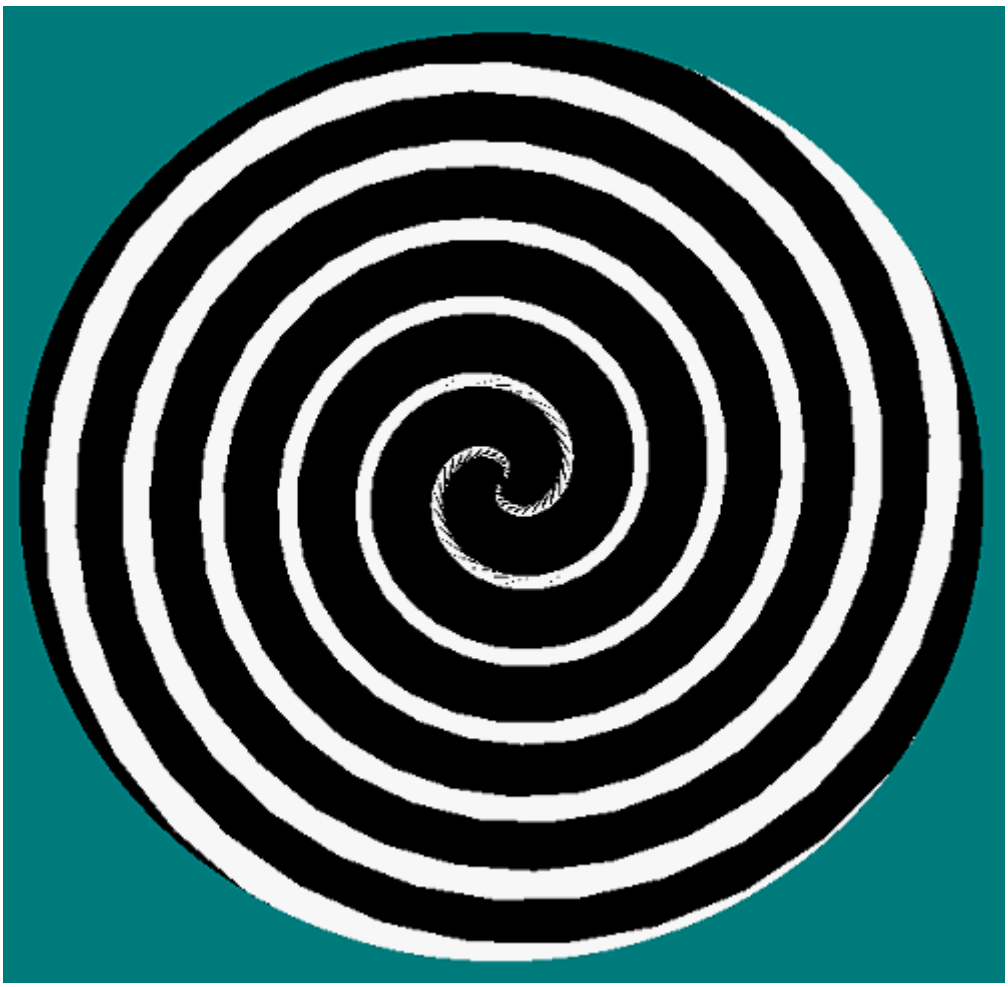
- **Le premier ver de ce type a été Happy99** (apparu en janvier 99) qui se présentait comme un message de bonne année accompagné d'un fichier affichant un feu d'artifice quand on cliquait dessus. En réalité cette opération installait le ver qui avait la possibilité de s'envoyer lui-même à d'autres correspondants. Mais celui qui a fait le plus parler de lui est **I love you en 2000.** En effet les média se sont fait largement l'écho des nombreuses contaminations dues à ce virus (connu aussi sous le nom **Loveletter**). Ce n'est pas le plus fréquent et il est facile à identifier mais il a une fâcheuse propriété : celle d'effacer le contenu de nombreux fichiers, les plus connus étant ceux d'extension **.JPG, MP2, MP3, .AVI.** Il s'envoie lui-même en grand nombre aux adresses trouvées dans le carnet d'adresse d'Outlook Express.



Normalement cet écran est animé

1999 a vu également la diffusion d'un virus curieux : **Melissa**. Ce virus est un virus de macro classique affectant les documents Word, à une exception près : en s'activant il envoie par mail une copie du document infecté à 50 destinataires. Il se trouve donc à mi-chemin entre les virus classiques des années précédentes et les nouveaux vers de mail.

- En 2000 le **ver Hybris**, également connu sous le nom de **Snow White** ou Blanche-Neige a piégé de nombreuses victimes en leur laissant penser que le document attaché était une illustration coquine des aventures **de Blanche-Neige et les sept nains.** Ses diverses variantes provoquent des dommages variés. En général il envoie un message contaminé à chaque correspondant à qui vous envoyez un mail.



Affichage de Hybris, variante C - En réalité l'image est beaucoup plus grande et elle tourne. C'est assez hallucinant.

- **L'année 2001 a été particulièrement féconde.** Il n'est pas question de passer toutes ces bestioles en revue, mais de citer les plus connues. Par exemple **Badtrans, Sircam, Nimda, Magistr (ou Magister)** et la première version de **Klez.** Il a été signalé précédemment que **Magistr** :

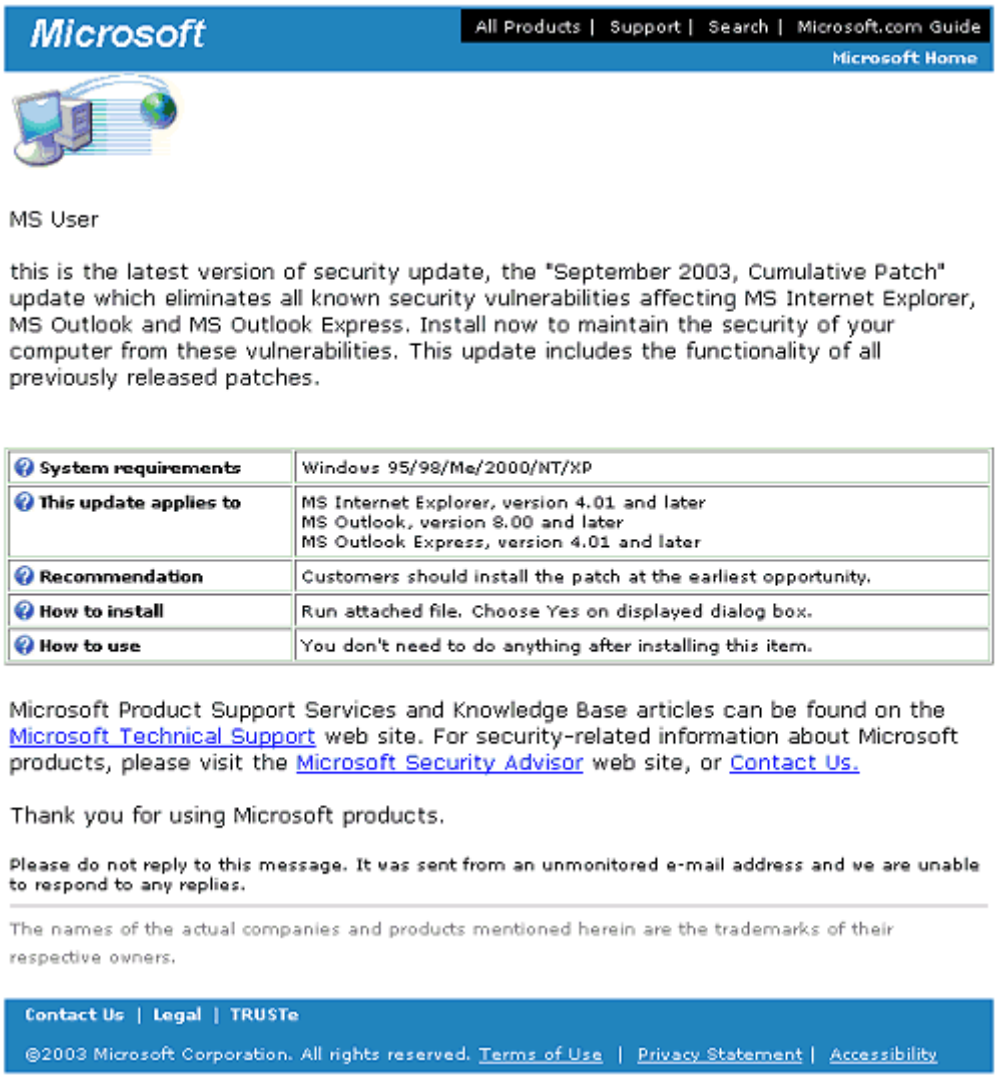
  1°) envoie des mails contaminés pour se propager en prélevant du texte sur votre ordinateur pour constituer le corps du message (ce qui peut avoir pour effet de diffuser des documents confidentiels présents sur votre ordinateur)

  2°) va dans certains cas modifier le contenu du BIOS et de la CMOS, ce qui nécessite généralement le remplacement de la carte mère. Sur un ordinateur infecté par Magistr on peut voir, certains jours, les icônes du bureau s'enfuir à l'approche du pointeur de la souris. Si ce signe apparaît il est urgent de désinfecter l'ordinateur avant la panne totale.

Le **ver Code Red** mérite une mention spéciale. C'est un ver qui ne se propage pas par le courrier, mais **directement par Internet**. Il était conçu pour infecter dans certaines conditions les serveurs Web Microsoft (connus sous le nom IIS, Internet Information Server) en utilisant une faille non corrigée à l'époque. Chaque serveur contaminé envoie vers des adresses aléatoires des requêtes sur le port 80 (celui qui est utilisé par tous les serveurs Web). S'il obtient une réponse à cette adresse le ver va essayer de contaminer la nouvelle machine (technique de scan aléatoire du réseau Internet). Les conséquences sont multiples : activité excessive du serveur dont les performances se dégradent, encombrement du réseau par un trafic parasite, dégradation des pages hébergés sur le serveur.

Le ver ayant fait son apparition en Juillet 2001, l'attaque s'est déroulée principalement sur juillet et août et plus de 250000 serveurs semblent avoir été victimes de **Code Red** dès le mois de juillet. Un nombre non négligeable de responsables de réseau n'ont découvert le problème qu'au retour de vacances.

- **2002 a vu l'apparition de diverses variante de Klez**, en particulier **Klez.H**, toujours très actif et **Bugbear**, encore fréquemment rencontré.
- **En 2003 la vedette des vers de mail a été Swen (ou Gibe), précédé par Dumaru.** Ces deux vers se font passer pour des messages de Microsoft qui proposent un correctif à installer sur l'ordinateur. Bien entendu Microsoft n'envoie jamais de correctif ou d'information par mail, et le prétendu correctif attaché au message est le ver lui-même. Ce ver peut s'installer de lui-même avec des versions non mises à jour d'Outlook Express, sinon il s'installe si on clique sur la pièce jointe. Ce qui a fait le succès de Swen, c'est qu'il imite parfaitement un message de Microsoft si on affiche les mails en mode HTML.



Capture d'écran réduite

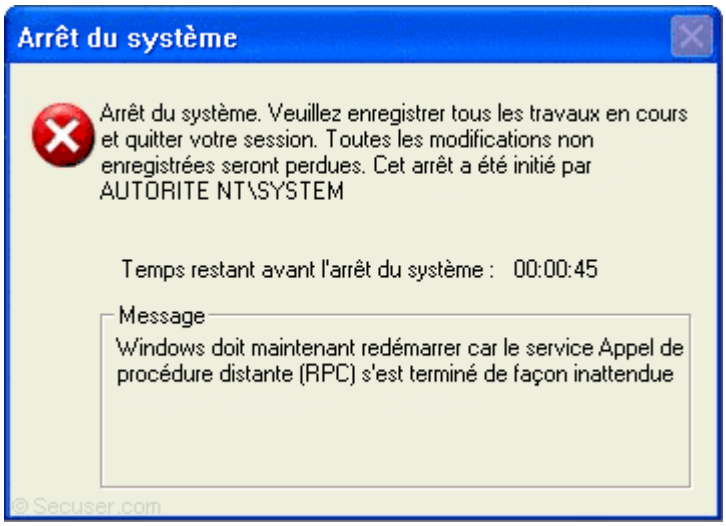
Le ver Sobig a été aussi très actif. Dans sa forme initiale (Sobig.A) expéditeur était big@boss.com. Pour tout dire il fallait être bien naïf pour se laisser abuser par un message provenant d'une telle adresse ! Mais les versions suivantes (en particulier Sobig.F) utilisent d'autres adresses. La stratégie complexe de Sobig sera vue page suivante.

Deux mentions spéciales pour l'année 2003 :

- **Votre ordinateur s'éteint tout seul ?**

  Le **ver Blaster (encore appelé Lovesan, ou Poza).** C'est un ver qui se transmet directement par Internet car il exploite une faille maintenant corrigée (si vous êtes à jour) du service RPC de Windows (c'est le service qui permet les

communications à distance). Ce ver a la particularité de programmer l'extinction automatique de l'ordinateur au grand désespoir de l'utilisateur car il est pratiquement impossible de l'empêcher.



- **Internet s'effondre le 25 janvier 2003**

L'autre mention spéciale concerne le **ver Slammer (ou Sapphire).** Ce ver est remarquable à plusieurs titres. Tout d'abord il exploitait une faille du système de base de données SQL Server de Microsoft. Cette faille avait fait l'objet d'un correctif plusieurs mois auparavant mais, bien que SQL Server soit employé presque exclusivement en milieu professionnel, beaucoup d'organismes n'avaient pas appliqué le correctif. Deuxième caractéristique : le ver ne contenait aucune fonction agressive, se propageait uniquement au travers du réseau Internet, résidait dans la mémoire de l'ordinateur victime sans s'enregistrer dans le disque dur et sa taille n'était que de 376 octets !

Malgré cette taille ridicule Slammer a provoqué une véritable catastrophe. La raison de cette catastrophe est que Slammer générait à grande vitesse des adresses IP aléatoires vers lesquelles il s'envoyait (dans l'espoir qu'à cette adresse il y aurait peut-être un ordinateur utilisant SQL Server). C'est une technique de scan du réseau un peu comparable à celle de Code Red, mais à peu près 100 fois plus efficace. En raison de la conception du ver la fréquence d'envoi n'était limitée que par la vitesse des connexions et des fréquences de 26000 scans/secondes ont été observées. On comprend que malgré la taille très faible du paquet envoyé **des segments entiers de réseau ont pu être saturés.**

Ce n'est probablement pas un hasard si le ver a été lancé sur Internet un week-end, c'est-à-dire à un moment où la plupart des responsables et techniciens réseaux n'étaient pas disponibles. L'attaque a débuté vers 5h30 (temps universel) le samedi 25 juin 2003, peut-être en Asie du sud-est et spécialement en Corée (ce qui correspond à 14h30 pour ce pays) mais l'origine est difficile à certifier en raison de la rapidité de la propagation. **Dans la première minute le nombre de postes infectés doubla toutes les 8,5 secondes ce qui multiplia exponentiellement le nombre d'attaques.** Au bout de 3 minutes le ver atteignit son taux maximum de scan sur le réseau mondial (plus de 55 millions par seconde !). La plupart des machines vulnérables du monde entier ont été infectées dans les 10 premières minutes, mais elles ont continué à scanner le réseau avec la même intensité. La carte des infections montre qu'au bout de 30 minutes l'Asie du sud-est, toute l'Europe et la quasi-totalité des États-Unis étaient totalement contaminés. Le réseau coréen s'effondra totalement avec des conséquences catastrophiques, en particulier pour des établissements bancaires. La plupart des axes principaux du réseau Internet (backbone, dans le jargon des spécialistes) arrivèrent tant bien que mal à maintenir leur connectivité, mais de très nombreux pans du réseau furent complètement paralysés.

Témoignage : tout le réseau universitaire de Bordeaux repose sur une architecture de fibre optique gigabit et il est relié au réseau à haut débit interuniversitaire **RENATER** (une des mailles les plus importantes d'Internet au niveau français). On dispose donc dans l'université de conditions qui relèguent presque l'ADSL au niveau des outils préhistoriques. Pourtant l'accès à l'Internet a été impossible pendant pratiquement tout le week-end. La situation n'est revenue normale que le lundi.

La solution était pourtant simple : il suffisait, au niveau des routeurs principaux des réseaux, de fermer le port UDP 1434 (celui qui permet de communiquer avec SQL Server), d'éteindre les machines contaminées et de les relancer (et bien entendu d'appliquer le correctif qui existait depuis longtemps). Le ver étant uniquement en mémoire centrale, tout rentrait dans l'ordre. **Mais, compte tenu du week-end, du nombre d'ordinateurs à identifier, du nombre de routeurs à programmer, des problèmes de décalage horaire, cela a pris du temps et on a frôlé la catastrophe mondiale (sans parler de catastrophes locales bien réelles).** Heureusement le ver ne contenait aucune fonction de destruction !

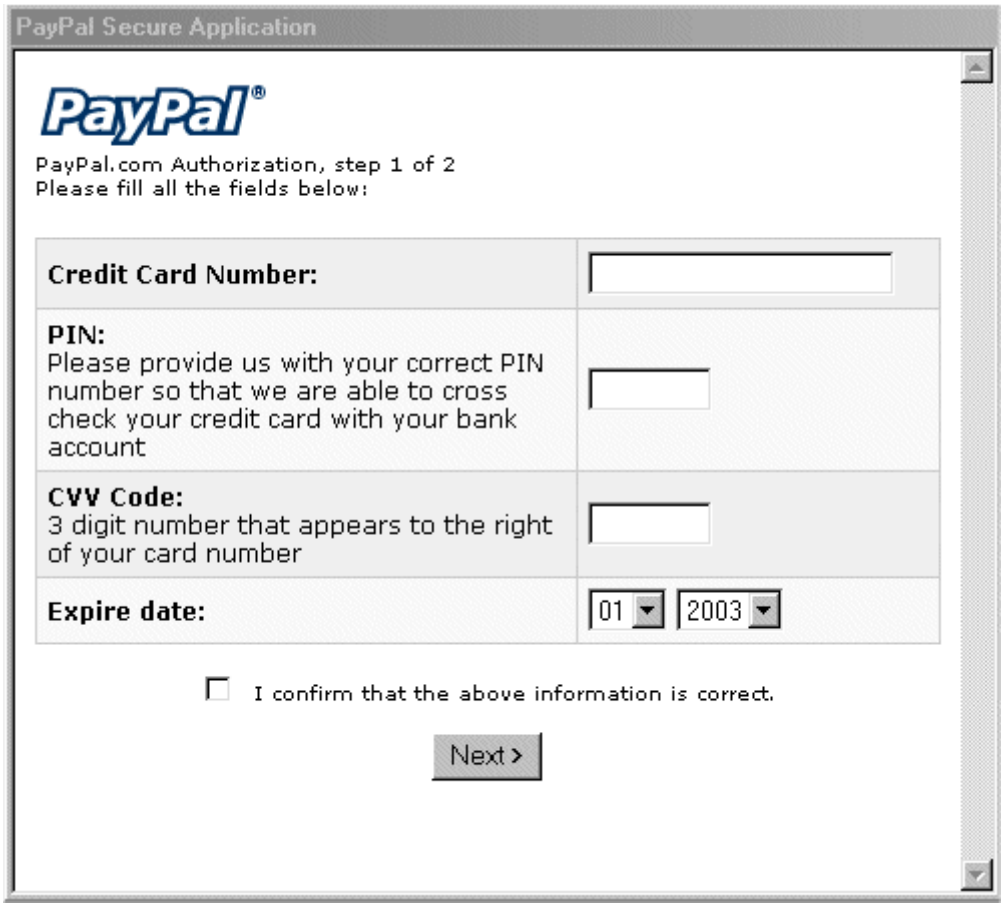
4°) Du jeu pervers à l'escroquerie à grande échelle

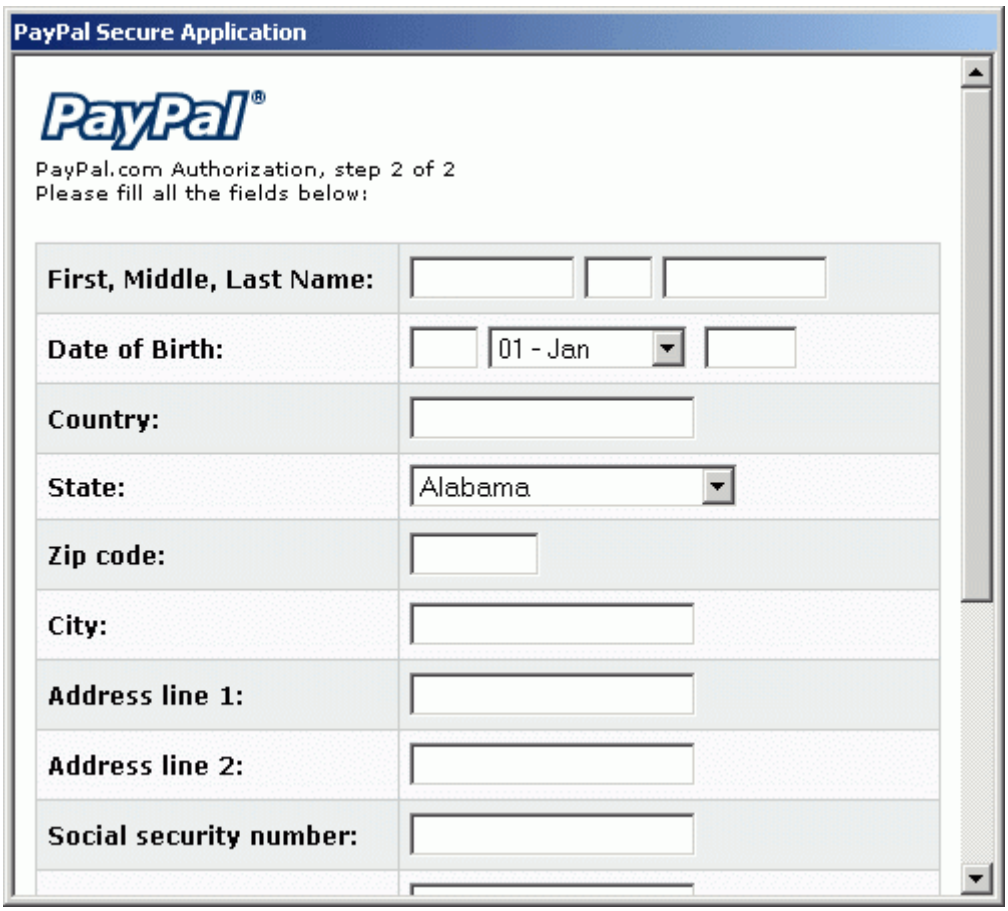
Sans entrer dans le détail du fonctionnement de tous ces vers il faut savoir que certains présentent une grande complexité et des caractéristiques de nuisance importantes.

Par exemple ils peuvent se comporter en **émetteurs massifs de messages** (mails bombers) ce qui peut fortement ralentir l'ordinateur ou saturer la connexion ; ils peuvent installer des **chevaux de Troie** qui permettent à un pirate d'entrer dans l'ordinateur contaminé, ou qui se comportent en **espion du clavier** (key loggers) enregistrant et envoyant à l'auteur du ver tout ce que vous tapez au clavier (mots de passe, numéro de carte bancaire…). Plusieurs d'entre eux peuvent contaminer de proche en proche les **réseaux locaux**, ou se diffuser par IRC, KAZAA, eMule… ou encore contaminer des pages Web qui contamineront à leur tour les visiteurs de ces pages. Certains peuvent aussi contaminer des fichiers de programme et le ver s'exécutera au lancement du programme (fonction virus en plus de la fonction ver). Certains sont aussi capables de **se mettre à jour automatiquement** en contactant des serveurs où les auteurs sont susceptibles de mettre de nouvelles versions.

Pendant longtemps les virus et vers n'ont pas eu d'autres objectifs que de créer des perturbations plus ou moins graves sur les ordinateurs de leurs victimes. Depuis peu ils sont utilisés de façon méthodique pour des délits divers. Ainsi **Bugbear** contient une liste de plus de **1300 noms de domaines utilisés par des banques.** Si l'ordinateur infecté appartient à un de ces domaines (autrement dit, si c'est un ordinateur bancaire), le ver recherche les mots de passe qui pourraient être dans la mémoire cache ainsi que ceux qui sont tapés au clavier et les envoie vers l'une ou l'autres des adresses d'une liste prédéfinie, où l'auteur du ver pourra les récupérer. **Bugbear** installe aussi une backdoor qui permet à un pirate de lire le contenu du disque dur, de copier des fichiers, d'acquérir des informations sur le réseau auquel est relié l'ordinateur, d'effacer des fichiers, etc. Il peut aussi se propager spontanément sur le réseau local (mais comme il ne sait pas distinguer dans le réseau une imprimante d'un ordinateur, un des symptômes possibles est qu'il peut entraîner l'impression d'une suite de caractères incohérents et consommer ainsi jusqu'à 500 pages). **Il est capable d'arrêter le fonctionnement de certains pare-feux et de nombreux antivirus. Bien sûr il s'envoie aussi en masse par mail vers d'autres destinataires.**

Mimail, dans ses variantes I, J et P se présente comme un message de Paypal, un organisme de paiement par Internet très connu et invite, pour mettre à jour le compte du destinataire, ou pour bénéficier d'une offre intéressante, à remplir deux formulaires avec toutes les indications concernant la carte bancaire, l'identité personnelle et l'adresse du destinataire. Ces informations sont envoyées en réalité à l'auteur du ver.

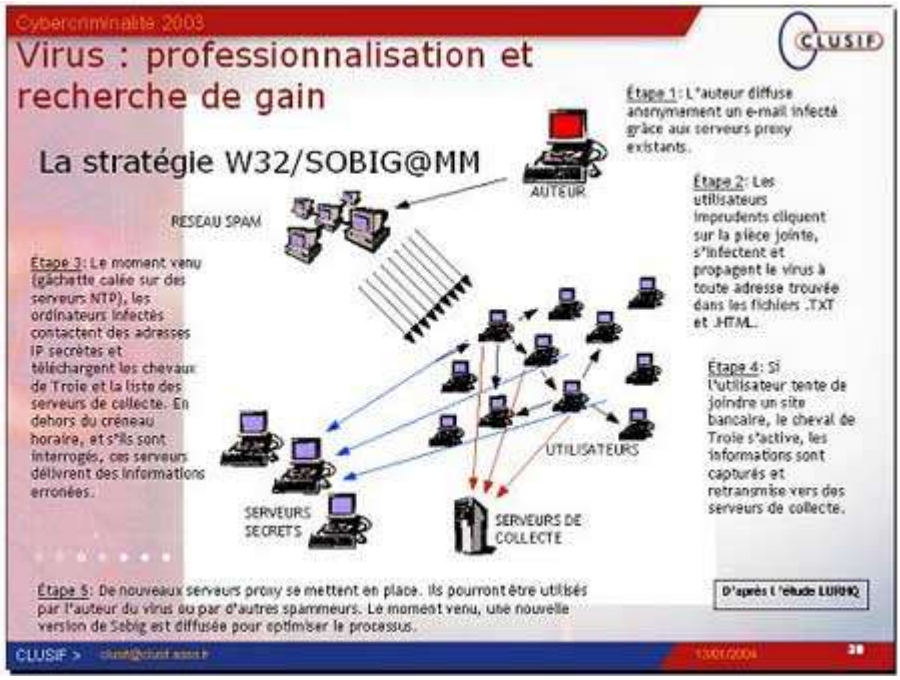



PayPal Secure Application
PayPal
PayPal.com Authorization, step 2 of 2
Please fill all the fields below:
First, Middle, Last Name:
Date of Birth:
01 - Jan
Country:
State:
Alabama
Zip code:
City:
Address line 1:
Address line 2:
Social security number:

Cayam, qui se propage non seulement par mail, mais par P2P utilise un principe comparable en se faisant passer pour eBay, un site d'enchères très connu d'Internet.

S

obig se comporte de manière assez complexe et comporte diverses versions (de a à f à la date de la rédaction de ce dossier). La stratégie de Sobig.e est représentée dans le schéma suivant :



On retiendra que Sobig est capable de capturer de informations confidentielles quand un ordinateur infecté se connecte à certains sites bancaires et qu'en outre il installe sur les ordinateurs infectés des proxy clandestins (programmes servant de relais vers Internet qui permettent de masquer l'origine et l'identité de celui qui les utilise). Le pirate peut donc disposer de milliers de proxy dont il aura recueilli la liste, et par lesquels il pourra diffuser du spam de façon complètement anomyme. Selon certaines sources les 2/3 des spams sont actuellement diffusés par le biais de proxy créés par des vers ou virus.

Et la suite

Ce dossier sera probablement dépassé très rapidement. En effet des mécanismes qu'on n'avait même pas imaginés il y a peu d'années sont couramment utilisés par les malwares actuels. De nouveaux mécanismes seront sans doute rapidement inventés et, si votre ordinateur est bien protégé aujourd'hui, il ne le sera probablement plus bientôt. Mais l'expérience montre qu'il y a tellement d'ordinateurs dont les systèmes et les programmes ne sont pas mis à jour, et tellement d'utilisateurs imprudents, que les vieilles recettes vont certainement être exploitées longtemps.

Plusieurs nouveaux virus ou vers apparaissent chaque semaine. Pour vous tenir informés vous pouvez regarder les actualités de Futura-sciences (et utiliser le moteur de recherches pour retrouver les news passées). N'oubliez pas enfin qu'il existe sur Futura-sciences un forum informatique où vous pourrez poser toutes les questions si vous rencontrez un problème, ou simplement si vous avez besoin d'un conseil.

Tous les éditeurs d'antivirus ont une base de donnée décrivant les divers virus, mais c'est souvent complexe et rarement en français. Des descriptions plus simples dans notre langue peuvent être trouvées ici :

http://www.secuser.com

L'abonnement gratuit aux deux listes de diffusion de ce site est également recommandé.

On peut lire le rapport du Clusif ici :

https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER-CRIMINALITE

en particulier les pages 23-41

Le point préoccupant souligné par ce rapport est la criminalisation de ces procédés d'attaque. **Le monde des vers et des virus passe des mains de programmeurs pervers à celui de milieux troubles cherchant à détourner des informations sensibles, à faire de l'escroquerie à la carte bancaire, ou à utiliser des**

milliers d'ordinateurs pour diffuser des spams douteux ou franchement condamnables de façon totalement anonyme. Il est probable que cette tendance va s'aggraver dans les mois qui viennent. Comme personne ne souhaite se rendre complice, même involontairement, d'un délit ceci signifie qu'utiliser et **mettre à jour son antivirus**, **utiliser correctement un pare-feux, ne sont plus uniquement une affaire de choix et de confort personnel, mais engage notre responsabilité à l'égard d'autrui** (de la même manière que conduire une voiture dont les freins ou la direction sont en mauvais état met en danger la vie des autres automobilistes).

Crédits pour certaines recopies d'écran : Clusif, McAfee, Symantec.

5°) Dernières nouvelles

Depuis la rédaction de ce dossier la communauté des internautes a été confrontée à plusieurs vers dignes d'intérêt. Il n'est pas question de tout récapituler car il apparaît un ou plusieurs vers/virus pratiquement tous les jours. Beaucoup sont des variantes de malwares déjà connus, mais il y a eu quelques créations originales qui ont posé de sérieux problèmes. L'objectif de cet additif est de montrer l'activité incessante des créateurs de ces programmes malveillants. Dans l'avenir il sera complété chaque fois qu'un ver ou virus ayant un impact très important apparaîtra.

- **23/01/04**

  Dumaru.Y, a été suivi le 25 par **Dumaru.Z**, le 3/02 par **Dumaru.AD** et le 10/02 par **Dumaru.AH**. Toutes ces versions se présentent de manière assez différente du Dumaru initial. Le message semble provenir d'une dénommée Elene (sauf pour AH) et possède une pièce attachée intitulée **myphoto.zip** qui contient un fichier appelé

  myphoto.jpg .exe

.Compte tenu de la distance que sépare jpg de exe, l'immense majorité des utilisateurs n'a pas vu qu'il s'agissait d'un exécutable. Si on clique sur le fichier dans l'espoir de voir une photo ce dernier est exécuté. Le ver s'envoie aux correspondants dont les adresses e-mail figurent dans le carnet d'Outlook Express et dans divers autres fichiers, installe **un cheval de Troie** puis un **keylogger** qui espionne les frappes au clavier. Toutes ces versions semblent d'être répandues rapidement et ont fait de nombreuses victimes.

- **26/01/04**

  Apparition de **Mydoom.A** (appelé Novarg ou Worm_Mimail.R par quelques éditeurs d'antivirus), ver qui a beaucoup fait parler de lui dans les media. Le texte du message est du type :

  The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
  ou
  The message contains Unicode characters and has been sent as a binary attachment.

Mais ce texte peut parfois être différent ou se présenter sous la forme d'une suite de caractères incohérents.
Le fichier attaché porte des noms divers mais sa longueur est de 22,258 octets (arrondi à 22,5 Ko par Outlook Express). Son extension est également variable ; dans certains cas l'extension peut être **zip** (la longueur du fichier compressé est alors un peu plus grande, ce qui n'est qu'un paradoxe apparent). Ce ver s'est répandu de façon extrêmement rapide (on soupçonne que sa diffusion massive a pu être préparée à l'avance). Il envoie de façon intensive des mails infectés, installe une **backdoor** qui ouvre les ports TCP 3127 à 3198, ce qui lui permet éventuellement de télécharger et d'exécuter des programmes nocifs venant de l'extérieur.

Il était aussi programmé pour effectuer entre le 1/02/04 et le 12/02/04 une attaque en masse à partir des ordinateurs contaminés vers le site www.sco.com (site de la version SCO d'UNIX). Cette attaque a abouti à un déni de service distribué (dDoS) qui a complètement paralysé ce site et la société a dû changer son adresse.
Il a été programmé pour arrêter sa diffusion et son attaque du site de SCO après le 12/02 ; un doute subsiste toutefois sur ce point à cause d'un bug dans son code. **Mais la backdoor installée restera active sans limitation de date.**

Par contre la variante **Mydoom.B** du 28/01 ne s'est pratiquement pas répandue en raison de bugs dans son code. Elle était programmée pour faire un déni de service sur **www.sco.com et www.microsoft.com**, mais ce fut un échec.

- **6/02/04**

Apparition de **Deadhat** initialement appelé **Vessel ou Vesser** selon les éditeurs d'antivirus (une variante B est apparue de 12/02). **Il ne se propage pas par mail** mais en recherchant sur Internet les ordinateurs infectés par **Mydoom**. En effet **Deadhat** exploite la backdoor de **Mydoom** en tentant d'entrer dans les ordinateurs contaminés par les ports 1080, 3127 et 3128. Il se copie alors dans le répertoire Windows\system (ou system32) sous le nom **sms.exe.** Il ouvre ensuite le port 2766 et attend une connexion (backdoor TCP). Seul un "client" identifié par une clé cryptée (l'auteur du ver) peut utiliser cette connexion.

Il se connecte aussi à un serveur IRC prédéfini et reste en attente de commandes envoyées par l'auteur (backdoor IRC). L'une ou l'autre des backdoors permettent le chargement et l'exécution sur l'ordinateur de

n'importe quel programme, a priori nocif. **Deadhat** supprime l'infection par **Mydoom**, mais interrompt toute une série de processus, et surtout bloque une liste impressionnante de programmes antivirus et de pare-feux. Si l'ordinateur utilise le système P2P **SoulSeek**, le ver se recopie sous divers noms attractifs dans le répertoire partagé, ce qui constitue sa deuxième méthode de propagation.

- **9/02/04**

  Doomjuice.A, qui a aussi été appelé temporairement Mydoom.C, est un autre ver exploitant la backdoor de Mydoom. Il pénètre par le port 3127, ouvert par cette backdoor, et se copie dans le répertoire système (comme le précédent). **Il lancera des attaques dDoS contre www.microsoft.com du mois de Mars au mois de Décembre.**

- **12/02/03**

  Doomhunter est un ver plus sympathique que les précédents. Lui aussi tente de se propager directement par l'Internet en exploitant le port 3127 ouvert par la backdoor de **Mydoom**. Lorsqu'il s'est installé il tente d'arrêter tous les processus reliés à **Mydoom** ainsi que **Blaster (il se comporte comme un outil de désinfection !)**. Ensuite il scanne des adresses au hasard jusqu'à ce qu'il trouve d'autres ordinateurs contaminés par **Mydoom**. Malgré son caractère curatif il ne faut pas laisser ce ver sur l'ordinateur car il génère une activité parasite en recherchant d'autres adresses. De plus rien ne garantit qu'il soit totalement efficace et ne produise aucun effet secondaire.

  Ces trois vers qui exploitent la backdoor de **Mydoom** ne sont probablement qu'un début. Toutefois leur propagation sera plus lente que celle de **Mydoom** puisqu'ils doivent obligatoirement trouver des ordinateurs déjà infectés par ce ver en scannant des adresses IP au hasard pour se propager. Il n'est donc pas sûr du tout que l'attaque du site de Microsoft par **Doomjuice** produise des effets importants.

- **11/02/04**

  Welchia.B (ou Nashi.B) est un autre ver se proposant de désinfecter les ordinateurs contaminés par **Mydoom** et de télécharger divers patches correctifs de Microsoft pour mettre à jour le système (seulement les versions anglaises, chinoises et coréennes) ! Il se propage lui aussi à travers le réseau Internet ; toutefois il n'utilise pas la backdoor de **Mydoom**, mais diverses failles de

Windows, dont la faille RPC déjà signalée pour **Blaster**. Il ne peut donc s'installer que sur un ordinateur dont le système n'est pas à jour. Il entraîne une instabilité du fonctionnement en interférant avec le service RPC. La première version de ce ver (18/08/03) tentait d'éradiquer **Blaster** des ordinateurs, mais installait aussi subrepticement un programme TFTP qui pouvait être employé pour des usages illicites.

Enfin nous terminerons (provisoirement) cette énumération par un ver plus classique, **Mimail.S**, apparu le 29/01/04. Bien que très malhonnête, il a un côté facétieux. En effet, au lieu d'afficher dans le mail un message de Paypal destiné à récupérer les informations de carte bancaire de lecteurs naïfs, celui-ci affiche un message de Microsoft annonçant que la licence de Windows de l'utilisateur est arrivée à échéance et demandant des informations sur la carte de crédit. Là, il faut être vraiment **très naïf** pour se laisser prendre !