Les virus informatiques

Table des matières

Ces pages sont à considérer comme un ensemble de **documents sur les virus**, plus que comme un cours proprement dit. Vous constaterez vite que l'on y parle, dès le début, de notions qui ne seront explicités que plus loin dans le texte... Effectivement, ce document ne veut pas être un cours sur la manière de créer des virus, mais bien plus un document de réflexion, un peu sur les virus, un peu sur l'informatique, beaucoup sur les enjeux, et sur le comportement que l'on pourrait avoir vis à vis des uns, et de l'autre.

A document particulier, méthode particulière. Il vous faut ici saisir un ensemble d'informations, souvent redondantes, au lieu d'une progression supposée (espérée…) logique. Il va vous falloir lire tout le document[1], y compris son annexe[2] avant de saisir tout ce que l'auteur a voulu y mettre à votre attention. Heureusement pour vous, si les paroles s'envolent, les écrits restent. Vous pourrez donc relire ce volume à plusieurs reprises, afin d'en tirer vos propres conclusions...

[1] - De préférence attentivement, sans hésiter à vous servir d'un dictionnaire et/ou du document consacré à la machine et à son système d'exploitation. Néanmoins, n'insistez pas trop sur les parties très techniques, comme par exemple certaines descriptions du fonctionnement interne des virus : ne retenez que l'esprit de la chose, et non le détail…

[2] - ...et surtout la dernière partie de cette annexe, qui permet de relativiser ce qui précède, ainsi que tout ce que vous entendrez sur les virus informatiques.

En guise d'introduction

Le phénomène des virus est apparu sur le devant de la scène vers la fin de 1988, mais il existait depuis près de dix ans. **Michelangelo** n'a pas été le premier à causer des déprédations, et il ne sera pas le dernier. Surtout, ne croyez pas que les virus les plus récents soient les plus dangereux. Selon la **NCSA** (**National Computer Security Association**), les virus **JerusalemB** (découvert en 1987) et **Stoned**[3] ont été responsables de 74% des incidents survenus en 1991. Pourtant, le plus jeune de ces virus avait déjà trois ans, et tous deux étaient bien connus. Viennent ensuite (toujours pour 1991) les virus **Brain** (découvert en 1986), **Vienna** (découvert en 1988), **Ping-pong** (également découvert en 1988) et **1701/1704** (découvert en 1989). Et ce n'est pas fini ! On pourrait continuer cette énumération sur plusieurs pages !

Lorsqu'une affaire comme celle de Michelangelo, celle de Melissa, ou encore celle de ILOVEYOU, survient, le débat s'élève entre ceux qui pensent que le **danger est énorme** et ceux qui estiment qu'il se trouve **gonflé à l'excès par les éditeurs d'antivirus**.

[3] - Découvert en 1988, STONED a été, à l'époque, considéré à juste titre comme très dangereux…

0.1 - Les virus existent

Les virus...

Les virus sont aux PC ce qu'est la grippe à l'hiver : un fléau bête et méchant contre lequel on ne peut que prendre des précautions. Et comme pour la grippe, il faut chaque année trouver de nouveaux vaccins (informatiques) contre de nouveaux virus (informatiques).

Sachez-le dès à présent, il n'existe aucun virus que l'on puisse qualifier de gentil. Qu'il se contente d'afficher un message, de se multiplier, de détruire vos fichiers, ou pire, de détruire toute la structure d'un disque dur, un virus est par définition dangereux. Même les plus inoffensifs en apparence sont susceptibles de provoquer les plus grands désastres. Sans oublier qu'ils sont la preuve de l'introduction d'un étranger dans votre espace de liberté...

...toujours en avance...

De plus en plus malins, de plus en plus vicieux, les virus informatiques sont toujours là, et aucun antivirus n'y pourra jamais rien. Intelligence (?) du créateur (*car les virus informatiques sont créés par l'homme, il ne faut pas l'oublier*) mise gratuitement (?) au service d'un petit morceau de programme destructeur, contre intelligence, rémunératrice celle-ci, des concepteurs d'antivirus : le combat est sans merci. Et inégal, puisque celui qui crée le virus a toujours une longueur d'avance sur celui qui tente de protéger. Le dindon de la farce ? L'utilisateur qui assiste, impuissant, à la destruction de ses données, faute d'avoir pris un minimum de précaution.

Les dernières nouveautés importantes dans le monde des virus ont été le virus polymorphe, et surtout les virus infecteurs de documents[4] (leur ancêtre est **Winword.concept**, dont a été victime le logiciel Microsoft Word, à partir de la version 6). Deux exemples qui prouvent l'acharnement sans borne des créateurs de virus.

...attaquent à présent vos documents.

Jusqu'à ces dernières années, une règle prévalait chez les victimes de virus : ce petit (bout de) programme indésirable ne pouvait être véhiculé que par un autre programme. En clair, seuls les fichiers exécutables (comme les **.COM** et les **.EXE**, par exemple) pouvaient être infectés. C'était déjà beaucoup. A contrario, les documents, par essence inerte et sans intelligence, puisque destinés à être uniquement consultés ou modifiés par un logiciel approprié, ne pouvaient pas être des facteurs d'infection. Une disquette ne contenant que des fichiers **.DOC** ou **.XLS** pouvait donc être échangée sans crainte, pour peu que l'utilisateur se protège un minimum : une telle disquette ne peut en effet renfermer que certains types de virus, biens connus.

Eh bien, c'est fini ! Pourquoi ? Simplement parce que les nouvelles versions des logiciels bureautiques comme (à partir de Word 6, et bien évidemment les versions suivantes) rendent vos documents soi-disant intelligents. Macrocommandes, Word Basic, VBA *(Visual Basic for Applications*), autant d'instructions qui constituent des mini-programmes. Or qui dit programme dit en même temps la possibilité d'infection par un virus ! Un concepteur de virus s'est aperçu de cette possibilité et désormais plus aucun fichier Word n'est à l'abri de nouveaux virus de type **Win-**

[4] - Incorporés aux macrocommandes associées à un document, ils constituent la famille des **macro-virus**. S'ils sont écrits dans un langage connu des logiciels de communication, comme le Visual Basic Script, ils peuvent se répandre encore plus vite par le biais des messageries. Beaucoup plus sournois que les virus classiques, ils en sont d'autant plus dangereux 'voir plus loin le cas de ILOVEYOU). Toutefois, il est (relativement) facile de lutter contre eux.

word.concept. Pire, aujourd'hui, la brèche est ouverte, le mal se propage rapidement aux autres applications utilisant des macrocommandes... (Excel, Access… par exemple, et cela quel que soit le système d'exploitation !)

Ils peuvent se cacher...

La bonne vieille méthode de recherche de virus qui consistait jadis[5] à contrôler la taille des fichiers est aujourd'hui dépassée. Car si dans les premiers temps les virus se greffaient effectivement à la suite des fichiers exécutables, modifiant leur taille, il y a belle lurette que cette tactique, trop aisément identifiable par les programmes antivirus a été remplacée par d'autres. Désormais les virus sont **furtifs** (ils donnent l'impression de se déplacer en apparaissant et en disparaissant) ou **polymorphes** (leur code, crypté, varie lors de chaque infection), et ils se dissimulent au cœur même du fichier exécutable en profitant des espaces vides laissés lors de la compilation, ou encore vont se loger au fond des clusters incomplets...

Aujourd'hui, ce qui se fait de mieux, c'est l'imitation de la nature. En clair, il s'agit d'observer les virus biologiques les plus méchants, les plus agressifs du monde réel et de s'en inspirer pour créer des virus informatiques.

... et changer de forme...

Les récents virus polymorphes (tels que **Smeg.pathogen** et **Smeg.queeg**) en sont la parfaite illustration. Directement inspirés de la réalité biologique, ces virus sont multiformes. Ils se répandent en changeant à la fois de taille et d'aspect. Bref, l'horreur absolue pour les détecteurs de virus. Ces derniers repèrent en effet le plus souvent les virus par leur **signature**, c'est à dire leur code. Si ce code change en permanence, vous imaginez aisément à quel point il devient délicat de les repérer. Seuls les antivirus les plus récents sont capables de détecter la présence de ces nouveaux monstres. Face à eux, les anciens antivirus sont presque aussi efficace que de l'aspirine saupoudrée sur une jambe de bois...

... pour utiliser les moyens les plus modernes.

Mais ce n'est pas tout : les inventeurs de virus continuent leur basse besogne dans d'autres directions. Ce que souhaite un créateur, c'est que sa créature devienne célèbre. Et pour atteindre la notoriété, un virus doit se répandre et se multiplier, faire parler de lui. Or, comment mieux circuler, si ce n'est par l'autoroute (de l'information) qu'est **Internet** ? C'est à la mode, pratique, rapide et efficace. Bref le ticket assuré pour la célébrité... Il est en effet possible qu'un PC soit infecté uniquement en consultant une page Internet[6].

Jusqu'à présent, le risque d'infection par réseau était limité aux fichiers programmes. Vous le télécharger, vous l'utilisez, et le virus se répand. Risque assez faible, il faut reconnaître. La majeure partie des prestataires de service auraient trop à perdre si l'un des fichiers proposés était infecté. Mais sur Internet, avec des centaines de milliers d'utilisateurs qui commencent à proposer des pages personnelles, à laisser un CV ou une petite annonce, comment tout contrôler ? Impossible ! **Internet, victime de son succès, est totalement incontrôlable**. Il y a pire. A un message électronique (un mail) peut être attaché un fichier contenant un virus. Vous consultez le message, vous regardez le fichier attaché, et votre disque dur est infecté. Ni vu ni connu. Avec les derniers virus apparus, il n'est plus nécessaire d'ouvrir un fichier attaché. Le virus est présent à l'intérieur du message...

[5] - Terme à relativiser en informatique...

[6] - C'est possible, mais (encore) très rare. Par contre, le courrier électronique, avec sa possibilité d'expédier des documents attachés est un redoutable vecteur de macro-virus, comme c'est mentionné dans le paragraphe suivant…

Faut-il en déduire que tous les services de communication en ligne et tous les services de téléchargement sont susceptibles de véhiculer de nombreux virus ? Non. L'expérience le montre, seul Internet, par sa liberté totale, est un facteur de risque (plutôt faible, il est vrai). Tous les autres services proposent des fichiers contrôlés à plusieurs reprises...

0.2 - Les virus font peur

La plupart des média, et pas seulement les revues spécialisées, parlent un jour ou l'autre des virus informatiques. Le ton est toujours le même, alarmiste...

Mélissa se propage via le courrier électronique, **W95.CIH** contamine Windows 95/98 et détruit, le 26 du mois, les données des disques durs, **WIN95.CIH**, dit aussi Tchernobyl, est considéré comme excessivement dangereux... On ne compte plus le nombre de personnes mises en difficultés parce que leur système a été endommagé par un virus. C'est un fait, à la veille du XXI° siècle, plus de vingt ans après leur première apparition, les virus informatiques constituent toujours une véritable menace.

Télévisions et radios produisent des reportages sur le sujet pour sensibiliser le public. Rien n'y fait. Malgré la (sur)médiatisation du phénomène, certains oublient toujours de se protéger et se font infecter. Chaque mois de nouvelles formes d'attaque apparaissent. Plus complexes, plus difficilement détectables et même parfois armés pour lutter contre les antivirus, les virus ont su s'adapter aux nouvelles technologies. Ainsi, si ceux fonctionnant sous DOS ont pratiquement disparu, ceux qui attaquent Windows 32 bits[7] et les macrovirus ont émergé. Parallèlement, il faut savoir que le protection contre les virus est devenue, plus que jamais, un véritable commerce. Les antivirus demeurent une solution largement adoptée par les entreprises. Ainsi, selon une étude IDC, le marché de l'antivirus a généré, en 1998, un chiffre d'affaires de plus de 600 millions de francs sur le territoire français. De fait, les éditeurs d'antivirus se mènent une guerre commerciale de plus en plus rude.

Jusqu'à ces dernières années, les virus s'échangeaient par le biais des disquettes. Aujourd'hui, les réseaux, et en particulier **Internet**, constituent le principal vecteur d'infection. Ils permettent la diffusion de virus au travers du courrier électronique (c'est le cas de Mélissa). En ouvrant un document Word infecté, ou en exécutant un fichier contaminé, le destinataire propage le virus sur sa machine. Dans la majorité des cas, l'auteur du message n'est pas conscient du fait qu'il a émis un virus, celui-ci s'étant installé à son insu... Il y a là de quoi alimenter les peurs...

Alors, doit-on céder à la paranoïa ?

Ou bien faut-il dire « *lisez ce document et soyez rassurés* » ?

[7] - En particulier les versions 95 et 98 (et Windows NT)

Chapitre 1 : Pour mieux comprendre

Le titre complet de ce chapitre aurait pu être...
Pour mieux comprendre des mythes difficiles à combattre

Des fichiers sont endommagés, c'est la preuve formelle que l'ordinateur a été victime d'une attaque de virus.

c'est FAUX...
le problème peut avoir été provoqué par n'importe quoi,
et souvent par une fausse manœuvre de l'utilisateur.
.

Un logiciel du commerce protégé contre la copie ne peut pas subir d'attaque virale.

c'est FAUX...
ce sont au contraire les plus vulnérables en cas d'attaque par
un "Cheval de Troie", car ils sont les plus difficiles à protéger.

Les virus peuvent se propager sur toutes sortes d'ordinateurs.

c'est FAUX...
mais en partie seulement !
chaque virus "classique" est limité à une famille d'ordinateurs,
un virus PC sera incapable d'infecter un Macintosh et inversement.
Il n'en est plus de même avec les macro-virus les plus récents…

Les virus peuvent se cacher dans n'importe quel fichier, même un simple fichier de texte.

c'est FAUX...
mais en partie seulement !
un fichier exécutable peut provoquer des dommages, mais
depuis peu, c'est aussi le cas de certains documents complexes !
Toutefois, soyez rassuré, les documents ordinaires restent à l'abri des attaques.
Aucun virus ne peut infecter un fichier de type texte seul.

1.1 - Quelques idées fausses à bannir...

La cause est entendue, tous les responsables informatiques ou les administrateurs de réseaux, alertés par le problème des virus, vous diront exactement la même chose : « *Les utilisateurs sont complètement irresponsables en ce qui concerne la protection de leur poste de travail* » Pourtant, il n'est pas rare que certains de ces irresponsables exploitent au moins un antivirus, souvent plusieurs, sur leur poste de travail ou sur leur machine personnelle, alors que le serveur et les applications présentes sur ses disques n'ont jamais inquiété le responsable système. C'est lui qui a installé tout cela, donc c'est bien fait...

Certains administrateurs interdisent, sans autre forme de procès, l'introduction de fichiers exécutables sur les postes individuels[8] et condamnent sans appel toute connexion à un **BBS** (**B**ulletin **B**oard **S**ystem) ou au **réseau des réseaux**, Internet. Au contraire, d'autres ne se soucient guère des virus, les considérant encore comme une simple invention médiatique ou un phénomène pour le moins étranger.

Si cette dernière attitude demeure ridiculement insouciante, la première ne l'est pas moins. En général, les paranoïaques du virus, et les dictateurs en puissance[9], s'ils n'ont pas réussi à retirer tous les lecteurs de disquettes et à déconnecter tous les ports de communication des stations de travail, « éduquent » leurs utilisateurs non pas en leur donnant des moyens de lutte efficaces (qu'ils ne possèdent d'ailleurs pas toujours eux-mêmes), mais en véhiculant tout un **éventail de légendes**. En voici quelques exemples, parmi les plus classiques.

PAS DE PIRATAGE DANS L'ENTREPRISE

C'est indiscutablement une excellente chose, mais les disquettes contenant un logiciel piraté n'ont ni plus ni moins de chances que les autres d'être infectées. Le battage fait à ce sujet, notamment par l'**Association française des éditeurs de logiciels** (Afel) et quelques autres organismes de protection des droits de copyright des programmes, ne correspond qu'à l'entretien soigneux du mythe alliant virus et piratage. Et le Père Fouettard de menacer : « *Si vous piratez, vous aurez des virus...* » Pourtant, rien n'interdit de vérifier l'intégrité d'une disquette, même piratée. C'est d'ailleurs ces dernières que l'on vérifie le plus souvent. On fait confiance aux autres. L'expérience montre que c'est parfois une erreur ! Parfois ? Non, presque toujours...

Quant au piratage en lui-même, que vous en soyez conscient ou non, c'est une forme d'appropriation indue du résultat du travail d'autrui, et **donc un vol, condamnable** en temps que tel d'amendes ou de peines de prison... Sans compter le manque à gagner des éditeurs, qui les pousse à se rattraper sur ceux qui jouent le jeu, et qui payent pour les autres...

LES LOGICIELS GRATUITS SONT INTERDITS DANS L'ENTREPRISE

Les programmes commerciaux dûment achetés et sous emballage ne présentent pas beaucoup moins de risques que les freewares et sharewares diffusés par le biais de société sérieuses où la menace est prise très au sérieux, et depuis longtemps. Néanmoins, plusieurs éditeurs réputés se sont déjà laissés prendre, ou plutôt surprendre, par le piège d'une contamination sans que jusqu'à présent les conséquences ne se soient révélées dramatiques. En fait, par précaution,

[8] - En réalité, cette mesure est le plus souvent un moyen de lutter contre le piratage, le problème des virus n'étant alors que le moyen de faire peur à l'utilisateur peu averti. Néanmoins, il faut aussi savoir qu'il peut exister des incompatibilités entre certains logiciels et le bon fonctionnement d'un poste à l'intérieur d'un réseau. Dans ce cas, aucune installation de logiciel ne doit donc être faite, en principe, sans l'avis d'une « personne autorisée ».

[9] - Du style « *vous ne faites sur votre ordinateur que ce que je vous laisse faire, et encore...* »

avant l'introduction de tout nouveau programme au sein d'un réseau, il faudrait en passer par un détecteur de virus, voire par plusieurs. Retenez dès à présent qu'aucun logiciel antivirus n'est efficace à 100 %. La sécurité absolue n'existe nulle part. Pas plus en informatique que sur la route. Par contre, on peut faire en sorte de tendre vers elle en multipliant les précautions…

PAS DE TÉLÉCHARGEMENT SUR UN SERVEUR TÉLÉMATIQUE

Les responsables des BBS se tiennent en permanence informés de l'évolution des risques. Prompts à combattre activement le mal, ils proposent également des solutions antivirales en freeware et en shareware. En outre, ils permettent de récupérer des informations sur les nouveaux virus et éventuellement leur signature. L'autre idée reçue qui prétend qu'en téléchargeant on s'expose totalement aux contaminations virales n'est pas plus véridique que la précédente. Disons simplement qu'**il faut choisir avec précaution** les BBS et autres serveurs sur lesquels on se connecte. Les services ayant pignon sur rue et dont les numéros d'accès apparaissent régulièrement dans les colonnes des revues sérieuses sont généralement très protégés. En conséquence, une entreprise court beaucoup plus de risques en téléchargeant par modem les programmes d'une succursale dont elle ne contrôle pas les accès informatiques !

Il en est de même des services de téléchargement offerts par Internet : ce sont aussi des BBS. Seul le mode de connexion change. La principale différence est que leur zone d'activité n'est plus locale, ou nationale, mais bien mondiale. Les fournisseurs sérieux n'offrent pratiquement aucun risque, par contre, il est conseillé de se méfier d'un site créé par un inconnu qui propose le téléchargement de deux ou trois programmes artisanaux…

N'EXPLOITEZ AUCUNE DISQUETTE PROVENANT DE L'EXTÉRIEUR

Il s'agit évidemment d'une bonne solution pour empêcher de très nombreuses infections, mais l'utilisateur n'a plus alors la possibilité d'échanger simplement des informations, pas plus que de faire des sauvegardes, ni d'emporter du travail hors du bureau (pour la clientèle, les heures supplémentaires réalisées à domicile ou en voyage, etc.) ni même de personnaliser son environnement de travail. Pourtant, il est parfaitement possible de configurer certains antivirus afin qu'ils examinent systématiquement toute disquette introduite dans le(s) lecteur(s).

Le terme **extérieur** est aussi à préciser. En effet, si plusieurs systèmes sains à un instant donné n'échangent de disquettes qu'entre eux, et uniquement entre eux, le risque d'infection est faible, quasi nul. Par contre si une disquette infectée s'introduit dans le circuit...

NE VOUS INQUIÉTEZ PAS, LES VIRUS SE TROUVENT ESSENTIELLEMENT AUX ÉTATS-UNIS

Ou la version micro-informatique du « *cela n'arrive qu'aux autres* ». S'il est vrai que les Américains sont plus touchés par le phénomène, force est de reconnaître que les micro-ordinateurs et les réseaux locaux sont aussi plus nombreux outre-Atlantique qu'en Europe. Toutefois, il ne faut pas oublier qu'un grand nombre de virus proviennent d'Europe (Bulgarie, Hollande, Italie, Pologne, Allemagne, etc.), sans omettre les virus tricolores (Malaise, Paris, Fiché, Mardi Bros, etc.). Enfin, rappelons que la moitié des responsables informatiques français reconnaît **officieusement** avoir déjà eu affaire à un virus, une quantité somme toute beaucoup plus élevée que celle révélée par les statistiques officielles américaines (et françaises)...

1.2 - Des micro-ordinateurs en terrain découvert

La micro-informatique s'est développée à une vitesse extrêmement rapide, trop rapide même de l'avis de ceux qui doivent changer de matériel tous les deux ou trois ans, et ses utilisateurs n'ont pas réalisé qu'ils manipulaient des outils à haut risque. Alors que les mini et grands systèmes faisaient l'objet de normes de sécurité avancées et de stricts contrôles des droits d'accès aux données, **les micro-ordinateurs sont demeurés accessibles à tous**[10]. Y compris, malheureusement, à des individus aux intentions peu amicales. Lesquels ont concocté des nuisances logicielles qui sont aujourd'hui la hantise des directeurs bureautiques. C'est peut-être le prix à payer pour préserver un certain mode de vie...

Aucune grande entreprise ne devrait aujourd'hui utiliser des PC sans avoir mis en place des mesures de protection d'une rigueur absolue. Les utilisateurs individuels de PC peuvent éventuellement se passer d'un antivirus s'ils n'emploient que très peu de logiciels ou s'ils ne manipulent qu'un nombre restreint de disquettes en provenance de cet « extérieur » évoqué plus haut. L'installation d'un logiciel antivirus récent dans chaque machine reste cependant fort recommandée à tous, de même que sa mise à jour régulière (mensuelle ou trimestrielle). **Nul ne se trouve totalement à l'abri en l'absence de la protection adéquate**. Cette protection peut être assurée par la limitation des échanges de logiciels, par les précautions d'usage lors d'échanges d'informations, et/ou par des solutions logicielles, sans oublier les verrouillages divers, ou l'absence de lecteur de disquette...

Une enquête de **Dataquest** concernant le Nord des **États-Unis** a montré que 38% des sociétés consultées avaient perdu des données à un moment ou à un autre pour cause de virus. **Le problème est qu'un grand nombre de PC sont infectés et que leurs propriétaires n'en ont pas conscience**[11] **!** En effet, un utilisateur peut fort bien posséder un PC dont le disque dur fourmille de virus, l'ignorer et donc ne prendre aucune mesure de défense. **Certus International** a réalisé une étude sur quelque 2500 sites et a découvert des PC infectés dans un cas sur deux.

En mars 1992, selon Winn Schwartau de la **NCSA** (**National Computer Security Association**), un million d'ordinateurs environ étaient infectés par un virus au niveau mondial. A la même époque, seules 15% des entreprises avaient mis en œuvre les mesures de sécurité adéquates, d'après Dataquest. Le risque est tellement important que plusieurs compagnies d'assurance refusaient purement et simplement de couvrir les entreprises qui en faisaient la demande.

Pour en terminer sur ce sujet précis, il faut rappeler que si les virus peuvent être à l'origine de problèmes ou d'incidents, ces derniers ne sont pas toujours provoqués par des virus. On prend trop souvent des incidents classiques et normaux pour des attaques virales. C'est une excuse facile, trop facile même, pour certains…

---

[10] - C'est là d'ailleurs que réside leur principale qualité. Si cette forme de liberté venait à être remise en cause, pour quelque raison que ce soit, ce serait pour le moins fort regrettable. N'oubliez pas qu'au temps de l'ex-URSS, la possession d'un ordinateur, d'un photocopieur, ou même d'un simple duplicateur à alcool était interdite à un particulier. Dans les administrations, on procédait régulièrement au **comptage** des feuilles de papier, y compris celles jetées dans les corbeilles à papier, pour empêcher la diffusion de documents subversifs...

[11] - ...et parfois, lorsqu'ils le découvrent, ils accusent d'autres personnes, ou leur entreprise, d'être responsables de cet état de fait, alors que le plus souvent, ils se sont infectés eux-mêmes en utilisant des disquettes de jeux échangées, et non contrôlées... On se fie trop souvent à la fausse sécurité suggérée par la présence d'un logiciel antivirus, sans se rendre compte que ce dernier n'a pas été mis à jour, ou pire, il n'a pas été mis en oeuvre correctement !

1.3 - Vrais et faux virus

Pour comprendre comment fonctionnent les virus, il est essentiel de bien les distinguer d'autres phénomènes analogues : bombes logiques, cheval de Troie, vers, bactéries, et autres programmes risquant de perturber le travail. Attention, cette division en familles distinctes est arbitraire. En outre, rien n'empêche un élément nuisible d'utiliser plusieurs des techniques sous-jacentes à ces différentes familles. En prime, ceux qui parlent des virus n'hésitent que rarement à créer ou à inventer de nouvelles catégories, avec des noms tous plus évocateurs les uns que les autres, afin d'augmenter l'effet médiatique de la chose. Parfois aussi, hélas, pour tenter de dissimuler leur totale incompétence en la matière.

Notez que cette section est relativement courte. Nous reviendrons par la suite sur certains des points évoqués ici afin de les approfondir.

1.3.1 - Les vrais virus

La présence d'un virus n'est jamais évidente. Un utilisateur peut avoir un disque dur infesté de virus et ne pas en être conscient le moins du monde. Au moins jusqu'à ce qu'un certain événement mette ces virus en action. Et alors, bonjour les dégâts... Comme toujours, il vaut mieux prévenir que guérir, mais cela suppose que l'on sache ce qu'est un virus.

Pour l'instant, il vous suffit de savoir que les virus sont de petits programmes parasites dont la plupart se chargent en mémoire afin de modifier ou de détruire les données présentes sur votre disque dur, ou simplement perturber votre travail. Tels des virus biologiques, ils se reproduisent très facilement et peuvent infecter de nombreux ordinateurs en très peu de temps en se propageant à travers les réseaux ou par voie de courrier électronique. Il en existe plusieurs milliers dans le monde, certains disent plusieurs dizaines de milliers.

Selon les endroits où ils se cachent et la manière dont ils agissent, on distingue quatre grandes familles : virus de démarrage, virus programme, virus polymorphe et macro-virus.

1.3.1.1 - Les virus de démarrage

Les **virus de démarrage**, dits aussi **virus de boot**, modifient la zone d'amorçage, voire la table de partition[12] présente sur tout les disques durs et toutes les disquettes. L'infection se produit souvent en laissant une disquette contenant le virus dans le lecteur au moment du démarrage de l'ordinateur. Dès cet instant, le virus se charge en mémoire et altère tous les dispositifs accessibles. L'action du virus peut être bénigne ou s'avérer désastreuse. Dans l'histoire des virus, ce type de contamination fait partie des premières à apparaître sur micro-ordinateurs. Heureusement, son mécanisme est bien connu, et elle est immédiatement détectée par tous les logiciels antivirus du marché. Il s'agit donc d'une espèce que l'on peut donc espérer en voie de disparition.

1.3.1.2 - Les virus programmes

Beaucoup plus sophistiquées que les précédents, les **virus programme** contaminent les fichiers .EXE ou .COM, parfois les fichiers .OVL, ainsi que les fichiers système (.SYS, .DRV, .BIN, etc.) Ils s'intègrent directement à eux, sans en altérer le fonctionnement. Ainsi, au lancement d'un programme infecté, le virus est lui aussi, chargé en mémoire, et commence immédiatement son activité néfaste. A noter l'existence de **virus hybrides** qui infectent à la fois le secteur de démarrage

[12] - c'est une « table » utilisée afin de permettre la division d'un disque physique en une ou plusiers unités logiques. Le même disque physique (la même mécanique) peut ainsi être vu par le système comme comportant un disque C: et un disque D: . Cette table existe toujours, même si le disque physique ne comporte qu'une seule partition (est vu comme un seul disque)

et les programmes. Une fois encore, les antivirus détectent bien ce genre de programmes nocifs et arrivent à les détruire le plus souvent sans détériorer le fichier original.

Il y a encore quatre ou cinq ans, ces virus infecteurs de fichiers se reproduisaient facilement. Efficaces, rapides et souvent parfaitement « silencieux », ils représentaient ce qui se faisait de mieux en matière de programme d'infection. Avec l'arrivée de **Windows**, 95 puis 98, les choses ont bien changé. Ces virus prolifèrent de moins en moins. Et cela pour plusieurs raisons. D'une part, les utilisateurs échangent de moins en moins des programmes exécutables. D'autre part, le lancement d'applications DOS devient lui aussi de plus en plus. rare. Enfin, Windows émule le DOS, tout en possèdant certaines failles de compatibilité. Un « vieux » virus pour DOS peut donc se trahir en faisant « planter » la machine avant d'avoir eu le temps d'agir.

1.3.1.3 - Les virus polymorphes

Les **virus polymorphes** sont en fait des virus programmes, comme les précédents, mais leur caractéristique particulière en fait certainement les plus coriaces et les plus redoutables de cette famille. Ils restent difficiles à localiser, même avec la détection générique qui repère l'action du virus sans le connaître à priori. Leur secret est de pouvoir changer leur code de manière dynamique, tels des mutants, à chaque fois qu'ils s'exécutent. Ils changent de forme à chaque fois. Ils passent ainsi à travers toutes les méthodes de détection traditionnelles, dont celle basée sur la table de signatures. Dangereux, ils sont toutefois peu nombreux à circuler.

1.3.1.4 - Les macrovirus

Il s'agit en fait d'instructions diverses placées dans des macrocommandes, qui ne sont elle-même que des sortes de petits programmes spécialisés placés à l'intérieur d'un document. Le nombre de ces virus est en constante augmentation. A la mi-97, on en comptait déjà plus de 250, écrits en **WordBasic** ou en **VBA** (**Visual Basic for Application**). Leur impact élevé a été révélé parce qu'ils se sont attaqués à une cible privilégiée[13] : les produits bureautiques de Microsoft. La conséquence de leur activité est redoutable. Ainsi, certains détruisent les fichiers, cryptent les documents ou formatent le disque dur.

Les premiers macrovirus ont fait leur apparition dès le mois d'août 1995, mais à cette date, ils n'étaient pas dangereux. Le précurseur, **Word.Concept**, n'avait comme effet que de se reproduire lui-même. Il s'agissait pour leurs auteurs de les expérimenter pour vérifier la fiabilité de leur code, et surtout évaluer le danger qu'ils pourraient occasionner. En plus, à cette époque, seuls les utilisateurs des versions anglaises de **Microsoft Office** pour Windows (versions 3.x, 95 et NT) étaient touchés, laissant un peu de répit aux Français, Italiens, Allemands et autres. Mais depuis, les événements se sont précipités. Les macro-virus fonctionnent désormais sur toutes les versions localisées de Word, d'Excel, et surtout sur toutes les plates-formes Windows**. Pire, ils s'avèrent extrêmement féroces**. Ils peuvent ainsi détruire les fichiers issus d'applications Word, Excel ou Access. Ils s'attaquent également aux fichiers de type programme ou système, et peuvent même donner au système l'ordre de formater un disque dur...

Les derniers en date utilisent des technologies de cryptage pour se cacher au sein des documents, se rendant ainsi quasi invisibles. Certains sont même porteurs d'autres types de virus, augmentant le niveau des dégâts possibles.

La version de **Microsoft Office 97**, disponible depuis février/mars 1997 a remplacé le langage de programmation simplifié **WordBasic** par le **VBA** (**Visual Basic for Applications,** une variante du Visual Basic). Ce dernier, déjà présent dans les versions 95 d'Excel et d'Access, est désormais le langage standard pour toutes les applications d'Office. Malheureusement, l'utilisation généralisée de ce langage, rend les virus plus puissants, et étend considérablement leur champ

[13] -...qui est en même temps pratiquement leur seule cible !

d'action ! De nouveaux virus utilisant VBA ont été écrits très rapidement, tel **Laroux** pour Excel, qui frappait dès Juillet 96. Celui-ci fonctionnait avec les versions 5.0 et 95 du tableur de Microsoft.

Mais le pire est encore à venir. En effet, **un macro-virus écrit en VBA peut infester tous les composants d'Office ainsi que la majeure partie des applications compatibles**, sur toutes les plates-formes capables de faire tourner des applications utilisant le VBA ! Cela signifie que ces virus peuvent allègrement sauter d'un document Word créé sous Windows à une feuille de calcul Excel utilisée sur un Macintosh, comme à un document de Powerpoint sous Windows NT ou OS/2... Connaissant la rapidité de propagation de ces virus, l'utilisateur qui va échanger des fichiers avec d'autres ne peut prendre le risque de rester sans protection. Pour l'instant, sa seule défense consiste à disposer d'un antivirus avec une table de signature la plus à jour possible[14]. Presque tous les éditeurs de ce genre de logiciel disposent d'un site Internet à partir duquel un utilisateur peut télécharger les signatures des derniers virus connus.

Pourtant, il semblerait qu'aucun logiciel actuel ne permette actuellement de détecter la totalité des virus VBA dernier cru[15]. Prenez donc garde aux documents Word, Excel ou Access que vous recevez, principalement sous Windows, mais aussi sous Macintosh, chaque fois qu'il existe une compatibilité au niveau du langage de programmation des macro-commandes. Et n'oubliez pas de sauvegarder vos données de manière régulière.

1.3.2 - Les faux virus[16]...

Les **bombes logiques** constituent des instructions placées intentionnellement dans un programme et censées s'exécuter lorsqu'une certaine condition est rencontrée. Le plus souvent, l'origine d'une telle bombe est à rechercher à l'intérieur de l'entreprise.

Un programmeur américain avait mis au point un tel système qui est **entré en action deux jours après qu'il ait été renvoyé** par ses patrons : sa bombe a provoqué l'effacement de près de 168.000 enregistrements. Un programmeur peut également implanter une bombe logique afin de **faire valoir ses compétences** : la paie se déroule de façon excentrique, l'informaticien intervient alors et répare le problème, qu'il connaît bien, puisqu'il en est l'auteur, etc. Par le passé, les bombes logiques ont souvent été utilisées pour garantir le paiement de certains logiciels, ou pour éviter l'utilisation prolongée de logiciels prêtés à titre de démonstration. Aujourd'hui, **ces pratiques sont illégales**, et sanctionnées par la loi du 5 janvier 1988, sur la fraude informatique.

L'appellation **cheval de Troie** (Trojan Horse) fait allusion au poème épique d'Homère. Il décrit un programme qui semble accomplir une action normale (jeu, traitement de texte...) alors qu'il en effectue une autre en arrière-plan telle que la destruction de fichiers. Malheureusement, ce type de programme est difficile à repérer[17] avant qu'il n'effectue sa mission, car son action est immédiate. Il n'agit pas, comme un vrai virus en deux temps, reproduction et infection. Il ne se reproduit pas de lui-même, mais uniquement par copies volontaires. Toutefois, un vrai virus peut aussi bien accompagner un « Cheval de Troie » que n'importe quel autre programme.

---

[14] - Une autre méthode, brutale mais efficace, consiste à interdire l'exécution des macro-commandes. Toutefois, cela ne peut se faire qu'à condition que le logiciel le permette, et surtout que l'on ait pas besoin de macrocommandes ! Or les applications développées par exemple sous Excel ne sont en fait que des ensembles de macrocommandes...

[15] - La défense est toujours en retard sur l'attaque…

[16] - Attentio, ce n'est pas parce qu'il ne s'agit pas de « vrais » virus » que ces « machins » sont moins dangereux. Bien au contraire : aucun programme antivirus ne peut les détecter !

[17] - Ils sont d'autant plus difficiles à détecter qu'ils ne contiennent que des commandes que l'on peut considérer comme classiques et normales, mais dont l'exécution dans certaines circonstances peut être néfaste à vos précieuses données, comme par exemple lancer le formatage du disque dur...

Le programme Aids Info, envoyé anonymement en décembre 1989 à plusieurs centaines de personnes du milieu médical, avec la mention « Aids Information Introductory Diskette » contenait un Cheval de Troie. En apparence, il ne s'agissait que d'un simple questionnaire sur le Sida. Seulement, quand un utilisateur démarrait le programme, le répertoire principal était aussitôt crypté, et il y avait tentative de destruction de toutes les données du disque.

Les programmes ainsi minés ne sont généralement pas longtemps nocifs. A partir du moment où un tel programme a été repéré, les responsables de serveurs peuvent rapidement les supprimer et informer les utilisateurs du danger encouru[18].

Les **vers** (worms) sont des programmes qui s'apparentent à une farce de mauvais goût. Ils n'ont pas pour but de causer des dégâts à l'ordinateur. Ils se contentent de se dupliquer et d'occuper au maximum la mémoire vive disponible, ce qui a pour effet de réduire de façon importante la vitesse de traitement d'une machine. Les ordinateurs multitâches sont les plus sensibles à ces attaques. Le concept est apparu en 1975 dans un roman de science-fiction de John Brunner. Celui-ci décrivait des programmes « **vers solitaires** » voyageant de réseau en réseau, emmenant au passage des informations. Sept ans après, deux programmeurs du Xerox Parc, John Shoch et John Hupp, eurent l'idée de développer de tels vers à des fins utiles. Ces petits programmes capables de migrer d'une station de travail à une autre permettaient, en principe, de récupérer de l'espace disque ou de mettre hors fonction un poste inactif. L'utilité pratique de ces vers s'est révélée nulle, mais malheureusement l'idée était lancée.

En 1988, le **réseau Internet** a été la victime d'un ver nocif écrit par un étudiant de l'université Cornell : celui-ci se reproduisit d'un bout à l'autre des États-Unis entraînant un plantage général du système. Cet événement a eu une grande portée et a fait connaître au grand public l'existence des virus. **Pourtant, les vers ne constituent qu'une forme relativement bénigne de ce phénomène**. Ils nécessitent une connaissance profonde de la façon d'opérer d'un réseau, ce qui limite leur portée. Ils ne représentent généralement pas une menace sur les informations mêmes.

On trouve encore de nombreuses autres appellations, plus ou moins contrôlées. Par exemple, les **lapins**[19] sont des programmes dont la seule tâche consiste à se dupliquer sur les mémoires de masses (disques, disquettes). Ils peuvent se reproduire à un niveau tel que le disque dur se trouve saturé et que l'ordinateur ne parvient plus à opérer correctement. Mais ils ne causent généralement pas de dommages aux informations elles-mêmes. Les **bactéries**, pour leur part, agissent de façon similaire, mais sur un réseau.

1.3.3 - Les canulars ou hoaxes...

De très nombreux canulars circulent dans le monde informatique, et le courrier électronique est un excellent moyen de les diffuser rapidement, d'une manière quasi anonyme. la croissance des utilisateurs d'internet ne fait qu'amplifier ce phénomène. Bien évidemment, ceux qui lancent ce genre de plaisanteries (?) préfèrent toucher le point le plus sensible de la masse des utilisateurs peu avertis : la peur des virus. On peut se poser la question de savoir si l'auteur du premier hoax n'a pas réussi à créer un virus sans écrire une seule ligne de code !

---

[18] - J'ai été personnellement victime d'une de ces bestioles. Il s'agissait d'un logiciel de dessin, en shareware. Lorsqu'on demandait une impression, le programme lançait le formatage du disque dur... Il m'a fallu ensuite une bonne journée pour reconstituer les données à partir des sauvegardes. J'avoue ne pas comprendre le plaisir que certains individus peuvent prendre à modifier ainsi de vrais programmes pour les transformer en pièges...

[19] - Est-il vraiment nécessaire de vous expliquer l'origine de ce nom ?

En plus de faire peur aux utilisateurs peu avertis, le principal effet d'un hoax (et souvent le seul !) est de polluer les systèmes de messagerie par la réexpédition des messages qu'il véhicule. L'accentuation sur un danger plus ou moins important, fait que ces messages sont retransmis au lieu d'être tout simplement détruits, comme ils le mériteraient. Selon les producteurs de logiciels antivirus, ce sont de mauvaises plaisanteries comme il y en a de plus en plus, avec pour thème des virus imaginaires. Elles proviennent de personnes mal intentionnées qui veulent faire paniquer les utilisateurs d'ordinateurs, surtout ceux qui sont inexpérimentés. Si vous recevez ce type de message, ne les retransmettez pas à d'autres, détruisez-les sans pitié.

Leur existence n'est pas un fait nouveau. Dès novembre 1996, le centre de recherche de Symantec signale que plusieurs virus avec lesquels certains s'amusent à faire peur n'existent pas ! Selon Symantec, les cas les plus répandus concerneraient les faux virus « Good Times », « Deeyenda », « Email », « Irina », « 3b Trojan », « Trojan », « PKZip » et « PKZ300B.ZIP ». Seul ce dernier aurait existé en 1995 mais juste sur une courte période et il a entièrement disparu depuis, même s'il y a encore des gens qui envoient des messages disant de s'en méfier.

Dorénavant, il ne faut donc plus se méfier uniquement des virus mais aussi des petits rigolos qui en imaginent pour faire peur aux autres. Voici quelques exemples de canulars circulant actuellement sur le WEB

WIN A HOLLIDAY

En 1998, beaucoup d'internautes ont reçu par courrier électronique un message concernant un virus nommé « WIN A HOLIDAY ». Il y est dit de ne pas ouvrir un message avec ce nom de virus comme sujet du message et d'avertir les autres internautes qu'ils connaissent. En réalité, aucun virus ne peut avoir les caractéristiques attribuées à WIN A HOLIDAY.

CALEFORNIA

Apparition début juin 1999, d'un nouvel hoax, nommé CALEFORNIA, dont le contenu du message est traduit ci-après :

> *Si vous recevez un dossier appelé « calefornia » NE L'OUVREZ PAS !!!!! Il contient le Virus Wobbler, pire que le virus Melissa. Un individu a réussi en utilisant la fonction Reformat de Norton utility pour effacer complètement tous les documents sur le disque dur. Il est conçu pour travailler avec Netscape Navigateur, Microsoft IE et détruit les ordinateurs Macintosh et compatibles IBM.*

Comme tous ces congénères, ce canular va circuler quelques temps sur INTERNET. Le seul conseil à suivre, ne le retransmettez pas, détruisez le. Mais évitez quand même d'envoyer à vos correspondants un dossier nommé « calefornia »...

PENPAL GREETING

Penpal Greetings n'est pas un virus non plus mais une mauvaise farce comme les supposés virus Good Times et E.mail, entre autres. Voici ce qu'en dit le centre de recherche sur les virus de Symantec

> *Penpal Greetings is not a virus. It is a hoax. The « virus » does not exist. There is currently no virus that has the characteristics ascribed to Penpal Greetings. The e-mail message describing the virus is similar to the original Good Times virus e-mail hoax. It could even be described as a virus hoax strain. Please ignore any messages regarding this supposed « virus » and do not pass on any messages regarding it. Passing on messages about this hoax serves only to further propagate it.*

HOAX AOL ou **RETURNED OR UNABLE TO DELIVER**

Le message retransmis par courrier électronique est le suivant :

> *There is a new virus going around in the last couple of days !!! DO NOT open or even look at any mail that you get that says : « Returned or Unable to Deliver » This virus will attach itself to your computer components and render them useless. Immediately delete any mail items that says this. AOL has said this is a very*

dangerous virus, and there is NO remedy for it at this time, Please Be Careful, And forward to all your on-line friends

Vous pouvez effacer sans crainte ce message. Ne le transmettez surtout pas à d'autres car vous joueriez le jeu de ceux qui l'ont diffusé pour faire peur aux utilisateurs d'ordinateurs.

Attention : surtout NE LE CONFONDEZ PAS avec le « cheval de Troie » nommé AOL4FREE.COM. Vous pouvez recevoir ce fichier dans un fichier attaché à un message de courrier électronique ou, à la limite, sur une disquette remise par quelqu'un de malveillant ou d'inconscient. En aucun cas, il ne faut exécuter ce fichier sinon on risque de faire effacer tous les fichiers du disque dur. Même s'il est sur le disque une fois qu'on l'a reçu, il n'est pas dangereux tant qu'on a pas cliqué sur son nom pour le lancer et on peut l'effacer sans risque. Si vous l'exécutez par erreur, pressez immédiatement sur Ctrl-C pour limiter les dégâts et servez-vous d'un logiciel de récupération de fichiers effacés pour essayer de rétablir votre disque dur dans son état précédent. N'écrivez rien d'autre sur le disque tant que ce n'est pas fait.

JOIN THE CREW

Des internautes ont reçu un avertissement au sujet du prétendu virus « Join the Crew ». Ne transmettez pas ce message à d'autres si vous le recevez. Il s'agit en fait d'une farce qui dure depuis des mois sur Internet. Il est également faux aussi qu'IBM ait transmis un tel message. Voici le message officiel d'IBM pour « Join the crew » :

We have found yet another virus hoax being passed around on the Internet. This one is very similar to all the others : it warns of a nefarious e-mail message with a certain title that will « erase your whole hard drive » when opened. In this version of the hoax, the title of the e-mail is « Join the Crew ». As usual, we have no reason to think that any actual disruptive e-mail (except the warnings themselves!) is circulating with this title, and we remind readers that in well-run mail systems simply opening a piece of mail does not run any program contained in it. On the other hand, of course, everyone should continue to be suspicious of unexpected programs received in the mail, and not run them. Help prevent Internet litter: do not forward hoax warnings to others, no matter how strenuously the warning itself urges you to. Just Say No...

TIME BOMB

Time Bomb est également reconnu comme une mauvaise farce. De nombreuses personnes ont reçu un message leur disant de se méfier de **Time Bomb**, alias **Win95_October 1**, le 1er octobre. En fait, ce soi-disant virus n'existe pas selon les chercheurs de Symantec et aucun virus ne peut avoir les caractéristiques décrites dans le message en question. Vous pouvez donc détruire sans crainte tout message que vous recevrez à ce sujet, y compris les lignes qui disent :

There is a macro virus going off on Oct 1!!! All computers installed with Windows 95 are installed with this virus. It is a time bomb virus. Microsoft has already apologized for the mass breakdown of computers around the world on that day. However they had yet to come up with a remedy. Some versions of Win95 are safe but some are not. Please Be Careful, and forward to all your on-line friends A.S.A.P. not a lot of people know about it, just let everyone know, so they won't be a victim. Please forward this e-mail.

Chapitre 2 : La grande aventure des virus

Le terme **virus** (au sens informatique) est utilisé pour la première fois dans un livre de David Gerrold publié en **1972** (« *When Harley was one* »). Le 3 novembre **1983**, Fred Cohen, étudiant de l'université de Californie du Sud appelé à participer à un séminaire sur la sécurité des ordinateurs, définit le mot de manière formelle. Il montre au public un curieux programme réalisé à des fins expérimentales sur un VAX 11/750 : il peut, en effet, s'insérer de façon discrète dans un second programme, puis en contaminer d'autres. Lors de la démonstration, il apparaît que le virus en question est en effet capable d'infecter assez rapidement les programmes de ceux qui se connectent au VAX : il lui faut environ trente minutes pour y arriver...

Si les premiers virus sont apparus assez tôt sur l'Apple II, le phénomène a touché l'IBM PC à partir de **1986**. On rapporte alors l'existence d'un certain virus appelé selon le cas Brain, Pakistani Brain, Lahore ou Basit. Il est capable de contaminer le secteur de démarrage du disque dur. Son action essentielle consiste à réduire l'espace disponible sur disque et dans la mémoire. (Une variante plus nocive apparue par la suite, **CloneB**, peut détruire la table d'allocation des fichiers, rendant le PC inopérant).

Cinq nouveaux virus sont recensés en **1987** : Alameda, South African, Lehig, Vienna et Israeli. L'année 1988 voit l'arrivée d'Italian, DOS 62, New Zealand, Cascade et Agiplan. Au début des années 90, le phénomène commence à devenir inquiétant : on dénombre plus de 150 virus, et leur nombre n'a fait qu'augmenter. Au début de 1992, selon McAfee, ils sont plus de 1200 en circulation, et on peut voir apparaître jusqu'à dix nouveaux spécimens par semaine, prétendent certains spécialistes es-virus !

Et cela continue ! A la fin de mai 1999, on recensait plus de 42 000 virus capables d'infecter les PC fonctionnant sous DOS ou Windows...

2.01 - Du déplombage à la création de virus

Les pirates informatiques, des programmeurs doués, sont apparus à l'émergence de la micro-informatique grand public. Leur matière première : les **copyrights**[20]. Ils s'ingénièrent à détruire les protections et les codes de sécurité des programmes (la plupart du temps des jeux, y insérant parfois leur pseudonyme afin de signer leurs réalisations). Le logiciel ainsi déplombé était alors fin prêt pour engendrer des copies illégales, parfois simplement distribuées aux amis, mais plus souvent vendues avec profit...

Après s'être fait la main sur les logiciels grand public, vînt le tour des réseaux. Les fameux *hackers* en RFA en forcèrent les sécurités d'un très grand nombre de systèmes informatiques : le **Centre de Recherche Spatiale allemand**, l'**Agence Spatiale Européenne** (ESA), la **NASA**...etc. (les codes internes d'accès étaient parfois récupérés par l'implantation de Chevaux de Troie aux endroits stratégiques). Heureusement, la grande majorité de ces pirates n'étaient pas empreints d'intentions malveillantes. On imagine les conséquences de telles intrusions dans les réseaux d'établissements financiers, ou d'administrations diverses. Les exemples ne manquent pas aux USA. En réaction, les entreprises de conception informatique développèrent des sécurités de plus en plus complexes pour protéger leurs droits de propriété intellectuelle, et les systèmes informatiques. L'éternel antagonisme entre l'épée et la cuirasse, l'obus et le blindage...

Hackers et Cyberpunks[21]

Pour simplifier les choses, les termes Hackers et Cyberpunks désignent à peu de chose près le même type d'individus, les premiers dans les années 80, les autres dans les années 90 : des passionnés d'informatique au comportement atypique, dans les brèches de la légalité. Ils se distinguent des fraudeurs, qui arnaqueront les Télécom, et des pirates, qui n'ont que des activités de bas niveau, le plus souvent à but commercial. En général, ils n'ont pas d'intention malveillante (par contre un goût peut-être irraisonné du défi technologique, et certainement aussi de la prise de risque). Eric Corley, rédacteur en chef du magazine 2600 (cité par Pamela Kane), témoigne : « *Dans ma vie de tous les jours je me retrouve à hacker tout et n'importe quoi. Je hacke les feux rouges, les cabines téléphoniques, les répondeurs automatiques, les fours à micro-ondes, les magnétoscopes. Pour moi, 'hacker' signifie changer perpétuellement les conditions d'entrée d'un système jusqu'à ce que la réponse obtenue diffère. Dans le monde mécanique dans lequel nous vivons, les possibilités de pratique du hacking sont inépuisables.* »

L'activité des hackers sur les réseaux a parfois (mais rarement) été bénéfique. Elle a permis de mettre à nu des déficiences notoires sur des sites qui auraient dû être sérieusement protégés (le centre d'études cancérologiques américaines, la Nasa...). On peut imaginer par exemple ce qu'un psychopathe pourrait faire dans une banque de données médicales (intervertir des groupes sanguins, manipuler des informations sur des substances chimiques...). Dans un registre plus feutré, des compagnies aux pratiques commerciales douteuses (ou des institutions d'état) pourraient constituer des fichiers particulièrement précis, en pénétrant des bases de données confidentielles contenant des détails sur la vie privée. En ce sens, c'est à dire en mettant en évidence des failles dans les systèmes de sécurité, l'activité des hackers a été bénéfique. Là où le bât blesse, c'est que la circulation d'information dans leur underground n'est pas forcément sélective des personnes. Bien au contraire, n'importe qui, une fois introduit dans ce milieu, peut accéder à des techniques de hacking aux potentialités dangereuses.

Sur un plan éthique, les hackers s'opposent à la société technologique où l'outil prévaudrait sur l'humain. Ils se prétendent les représentants dans l'informatique d'une contre-culture qui essaie de faire front au modèle dominant (au même titre que l'écologie face au néolibéralisme, ou que l'alchimie au milieu de l'obscurantisme chrétien d'autrefois, par exemple).

[20] - ... les logiciels protégés contre la duplication.

[21] - ... ou punk cybernétiques.

Malheureusement, il se trouve que créer ou déplomber une protection, éliminer ou concevoir un virus, tout cela relève des mêmes compétences en programmation : le langage Assembleur. Du piratage de logiciels à leur infection par des programmes nuisibles, il n'y a donc qu'un pas, que certains passionnés ont allègrement franchi.

En fait, le concept de virus informatique semble être né en même temps que l'informatique elle-même. Dès 1949, **John von Neumann**, l'un des plus brillants mathématiciens de l'époque, et à qui nous devons l'architecture des ordinateurs actuels, mentionnait la possibilité de créer des mécanismes d'auto-copie des logiciels dans un rapport intitulé « *Theory and Organisation of Complicated Automata* ».

2.02 - Les années *Core War*

C'est au cours des années soixante que se multiplièrent les premiers **vers**, à l'intérieur des environnements multitâches (qui permettent l'exécution simultanée de plusieurs programmes par un ordinateur). Une expérience mérite notamment d'être rappelée plus que d'autres, car elle fit rapidement de très nombreux adeptes : il s'agit d'un jeu nommé **Core War**.

C'est dans les laboratoires **Bell** de la compagnie AT&T, aux Etats-Unis, que naquit l'idée de ce jeu, définit par trois informaticiens : **Douglas McIlroy**, **Victor Vysottsky** et **Robert Morris**. Core War ne fait pas intervenir d'être humain, il oppose deux programmes entre eux, dans un espace délimité de la mémoire de l'ordinateur. Le jeux débute simplement : deux programmes de très petite taille sont placés dans la mémoire centrale d'un ordinateur. Le but est de s'anéantir mutuellement en modifiant le contenu de la mémoire vive. Chacun peut essayer de localiser l'adversaire, le bombarder de 0, il peut aussi se déplacer pour éviter d'être repéré, s'autoréparer ou s'autocopier pour éviter la destruction, etc. Le système d'exploitation partage le temps de l'ordinateur entre les deux programmes.

Selon les versions du jeu, le gagnant est celui qui arrive à modifier son adversaire au point de le rendre inactif, ou celui dont il reste le plus grand nombre de copies dans la mémoire quand le jeu est arrêté. Core War fit des adeptes dans de nombreux lieux de l'informatique de pointe. Mais il resta longtemps un jeu pratiqué par un nombre limité d'initiés.

2.03 - Les débuts de la vulgarisation (les années 70/80)

Durant les années 70 et le début des années 80, des articles commencent à décrire des programmes dérivés de Core War. En 1983, **Ken Thomson**, père du système d'exploitation **UNIX**, fut le premier à parler publiquement de Core War. Dans son discours, il détailla les grandes lignes du jeu et encouragea même à expérimenter ces « *petites créatures logiques* ».

Une rubrique de la revue **Scientific American** de mai 1984, explique de manière fort détaillée le principe du jeu et la programmation des « *différents programmes de bataille* ». Cet article déclencha un véritable engouement pour Core War. Par la suite de nombreux exemples éloquents ont pu montrer que la vulgarisation avait réussi. Au delà de toute espérance...

On peut faire coïncider la fin de cette période avec l'apparition du virus pakistanais.

2.04 - 1986 : Le virus pakistanais, Lehig, Vendredi 13

Le programme connu sous le nom de ***virus pakistanais*** s'attaque aux ordinateurs fonctionnant sous le système d'exploitation MS-DOS. Il fut distribué par deux programmeurs pakistanais, les frères Alvi. Leur cible privilégiée : les nombreux **touristes américains** venus visiter leur pays et qui en profitent pour acheter à très bon compte des **copies illégales** de logiciel. C'est, prétendent-ils, dans le but de punir ces étrangers enfreignant les lois de leurs pays, qu'ils mirent au point un virus capable de ralentir considérablement les performances de toute machine contaminée et même de causer occasionnellement des pertes de données. La punition fut assez sérieuse puisque des milliers de machines semblent avoir été contaminées par ce virus.

En 1987, un virus est détecté aux États-Unis à l'**université de Lehig**. Sa logique était très simple : il devait se reproduire quatre fois avant de détruire tous les volumes (disques durs et disquettes) montés sur le système en effaçant définitivement leur table d'allocation. ***Lehig*** était l'un des plus destructeurs des virus détectés jusque là...

En décembre de la même année, à l'Université de Jérusalem, un autre virus, baptisé **virus israélien,** ou plus communément, ***Vendredi 13,*** destiné à l'environnement MS-DOS, est découvert. Il contenait les instructions nécessaires à la destruction de tout programme exécuté à la date anniversaire de l'état d'Israël, le Vendredi 13 mai. C'est son mécanisme de reproduction particulièrement excessif qui a permis de le détecter, bien avant la date fatidique.

2.05 - 1988 : L'âge d'or des virus

En 1988, le nombre et l'importance des foyers d'infection ont atteint des proportions véritablement alarmantes : 400 foyers d'infection, pour les États-Unis seulement, soit au total plus de 90 000 machines concernées par le problème. De telles statistiques ne sont pas disponibles pour l'Europe, mais la situation n'était pas aussi sérieuse de ce côté-ci de l'Atlantique.

MagMac fut le premier virus auquel la presse générale accorda une large publicité. Alors que les virus jusqu'alors affectaient surtout les grands réseaux et les systèmes partagés par de nombreux utilisateurs, ce virus concernait les utilisateurs de Macintosh. L'idée de ce virus tenait à la fois de la démarche publicitaire et de la gageure : il s'agissait de répandre un virus qui, le 2 mars 1988, date anniversaire de la sortie du Macintosh II, afficherait un message de paix à l'écran des Macintosh contaminés. Le programme était dépourvu de toute intention malveillante et devait ensuite s'autodétruire. Il infecta non seulement les États-Unis, mais aussi l'Europe et il fut le premier virus à être distribué accidentellement sur des disquettes commercialisés.

Curieusement, et malheureusement, les auteurs du virus **MacMag** reçurent un prix pour avoir attiré l'attention des utilisateurs de micro-informatique sur les dangers potentiels que représentent les virus, mais ils n'en furent pas moins condamnés sévèrement par l'ensemble des utilisateurs touchés, ou non.

En Novembre 1988, **Robert T. Morris**, fils d'un des inventeurs de Core War, devenu responsable du Conseil National de Sécurité Informatique, branche de la **National Security Agency** (**NSA**), travaille à partir d'une console lui donnant accès à un ordinateur universitaire. En principe, il expérimente ce jour-là un **programme autoreproducteur.** Malheureusement, il en perd presque aussitôt le contrôle et des copies du ver passent rapidement en dehors du système pour se répandre à travers le réseau **Internet** auquel il est relié. En moins de 24 heures, c'est la panique : 6200 terminaux sont affectés, un grand nombre d'entre eux étant momentanément rendus non opérationnels. Au cours de cet épisode, plusieurs milliers de terminaux disséminés à travers les États-Unis furent rendus partiellement ou totalement non opérationnels, et les dégâts causés furent évalués à près de 100 millions de dollars américains...

Cet incident, si on peut le qualifier ainsi, a particulièrement attiré l'attention de l'opinion publique sur la menace grandissante des virus et sur la vulnérabilité des réseaux informatiques. Selon **R.P. Balme** (novembre 1988), il s'agirait sans doute d'un coup monté par la **NSA**, afin de vérifier la qualité de la sécurité des sites qui travaillent pour le gouvernement américain... Vrai ou faux, on ignore, mais quoi qu'il en soit, la démonstration a été éclatante.

2.06 - 1989 : La prise de conscience en Europe

La situation ne semble pas s'améliorer puisque le nombre de machines contaminées dépasserait largement les 100.000 aux USA. **En Juillet 1989, les virus reconnus comme très dangereux étaient plus de 30**.

Ce n'est que durant cette même année 1989 que les pays européens prennent véritablement connaissance de l'existence du phénomène des virus informatiques, lors de l'alerte **Datacrime**. C'est un exemple particulièrement éloquent de l'utilisation des phénomènes de virus par la presse. En octobre, la plate forme **Anti Computer Crime**, mise sur pied par la police des Pays-Bas, fait part de sa découverte de trois virus de MS-DOS. Ils seraient programmés pour agir les 12 et 13 octobre, en endommageant gravement les volumes des ordinateurs contaminés (*en plus, le 13 octobre 1989 était un vendredi, donc un jour néfaste par excellence !*). Les polices de La Haye et de Utrecht mettent aussitôt en vente un ensemble de programmes capables de détruire les trois virus désignés sous le nom générique de **Datacrime** et d'en détecter de nombreux autres. Plus de cinq mille copies en sont vendues en l'espace de quelques jours. En France, **IBM** fait de même. Finalement, rien d'anormal ne devait se produire le 12, ni même le 13.

Lors de cette alerte, les journalistes ont joué un rôle très important, à la fois par sa sur-médiatisation, et par l'impact obtenu sur le grand public. Ce ne sera pas la dernière fois...

2.07 - 1990 : Le développement des virus s'accentue

Le mois de Janvier 1990 est marqué par les dommages causés par une disquette sur le SIDA (**AIDS**) de PC CYBORG, un **cheval de Troie** provenant très probablement des États-Unis. Le produit, présenté comme un logiciel commercial traitant un sujet d'actualité, est proposé à des cibles particulièrement bien choisies (professions médicales et paramédicales). Il est aussitôt essayé... Après installation et quelques essais décevants, le produit est vite oublié. Il ne fait à nouveau parler de lui que lorsqu'il est trop tard : le disque dur du micro-ordinateur est inutilisable. Les vendredi 13 qui suivent, en particulier en avril et juillet, ne font l'objet d'aucune nouvelle alerte ni d'aucune information particulière malgré les risques inhérents à ces dates. Au cours de cette période, le nombre de virus recensés prend son essor, en un an, **il est passé d'une trentaine à plus de 250**. La masse critique est atteinte, le phénomène est en expansion et commence à être connu...

2.08 - 1991 : FRODO, distribué gratuitement !

Au cours du mois de mai 1991, le virus **FRODO/4096**[22] est diffusé à plus de 60.000 exemplaires par l'intermédiaire d'une disquette contaminée encartée dans la revue informatique **Soft & Micro**. La procédure d'installation entraîne la contamination de l'ordinateur utilisé même si elle n'est pas menée à son terme. Comble de malheur, le virus FRODO/4096 est un virus de type furtif

[22] - Ce chiffre 4096 correspond à la taille du virus, ou plus précisément à l'augmentation de la taille du fichier infecté par le virus.

c'est à dire qu'il est capable dans certaines conditions de masquer sa présence et les contaminations qu'il opère. C'est d'ailleurs probablement pour cela qu'il n'a pas été détecté lors de la réalisation de la maquette de la disquette.

Une procédure de détection et de décontamination est rapidement mise en place et diffusée rapidement grâce au serveur Minitel **INFOVIRUS**. Malgré tous ces efforts, de nombreuses disquettes infectées sont disséminées dans le grand public. Le virus FRODO/4096 devient ainsi en quelques jours le premier au hit parade de la contamination virale en France...

2.09 - 1992 : Michelangelo déclenche une panique...

L'un des plus célèbres des virus informatiques, **Michelangelo**, du nom du génial artiste italien, s'est répandu à une vitesse étonnante. Le **Vendredi 6 mars 1992** correspondait à la date du 517ième anniversaire de l'artiste italien de la Renaissance : Michelangelo Buonarroti dit Michel-Ange. Pour des centaines d'utilisateurs[23] de PC, cette journée n'a pas été pareille aux autres... Sauf indication contraire, tous les éléments rapportés ici concernent le 6 Mars 1992. Michelangelo a encore frappé le 6 Mars 1993, mais c'était un samedi. En 1994, le 6 Mars était un dimanche, pratiquement personne n'en a parlé. Le 6 Mars 1995 était un Lundi, mais il y avait d'autres sujets à traiter pour les médias. A titre d'exemple d'une affaire menée en grande partie par les média, disons quelques mots de cette **Affaire Michelangelo**.

2.09.1 - Panique dans les villes

Selon John McAfee, président de **McAfee Associates** qui édite un antivirus diffusé en shareware, Michelangelo a été découvert aux Pays-Bas en février 1991 et s'est rapidement répandu. Il se transmet par l'intermédiaire d'une disquette (**même exempte de données**) et se dissimule dans l'ordinateur. Il entre en action le 6 mars de chaque année. Il efface alors chaque secteur du disque dur et remplace les données par des caractères générés de façon aléatoire. En 1991, il n'a frappé qu'un nombre insignifiant de machines. Son attaque n'a donc pas soulevé beaucoup de commentaire dans la presse, mis à part dans quelques revues spécialisées.

La situation a été plus critique en 1992. En un an, le virus avait eu la possibilité de se propager. En outre, dès la fin de janvier, l'éditeur **Symantec** a contribué à attirer l'attention du public en informant de l'imminence du danger au moyen de grandes pages de publicité. Il proposait de fournir des **copies gratuites** de son Norton Antivirus, ou plutôt d'une version spécifiquement adapté à la protection des PC contre Michelangelo. Plus de 250.000 copies de cette version réduite ont ainsi été distribuées. La menace fut prise au sérieux, et pour la société Symantec, la **publicité fut excellente**, car après la version limitée et gratuite, de nombreux utilisateurs voulurent se procurer la version complète, et payante !!

Quelques jours avant l'attaque annoncée, les ventes d'antivirus sont montées en flèche. Aux **États-Unis**, Egghead Software indique que les commandes ont progressé de 3 000 % dans la semaine précédant le jour J. D'autres boutiques rapportent qu'elles ont été submergées d'appels d'utilisateurs terrifiés. Le directeur du Los Angeles Software Supermarket raconte qu'il a vendu plus de logiciels antivirus le mercredi 4 mars qu'en une année complète ! En **Amérique du Sud**, IBM a distribué des antivirus à ses clients...

La **Pologne** a pris la menace très au sérieux et le quotidien ***Glob 24*** a fait sa une du jeudi 5 mars sur le phénomène. Dans ce pays (comme malheureusement dans beaucoup d'autres), en raison de l'absence d'une loi protégeant le droit d'auteur sur les logiciel, le piratage des pro-

[23] - D'autres disent des milliers, voire des millions ! Ah, ces journalistes... En réalité, on ignore encore le nombre réel de victimes. Beaucoup d'utilisateurs n'ont pas osé avouer qu'ils avaient été surpris par la bestiole, malgre le battage médiatique fait autour de ce virus.

grammes est effectuée à très grande échelle. De ce fait, de très nombreux virus sont en circulation. Le 5 mars, les magasins de logiciels de Pologne ont été littéralement envahis par les acheteurs d'antivirus, formant des queues impressionnantes. Certains éditeurs de logiciels ont procédé à la distribution gratuite de programmes antivirus. Le plus souvent des versions limitées, afin d'inciter les utilisateur à acheter la version complète…

2.09.2 - Une épidémie dévastatrice ?

Qu'en était-il en réalité ? Combien d'ordinateurs étaient en fait infectés ? Les chiffres varient énormément en fonction des sources et vont de quelques dizaine de milliers à plus de 5 millions. Les organisations qui ont découvert que leurs ordinateurs avaient été touchés ne sont pas les moindres. Parmi elles se trouvent la Nasa (200 ordinateurs infectés), le Sénat américain, le ministère des Affaires étrangères des États-Unis et trois ambassades américaines : Toronto (Canada), Addis Abeba (Ethiopie) et La Paz (Bolivie). Le New Jersey Institute of Technology l'a découvert sur 2400 de ses 3000 PC. Dans chacun des cas, le virus a été détruit avant d'être en mesure d'opérer.

Michelangelo a même été diffusé par des constructeurs et par des éditeurs de micro-informatique ayant pignon sur rue. Selon l'hebdomadaire Info-world, il s'est retrouvé sur 500 machines livrées en décembre 1991 par Leading Edge. La société Chips Technologies a également diffusé par inadvertance des disquettes contaminées lors du Comdex de Las Vegas. Michelangelo s'était aussi incrusté dans un lot de disquettes de démonstration de la messagerie e-mail 2.0 diffusée par Da Vinci Corp. La Pologne, étant donné le taux de piratage des logiciels qui s'y pratique, a été l'un des pays les plus touchés par Michelangelo. Si l'on en croit le journal Gazeta Wyborcza, un quart des entreprises de la région de Krakow ont découvert que leurs PC avaient été victimes du virus.

Durant cette journée noire, en dépit des **messages alarmistes** diffusés longtemps à l'avance par des éditeurs tels que **Symantec**, un nombre important[24] de PC a subi des dommages, faute d'avoir été protégés. Les dégâts s'élèveraient globalement à plusieurs millions de dollars (en y incluant le temps passé à reconstituer les informations). Selon Symantec, près de 1800 compagnies américaines ont fait savoir qu'elles avaient eu des PC endommagés[25]. Rod Turner, de cette même société, cite au passage l'histoire d'un consultant qui avait conseillé à ses clients d'avancer la date de leur ordinateur d'une journée pour éviter tout danger : seul problème, il s'était trompé d'un jour et il a provoqué l'effacement de disques durs vingt quatre heures avant la date fatidique...

2.09.3 - Le grand nettoyage

L'université de l'Illinois a ainsi perdu les informations de six de ses ordinateurs, malencontreusement réglés à la date du 6, un jour trop tôt. En **Afrique du Sud**, plus d'un millier d'ordinateurs contaminés ont été recensés. Au **Japon**, ils étaient au nombre de huit. Le ministère de la Sécurité publique de **Chine** rapporte qu'il n'aurait trouvé qu'une dizaine de cas, lors d'une enquête nationale. Au **Paraguay**, dix réseaux d'ordinateurs ont été agressés. Selon Ricardo Irrazabl d'lBM Paraguay, le virus a effacé les bases de données de la société Paraguayan Ceramics et celles du groupe financier Curpayty. En **Argentine**, le journal Norte a réussi à stopper les avancées du virus avant qu'il ne nettoie l'ensemble du système informatique. Trois ordinateurs dédiés à la gestion de la publicité ont cependant été affectés. Le journal Rio Negro a été moins chanceux : toutes ses données informatiques ont été corrompues. Pendant plusieurs semaines, la rédaction est même revenue aux machines à écrire traditionnelles !

Le 6 mars n'était qu'une étape parmi de nombreuses autres. Quelques jours plus tard, un autre virus s'apprêtait à entrer en action : l'**amibe de Malte** qui efface des fichiers le 15 de ce

[24] ...mais que personne n'a jamais pu estimer avec précision.

[25] - En réalité, il ne pouvait s'agir que de perte d'informations, le virus ne s'attaque pas au matériel...

même mois.

2.10 - 1997 : Très bref état des lieux

Depuis 1991, le nombre de virus n'a cessé de croître, ce qui fait, aujourd'hui des virus un phénomène important. L'évolution est exponentielle. Toutefois, il ne s'agit plus des mêmes familles de virus.

En 1995...

En juin 1995, on estimait le nombre de virus connu à environ 5000, soit 100 à 200 nouveaux virus par mois, en moyenne, depuis 1989. Parmi ces virus, on distingue différents types : environ **90 %** sont des **virus de fichier standard** (toutefois, ils n'interviennent que dans **15 %** des cas d'infection), seulement 5 % sont des **virus de secteur de boot**, mais ils interviennent dans 70 % des cas d'infection, et environ 5 % sont des **virus polymorphes**.

En 1996...

Selon une enquête publiée dans la revue Info-PC de Juillet/Août 1997, les "attaques" recensées en 1996 s'établissent ainsi (en %) :

macro de Word	**49**
Form	**15**
Stealth B ou C	**10**
Anti-Exe	**4**
Monkey	**4**

Stoned	**3**
Anti-CMOS	**2**
NATA	**2**
NVB	**2**
Michelangelo	**2**

Dix virus seulement sont donc responsables de 94 % des infections recensées. L'ensemble des autres virus (plus de 6000 encore actifs à en croire des spécialistes) ne représente que 6 % des attaques, c'est à dire presque rien pour chacun d'entre eux...

En 1997...

Selon un article paru dans l'**Ordinateur Individuel** de Juillet/Août 1998 et faisant le bilan de l'année 1997, les trois plus grands ennemis des données sont respectivement...

les macro-virus, responsables de 80 % des infections,
les virus de boot, responsables de 15 % des infections,
les virus de fichiers, responsables de 5 % des infections.

Les macro-virus représentent à présent 80 % des infections rencontrées, contre 49 % l'année précédente. Le principal accusé est toujours **Word.Concept**, responsable de près de la moitié des infections. En outre, ce même article annonce pour bientôt de nouveaux virus, propres aux modules **ActiveX** de Microsoft. Ces modules sont de petits programmes véhiculés par Internet. S'ils sont malsains, ils pourront (ils peuvent déjà...) contaminer les ordinateurs. En 1997, cette menace est purement théorique : les seuls virus connus ont été créés par les chercheurs des éditeurs de logiciels antivirus... L'antidote est très simple : il suffit de désactiver le chargement de ces modules dans les navigateurs Web. Toutefois, les prochaines générations d'antivirus devront tenir compte de cette nouvelle famille.

2.11 - 2000 : I love you

2.11.1 - Les virus de demain

En quelques heures, ILOVEYOU (I love you) a infecté les cinq continents. Son attaque préfigure l'arrivée massive des « mass-mailing virus » qui empruntent l'autoroute des messageries et peuvent causer d'énormes dégats. Des messageries, et non seulement d'Internet ! Déjà, les téléphones mobiles ont essuyés une première attaque...

Il s'appelle Timofonica, il est d'origine espagnole, et son nom restera gravé dans les mémoires. C'est le premier virus qui frappe les utilisateurs de téléphone portable. Rien de bien méchant en fait, puisque ce « ver » qui envoie des messages écrits aux abonnées du réseau espagnol Movistar ne détruit aucun fichier. En revanche, étant d'un naturel très communicatif,, il se propage rapidement, par le messagerie. Exactement comme ILOVEYOU. Acun abonné de ce réseau n'est à l'abri de la contamination.

Coïncidence ? Non ! Ces virus, baptisés par les spécialistes ***mass-mailers ou mass-mailing virus***, ont le vent en poupe. A plusieurs égards, ils préfigurent ceux qui déferleront bientôt sur nos machines. Leur principale caractéristique ? Ils transitent pas les messageries ou les réseaux et disposent d'une formidable vitesse de propagation, en augmentation constante. Alors que le premier rejeton de cette famille, **W32/SKA**, dit aussi **Happy99** (apparu en janvier 1999), ciblait un individu dans le carnet d'adresse, MELISSA, découvert au premier trimestre 1999), en visait cinquante. Plus récemment, ILOVEYOU s'est attaqué à l'intégralité du carnet d'adresses. Résultat : pour faire le tour du monde, W32/SKA a mis plusieurs mois, Melissa quelques jours, contre seulement quelques heures pour YLOVEYOU.

Les virus ne sont plus ce qu'ils étaient ! Non seulement ils se propagent plus rapidement, mais ils sont aussi plus facile à concevoir pour le profane. En ce début de millénaire, nul besoin d'être un programmeur système fr haut niveau pour jouer les apprentis sorciers. C'éer un « script » comme ILOVEYOU ne présente aucune difficulté technique majeure ! En effet, ce virus repose sur un langage de programmation très simple : le **Visual Basic Script**, d'où l'extension **vbs**. Une simplicité qui a déjà permis à de nombreux pirates en herbe de le modifier sans difficulté pour tenter de brouiller les pistes. Moins d'une semaine après l'arrivée de ILOVEYOU, on recensait déjà plus d'une vingtaine de clones. Dont certains, beaucoup plus virulents, puisqu'ils tentaient d'écraser les documents Word et Excel en ciblant les fichiers dox et xls. Pour leurs auteurs, les créer ne fut l'affaire que de quelques minutes.

Simple d'usage, le langage VB script dispose également d'un autre avantage, qui ne va pas manquer d'intéresser les amateurs d'attaques virales. C'est un langage d'une puissance redoutable qui perrmet d'établir des liens avec les langages de programmation d'Internet et de la messagerie. Idéal donc, pour frapper vite et fort. Deux raioso,s supplémentaires de craindre une flambée de virus de ce type dans les mois qui viennent.

Face à cette menace, les utilisateurs des logiciels Microsoft seront en première ligne. En effet, si d'autres plateformes ont fait l'objet d'attaques, le quasi monopôle de Microsoft conduit les auteurs de virus à privilégier cette cible. D'autant plus que la firme de Seattle semble se faire un malin plaisir de leur faciliter la tâche : elle a fait attendre ses clients trois semaines avant de leur proposer un antidote. Et on se demande toujours pourquoi, après avoir diffusé un correctif modifiant les commandes de Word, après les attaques du virus Melissa, elle n'a pas songé à protéger les macros du programme de messagerie Outlook, à travers lequel s'est engouffré ILOVEYOU.

Mais que les utilisateurs des autres systèmes d'exploitation se gardent bien de souffler pour autant ! Même les systèmes les plus sécurisés ont leurs limites. Témoin, Unix, réputé in-

violable, dont les défenses sont tombées au début de l'année 99 à l'occasion d'une attaque virale effectuée et vase clos et à titre expérimental...

Outre les modes de progagations traditionnels, d'autres, beaucoup plus foudroyants, pourraient apparaître. Ainsi, une expérience mettant en scène un virus s'attaquant à Word, Excel et PowerPoint, a montré que le simple fait d'ouvrir une page Web, en l'absence de tout téléchargement, suffirait à comtaminer le disque dur. Imparable ! Dans ce cas, il n'existe qu'une solution pour endiguer l'épidémie : fermer le site Web !

2.11.2 - Chronologie d'une guerre

Soirée du 3 mai 2000, Philippines

Fin de l'après-midi. Les bureaux sont fermés. Les premiers messages contenant le virus ILOVEYOU sont envoyés via deux adresses e-mail situées à Manille...

Nuit du 3 au 4 mai, Etats-Unis

Tandis que l'Amérique dort profondément, le virus cotamine les noctambules qui veillent devant leur écran. Les dégats sont superficiels. Entreprises et administration ne eront touchés qu'au matin.

Aube du 4 mai, Norvège

L'alerte est donnée à l'aube, d'abord en Norvège, puis au Danemark et au Royaume-Uni. Les éditeurs d'antivirus se lancent dans une course contre la montre. Pendant ce temps, ILOVEYOU se répand comme une trainée de poudre dans les autres pays.

Matinée du 4 mai, France

Le premier correctif permettant de neutraliser l'intrus est disponible sur Internet. Devant la demande, la plupart des sites diffusant des solutions sont saturés. Dans nombre d'entreprises, les services informatiques, débordés, déconnectent les messageries infectées et parent au plus pressé

Journée du 4 mai, Asie

Après s'être répandu sur la majeure partie de la planète, le virus sevient en Asie douze heures plus tard. Mais la « signature » du virus a été identifiée, et les consignes de sécurité ont été diffusées. Les premiers clones de ILOVEYOU vont entrer en scène...

Chapitre 3 : Les virus

Selon certains, leur nom (V.I.R.U.S) provient d'une définition très générale qui les identifie à une menace sur les ressources informatiques vitales, soit, en anglais, « **Vital Information Ressources Under Siege** ». Selon d'autres, leur nom est dû uniquement à une analogie avec la biologie, analogie sur laquelle nous reviendrons plus loin.

3.1 - Un virus, qu'est ce que c'est ?

Les virus sont des programmes

Les virus ne sont que des programmes, c'est à dire des séquences d'instructions destinées à un ordinateur. Ces programmes, loin de constituer une application utile à l'ordinateur, s'attaquent à d'autres fichiers (pas toujours de type exécutables) en leur ajoutant un certain nombre d'instructions et en s'assurant qu'elles seront exécutées lorsque l'utilisateur voudra ouvrir ou lancer le fichier infecté.

Le virus est en général constitué de deux parties

La partie infectieuse lui permet de se propager. En fait, cette partie permet au virus de se reproduire en attachant des copies de lui-même à d'autres logiciels. C'est cette propriété qui fait des virus des programmes auto-reproductibles. Ainsi, chaque programme infecté pourra à son tour copier des noyaux de virus dans d'autres programmes. Un virus requiert les services d'un type d'hôte spécifique pour se dupliquer. Toutefois, au cours d'un procédé de recopie, de reproduction ou de propagation, certains virus récents sont capables de muter. Cette partie infectieuse est parfois seule. Ainsi, parmi les virus connus, certains se limitent à leur fonction de reproduction.

La partie active contribuera à la modification, ou à la destruction des logiciels ou des données qui les environnent, ou encore à des effets visuels aussi divers que variés (par exemple, l'affichage d'une balle de ping-pong, ou la chute progressive des caractères en bas de l'écran, etc.). Les effets possibles varient à l'infini : destruction de la table d'allocation des fichiers (FAT), destruction progressive des fichiers de données, destruction des fichiers du système d'exploitation, etc. Cette partie active est également nommée **charge utile** (!?) par allusion à la charge dite aussi utile emportée par un missile...

Propriétés générales

D'une manière générale, un programme doit être considéré comme un virus s'il réunit les propriétés suivantes :

1 - il modifie des logiciels extérieurs par inclusion de ses propres structures dans ces logiciels.
2 - les modifications qu'il provoque ne se limitent pas à un seul logiciel mais touchent au moins un groupe de programmes.
3 - il sait reconnaître si un logiciel a déjà été infecté.
4 - il reconnaît un logiciel déjà modifié, il s'interdit de procéder à une nouvelle modification.
5 - le logiciel infecté présente désormais les propriétés 1 à 4.

Si un logiciel ne possède pas simultanément toutes ces propriétés, il ne peut être considéré comme un virus au sens strict du terme.

3.2 - Quelques symptômes à reconnaître

Certains virus ont des effets évidents dès qu'ils entrent en action (apparition de messages bizarres, bruits incongrus, ou plus radicalement formatage du disque dur...). Par contre certains autres ont des actions beaucoup moins évidentes, surtout dans un premier temps. C'est pourquoi il est bon de connaître certains petits signes qui peuvent permettre à l'utilisateur d'agir avant qu'il ne soit trop tard. Bien évidemment, aucun de ses symptômes pris isolément ne prouve avec certitude la présence d'un virus, tout juste s'agit-il d'une présomption, plus ou moins forte. Par contre lorsque plusieurs indices concordent...

1 - Augmentation de la taille des fichiers exécutables

Des programmes peuvent se trouver dans l'impossibilité de se charger en mémoire vive. C'est le cas lorsqu'un virus utilisant une contamination par ajout ne reconnaît pas les fichiers déjà contaminés. Il peut s'ensuivre une augmentation de la taille du programme telle qu'il ne peut plus se charger par manque de mémoire. C'est assez exceptionnel, et quasi impossible, sous Windows.

2 - Blocage impromptu

Un blocage impromptu de programme peut se produire à la suite de l'actions indirecte d'un virus. (interférences avec d'autres programmes...). C'est peut-être aussi un problème de baisse de la tension d'alimentation électrique, ou encore un problème d'impression, ou n'importe quoi d'autre...

3 - Mauvais fonctionnement d'un programme

Le dysfonctionnement d'un programme peut éventuellement être dû à la disparition d'informations, suite à l'introduction d'un virus. Ces dysfonctionnements peuvent être plus ou moins importants selon l'endroit où s'est installé le virus. C'est parfois aussi, plus simplement, un problème de disque.

4 - Pertes inexplicables de données

C'est assez significatif, mais cela peut aussi provenir d'une fausse manœuvre oubliée, ou d'une erreur de manipulation passée inaperçue. Quoi qu'il en soit, sauvegardez encore et toujours sur des différents supports !

5 - Augmentation du nombre de programmes

On pourra constater une augmentation du nombre de programmes sur le disque dur. C'est le cas lors de contamination par un virus de type « compagnon ».

6 - Augmentation du nombre de secteur déclarés défectueux

Cela est surtout fréquent lors d'infection par des virus systèmes. Ce phénomène est typique d'une infection par le virus Ping-pong par exemple.

7 - Lenteur

L'exécution de certains programmes, ou l'accès aux périphériques (lecteurs, imprimantes...) prend un temps de plus en plus considérable.

8 -. Redémarrage automatique de votre ordinateur

Ne cherchez pas plus loin. A moins d'une microcoupure de courant d'alimentation, l'explication la plus probable est la présence d'un virus.

9 - Accès inhabituels aux disques

Le voyant d'accès sur le lecteur de disquettes ou le disque dur clignote plus fréquemment que de raison[26], c'est peut-être un virus qui essaie de se propager dans vos mémoires de masse...

10 - Fichiers apparaissant ou disparaissant sans raison apparente, qui changent de noms ...

Dans cette catégorie de symptômes, on peut citer l'action de certains virus qui agissent par chiffrement. Ils se contentent en fait de modifier complètement les noms de fichiers (et les extensions, tant qu'à faire). En fait aucune information n'est perdue mais il est tout à fait impossible d'identifier quoi que se soit. Quand vous en êtes au stade terminal, il n'y a plus qu'a reformater le disque dur. C'est par exemple l'action du virus **Pretoria**.

[26] - Attention : n'oubliez pas que Windows utilise le disque comme mémoire virtuelle. De nombreux accès au disque peuvent aussi être la preuve d'un manque de mémoire vive.

Ce sont là, quelques points à vérifier quand vous avez un doute sur l'intégrité de votre ordinateur. Il existe naturellement bien d'autres conséquences dues au virus mais en ce qui les concernent, vous saurez rapidement à quoi vous en tenir. Le déclenchement de la marche funèbre (virus **Berlioz**) en pleine session Windows, par exemple, laisse planer peu de doute.

3.3 - Spécificité des virus ?

Jusque vers 1998/98, on affirmait haut et clair que le virus qui s'attaquait à votre ordinateur dépendait avant tout du système d'exploitation de celui-ci. A priori, un virus créé pour agir sous un environnement DOS par exemple était tout à fait inopérant sous un environnement Macintosh ou Unix. Cette spécificité de système descendait même parfois jusqu'aux composants matériels de la machine. Ainsi, la première version du virus Ping-pong ne pouvait contaminer que des ordinateurs munis d'un microprocesseurs 8088 ou 8086. Il a donc disparu avec eux. Ceci n'est plus vrai. Les macrovirus, heureusement encore peu nombreux, peuvent passer d'un environnement à l'autre chaque fois qu'ils sont écrit dans un langage commun aux deux systèmes d'exploitation. Toutefois il faut savoir que, même s'ils sont peu nombreux, ils sont à l'origine de la grande majorité des attaques virales actuelles, probablement plus de 80 %.

Le système d'exploitation où l'on recense le plus grand nombre de virus est sans conteste l'environnement DOS (et Windows) du fait du très grand nombre de micro-ordinateurs sur le marché et de sa relative simplicité. L'environnement Macintosh est mieux protégé contre les virus (architecture moins favorable au développement de virus et programmation beaucoup plus stricte). Des systèmes tels que UNIX ou OS/2 sont théoriquement susceptibles d'être attaqués par des virus mais on n'a encore pas rapporté de cas important de contamination. La relativement faible diffusion de ces systèmes d'exploitation rend également le phénomène moins « intéressant »...

Toutefois, il ne faut pas se bercer d'illusion. Les passerelles sont de plus en plus nombreuses entre les environnements Windows et Macintosh, les virus, comme les utilisateurs, en profitent pour échapper à un certain nombre de contraintes. Les virus les plus dangereux à l'heure actuelle sont les macrovirus, et en particulier ceux écrits pour les logiciels Microsoft Office. Les procédures d'écriture des macrocommandes ayant été uniformisées, les virus les plus récents, ceux qui utilisent ces mêmes techniques, sautent allègrement d'un logiciel à l'autre, d'un environnement à l'autre... La spécificité n'est plus de règle.

3.4 - Les créateurs de virus

Remarquons tout d'abord que, comme le nom original d'un virus n'est pas toujours indiqué par le concepteur, celui qui le découvre le baptise en se basant sur sa taille (**1701**), sur le pays d'origine **(Italian**), sur une partie du texte qu'il contient éventuellement (**Amobea**) ou sur son action (**Friday the 13th** ou **Vendredi 13**). Il est encore plus difficile de parvenir à déterminer l'origine exacte des virus, sauf quelques exceptions où le repérage a été réalisé en comparant les différentes versions, ainsi que les améliorations apportées. Il est cependant intéressant de tenter d'analyser les motivations des créateurs...

Les **pirates** sont des personnes dont le seul but est la recherche de nouveauté qu'ils atteignent par l'écriture de virus. C'est surtout l'intérêt personnel qui les motive. Pour citer un exemple, à la fin de l'année 1987, les programmeurs du magazine canadien MacMag développent une pile hypercard qui, à la date du 2 mars 1988 affiche sur les écrans (des Macintosh) un message de paix avant de s'autodétruire.

Parmi ces pirates, on trouve aussi des **psychopathes** (irresponsables) qui manifestent une rancœur personnelle mal définie, et qui ont souvent de sérieux problèmes, essentiellement relationnels, envers la société. Ils réalisent des virus pour l'argent, pour l'amusement ou par méchanceté gratuite. C'est le cas du virus AIDS, sur PC, qui fut expédié depuis Londres, dans le monde entier. Cette histoire est tristement déconcertante. Une disquette infectée où figure un programme nommé **AIDS Information 2.0** est envoyée à un grand nombre de médecins, chercheurs et responsables d'organisation de santé. Pris dans une succession de questions et de messages menaçants, l'utilisateur se rend vite compte que le logiciel n'offre aucun intérêt. Seulement, il est déjà trop tard... La seule solution efficace est de reformater le disque dur. Il semblerait que le piège ait été déjoué assez rapidement, et qu'il n'y ait eu finalement que peu de victimes**. Pourtant, malheureusement, à l'hôpital Bichât, à Paris, tous les fichiers concernant plusieurs années de recherche sur le SIDA auraient été perdus[27]...**

Les **étudiants** sont aussi parmi les créateurs et surtout les propagateurs (parfois involontaires) de virus. Ayant accès gratuitement à des installations informatiques, bon nombre y utilisent des logiciels recopiés chez des amis, c'est à dire piratés. De nombreux virus se manifestent de cette manière. Seulement, la compétence technique (en informatique) requise pour un tel exercice est accessible à beaucoup d'entre eux, et certains y voient un défi intellectuel. Ainsi, en Mai 1990, est découvert le virus **MDEF**, sur Macintosh. Il a contourné la protection des antivirus que l'on croyait encore infaillibles à l'époque. En Août 1990, un second virus apparaît, également sur Macintosh. L'enquête montrera assez facilement que les deux ont été mis au point par un même étudiant, qui n'a pas su canaliser ses talents de programmeur. L'histoire ne dit pas s'il a pu continuer ses études. Par contre, il a été exclu à vie des universités américaines...

Les **employés** souhaitant manifester leur mécontentement au sein de l'entreprise constituent un risque pour la sécurité informatique de cette dernière. Seulement, peu nombreux sont ceux capables de réaliser de véritables virus. Toutefois, de nombreux cas de **bombes logiques** ou de Chevaux de Troie implantés dans les systèmes informatiques ont été signalés. Par exemple, pour garantir son emploi, un salarié a mis une séquence introductive dans le programme de paie, de façon à vérifier que son nom se trouve dans la liste des salariés. En cas de licenciement, son nom disparaît, et la paie est perturbée...

Les **organisations terroristes** ne sont pas les dernières à œuvrer sur le terrain informatique. Ce sont en général des fanatiques pour lesquels rien ne compte, et surtout pas le monde extérieur, hostile par définition. Ils sont endoctrinés, et fidèles à leur groupe. Le virus **Jérusalem**, plus connu sous le nom de Vendredi 13, aurait ainsi été écrit par des sympathisants de l'OLP, bien que cette dernière conteste cette paternité. Pourtant, il devait entrer en action le jour anniversaire de la fondation de l'état d'Israël...

Les **pays de l'Est** ont aussi été la source de nombreux virus. C'est le cas, en 1992, de la Bulgarie qui compte parmi sa population un grand nombre de programmeurs hautement qualifiés, mais sous-payés. Pour eux, la création de virus constitue à la fois un défi à une société qui ne reconnaît par leur talent, et un bon moyen de sortir de l'ombre. Le fait qu'une grande partie de leurs virus indique le nom ou le pseudonyme de leur créateur est assez significatif. De plus, ces pays ne possèdent pas, ou pas encore, de législation efficace relative aux délits informatiques...

Attention, si vous avez l'intention de lancer un virus dans la nature, sachez que tout évolue. Avec la multiplication des logiciels de détection, et grâce (?) aux traces laissées sur Internet et le courrier électronique, il est actuellemet possible de retrouver l'origine d'un virus. Aux Etats-Unis, plusieurs personnes sont en prison, ou en attende de jugement, pour avoir crée et diffusé des virus informatiques.

[27] - Je donne cette information sous toutes réserves ; elle n'a jamais été confirmée, ni démentie.

3.5 - Le discours médical

Si les virus informatiques ont été ainsi baptisés, c'est que leur comportement rappelle celui de ces organismes vivants, les virus biologiques. Malheureusement, la presse générale exploite régulièrement cette analogie avec les virus biologiques, alimentant le mythe du *virus informatique : maladie de la machine* au lieu d'en simplifier la définition. Il faut avouer que ce type de programme présente une étonnante similitude avec les virus biologiques. Chez ce dernier, l'ADN ou l'ARN contient les instructions génétiques qui assurent son infiltration dans la cellule saine qui sera ensuite amenée à en produire des copies. De la même manière, le virus informatique contient des instructions permettant sa copie et la fixation de celle-ci à un support. D'une manière générale, les parallèles entre virus biologiques et virus informatiques sont nombreux, et même souvent justifiés. En effet, les virus se comportent dans l'ordinateur, un peu comme des virus dans un organisme vivant.

Malheureusement, l'image (négative et) déformée offerte par le terme de virus a pour conséquence de déclencher à leur sujet tout un spectre d'opinions diverses, allant du sourire condescendant, à la peur panique de l'infection en passant par les ricanement du connaisseur. Le mot virus est racoleur, évocateur et reconnaissable de loin. Dans les années « SIDA », il évoque des visions horribles et terrifiantes. Virus, ça fait meilleur effet dans un titre que **code destructeur**. Résultat : un mot ancien et courant se voit embarqué dans des processus de définition et de redéfinition sans fin. Cela va jusqu'aux mesures de prévention contre les virus, qui sont bien sûr désignées par le terme de vaccins... Le vocabulaire concernant les virus informatique s'est beaucoup inspiré du domaine médical.

3.5.1 - Rappel de Biologie[28] ...

En biologie, le virus est un micro-organisme, le plus petit élément vivant, entouré de protéines et composé d'une chaîne d'ADN ou d'ARN qui contient son patrimoine génétique. Il ne peut survivre qu'en s'introduisant dans une cellule saine qu'il va parasiter pour se reproduire.

La reproduction du virus s'effectue par duplication. Son ADN s'intègre aux chromosomes de la cellule infectée et produit alors un ARN qui, soit s'assemble aux protéines pour former des clones qui vont sortir de la cellule par bourgeonnement, soit parasite le double de la cellule lors de sa reproduction. Le virus peut dès lors se déclencher immédiatement ou après une certaine période de latente. Dans les deux cas, son action varie en fonction de l'état physique de l'individu, et du nombre de cellules infectées. Plus elles sont nombreuses, plus l'organisme est atteint. Heureusement, tous les virus ne provoquent pas des maladies incurables, certains sont même presque inoffensifs.. L'organisme est capable de se défendre contre la majorité d'entre eux, et de nombreux vaccins existent. Une sacrée chance : on imagine mal l'homme effectuer régulièrement des copies de sauvegarde de ses cellules[29] ...

On pourrait longtemps disserter sur les points communs. Mais, dans les faits, il existe une différence fondamentale entre les deux types de virus. Alors que le virus biologique a pour but principal de vivre et de se reproduire, comme tout être vivant, ses effets n'étant qu'un sous-produit résultant de sa présence, le but premier du virus informatique n'est pas que la reproduction... Par contre, la prévention, la détection, la vaccination et le traitement d'un virus sont souvent comparables pour les deux types (biologique et informatique). C'est tellement vrai que cela a conduit un

[28] - Ne considérez les lignes qui suivent que comme quelque chose de très élémentaire. Relisez un cours de biologie pour plus de précision... et surtout, ne faites pas de mauvais jeux de mots. D'autres les ont déjà faits avant vous.

[29] - ...mis à part dans les romans de Science-fiction, par une technique dérivée du clonage bien connu de certains biologistes... Dans ce domaine, le problème est plus d'ordre moral que d'ordre technique.

médecin français à mettre au point un vaccin contre les virus informatiques en partant d'un raisonnement biologique...

Pour en terminer sur cette comparaison entre les deux espèces de virus le biologique et le programmé, notez que vous trouverez dans tout bon cours de biologie la définition de ce que l'on nomme parfois une particule virale... :
« *Particule virale : ensemble constitué par un axe d'acide nucléique (ADN ou ARN), caractéristique du virus en cause, et une coque de protéines qui l'entoure...* » [30]

3.5.2 - Biologie et Informatique : même terminologie

Qu'on se le dise une bonne fois pour toutes, un virus informatique est un programme, et n'est **rien d'autre qu'un programme** comme un autre, ou presque, dont le mode de fonctionnement permet d'opérer un rapprochement entre les termes qui décrivent ses mécanismes et le vocabulaire médical réservé à la pathologie virale. Il ne s'agit pas du tout de vers qui rongent les ROM, ni de microbes dont la propagation est due « *à la promiscuité des disquettes dans leur boite de rangement* », comme le laissent parfois entendre certains journalistes « scientifiques »... Inutile donc de revêtir un masque stérile avant de s'installer devant un ordinateur puisqu'il n'existe à ce jour aucun virus biologique susceptible de grignoter les secteurs d'un disque dur (contrairement à une idée évidemment fausse qui refait périodiquement surface dans certains médias).

Le fait de cultiver l'analogie entre virus informatiques et virus biologiques permet de disposer d'un **vocabulaire** porteur d'images fortes. **Le mot virus est, en effet, lourd de menaces**[31] . Cela étant, cette terminologie masque la réalité des virus informatiques derrière des concepts qui n'apportent aucune information sur leur fonctionnement. Les termes aussi poétiques que souche, mutation, infection, prolifération, dissémination, incubation ou encore activation sont à rattacher aux caractéristiques et aux phases de fonctionnement du virus biologique. Par contre, l'activité d'un programme, quel qu'il soit, se limite à exécuter différentes opérations au gré de conditions testées au moyen de fonctions logiques. Les virus informatiques n'échappent pas à cette règle. Lorsque la machine est éteinte, par exemple, rien ne peut plus se produire et l'exécution de la suite logique des instructions contenues dans le code du virus se trouve de facto stoppée jusqu'à la prochaine mise en service[32] .

3.5.3 - Autres points de comparaisons...

Virus biologiques	*Virus informatiques*
Attaquent seulement certaines cellules du corps.	*Attaquent seulement certains programmes (par exemple tous les *.COM ou tous les *.EXE).*
Transforment l'information héréditaire de la cellule.	*Manipulent un programme en lui faisant exécuter des tâches différentes de celles prévues.*
Les cellules touchées produisent de nouveaux virus.	*Le programme touché infecte lui-même d'autres programmes.*
Une cellule infectée n'est jamais infectée plu-	*Un programme n'est en général infecté qu'une*

[30] - ...mais surtout n'oubliez pas que...

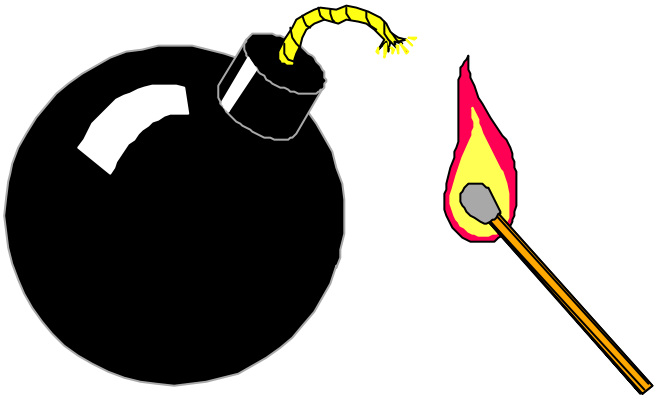
Je me les sers moi-même avec assez de verve,
Mais je ne permets pas qu'un autre me les serve.

Edmond Rostand - Cyrano de Bergerac (Acte 1 - scène 4)

[31] - Surtout depuis quelques années...

[32] - Donc, premier conseil : confronté à un virus lorsqu'on ne dispose d'aucun programme spécialisé pour le combattre, il est urgent de ne rien faire....

sieurs fois par le même virus.	*seule fois par la plupart des virus.*
Un organisme touché peut ne présenter aucun symptôme pendant très longtemps.	*Le programme infecté peut fonctionner long-temps sans erreur.*
Toutes les cellules entrant en contact avec le virus ne sont pas infectées.	*Les programmes peuvent être immunisés contre certains virus.*
Les virus peuvent muter et ne sont pas toujours facilement reconnaissables.	*Certains programmes de virus peuvent se transformer et échapper à des logiciels de détection.*



Chapitre 4 : Un peu de virologie

Un message comme vous pouvez en lire de temps à autre...

Kriz, le virus tueur

Le 18 août 1999, un nouveau virus, Kriz, a été découvert. Polymorphe résident classique, il s'attaque aux .exe et .src, et infecte le fichier **kernel32.dll**. Il s'active ensuite le 25 décembre, date à laquelle il efface non seulement les données du disque dur, mais écrase également le BIOS de la machine, rendant ainsi inefficace toute tentative de redémarrage.

Pour en savoir plus (une solution est proposée) :
http://www.datafellows.com/v-descs/kriz.htm
http://www.zdnet.com/zdnn/stories/news/0,4586,2316716,00.html

Alors, que faire ?
D'abord en savoir plus sur le(s) virus,
Ensuite, s'occuper de la prévention contre la « bestiole »,
Enfin, si nécessaire, trouver le moyen de « soigner » la machine.

Tel sont les buts des chapitres qui suivent...

4.1 - Comment agit un virus ?

Par définition, les virus sont des petits bouts de programme (de 200 octets à 4 Ko) capables de s'intégrer directement dans le code d'un autre programme et de se reproduire. Leur action se décompose le plus souvent en trois phases : infection, reproduction et attaque.

L'infection

La première action effectuée par un virus lorsqu'il s'introduit dans une machine (le plus souvent par le biais d'une disquette) est de s'insérer dans un autre programme ou dans un secteur particulier du (des) disque(s) dur(s). Pour ce faire, le virus ajoute son code à celui d'un logiciel présent sur ce disque dur. Il réside alors sur ce dernier mais ne peut être repéré directement puisqu'il n'apparaît nulle part lorsque l'on affiche la liste des fichiers.

Les premiers virus infectaient les programmes hôtes de façon voyante : la taille de ceux-ci augmentait. A titre d'exemple, le virus **DataCrime** se colle à la fin d'un programme, augmentant la taille de celui-ci de 1168 octets. **Jérusalem** fait de même et provoque un accroissement de 1813 octets. Les premiers logiciels antivirus se targuaient de les détecter sur cette base[33]. Mais, à présent, l'infection s'avère plus subtile : certains virus se logent dans le code d'un logiciel sans modifier la taille réelle ou apparente de celui-ci. Il faut alors avoir recours à d'autres méthodes pour les détecter : recherche de signature, calcul d'une somme de contrôle,...

La reproduction

Les virus informatiques se comportent comme leurs homologues biologiques : une fois dans l'organisme (l'ordinateur), ils sont capables de contaminer d'autres entités (des fichiers). Certains d'entre eux, tels que **Bloody** ou **Hunt**, se chargent dans la mémoire dès lors que l'on exécute un programme infecté. Ils peuvent alors à commencer polluer un grand nombre de logiciels. Dans le même temps, ils doivent demeurer cachés le plus longtemps possible. Ils laissent donc souvent une signature dans chaque programme infecté, afin de ne pas le contaminer à nouveau. En effet, si leur taille augmentait de façon trop visible, l'utilisateur pourrait soupçonner la présence de quelque chose d'anormal...

L'attaque

La contamination n'est pas toujours une fin en soi. Les virus s'installent sur le disque dur afin de déclencher tôt ou tard une attaque en règle. Un événement déterminé les fait entrer en action, tels l'arrivée d'une date précise ou le fait que l'utilisateur ait frappé une certaine séquence de touches. A ce moment-là, le virus commence son oeuvre pernicieuse : affichage pseudo-humoristique, destruction de fichiers, formatage du disque dur, brouillage des informations... Ainsi, **DataCrime** est opérationnel le 12 octobre, date à laquelle il formate le disque dur. **Maltese Amobea** (l'amibe de Malte, repéré en Irlande en septembre 1991) lance son agression le 15 mars ou le 1er novembre en effaçant les données des premiers secteurs des disques puis le secteur de démarrage, pour y inscrire un message: « *Maltese Amobea, infecteur universel, caché aux yeux de tous, sauf aux nôtres...* »

[33] - Lors de leur installation, ils relevaient la taille de tous les fichiers susceptibles d'être infectés. Ensuite, ils procédaient par comparaison. Ils étaient donc incapables de découvrir un virus déjà présent sur un disque, ou de prévenir une attaque. Lorsqu'ils décelaient la présence d'un virus, c'était trop tard l'infection avait déjà commencé...

Un virus informatique classique est un programme qui recopie, reproduit ou propage sa propre image avant de lancer son attaque, et ceci généralement à l'insu de l'utilisateur. Un virus peut être totalement caractérisé en trois points :

Sa méthode de **contamination**, c'est-à-dire la manière dont il se duplique et quelles sont les parties du système qu'il infecte ;
Son **action** proprement dite, c'est-à-dire ses conséquences finales, car un virus ne se contente que rarement de sa seule propagation ;
Les conditions ou critères de **déclenchement** de cette action.

4.2 - La méthode de contamination[34]

4.2.1 - Les vecteurs

Un vrai virus ne constitue pas un programme autonome. **Il est toujours inclus dans un programme hôte** qui lui sert de support. Pour pouvoir assurer sa fonction de reproduction, il doit obligatoirement être exécuté au moins une fois. Le virus va donc avoir pour but premier de détourner à son profit tous les moyens qui lui permettent d'être exécuté. Pour les premiers virus, cela limitait les contaminations à deux grandes catégories de code : les fichiers exécutables (sur un PC, il s'agit surtout des fichiers .COM .EXE .OVL ...) et les secteurs de boot chargés au démarrage de la machine. Chacun de ces moyens permettant à un virus de se propager avant de s'exécuter est appelé un **vecteur de contamination**.

Bien sûr, afin de mettre tous les atouts de son côté, un virus peut utiliser simultanément plusieurs vecteurs différents. Cela lui apportera une efficacité accrue lors de sa période de propagation, au prix d'une programmation plus complexe et d'une taille plus élevée, mais en même temps d'un risque accru de découverte. Comme on peut le deviner, un virus classique n'infectera jamais (sauf erreur de programmation toujours possible dans le code du virus lui-même) un fichier non exécutable (fichier de données, fichier texte...). Cela n'aurait aucune utilité dans l'action de propagation du virus[35]. Il n'en est plus de même avec la famille des macrovirus, qui connaît actuellement une véritable explosion (plus de 80 % des cas d'infection constatés). Au contraire des virus classiques, ils se placent dans des documents issus de logiciels permettant l'utilisation de macro-commandes (telles les nouvelles versions de Word, Access et Excel...).

Nous donnerons ici différents vecteurs accessibles aux virus classiques du monde des compatibles PC, où le choix offert est plus important que sur Macintosh :

Les fichiers exécutables .COM

C'est le principal mode de contamination (plus de 90% des virus y ont recours), car il est très facile de modifier un exécutable **.COM** pour y rajouter du code. Le virus s'insère au début ou à la fin du fichier et détourne la première instruction pour être appelé lors de l'exécution du programme infecté. Après son exécution, le virus remplace l'ensemble des ins-

[34] - Les lecteurs pressés, et ceux pour qui la technique ne présente que peu d'attraits, peuvent se contenter de lire le début pu paragraphe 4.2.1 avant de passer à la section suivante... mais ce serait dommage !

[35] - En conséquence, si l'utilisateur découvre un de ses fichiers, par exemple de traitement de texte, en mauvais état, cela ne signifie pas forcément que sa machine est victime d'une attaque virale. Le plus souvent il pourra s'agir d'un incident normal lié aux conditions de travail, ou d'un problème concernant la qualité du support magnétique.

tructions modifiées dans le programme par leur valeur originale et exécute ce même programme, rendant l'opération invisible pour l'utilisateur. Puisque le code du virus a été inséré dans le fichier, un programme infecté augmente de taille.

Les fichiers exécutables .EXE

C'est un mode de contamination également utilisé, bien que plus difficile à mettre en œuvre que le précédent, car l'entête du fichier **.EXE** ainsi que les données de relocation doivent être modifiées. En dehors de cette particularité, le fonctionnement général reste identique à celui d'un **.COM**.

Les fichiers overlays (.OVL ou .OVR)

Certains gros programmes utilisent des fichiers exécutables dits **overlays** qui sont chargés en mémoire et exécutés au fur et à mesure des besoins de l'application. Puisque ces overlays sont exécutés, ils peuvent également servir de code hôte à un virus. Ces overlays nécessitant les mêmes données de relocation qu'un fichier **.EXE**, la plupart des virus attaquant les **.EXE** contaminent également les overlays.

Le fichier COMMAND.COM

La plupart des virus infectant les **.COM** ne font aucune différence entre ces fichiers et le **COMMAND.COM**, qu'ils infectent donc de la même façon. Cependant, certains virus lui réservent un traitement spécial, en évitant son infection ou au contraire en n'infectant que lui. Le **COMMAND.COM** est en effet très intéressant pour un virus, car il lui permet d'être systématiquement chargé dans la machine dès le boot (dès le début du démarrage de l'ordinateur).

Les fichiers systèmes IO.SYS et DOS.SYS

Ces deux fichiers pourraient être l'objet d'attaques virales fort intéressantes (pour les virus...) car ils sont chargés et exécutés lors du chargement du DOS sur la machine. Cependant, il semble que très peu de virus s'intéressent à ces fichiers. En effet, d'une part leur modification peut être complexe, d'autre part l'infection des secteurs de boot apporte les mêmes avantages au prix d'une écriture beaucoup plus simple. Les créateurs de virus sont en général de bons programmeurs, mais pas forcément des génies, contrairement à ce que laissent entendre certains médias...

Le secteur de partition[36] du disque dur

Le secteur de partition d'un disque dur est le tout premier secteur du disque (cylindre 0, tête 0 et secteur 1). Il est créé par **FDISK** et contient notamment le descriptif de la table de partition. Le code est automatiquement chargé et exécuté par le Bios. après le traditionnel décompte de la mémoire et les tests internes. Ce code doit vérifier la présence d'une table de partition correcte (dans le cas contraire, message « *Table de partition invalide* »), puis l'existence d'une partition active (dans le cas contraire, message « *Disque non système* »). Le premier secteur de cette partition active (le secteur de boot) est alors chargé en mémoire et exécuté. On voit donc tout de

[36] - La partition d'un disque dur consiste à diviser le volume physique en plusieurs volumes logiques. Cela est parfois utilisé pour gagner de la place en diminuant la taille des unités d'allocation (les clusters). Il faut savoir que ce secteur de partition existe toujours sur les disques durs, même si le disque n'est pas partitionné (n'est pas divisé en plusieurs volumes logiques, ce qui est généralement le cas actuellement).

suite l'intérêt pour un virus d'infecter ce code de démarrage afin d'être systématiquement chargé lors de tout boot à partir du disque dur, et ceci avant même le chargement du système MS.Dos, et donc avant toute possibilité d'intervention d'un antivirus. Bien entendu, en cas d'infection, le secteur original est sauvegardé en un autre endroit du disque, afin de pouvoir continuer à mener à bien la procédure de mise en marche (de boot).

Le secteur de boot MS-DOS du disque dur

Il s'agit du premier secteur de la partition DOS. Lorsque cette partition commence au début du disque, comme c'est généralement le cas, il s'agit du secteur 1, tête 1, cylindre 0. Son utilisation par un virus est en tout point identique au secteur de partition car ils sont de toute façon chargés séquentiellement lors d'un boot DOS.

Le secteur de boot des disquettes

Sur disquette, il n'existe pas de secteur de partition. Le premier secteur de la disquette fait donc office de secteur unique de boot. Il a été historiquement le premier visé, à l'époque où les disques durs n'étaient pas aussi répandus. Le mode d'action du virus sur ce secteur est en fait très proche de celui existant sur les disques durs.

4.2.2 - Ensuite...

Lorsqu'un virus classique est chargé en mémoire par l'un de ces vecteurs de contamination, il dispose en fait de **deux possibilités** : il peut tout d'abord profiter du fait qu'il a la main pour **infecter immédiatemen**t un ou plusieurs autres vecteurs (par exemple le premier fichier exécutable du répertoire courant), puis continuer l'exécution de son programme hôte. Un tel virus ne se propagera donc que lorsqu'on lancera un programme infecté. Si les programmes infectés sont rarement utilisés, l'infection sera limitée. Autre manœuvre possible, le virus détourne certaines interruptions[37] sensibles (DOS, horloge, Bios...) afin de pouvoir être appelé par la suite, **s'installer résident en mémoire** et bien entendu continuer l'exécution de son programme hôte (c'est à dire de son vecteur). C'est l'option la plus intéressante, car elle permet au virus d'être actif en permanence jusqu'à l'arrêt de la machine. Les deux interruptions les plus intéressantes et donc les plus souvent détournées sont les suivantes :

* l'interruption permettant de **charger et d'exécuter un programme**. C'est notamment celle qui est utilisée par le système d'exploitation, par l'intermédiaire du fichier COMMAND.COM pour effectuer le lancement des programmes demandés par l'utilisateur. Le virus qui a détourné cette interruption peut analyser le nom du fichier à exécuter et décider ou non de son infection. Ainsi, après l'exécution d'un seul programme infecté, par exemple, d'un virus s'installant en mémoire et s'intéressant aux .COM, tous les fichiers .COM exécutés ensuite et cela jusqu'à l'arrêt de la machine, seront eux-mêmes contaminés !

* l'interruption permettant d'**ouvrir un fichier**. Seule l'ouverture d'un fichier exécutable (.COM ou .EXE) est susceptible d'intéresser un virus. Cela arrive rarement dans un programme utilisateur classique, mais en revanche cette fonction est utilisée systématiquement par les commandes DOS **COPY** et **XCOPY** pour lire le fichier source. On voit immédiatement tout le danger d'un virus interceptant cette fonction, puisqu'une fois résidant en mémoire, tous les fichiers copiés par COPY ou XCOPY seront systématiquement infectés ! Cela peut également arriver avec tous les programmes amenés à ouvrir des fichiers exécutables, par exemple un programme antivirus vérifiant tous les fichiers. Il est donc très important, au moindre doute, d'effectuer

[37] - Une interruption correspond, très grossièrement, à l'appel d'une commande DOS.

toutes les vérifications antivirus après avoir rebooté la machine à partir d'une disquette système d'origine, saine et protégée contre l'écriture.

4.3 - L'action du virus

Toute action possible est envisageable. Les seules limites sont en fait celles de l'imagination de l'auteur, ainsi que celles inhérentes aux possibilités du logiciel. Par exemple, mettre en panne définitivement une partie du matériel (écran, clavier, processeur...) n'est pas possible par un logiciel classique. Un virus ne pourra donc le faire[38].

L'action déclenchée peut être anodine tel l'affichage d'un message à intervalles réguliers ou le ralentissement de la machine, ou plus néfaste tel l'effacement de données sur disque dur ou sur disquette. Elle peut être aussi beaucoup moins franche et plus sournoise, comme la modification progressive de la table d'allocation, qui ne provoquera des problèmes qu'après un temps plus ou moins long. Le virus **Stoned**, dans sa forme originale, se contentait d'afficher un message demandant de légaliser l'usage de la Marijuana, alors que le virus **Dbase** trafique les données écrites dans un fichier .DBF, et les remet en ordre à la lecture. Le problème n'interviendra que lorsqu'on élimine le virus, ou lorsqu'on transmet un fichier de données. Une autre de ses activités consiste à détruire les fichiers .DBF âgés de plus de trois mois... Il est à noter que certains virus ne semblent pas présenter de phase d'action, se contentant d'une simple propagation de son code. Cela ne signifie pas pour autant qu'ils ne sont pas dangereux, car la phase de propagation peut également être destructrice, dans le cas où le virus insère son code dans le programme hôte sans en sauvegarder les parties réécrites, ou lorsque les secteurs de boot sont modifiés sans qu'aucune copie ne soit écrite ailleurs.

A titre d'exemple, de curiosité aussi, et pour montrer la diversité des actions possibles des virus, voici quelques cas intéressants (! ?) parmi des milliers d'autres...

1 - Le virus mélomane

Nom : Peter-II
Type : Résidant - secteurs d'amorçage

Peter-II infecte les secteurs d'amorçage des disquettes et des disques durs. Après l'infection, il est tapi dans la mémoire haute et se réveille chaque fois que l'ordinateur démarre. En plus, si vous essayez d'examiner les enregistrements d'amorçage sur un ordinateur infecté, il vous montrera l'enregistrement d'origine. Voici ce qui va vous arrivez quant vous rencontrerez Peter-II D'abord, un message (en anglais) sur l'écran :

> Bonjour tout le monde, je suis PETER-II ! N'éteignez pas votre ordinateur, ou vous allez perdre toutes vos données. Attendez une minute, s'il vous plaît...

Après cela, Peter-II cryptera le contenu du disque dur, en émettant la commande XOR 7878h à chaque octet de chaque secteur. Puis, il va revenir en affichant le questionnaire suivant :

> OK. Si vous donnez la bonne réponse aux questions suivantes, je sauverai votre disque dur :
> A. Qui a chanté "I'll be there" ?
> 1. Mariah Carey 2. The Escape Club 3. The Jackson Five 4. Les trois
> B. Qui est Phil Collins ?
> 1. Un chanteur 2. Un batteur 3. Un producteur 4. Les trois
> C. Qui a eu le plus de singles dans le TOP 10 dans les années 80 ?
> 1. Michael Jackson A. Phil Collins 3. Madonna 4. Whitney Houston

Si vous tombez juste, Miracle ! Peter-2 vous dit :

> Félicitations !!! Vous avez passé le quiz ! Vous pouvez maintenant récupérer vo-

[38] - Toutefois, il pourra tenter d'envoyer les têtes de lectures du disque dur vers une piste inexistante, et le bloquer irrémédiablement... Cela s'est fait. L'imagination de quelques farfelus est hélas sans limite; alors que leur bon sens...

> tre disque dur.

Mais si vous vous trompez, Peter II vous dit :

> Désolé ! Vas au diable ! Minable !

Notez que les bonnes réponses sont 4, 4 et 2.

2 - Le virus communiste

Nom : Russian-Flag
Type : Résidant - secteur d'amorçage ?

Un virus typique des secteurs d'amorçage. Russian-Flag s'active lorsqu'une machine est activé un 19 Août, et affiche un drapeau soviétique à l'écran. Si vous ne le savez pas déjà, apprenez que le 19 Août 1991 est la date d'un coup d'état militaire manqué en Russie.

3 - Le virus superstitieux

Nom : Jérusalem
Type : Résidant - Fichiers .COM et .EXE

Le virus Jérusalem est l'un des plus anciens et des plus courants. Il s'active toue les vendredi 13, effaçant les programmes qui sont utilisés ce jour-là. Dans sa version la plus courante, trente minutes après l'exécution d'un programme infecté, le virus ralentit l'ordinateur et fait baisser une partie de l'écran de deux lignes. Seulement, c'est souvent déjà trop tard pour certains de vos programmes... Pour de nombreuses variantes, cet effet secondaire est inactivé, ce qui les rend encore plus difficiles à déceler.

4 - Le virus « enceinte »

Nom : Pregnant[39]
Type : Résidant - fichiers *.COM

Ce virus s'active les vendredis, entre 22 h et 23 heures, et fait en sorte que tous les fichiers infectés s'appelle PREGNANT quand une commande DIR est lancée. Du coup, votre ordinateur ressemble à une maternité...

5 - Le virus mystique

Nom : Rescue
Type : Résidant - fichiers *.EXE

Le virus Rescue réside en mémoire et infecte les fichiers .EXE. Les fichiers infectés s'agrandissent d'à peu près 3434 octets. Une fois activé, il affiche un des messages suivants (ce ne sont pas les seuls possibles...):

> Tuez un satanique produit ANTI-VIRAL pour Jésus aujourd'hui !
> Arrêtez les désinfectants maintenant
> Et Dieu dit « Que la vie soit », et elle fut...
> Sauvez les virus ! Ils sont aussi des gens !
> Détruisez les cliniques pour ordinateurs !

6 - Le virus de Noël

Nom : Cantando
Type : non résidant - fichiers *.COM

Cantando est un virus non résidant simple, qui infecte d'autres fichiers .COM en copiant son code à la fin des fichiers. Il s'active le 24 décembre, de n'importe quelle année. Il affiche le message suivant :

[39] - En cas de besoin, consulter un dictionnaire anglais-français.

> CaN-TaN-Do-v01 : Onkos täälä kittrjä lapsia ?

Il paraît que ce texte est en finnois et qu'il signifie « y a-t-il des enfants sages ici ? ». Après cela, il vous plante la machine... Joyeux Noël !

7 - Le virus espiègle

Nom : Apocalypse
Type : Résidant - fichiers *.COM et *.EXE

Ce virus résidant en mémoire occupe 2208 octets de mémoire et infecte tous les fichiers .COM et .EXE qui sont exécutés (sauf ceux de petite taille). C'est surtout le moral qu'il attaque avec son message :

> Ceci est un virus - Eloignez vous de votre ordinateur, il a la grippe !
> Bonne chance pour les réparations - rien n'est perdu...
> Ne travaillez pas trop - n'oubliez pas de vous reposer !
> Ne me remerciez pas. C'est un plaisir de vous aider.
> Je reviendrais... Appuyez sur n'importe quelle touche !

4.4 - Les critères de déclenchement

Le virus a généralement pour but de mener à bien son action sur le maximum de machines. L'action du virus étant dans la majorité des cas perceptible à l'utilisateur, si elle était effectuée immédiatement, elle entraînerait la découverte prématurée du virus et donc un combat contre sa propagation. L'auteur du virus doit donc effectuer un arbitrage délicat entre la phase de propagation et la phase d'action. Une action trop rapide entraîne une faible propagation et touche donc un nombre peu élevé de machines. Une phase de propagation trop longue peut amener la découverte du virus et son élimination avant qu'il ne se mette réellement à l'œuvre. De la même manière, un taux de reproduction trop élevé peut le démasquer prématurément...

L'action peut être déclenchée suivant un nombre de critères variés, au premier rang desquels on trouve la date. Ce critère revient très souvent dans les facteurs de déclenchement, car il permet d'assurer au virus une période minimale de contamination. L'imagination de l'auteur du virus est là encore de mise pour choisir ses critères, qu'ils dépendent de la date (tous les vendredis 13, tous les dimanches, tous les jours entre 17 et 18 heures, etc.) ou non (nombre d'infections, taux d'occupation du disque, accès disquette...).

Les conditions de propagation et de déclenchement peuvent être compliquées à loisir par le concepteur du virus. Ainsi, il parait que le virus **123nhalf** n'agit que sur la version 3.0 du logiciel Lotus 123, fonctionnant sur une machine équipée d'un processeur 80286, avec un minimum de 3 Mo de mémoire vive... Une fois actif, il interfère avec la commande de sauvegarde, qui n'opère alors que sur le quart de la feuille. Pourquoi faire simple, si on peut faire compliqué...

Certains virus peuvent attendre longtemps avant de frapper. Ainsi, **Golden Gate** n'opère aucune attaque avant d'avoir contaminé 500 programmes, tandis que **Century** (une variante de **Jérusalem**) est programmé pour effacer tous les fichiers le 1er Janvier de l'an 2000, en affichant un message de bienvenue dans le 21ième siècle[40]...

4.5 - Souches et mutants

[40] - N'oubliez pas qu'en réalité le 21ième siècle ne commencera qu'au début de sa première année, c'est à dire le 1° janvier 2001. L'année 2000 n'est que la centième, et dernière, année du 20ième siècle.

Un virus classique doit être capable de s'intégrer de façon transparente dans les programmes hôtes et de manipuler adroitement les interruptions de la machine. Un tel virus est donc un morceau de code en général très court (souvent inférieur à 2 ou 3 Ko) écrit pratiquement exclusivement en assembleur, ce qui permet d'obtenir un code compact et performant. Il exige de son auteur des connaissances très complètes sur le « standard PC », l'assembleur, ainsi que le MS.Dos ou, pour les plus récents, Windows. Il nécessite aussi beaucoup de temps passé à écrire et à tester le code, ceci pour un résultat non monnayable. Le nombre de personnes susceptibles d'écrire un virus réellement nouveau est donc relativement restreint.

Il existe cependant une solution qui nécessite moins de connaissances et beaucoup moins de temps, tout en permettant de créer un virus, si on peut dire. Il suffit de modifier un virus existant... Ainsi sont apparues les notions de virus-souche et de virus-mutant, des termes qui maintiennent le parallèle avec le vocabulaire médical. La modification effectuée sur le virus souche peut porter sur l'une de ses trois caractéristiques :

* Son **mode de contamination** : alors qu'une souche a été prévue pour infecter un certain type de vecteur (les **.COM** par exemple), le mutant modifié pourra en infecter d'autres (**.EXE** par exemple).
* Son **action** : il peut s'agir de la modification de l'action initialement prévue (par exemple du message affiché) ou de l'ajout d'autres actions (écriture destructrice sur le disque dur...).
* Ses **critères de déclenchement** : un virus se déclenchant un vendredi 13 pourra être facilement modifié pour se déclencher un vendredi 23, un samedi 14, ou encore un jeudi 29 février, par exemple.

La modification peut également porter sur la signature utilisée par les programmes antivirus, afin d'éviter la détection du mutant. Un certain nombre de mutants ont également été créés en corrigeant des erreurs identifiés dans le virus souche, le rendant ainsi plus dangereux. La classification entre les **souches** et les **mutants** n'est pas toujours facile. Ainsi, dans le cas de grosses modifications apportant des changements importants dans le comportement du virus, on parle quand même de nouvelle souche, comme s'il s'agissait d'un nouveau venu.

En outre, il existe maintenant des virus appelés **automutants** qui opèrent des mutations automatiques en fonctions d'algorithmes aléatoires. Certains peuvent même modifier leur action... Ce type de virus est très difficile à éradiquer de par son caractère instable et changeant.

4.6 - La nouvelle génération[41]

4.6.1 - Virus furtifs

Les virus de seconde génération, présentant des capacités dites de furtivité, sont apparus vers 1990. De même que l'avion furtif cherche à échapper à la détection en diminuant au maximum sa signature radar, le virus furtif consacre une partie importante de son code à mettre en oeuvre des méthodes lui permettant d'échapper à la détection. Ces méthodes utilisées découlent directement des méthodes de détection employées par les programmes antivirus. La plupart d'entre elles sont actives, c'est-à-dire qu'elles nécessitent que le virus soit installé comme résidant en mémoire pour être effectives. Parmi les différentes méthodes mises en œuvre par ces virus furtifs, on peut relever les suivantes :

Masquage de l'augmentation de taille

[41] - Nouvelle, mais concernant uniquement les virus dit classiques, non les macrovirus.

provoquée par l'infection d'un programme. Le virus peut agir de deux manières, l'une passive, l'autre active. La **méthode passive** tient du fait que la plupart des programmes exécutables disposent de buffers qui sont généralement remplis par des zéros. Si un espace suffisant de zéros est disponible dans le programme, le virus peut y copier son code sans augmenter la taille du fichier infecté. Pour ne pas perturber le fonctionnement, il lui suffira, après s'être exécuté, de remettre à zéro toute cette zone avant d'exécuter le programme original. La **méthode active** nécessite de détourner l'interruption DOS utilisée pour obtenir la longueur d'un fichier. Lors d'une telle demande, le virus va alors déterminer si ce fichier a été infecté. Si c'est le cas, il rendra au demandeur non pas la taille réelle du fichier, mais sa taille diminuée de la taille du virus. Lors d'un **DIR** ou d'une commande affichant la longueur du fichier, celle-ci ne paraît pas avoir été modifiée.

Masquage de la modification du fichier.

Cette méthode suppose le détournement de pratiquement toutes les interruptions DOS relatives aux fichiers. Le but est, lors d'une demande de lecture du fichier infecté, de fournir en fait une version désinfectée identique au programme original. Cette méthode est extrêmement puissante, car elle permet d'échapper aux trois grands modes de contrôle classiques : recherche de signature, contrôle par comparaison et contrôle par checksum, puisque le fichier décelé par le programme antivirus ne contient plus le virus et est identique au programme avant infection.

Masquage de la modification d'un secteur de boot.

C'est le même principe que la méthode précédente, mais appliquée aux secteurs de boot. Cette opération nécessite que le virus ait sauvegardé le secteur original quelque part sur le disque, avant de le modifier. Toute lecture du secteur infecté est retraduite par le virus installé en mémoire, en une lecture du secteur original sauvegardé. Cette méthode permet également d'échapper aux contrôles classiques sur les secteurs de boot.

Modification permanente de la signature en mémoire.

Lorsque le virus est installé en mémoire, il est détectable par une recherche de sa signature. Afin de contrer cette opération, certains virus utilisent **un autoencryptage variable** rendant l'établissement d'une signature fiable très complexe.

Masquage du détournement des interruptions.

Puisque certains programmes antivirus inspectent toute utilisation de certaines interruptions, le virus peut tenter de remonter la chaîne des interruptions pour appeler directement le gestionnaire de l'interruption. Le virus pourra alors passer outre tous les contrôles effectués sur l'utilisation des interruptions.

Depuis leur apparition, les virus ont bénéficié d'année en année de perfectionnements impressionnants dans le but de les rendre plus difficiles à détecter. Dans ce domaine, l'imagination des créateurs de virus semblent sans limite...

4.6.2 - Virus compagnons

Ce type de virus tire parti d'une des caractéristiques particulières du système d'exploitation MS.DOS. En effet, celui-ci exécute, à nom identique, les fichiers ayant l'extension **.COM** avant les fichiers **.EXE**. Le virus recherchera donc un fichier ayant l'extension .EXE et le recopiera avec l'extension .COM en y insérant son code viral, sans modifier l'original. Lors du lancement du programme, le programme infecté sera chargé en mémoire et opérera de nouvelles contaminations. Certains de ces virus ont la capacité de se cacher, ou plus exactement de cacher le nouveau programme infecté, lors de exécution de la commande DIR.

4.6.3 - Virus armés

Ce type de virus, encore appelé **défensif** contient des routines conçues pour empêcher leur désassemblage et l'analyse de leur code. Par exemple, la majorité du code du virus **Whale** (9 Ko) est conçue pour empêcher toute tentative de désassemblage.

4.6.4 - Rétrovirus

Ce type de virus a pour but principal d'attaquer les logiciels antivirus installés sur l'ordinateur soit en les détruisant soit en empêchant leur bon fonctionnement (en désactivant la technique de détection dans l'antivirus, comme le fait, par exemple, le virus **PEACH**)

4.6.5 - Virus cryptés, ou à chiffrement

Ils ont comme caractéristique particulière d'encrypter leur code exécutable au moyen d'algorithmes de compression choisis de façon aléatoire. Sur certains d'entre eux, la clé d'encryptage évolue à chaque infection, à partir d'algorithmes très pointus indexés sur la configuration du système. Ainsi, un seul et même virus peut avoir plusieurs images différentes sur le disque infecté. Certains de ces virus ont également la capacité de muter au fur et à mesure de la contamination. A partir d'un même virus, on pourra donc obtenir des formes très différentes en fonction des fichiers infectés. Histoire d'améliorer l'efficacité de ces charmants parasites, l'auteur du virus **Dark Avenger** a crée récemment un générateur de chiffrement **MtE** (Mutation Engine). Ce MtE a la capacité de s'ajouter au code de n'importe quel virus pour créer un nouveau virus agissant de façon identique au premier, tout en s'insérant sur le programme infecté de manière différente...

Les techniques d'encryptage utilisées dans les virus ont recours à du code auto-modifiable, voire à l'encryptage pur et simple de portions de code avant, pendant et après l'entrée en action du virus. Ces stratégies, moins complexes à mettre au point que les concepteurs d'antivirus n'aiment à le faire croire, sont connues depuis longtemps. Ainsi, le code sera encrypté par un XOR (OU exclusif) dans une boucle, ou par diverses opérations telles que rotation ou opérations mathématiques élémentaires (incrémentation ou décrémentation).

L'encryptage complique la tâche des logiciels d'examen, contraints alors à rechercher plusieurs chaînes dans les fichiers ou en mémoire pour détecter un éventuel virus. Le recours à des caractères génériques n'est pas la panacée, puisqu'un virus habilement conçu comportera de nombreuses séquences typiques dans les applications. C'est même une recommandation importante des « artistes » en création virale ! Certains poussent le vice jusqu'à recommander de reprendre dans des applications commerciales (qu'elles soient ou non des *shareware)* les moteurs d'encryptage déjà écrits et impossibles à signaler comme empreintes de virus !

Les techniques employées par les programmeurs en Assembleur n'ont rien que de classique : exploitation de la file d'attente de prélecture des instructions, auto-modification du code qui devient difficile à comprendre même avec des outils comme un *debugger* ou un désassembleur « intelligent ». Plusieurs astuces font obstacle au *debugger* : exploitation de l'interruption **03h** pour lui souffler le contrôle, blocage du clavier, etc. Rien d'étonnant alors à ce que les descriptions de virus soient parfois discordantes, indépendamment de la qualité des examinateurs. Cependant, ces obstacles sont artificiels : l'habitude suffit à les rendre caducs. De plus, l'exploitation d'astuces est liée au processeur : telle méthode, adaptée à un processeur donné, sera inefficace avec autre.

Les moteurs d'encryptage peuvent prendre plusieurs formes, mais en nombre moindre qu'on ne le pense. En fait, il subsiste toujours quelques séquences de code aisées à identifier, ou du moins un algorithme reconnaissable, même si le moteur utilise diverses techniques (insertion de codes inutiles, exploitation des diverses manières de coder une même instruction, insertion de

code sans objet ou obtenant un résultat de manière peu naturelle, valeurs différentes d'encryptage...)

4.6.6 - Virus polymorphes

Lors de l'infestation d'un programme, un virus crypté doit en quelque sorte emporter avec lui un programme de cryptage. Un virus polymorphe doit inclure, en plus, un moteur de mutation. Ainsi, son code sera indécelable, en tant que virus crypté, mais en outre, le moteur de mutation produit des sous-programmes de cryptage aléatoire. L'ensemble du virus (virus proprement dit, programme de cryptage et moteur de mutation) est donc crypté d'une manière différente à chaque nouvelle infection. Sa détection est donc rendue plus difficile, quasi impossible par les méthodes « classiques ».

Il a fallu imaginer un nouveau type de parade pour combattre ces virus qui change d'apparence à chacune de leurs exécutions. Le principe consiste à observer la manière dont se comporte le fichier suspect en le plaçant dans une sorte de quarantaine dans un ordinateur virtuel à l'intérieur du PC. Si le programme tente des actions suspectes en direction des points sensibles du PC simulé (disque dur, fichiers système, base de registre sous Windows, BIOS de la machine...), c'est qu'il est infecté.

4.7 - Et demain ?

Les chercheurs se préparent à une menace d'un nouveau genre, une quatrième famille : les virus propres à Internet. Il est en effet possible d'en créer sous forme d'**ActiveX** (des modules logiciels au format Microsoft, téléchargeables sur Internet). Par exemple, en lisant un document contaminé par un virus ActiveX, un utilisateur pourra voir son PC s'éteindre tout à coup ! De telles formes virales sont rares. En effet, le risque de propagation est minime, car on n'échange pas les ActiveX comme on échange une disquette, un jeu ou un fichier Word ou Excel. Ces ActiveX sont localisés sur les serveurs des éditeurs de sites Web, qui veillent théoriquement à ce qu'ils soient sains. Le risque de télécharger un document infecté est donc faible. Mais demain, rien n'empêchera qu'un nouveau format de document comprenant des ActiveX se répande. Les chercheurs créent donc eux-mêmes de tels virus pour apprendre à les analyser et à détecter leur signature.

En revanche, l'attaque virale d'**applets Java** (petits programmes écrits en langage de programmation Java) sur un ordinateur est théoriquement impossible, puisque ceux-ci s'exécutent sur une **machine virtuelle**, c'est à dire un endroit en mémoire qui n'est pas susceptible de contaminer la machine (Mac ou PC)

Chapitre 5 : La prévention

La seule protection efficace *presque* à 100% s'appelle sauvegarde.

5.1 - Comment se prémunir ?

Le virus est un risque calculé avec lequel on doit apprendre à vivre, au même titre que la panne du disque dur. En fait, il est possible d'éviter 95% des infections virales par **quelques précautions simples**. Puisqu'une infection est introduite obligatoirement par un programme lui-même infecté, il est souhaitable de limiter au maximum les importations de logiciels dans la machine. Une machine saine sur laquelle on n'exécute aucun nouveau logiciel ne sera jamais contaminée, mais après quelques années, elle ne servira plus à grand chose...

L'**origine du logiciel** a également son importance. On prend évidemment beaucoup moins de risques à installer sur sa machine un logiciel original, acheté dans une enveloppe scellée, que ce même logiciel piraté, aimablement fourni sur une disquette par un copain qui la tient d'un autre qui lui-même... L'utilisation d'un détecteur de virus par recherche de signature[42] semble absolument nécessaire de nos jours. Un tel détecteur doit être utilisé pour vérifier systématiquement tout nouveau programme introduit dans la machine. La décision d'utiliser d'autres méthodes (notamment les moniteurs de surveillance résidents - voir plus loin) dépend des risques auxquels vous êtes confrontés (machine isolée[43] ou plus ou moins exposée aux logiciels extérieurs), du degré d'immunité aux virus que vous souhaitez ainsi que des contraintes que vous acceptez de subir du fait de l'installation de ce moniteur.

En pensant aux nécessaires mesures de précaution à prendre, n'oubliez pas que l'ennemi peut se dissimuler ailleurs que dans un fichier .EXE ou .COM . Il faut donc **tester la totalité de la disquette**, y compris le secteurs de boot et la table d'allocation, avant de tenter de la lire, avant même d'en lire le répertoire par une simple commande DIR.

Et surtout, veillez à suivre scrupuleusement la règle numéro 1 de l'utilisateur informatique : faites des **sauvegardes régulières**[44] ! Ayez toujours en tête qu'un programme de moins de 30 octets et quelques millièmes de secondes suffisent pour effacer irrémédiablement toutes les données d'un disque dur.

5.2 - Prévention : les gestes qui sauvent

Le respect de quelques règles essentielles de sécurité permet de conserver un environnement de travail sain. Si l'observation de certaines mesures élémentaires de sécurité et l'utilisation d'un antivirus ralentissent parfois la productivité, il est toujours risqué de vouloir court-circuiter les opérations préventives. L'essentiel étant d'aboutir à un compromis satisfaisant entre la protection et le confort d'utilisation.

5.2.1 - Il existe des opérations sans danger

Sachez que de nombreuses opérations peuvent s'effectuer sans trop de risque d'infection. La quasi totalité des virus[45] n'infectent que les seuls programmes exécutables, ou certains secteurs très particuliers. Les fichiers de données peuvent donc être échangés sans risques, à condition toutefois de ne pas utiliser la disquette qui les contient pour lancer le système, le secteur

---

[42] - Malheureusement, comme nous le verrons plus loin, cette méthode n'est pas absolument fiable. Il est nécessaire que le logiciel soit récent, et/ou mis à jour régulièrement

[43] - ...à la « Robinson Crusoé » !

[44] - ...en plusieurs exemplaires sur des supports différents (au moins 2, ou mieux, 3 pour les documents les plus précieux), refrain connu...

[45] - Les macro-virus, très prolifiques, restent nettement moins nombreux (au sens des variétés possibles) que les virus dits classiques, mais leurs attaques sont de plus en plus nombreuses, et dangereuses.

de démarrage pouvant héberger un virus. Les virus informatiques classiques sont des programmes qui ne peuvent être exécutés que dans leur environnement natif. Ainsi, une disquette PC se lit sur un Macintosh en toute sérénité : les différences entre les deux systèmes d'exploitation constituent un fossé infranchissable pour les virus dits classiques. Toutefois, depuis peu, les documents peuvent comporter des macrovirus…

5.2.2 - Surveiller les disquettes

Les disquettes constituent le principal vecteur de contamination. Il s'agit, en effet, du support le plus couramment utilisé pour les transferts de données ou la copie des logiciels. Il convient de les manier avec précaution.

- **Contrôler systématiquement** les disquettes dont l'origine paraît douteuse : avant toute opération, il faut en vérifier le contenu par un utilitaire antivirus. Toute disquette peut être infectée en dépit des contrôles draconiens mis en place par les sociétés de duplication. Pendant que vous y êtes, contrôlez aussi toutes les disquettes qui ont été utilisées sur des machines autres que la votre, ou sur des machines un peu trop « échangistes »...
- **Verrouiller les disquettes** contre l'écriture. Ainsi, aucun virus ne pourra lever ce barrage physique. contrairement au barrage logique que représente la protection « *read only* » (lecture seule). Il suffit de pousser le verrou de plastique des disquettes 3" 1/2 pour faire apparaître le trou.
- **Protéger en écriture** les fichiers exécutables : il est très facile de donner à un fichier exécutable (.COM, .EXE, etc.) l'attribut « *read only* » (lecture seule). Cependant, cette mesure peut se révéler gênante avec certains logiciels qui ont besoin d'écrire pour modifier leur structure ou leur paramétrage. Bien que cette protection ne soit efficace que pour une minorité de virus, elle mérite d'être appliquée en raison de sa simplicité.
- **Tester les nouveaux programmes**. S'il s'agit d'un programme compacté, il faut le décompacter avant de lancer l'antivirus.
- **Surveiller tout**, les disquettes de démonstration, les logiciels du domaine public. les copies illégales. les disquettes utilisées sur un autre ordinateur, etc.
- **Éviter de démarrer à partir d'une disquette non protégée** : mieux vaut le faire à partir du disque dur. En effet, le secteur de démarrage est un refuge privilégié pour les virus.
- **Utiliser d'autres supports pour les transferts de données** : les modems et les logiciels de transfert, voire les messageries de réseau, présentent moins de risques que les disquettes voyageuses.

Une astuce utilisée par certains programmeurs consiste à utiliser une **échelle de risque** et à noter sur chaque volume un indice de risque (en anglais, **Safe level**) :

0. risque quasi nul
disques vierges non formatés ; disques livrés avec la machine

1. risque faible
originaux de logiciels commerciaux ; première sauvegarde

2. risque éventuel
volume ayant porté un fichier programme, issu d'une machine ou d'un disque présumé sain

3. risque moyen
volume ayant porté une copie de fichier programme issue d'une machine ou d'un disque contaminé mais présumé soigné, ou d'une source considérée comme à risque

4. risque élevé
volumes contaminés présumés soignés

5. risque très élevé

volume étranger de source non contrôlée (disquettes promotionnelles, téléchargement, programmes piratés...)

6. risque presque certain

volumes contaminés, issus de systèmes contaminés, ou de systèmes soignés qui ont déjà rechuté. Pour les collectionneurs de virus, le nombre de 6 peut indiquer la virulence de la bestiole (6, 66 ou 666[46] !).

Pour mieux décrire cet indice, prenons un exemple. Lucien découvre un cybercafé et (télé)charge un jeu depuis **Internet**, directement sur ses disquettes. Ces disquettes porteront la mention **Safe level 6** (risque très élevé). Prudent, il les examine à l'aide de 2 ou 3 antivirus **récents** et performants. Si les disquettes passant le test avec succès, elles sont gratifiées du **niveau 3**. A moins d'être démagnétisées, puis reformatées sur une machine de niveau 0, 1 ou 2, ces disquettes ne reviendront pas à un indice plus bas.

5.2.3 - Protéger l'accès des micro-ordinateurs

Toutes les procédures qui visent à protéger le secret des données représentent également un facteur de lutte antivirus. Dans une entreprise, les mesures suivantes sont probablement le niveau minimum de sécurité.

- **Installer des dispositifs de sécurité** : mots de passe, clés, etc.
- **Responsabiliser les utilisateurs** et les sensibiliser aux virus.
- **Réserver certaines opérations** (installation des logiciels, gestion du réseau local, etc.) à un responsable qualifié (le responsable informatique, par exemple), formé et sensibilisé.
- **Renforcer les contrôles** autour du serveur de réseau. Cette machine renferme, en effet, la majeure partie des informations et des ressources logicielles d'un réseau local. Un serveur est une cible idéale...
- **Donner l'alerte dès qu'un virus est repéré**. Il faut alors isoler la machine concernée, puis éradiquer ledit virus, et ne pas oublier de prévenir **tous** les utilisateurs ayant été en contact avec le poste contaminé.
- **Prévoir un poste isolé** du reste du réseau, pour l'ensemble des tests des disquettes. Il permettra un contrôle sanitaire des disquettes, jouera en quelque sorte le rôle d'appât et révélera la présence d'éventuels virus.
- **Contrôler tout nouveau micro-ordinateur** : le disque dur d'une machine neuve peut, en effet, comporter des virus à sa sortie d'usine (mais c'est exceptionnel).

5.2.4 - Anticiper une éventuelle contamination

- **Préserver les disquettes programmes originales** en procédant à des copies. Pour plus de sécurité, la disquette d'origine doit rester verrouillée contre l'écriture. En cas d'infection, ou si un formatage du disque dur s'impose, celle-ci permettra de réinstaller le logiciel.
- **Procéder à des sauvegardes régulières**. Ainsi, en cas de dégâts sur le disque dur, les données pourront être restaurées. Accorder une attention particulière aux fichiers sensibles.

5.2.5 - Limiter les conséquences possibles

Si malgré toutes vos efforts un virus parvient à contourner les mesures de sécurité évoquées précédemment, certaines précautions élémentaires pourront quand même en atténuer les nuisances.

[46] - En numérologie, 666 est le chiffre « de la bete », c'est à dire du diable... Pour en savoir plus, (re)lisez donc l'apocalypse selon Saint Jean, et allez au Chateau d'Angers voir la célèbre tapisserie

- **Éliminer les virus**. La méthode la plus radicale consiste à supprimer les applications infectées. Dans le cas d'un virus du secteur de démarrage, seul un antivirus pourra l'éradiquer. S'il s'agit de disquettes, démagnétisez-les, ou mieux, détruisez-les physiquement, c'est encore plus sûr que tout remède miracle...

- **Vacciner la mémoire**: le module résident des antivirus signale toute intrusion suspecte dans la mémoire vive de l'appareil. L'utilisateur doit alors relancer l'ordinateur et vérifier que le virus n'est plus présent.

- **Reconstituer le secteur de démarrage** à partir d'une copie récente, effectuée au moyen d'un utilitaire de sauvegarde ou d'un antivirus.

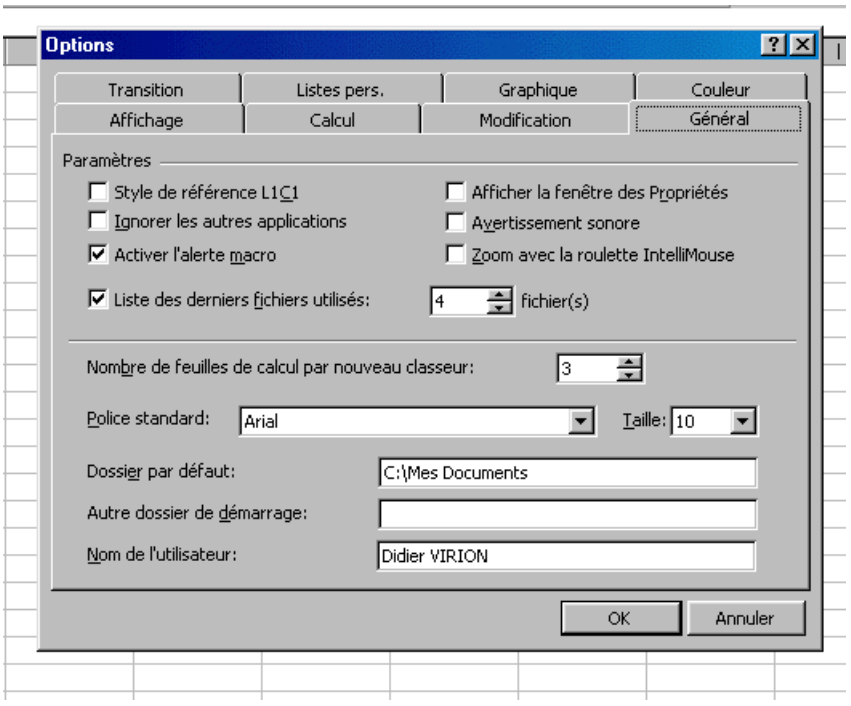
5.3 - Lutter contre les macrovirus

Contrairement à ce que l'on pourrait penser, se prémunir contre les macrovirus est presque plus simple que se prémunir contre les virus traditionnels. Les macrovirus, s'ils font parler d'eux et s'ils représentent bien la majorité des virus actuellement en circulation, sont loin d'être des joyaux de programmation. N'importe quel bidouilleur un tant soit peu doué est capable d'en réaliser un. En contrepartie, il est relativement aisé de s'en préserver. Puisqu'ils sont véhiculés par les documents classiques, il suffit de refuser tous les documents d'origine suspecte, ou de les examiner à l'aide d'un logiciel antivirus. De même, il est facile de leur interdire d'agir en désactivant les macrocommandes présentes dans les documents !

Les versions récentes de tous les logiciels de bureautique offrent cette possibilité. Nous allons voir comment dans deux cas particuliers., Excel 97 et Word 97. Dans les deux cas, la « solution » se trouve dans le tableau proposé par la commande **Option** du menu **Outils** (ou, si on préfère, par la commande **Outil/Options**)

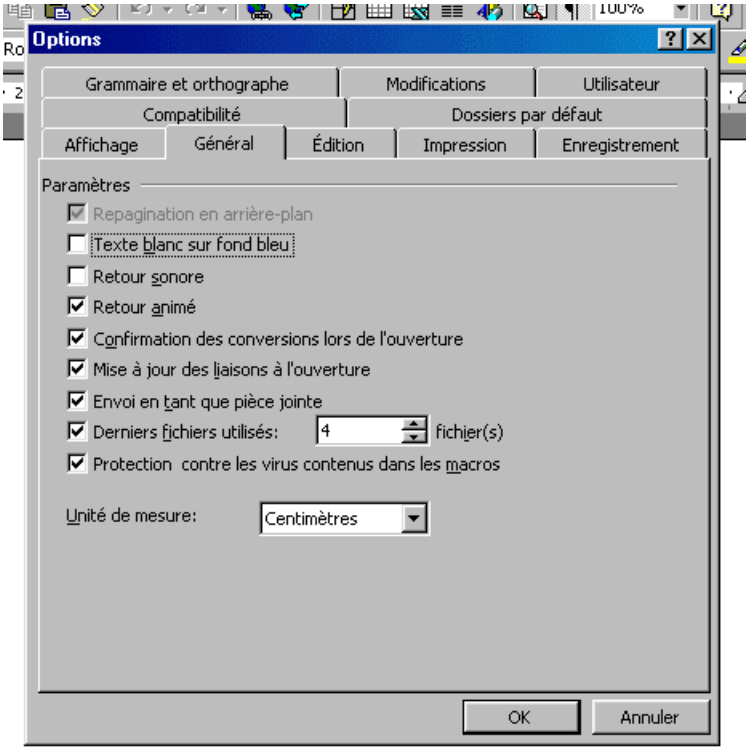
Cas d'Excel :

Dans Excel 97, il faut cocher la case «**activer l'alerte macro** ». Ainsi, au lieu d'exécuter automatiquement les macrocommandes que la feuille de calcul contient, le logiciel va prévenir de leur existence, et demander une confirmation de la part de l'utilisateur.



Cas de Word :

Dans Word 97, le principe est identique. Il faut cocher la case **« protection contre les virus contenus dans les macros** ». Ainsi, l'utilisateur sera prévenu de la présence de macrocommandes et pourra décider ou non de les charger et de les exécuter.



5.4 - Lutter contre les virus VBS

La déferlante de ILOVAYOU, en mai 2000, a pris tout le monde de court. Or plusieurs signes avant-coureurs annoncaient une attaque de ce genre. Déjà, en 1997 et 1998, des tentatives avaient eu lieu pour diffuser des virus en utilisant les messageries. Elles se soldèrent par des échecs. Au premier trimestre de 1999, ce fut au tour du virus **Happy99** et de **Melissa** d'utiliser le carnet d'adresses pour se répandre. Ce furent les premiers virus ayant une telle capacité de propagation. En octobre 1999, un nouveau pas fut franchi avec **Kak.Worm** et **Bubbleboy**, les premiers virus à se répandre sans l'intermédiaire de pièce jointe. La simple ouverture de le-mail suffisait à provoquer l'infection de l'environnement. Mais leur propagation fut, et reste, heureusement limitée car elle exploitait un bug présent sur Internet Explorer 5. Cette erreur a été, depuis, corrigée sur les dernières versions du logiciels. Vint ensuite **ILOVEYOU**... Ce n'est qu'un début. L'ère des virus de messagerie s'annonce faste.

Pourtant, il est relativement facile de se mettre à l'abri d'une telle attaque. Comme pour les autres types de virus, quelques précautions simples permettent de limiter les risques de récupérer un virus dans sa boite à lettre.

Ne lisez pas les messages, et encore moins les fichiers qui les accompagnent, emanant de personnes que vous ne connaissez pas, et qui ne correspondent pas à une demande faite par vous. Vous devez directement les transférer dans la corbeille

N'ouvrez pas les pièces jointes portant l'extension vbs et js (ou une autre extension de fichier exécutable). Ce sont des programmes qui pourraient se révéler être des virus.

Télécharger les logiciels correctifs d'Outlook sur le site Micrsotf.

Configurez Windows pour augmenter la sécurité du système. Effectuez un clic droit sur l'icône d'Internet Exploret située sur le bureau et optez pour Propriétés. Cliquez sur l'onglet Sécurité et cocher l'option Haut (niveau le plus élevé). Validez pour que les modifications prennent effet.

Désactivez l'execution des scripts dans Outlook Express. Cliquez sur Options du menu Outils et choisissez l'onglet Lecture. Désactivez Télécharger automatiquement lors de leur affichage dans le volet de visualisation. De pluis, dans la page définie par l'onglet Sécurité, cochez l'option Zone Sites Sensibles et validez.

5.5 - Que faire en cas d'attaque virale ?

Certains signes permettent de détecter qu'un système a été contaminé avant que l'attaque ne commence. Le fait que l'espace disponible sur disque dur décroisse de façon évidente en est un. Un ralentissement notable et soudain des performances peut également indiquer qu'un ou plusieurs virus empruntent du temps de traitement au système. Lorsqu'une telle manifestation se produit, il faut immédiatement éteindre l'ordinateur puis le rallumer à partir d'une disquette DOS protégée contre l'écriture et dont on a la certitude qu'elle n'est pas infectée. Il convient ensuite de lancer un logiciel antivirus afin qu'il analyse l'état du disque, et, dans le cas d'une contamination, tenter de réparer les dégradations.

Toutefois, ne tombez pas dans la paranoïa ! Tout problème inconnu n'est pas forcément d'origine virale, bien au contraire. Sur un PC, comme sur un Macintosh, les origines des problèmes peuvent être nombreuses et variées. Parfois il peut s'agir d'erreur de programmation (de bugs dans le programme), parfois plus simplement d'une mauvaise qualité du support magnétique, ou encore de problèmes liés à l'alimentation électrique...

Si vous suspectez une attaque virale, il importe de suivre scrupuleusement la méthode suivante :

- Éteignez votre machine.
- Introduisez dans le lecteur de disquette une disquette système **protégée en écriture** (si possible, la disquette originale qui vous a été livrée par le constructeur de la machine, ou la disquette de secours de l'antivirus).
- Rallumez la machine pour démarrer à partir de la disquette.
- Utilisez un programme de détection antivirus, toujours à partir d'une disquette protégée en écriture.

5.6 - Les fonctions des antivirus

Les faits indiquent qu'il est vital de se prémunir. Chaque PC devrait être doté d'un utilitaire antivirus régulièrement mis à jour. Se contenter de mesures temporaires[47] revient à prendre des risques irraisonnés. Les antivirus sont assez nombreux pour qu'il en existe au moins un adapté à vos besoin. Ils offrent généralement au moins trois services, aussi utiles qu'indispensables : détection, désinfection et prévention...

[47] - ...telles que changer la date de l'ordinateur le jour présumé de l'attaque !

Détection

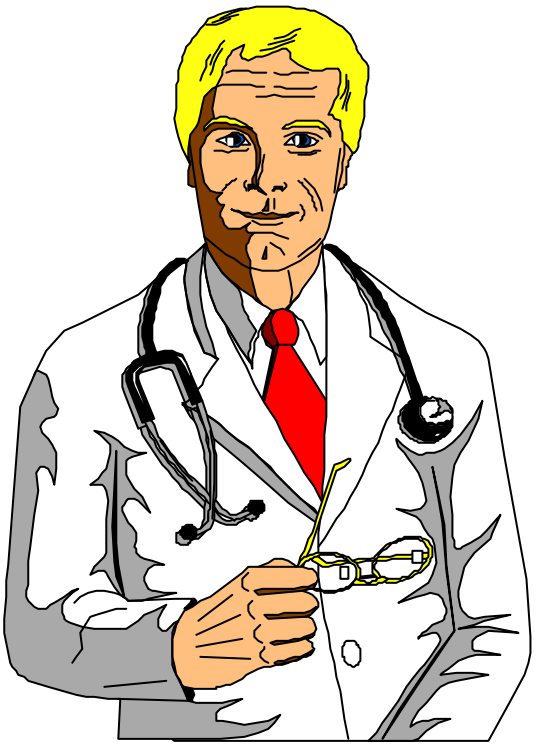
Lorsque l'on installe un logiciel antivirus, celui-ci commence par scruter le disque dur afin de détecter la présence éventuelle de virus. Pour ce faire, certains antivirus recherchent des signatures connues. D'autres affichent un signal d'alarme à la moindre tentative de modification d'un programme.

Désinfection

Lorsqu'ils découvrent qu'un programme a été contaminé, certains antivirus peuvent le désinfecter, c'est-à-dire détruire la trace du virus. Mais cela n'est pas toujours possible et il faut bien souvent réinstaller les logiciels infectés.

Prévention

La prévention s'effectue par une surveillance permanente destinée à empêcher l'intrusion de nouveaux virus. Elle est souvent réalisée par un module résidant en mémoire, capable de déclencher une alerte dès qu'il soupçonne une action peu orthodoxe telle qu'une tentative d'écriture sur le secteur de démarrage du disque dur.



Chapitre 6 : Les antivirus

Un bon logiciel antivirus (ou un « package » antivirus, c'est à dire un ensemble de logiciels) doit pouvoir remplir au minimum les trois fonctions suivantes :

• **Détection** de l'intrusion d'un virus (en mémoire, sur les secteurs de boot, dans les fichiers exécutables ou dans les macro-commandes d'autres fichiers). Cela doit être la tâche primordiale d'un package antivirus : prévenir l'utilisateur que sa machine est contaminée, ou risque de l'être. Cela permet de prendre immédiatement les mesures qui s'imposent et de stopper l'infection. Cela peut permettre aussi d'éliminer le virus avant que ne soit déclenchée son action destructrice.

• **Identification**, s'il s'agit d'un virus connu. Cela permet de savoir à quel virus on a affaire, et donc de savoir quels sont ses modes de contamination, son critère de déclenchement et son action.

• **Élimination** du virus et **récupération** des fichiers infectés lorsque cela est possible, afin de revenir à une exploitation normale de la machine.

Si les deux dernières fonctions sont relativement faciles, il n'en va pas de même pour la détection qui doit faire face à la menace de virus connus et inconnus. C'est dans ce domaine que se situent les principales différences entre les multiples programmes antivirus. Il existe actuellement plusieurs méthodes de détection de virus. Les plus utilisées sont la recherche de signatures, la comparaison avec une sauvegarde préalable, la méthode des sommes de contrôle (checksum) et les contrôles actifs par programmes résidents dits TSR.

Prise séparément, aucun méthode n'est absolument fiable, seule la convergence des résultats peut permettre de faire un bon diagnostic.

6.1 - Comment réalise-t-on un antivirus ?

(d'après l'Ordinateur Individuel - N° 97 - Juillet/Août 1998)

Cette course contre la montre est le lot quotidien des spécialistes des deux plus grands laboratoire antivirus au monde, financés par des éditeurs. Ce sont des entités américaines :le **SARC** (Symantec Antivirus Research Center, de Symantec, qui commercialise **Norton Antivirus**), à Santa Monica, qui emploie dix chercheurs, et l'**AVERT** (Antivirus Emernency Response Team, de l'éditeur Network Associated, ex- McAfee, éditeur de **VirusScan**), qui compte quinze spécialistes à Santa Clara. Certes, l'édition d'antivirus est une niche, mais elle est lucrative : le marché s'élève à 10 milliards de dollars par an.

Les chercheurs du SARC et de l'AVERT ont ceci en commun qu'ils utilisent la même solution de détection de virus : le fichier de signature. Il s'agit pour eux de découvrir au plus vite de nouvelles souches virales, ce que les initiés nomment la **chasse aux papillons**. Pour cela, les chercheurs récupèrent des documents que les utilisateurs croient être contaminés par un virus inconnu. Ou bien, ils « surfent » sur Internet et téléchargent les fichiers suspects qui seront ensuite analysés. S'ils sont effectivement malsains, il faudra découvrir une séquence d'instruction propre au virus : sa signature, qui sera ensuite référencée par la nouvelle mise à jour du logiciel antivirus maison. L'acquisition de cette mise à jour donnera au client l'assurance que le virus sera immédiatement détecté, avant d'avoir eu le temps de se propager dans la machine.

Mais la réalité n'est pas aussi simple, et l'analogie avec la biologie s'impose encore ici : comme le virus de la grippe, certains virus informatique, dits polymorphes mutent, c'est à dire chan gent de caractéristiques. Le record est détenu par un virus qui peut se transformer jusqu'à quatre mille fois. Il faut alors découvrir la ou les signatures communes à ces quatre mille formes virales, un travail qui peut prendre plusieurs semaines. Par ailleurs, avec l'apparition d'outils simples pour créer des virus, notamment le **Visual Basic for Application** (ou VBA) (de Microsoft) qui permet de concevoir des macrovirus dans Word ou Excel, la production est plus forte que jamais. Certes, il ne s'agit le plus souvent que de variantes de virus déjà existants, mais qui, elles aussi, doivent être référencées. Enfin, si découvrir une signature prend généralement peu de temps, quelques minutes pour les cas simples, la phase de test peut nécessiter plusieurs heures pour un seul virus. C'est ainsi que les chercheurs travaillent, au jour le jour, pour éviter la propagation des macrovirus, des virus de boot et ceux des fichiers, les trois grandes familles actuelles. Et ils ont fort à faire, surtout depuis que le courrier électronique est devenu un moyen d'échanger facilement des documents et des données.

En France, le laboratoire de recherche antivirus le plus important emploie cinq personnes. Il s'agit de celui de **TEGAM**, l'éditeur de **Vi Guard**. Là, l'approche est fondamentalement différente de la reconnaissance de signature. antivirus ne détecte pas un virus en particulier, mais repère les instructions de propagation ou les tentatives de déclenchement d'opérations sensibles (formatage du disque dur, par exemple). L'antivirus ne nécessite donc pas de mises à jour régulières, hormis à la sortie d'un nouveau système d'exploitation, ou lorsqu'une nouvelle famille de virus est découverte (c'est arrivé trois fois en dix ans). En contrepartie, les fausses alertes sont plus nombreuses qu'avec les antivirus à reconnaissance de signature. Une macrocommande que l'utilisateur crée afin de modifier la mise en page d'un texte peut être considéré comme une forme virale...

Cette approche plus globale n'empêche pas les chercheurs de TEGAM de vérifier en effectuant des test sur plusieurs machines, que les nouveaux virus sont correctement détectés par leurs produits. Ces examens sont aussi l'occasion de comparer leurs produits à d'autres antivirus. Car la concurrence entre les laboratoires, doublée d'une rivalité commerciale, est très forte.

6.2 - Quelques idées sur les méthodes de détection

La méthode scanner

Elle repose sur l'emploi d'une **table de signatures**, c'est à dire une base de données récapitulant des suites d'octets en principe significatifs afin d'identifier les types de virus en présence. Cette méthode permet de détecter les virus connus, qu'ils soient présents en mémoire ou sur le disque. Pour l'instant, elle constitue le seul moyen efficace pour détecter et éradiquer les macro-virus. En revanche, il est indispensable de garder cette liste à jour, car ce système ne permet pas de découvrir les virus inconnus. En fonction des éditeurs d'antivirus, les mises à jour des tables de signatures sont librement téléchargeables sur Internet, ou envoyées par la poste, dans le cas d'un abonnement payant. Cette méthode n'est toutefois valable qu'avec des virus répertoriées. Il est donc indispensable de l'employer conjointement avec la méthode générique pour parer à l'attaque de nouveaux virus.

La méthode générique

Elle regroupe un ensemble de techniques (contrôle d'intégrité, scanner heuristique, appâts, etc.) adaptés à la découverte de virus inconnus. Cependant, celle-ci ne marche pas pour les macro-virus présents dans des documents de Word ou Excel. Autre reproche à lui faire : les trop nombreuses fausses alertes qui agacent l'utilisateur. Néanmoins, en s'affinant, elle demeure l'auxiliaire indispensable du scanner.

La méthode algorithmique

Elle s'adresse aux virus polymorphes (contenant une clé de déchiffrement qui est employée à chaque nouvelle infection de fichier pour lui donner une signature différente). C'est la plus sophistiquée, mais elle n'est pas infaillible : il est préférable de l'utiliser en complément des deux méthodes précédentes.

En d'autres termes, aucune méthode n'est infaillible !

6.3 - La recherche des signatures

Cette méthode a été la première contre-mesure mise en oeuvre après l'apparition des virus sur PC. Elle est la plus simple et elle constitue toujours la base de nombreux programmes antivirus. Chaque virus peut être éventuellement caractérisé par une séquence d'octets spécifiques qui est soit une chaîne de caractères inclus au virus (du genre « *bye bye hard disk* »), soit une suite d'instructions représentatives du fonctionnement du virus.

A partir d'une table contenant les **signatures** de tous les virus connus, un programme de recherche de signature analyse l'ensemble des fichiers pour trouver ceux qui sont infectés. C'est une méthode très sûre et très efficace mais ne peut s'appliquer qu'aux virus connus. Elle peut être utilisée pour la vérification de la mémoire ou pour celle des fichiers stockés sur un support quelconque (disquette, disque dur, disque réseau...). La vérification mémoire est très importante, car elle permet de s'assurer qu'aucun virus connu n'est déjà chargé en mémoire et actif. En effet, si tel était le cas, le programme de recherche de signature risquerait d'une part de ne pas trouver un éventuel virus furtif, mais aussi et surtout de propager l'infection à tous les fichiers vérifiés.

L'**efficacité** du programme dépend bien sûr de la taille de la base de signatures, c'est-à-dire en fait le nombre de virus reconnus et détectés. Mais, elle repose également sur un second facteur : la qualité de la base de données des signatures. Un choix judicieux de la séquence spécifique au virus doit permettre de l'identifier de façon certaine, de pouvoir éventuellement identifier ses mutants, mais aussi d'éviter les fausses alarmes. Cette méthode de recherche de signature a cependant plusieurs inconvénients :

- Le premier et non le moindre est l'impossibilité de détecter un nouveau virus tant que la base de signatures n'aura pas été **mise à jour** pour ce virus. Le virus doit donc être d'abord isolé, puis transmis au concepteur du logiciel antivirus qui inclura sa définition dans une nouvelle révision de la base de données des signatures. Cette base devra ensuite être mise à jour chez tous les utilisateurs.
- Il est relativement facile de modifier très légèrement un virus, et d'altérer ainsi des éléments de sa signature. Le mutant ainsi obtenu nécessitera une nouvelle mise à jour de la base pour être détecté.
- Certains virus de nouvelle génération sont capables de s'auto-modifier ou de s'auto-crypter, rendant difficile la détection basée sur la recherche de signature. Le nombre total de virus (connus...) est en croissance permanente (entre vingt et trente souches ou mutants supplémentaires par mois), ce qui conduit à des temps de recherche de plus en plus importants.
- C'est une méthode passive, qui laisse à l'utilisateur le soin de définir la périodicité du contrôle.

6.4 - La comparaison avec une sauvegarde

La méthode consiste à sauvegarder la forme initiale (supposée exempte de virus) d'un élément pouvant servir de vecteur d'infection, puis de comparer de façon régulière la forme courante et cette valeur de référence. Toute modification peut être significative d'une attaque virale. Cette sauvegarde en double n'est bien sûr pas envisageable avec tous les types de vecteurs (par exemple les exécutables **.COM** ou **.EXE**). Elle doublerait systématiquement le nombre de fichiers et la place occupée. Elle a cependant trouvé son utilité avec les secteurs de partition et de boot dont la taille est en général modeste, surtout comparée au reste du volume.

L'immense avantage de cette méthode est, bien sûr, de conserver une sauvegarde de ces secteurs primordiaux pour les données stockées sur disque et donc de permettre de les restaurer en cas de besoin. En cas d'attaque virale ciblée sur ces secteurs, leur réécriture à partir des sauvegardes entraîne dans la plupart des cas l'élimination du virus.

6.5 - La méthode des sommes de contrôle (checksum)

La méthode consiste à calculer une valeur directement dépendante du contenu d'un fichier ou d'un secteur. Cette méthode n'est pas nouvelle et a souvent été utilisée dans le passé comme contrôle de l'intégrité des données, lors de transmission notamment. Son application à la lutte antivirale est récente. Chaque chargement de programme est dès lors précédé d'un calcul de checksum, puis d'une comparaison avec la valeur d'origine stockée soit dans le programme lui-même, soit dans un fichier associé au programme, soit dans une base externe. Séduisante a priori puisqu'elle permettrait de détecter toute modification des programmes, y compris par des virus inconnus, cette méthode a aussi ses inconvénients :

- Beaucoup d'applications peuvent changer elles-mêmes leur code suite à une reconfiguration, un changement de mot de passe, une mise à jour de la version. Cela

conduit à un taux élevé de fausses alarmes que l'utilisateur moyen ne sera pas toujours à même de distinguer d'une véritable tentative d'infection.

- Il s'agit également d'une protection passive, nécessitant de surplus une manipulation pour chaque nouveau programme ou version.

- Enfin, et c'est le plus important, les virus de nouvelle génération ont mis en oeuvre des techniques permettant la non détection des modifications apportées au programme, rendant ainsi inopérante toute détection par somme de contrôle (checksum).

6.6 - Les programmes résidants[48]

Un **moniteur**[49] **antivirus résident** a pour principal avantage de proposer une protection active et non plus passive. Ainsi, tous les fichiers exécutés ou même seulement ouverts seront contrôlés automatiquement, sans intervention spéciale de l'utilisateur. L'intérêt est évident puisque, dans le cas où un virus est détecté, cette détection intervient avant l'exécution du programme infecté, permettant ainsi d'éviter toute contamination supplémentaire du disque. Les techniques de détection employées dans ces programmes résidents s'inspirent tout d'abord de deux des possibilités décrites ci-dessus, à savoir la **recherche de signature** des virus connus et l'utilisation des **sommes de contrôle** (checksum).

Le plus apporté par un programme résidant est que le contrôle s'effectue de façon transparente avant l'exécution d'un fichier ou lors de l'ouverture de tout fichier (exécutable ou non). Du fait de sa particularité d'être résidant, le moniteur antivirus peut également mettre en oeuvre de nombreuses autres techniques de contrôle dynamique. Ces techniques vont être dérivées de l'analyse du comportement d'un virus :

• Un virus doit obligatoirement modifier un vecteur de contamination. Le moniteur antivirus peut donc contrôler tous les appels DOS d'écriture dans un fichier, pour vérifier qu'il ne s'agit pas d'un fichier exécutable. Cela peut être difficile à analyser car certains programmes écrivent dans des fichiers exécutables. De plus, toute installation de logiciel, toute commande COPY du DOS peut générer des écritures dans les fichiers exécutables. Le moniteur peut également contrôler les appels Bios d'écriture au disque dur, afin de vérifier que l'écriture ne touche pas l'un des deux secteurs de boot (cylindre 0 tête 0 secteur 1 et cylindre 0 tête 1 secteur 1). Il peut enfin contrôler les appels Bios d'écriture aux disquettes et vérifier qu'il ne s'agit pas d'un accès au secteur de boot (cylindre 0 tête 0 secteur 1).

• Un virus cherche souvent à s'installer résidant en mémoire. Il peut le faire de plusieurs manières :

•• En se copiant sauvagement à une adresse fixe en mémoire. Il écrase donc ce qui s'y trouvait, et il pourra à son tour être éventuellement écrasé par la suite. Inutile de dire que ce comportement est générateur de "plantages" réguliers qui peuvent attirer l'attention de l'utilisateur.

•• En utilisant les possibilités du DOS. Dans ce cas, le moniteur antivirus interceptera l'appel pour contrôler le nom du programme cherchant à s'installer. L'accord d'installation peut alors être demandé à l'utilisateur. Il est possible également de prévoir une liste de programmes autorisés à s'installer en résidant.

---

[48] - Il s'agit d'un programme stocké en mémoire, en plus du système d'exploitation et de l'application. Un tel programme est immédiatement exécutable, souvent même à travers l'application en cours.

[49] - Un moniteur (ou programme moniteur) est un programme qui se charge des opérations de coordination, de succession ou de direction d'un système. C'est aussi un programme qui optimise l'utilisation d'une machine. (ne pas confondre avec l'écran !).

• Pour tous les virus attaquant le secteur de boot, le problème est différent puisqu'ils sont chargés avant le DOS. Ils s'installent dans la partie mémoire la plus haute (en général au-dessus de l'adresse 9F000 sur une machine avec 640 Ko). L'interruption 12h du Bios est interceptée afin de rendre en paramètre une taille mémoire inférieure de 1 à 4 K à la mémoire réelle. Le moniteur antivirus pourra dans ce cas-là comparer la taille mémoire fournie par l'interruption 12h avec la valeur théorique donnée par l'utilisateur.

• Puisqu'un virus doit nécessairement détourner au moins une interruption de la machine, il est possible de tester la table des interruptions afin de détecter toute modification. Bien entendu, chaque programme autorisé à détourner les interruptions doit être déclaré préalablement.

Si les techniques mises en oeuvre par un moniteur résidant en mémoire peuvent permettre d'espérer échapper à toute contamination, y compris par un virus inconnu, les désavantages d'un tel moniteur sont multiples :

• la complexité d'analyse, par un utilisateur non averti, des alarmes du moniteur. Il est nécessaire de très bien connaître la machine et le mode d'action des logiciels lancés, afin de déterminer si ces logiciels doivent être autorisés à modifier les fichiers exécutables, s'installer résidant, modifier les interruptions... Cette connaissance n'est certainement pas à la portée d'un utilisateur moyen.

• les opérations nécessaires après chaque ajout de logiciel, modification de version, modification de configuration, pour déclarer et enregistrer les autorisations d'accès.

• son occupation mémoire, alors que à une époque la limite des 640 K est toujours contraignante pour les logiciels sous MS.Dos.

• la perte de performance due au temps requis par le moniteur pour contrôler l'ensemble des opérations.

Les programmes antivirus utilisent en fait un panachage de toutes ces méthodes de détection. La plupart propose des méthodes permettant la détection de virus inconnus. La raison en est d'une part la prolifération des virus (entre 20 et 30 nouveaux par mois), d'autre part l'aspect purement commercial. L'utilisateur sera beaucoup plus attiré par un produit lui promettant (à tort ou à raison, c'est là le problème...) une protection absolue contre les virus à venir.

6.7 - Comment choisir un antivirus...

6.7.1 - Les niveaux de protection

Jugés sur leur efficacité, les programmes antivirus doivent offrir la meilleure protection, sans que leur présence ne devienne, pour autant, envahissante. Outre la chasse et la destruction des virus, ces utilitaires s'attachent à prévenir une éventuelle contamination. Un système efficace de protection contre les virus informatiques ne peut se concevoir sans le soutien d'un logiciel spécialisé. Aucun système de prévention, aussi drastique soit-il, n'est à l'abri d'une défaillance humaine. L'intérêt des programmes antivirus consiste en leur capacité d'intervention sur des systèmes contaminés, afin de repérer et détruire les virus. Dans les faits, les antivirus offrent différents niveaux de protection.

Vérification des supports

Le programme entre en action dès qu'une disquette est introduite ; il en contrôle le contenu, recherchant la présence de virus. Peu contraignante, cette phase monopolise le système quelques secondes seulement.

Contrôle périodique du contenu du disque dur

On parle alors de fonction de balayage. L'antivirus parcourt tout ou partie des fichiers (selon les paramètres définis par l'utilisateur) et note les anomalies pouvant révéler la présence de virus : augmentation de la taille des fichiers, modification de la somme de contrôle, signatures virales.

Détection des activités suspectes

La plupart des antivirus comporte un module résident (en mémoire tant que l'ordinateur est sous tension). Ainsi, il surveille l'activité générale du système, signalant les tentatives de chargement d'applications résidentes (qui peuvent être des virus), les accès en écriture vers le disque dur, etc.

Éradication des virus

Une fois identifié et repéré, le virus doit être éliminé. Les antivirus sont capables d'accomplir cette mission.

Restauration des fichiers endommagés

Il ne suffit pas d'éliminer le virus, encore faut-il que le fichier contaminé soit utilisable. Certains programmes de lutte antivirus procèdent à des copies de sécurité des secteurs sensibles des fichiers exécutables et, en particulier, du secteur d'exécution. Ce double sain sera installé automatiquement en lieu et place du secteur infecté.

L'efficacité constitue certes le principal critère de choix d'un programme antivirus, mais d'autres éléments interviennent, comme la rapidité, la richesse fonctionnelle, ou la facilité de mise en oeuvre. La difficulté pour l'utilisateur consiste à trouver un produit qui parvienne à concilier des exigences parfois contradictoires. Le logiciel parfait reste à développer. Aucun antivirus n'offre à la fois une protection absolue, une vitesse satisfaisante, et une interface utilisateur parfaitement conçue. Certains privilégient l'efficacité. Ils donnent leur pleine mesure lors des phases de prévention et de détection. D'autres misent sur la rapidité et l'ergonomie. Un peu moins efficients en matière de protection, ils sont en revanche plus discrets et ralentissent peu le système. L'affichage de messages d'alerte trop fréquents, pour signaler des opérations supposées suspectes (écriture sur le disque), pénalise grandement la productivité.

6.7.2 - On peut aussi doubler la protection

Puisqu'il n'existe pas de programme idéal, la solution consiste souvent à choisir au moins deux antivirus aux vertus complémentaires, l'un possédant une fonction de balayage efficace des fichiers, l'autre capable de surveiller de manière imperceptible toute activité suspecte. En adaptant finement le paramétrage de chacun, il est même possible d'éviter que trop d'options ne doublonnent. La valeur d'un antivirus est, d'autre part, directement liée à la vitalité de son éditeur. En effet, puisque de nouveaux virus apparaissent chaque jour et que l'efficacité des logiciels repose sur l'exhaustivité de leur base de données (qui contient les signatures des virus référencés), il est nécessaire de diffuser de fréquentes mises à jour. Les utilisateurs auront tout intérêt à opter pour un éditeur qui propose une politique d'abonnement et un support technique développé.

Chapitre 7 : Les enjeux...

On peut se poser de nombreuses question sur le « pourquoi » et le « comment » des virus. Toutefois, les plus importantes sont au nombre de trois :

Qu'en est-il en réalité du danger des virus ?
A qui profite le « crime » ?
De quoi demain sera-t-il fait ?

7.1 - Virus informatiques : mythes et réalités

Selon la presse, spécialisée ou non, les systèmes informatiques sont à la merci d'un nombre impressionnant de hasards et de désastres, dont les plus redoutables seraient les programmes appelés, par une analogie fâcheuse, des virus : développés par de jeunes *hackers* géniaux et psychopathes, ces virus seraient presque dotés d'une forme de vie autonome, qui leur permettrait de croître et de se multiplier en semant impunément la désolation dans les systèmes qu'ils contaminent. Dits polymorphes et furtifs, les plus sophistiqués déjoueraient toutes les surveillances logicielles pour perpétrer leurs forfaits...

Du moins, telle est la légende que propagent volontiers des journalistes généralistes ou spécialisés dès que l'occasion s'en présente (la dernière remonte à 1992 avec le virus Michelangelo). D'autres menaces, plus prosaïques, ont beau provoquer davantage de dégâts objectifs, les virus restent, dans l'imaginaire des utilisateurs de PC, **le fléau par excellence**, d'autant plus redoutable qu'il semble mystérieux, sans doute parce qu'il est moins objet d'expérience que de discours - à de rares exceptions près.

Cette menace anonyme est à l'origine **d'un fructueux marché de la peur**. Parmi les personnalités qui en ont su le mieux profiter figurent John McAfee, Patricia Hoffman, Fred Cohen, Vesselin Bontchev, Fridrik Skulason et Ross Greenberg. Un Diogène Laerce s'imposerait pour faire le pittoresque récit des inimitiés qui, paradoxalement, soudent ces experts autoproclamés de la lutte antivirus, prompts à sonner en chœur l'alarme à chaque nouveau virus. Cela ne leur interdit pas de s'entre-déchirer à belles dents, par bancs d'essai interposés : chacun d'eux, ayant un produit à défendre, et surtout à vendre, s'efforce de démontrer qu'il est supérieur à ses concurrents. Ainsi, de nombreux rapports démontrent, avec toutes les apparences de la rigueur, que tel antivirus côtoie le sublime... ou le médiocre. Le recours aux associations américaines spécialisées - la *Computer Virus Industry Association* (CVIA) et la *National Computer Security Association* (NCSA) - n'éclaire guère la question : l'une et l'autre seraient particulièrement liées à l'un des acteurs de l'industrie, dont elles célébreraient le produit vedette dans d'étonnantes conditions (à en croire un article paru dans le *New York Newsday* sous la plume de Joshua Quittner en 1992, l'éditeur en question n'hésiterait pas à fournir lui-même les virus faisant ainsi monter le score de son détecteur de virus, et irait jusqu'à payer pour tester les produits des concurrents qui n'ont pas daigné entrer dans la compétition !). Une autre personnalité bien connue contraindrait presque les éditeurs d'antivirus à passer par les fourches caudines de sa base de virus pour obtenir une certification plus que contestable.

Tout suscite l'étonnement quand il est question de virus : désassemblés par de soi-disant génies de l'analyse rétro-technique, leurs descriptions sont étonnamment vagues, contradictoires ou inexactes... Mentionnés comme expérimentaux, certains figurent pourtant dans les listes de virus répandus. Censés compter plus de 4 000 variétés différentes, plus de 30 000 selon certains « *spécialistes es virus* », ils semblent n'être qu'une vingtaine, peut-être moins, à provoquer la majorité des contaminations... Et ainsi, ad *infinitum.*

7.2 - Les dangers à venir

Si les virus avaient la partie belle avec le DOS, c'était à cause du caractère primitif de ce système d'exploitation, vulnérable aux attaques les moins élégantes, et surtout sans secrets ou presque. Seule sa conception laxiste explique l'existence de virus autrement qu'à titre de curiosités de laboratoire. Quelques contre-mesures élémentaires, à peine contraignantes, ainsi qu'un minimum de discipline suffisent d'ailleurs à remédier de manière efficace au danger qu'ils représentent pour les données et programmes. Un progrès supplémentaire sera accompli quand le BIOS et le système d'exploitation seront conçus de façon à sécuriser le poste de travail (droits d'accès aux fichiers, auto-vérification du code, etc.).

L'avenir appartenant aux réseaux mondiaux interconnectés, aucune station ne sera plus une île, accentuant le caractère crucial des problèmes de sécurisation. Des virus créés par des professionnels pourraient bien prendre la relève des virus actuels (créés, à de rares exceptions près, par des amateurs moyennement doués), pour peu que les récompenses potentielles d'actes de sabotage ou d'espionnage en valent la peine aux yeux de développeurs confirmés.

Dans cette hypothèse, les menaces connues sur la plate-forme PC apparaîtront rétrospectivement comme d'aimables divertissements... Les nouveaux virus envisageables ne serviront plus à satisfaire un quelconque désir de notoriété facile, mais seront peut-être de véritables missiles logiciels de type **Fire & Forget**, polarisés sur une mission qu'ils accompliront avec d'autant plus d'efficacité qu'ils auront su se faire discrets (le propre du crime parfait, c'est de n'être pas découvert). Les couleuvres informatiques évoquées dans le grand roman de John Brunner intitulé *Sur l'onde de choc (The ShockWave Rider)* seront alors peut-être une réalité.

7.3 - A qui profite le crime ?

Les coûts engendrés par la prolifération des virus ne sont pas chiffrables. Mais il est indéniable que les premiers acteurs économiques auxquels les virus apportent des bénéfices ne sont autres que les éditeurs antivirus. Une minorité d'entre eux n'ont d'ailleurs de cesse d'entretenir un climat de psychose afin de gonfler les ventes.

Toutefois les choses ne sont peut-être pas aussi claires qu'il n'y paraît, et le manque de transparence et de communication sur toutes ces activités autorise toutes les suspicions : des créateurs de virus monnaieraient la signature de leur code source ; les firmes n'ont aucun intérêt à éditer des logiciels trop performants (par rapport à la concurrence, au développement des différentes souches de virus) ; de nombreux consultants employés en Freelance par les firmes seraient également des hackers, pas toujours animés de sentiments bienveillants…

En ce qui concerne les entreprises, deux types d'action relèvent du délit informatique : l'introduction de virus pour nuire à un concurrent, et l'introduction de virus pour motif personnel, tel que vengeance (licenciement...), jalousie (nuire à un collègue...), inconscience, provocation, farce...

Avenir proche

Depuis 1992, le nombre de virus différents en circulation double approximativement chaque année[50], et les différentes sources du domaine public (BBS, Internet, publications diverses) tendent à élargir la population susceptible de produire ou manipuler des virus. La recherche sur les antivirus arrive pourtant à présent à un tournant, avec le développement d'algorithmes basés sur l'intelligence artificielle.

Ralph Burger évoque la prolifération des virus comme un nouveau round de la Soft War, opposition entre programmeurs malveillants d'une part et concepteurs de sécurité et antivirus d'autres part. Le premier terrain de conflit se situait au niveau du piratage de logiciels : les hackers cherchaient à déplomber, tandis que les firmes de logiciels cryptaient. Puis vint le tour des sécurités de réseaux informatiques. Et à présent, les rôles ont été inversés Guignol a remplacé Gnâfron : ce sont les éditeurs qui cherchent à décrypter les virus.

[50] - Celui des virus réellement dangereux augmente beaucoup moins vite

Intérêts stratégiques

Le roman de Thierry Breton et Denis Beneich (**Soft War** : la guerre douce) illustre les possibilités d'agression informatique entre états... L'histoire est simple, et très plausible. En pleine guerre froide, les soviétiques parviennent à acheter un super-ordinateur américain. Ce qu'ils ignorent, c'est que les services secrets américains ont programmé la machine de sorte qu'elle déclenche une véritable catastrophe logique dans le réseau auquel elle sera attachée, détruisant tous les logiciels et toutes les données à sa portée. Ce sont les services météorologiques américains qui seront chargés de faire exploser la bombe, en lui communiquant une donnée de température particulière pour la ville de St Thomas.

A présent, avec l'effondrement du bloc de l'Est, le rôle de la CIA s'est réorienté vers la protection des intérêts du moment : l'hégémonie économique. L'importance à venir des réseaux mondiaux dans le domaine commercial est évidente. Aussi les recherches portant sur le cryptage et la sécurisation de données tendent à devenir des sujets sensibles outre-Atlantique. Signe des temps, la rumeur (à prendre avec des pincettes) circule qu'un brillant informaticien se trouverait en prison, pour avoir voulu placer dans le domaine public (en shareware) un algorithme de cryptage simple et révolutionnaire. Depuis la mise au secret de cette personne, le mouvement de contre-culture Cyberpunk s'efforcerait de disséminer le code source en question, afin que la détention de son auteur devienne sans objet.

Avec la mondialisation croissante des réseaux, ceux-ci deviendront d'une manière ou d'une autre le terrain de jeux de groupes d'intérêts contradictoires. Quand l'on sait que les réseaux financiers, les instituts de recherche, les multinationales, mais aussi diverses mafias, sectes, mouvements terroristes, gouvernements peu scrupuleux... que tout cela se retrouve sur le Web... la maîtrise des codes autopropageables constituera une arme de choix.

7.4 - Une nouvelle forme de vie ?

Dans l'essentiel de la littérature, les concepteurs de virus sont évoqués au travers d'un registre moral. D. Laloux parle de « *l'esprit malade de délinquants irresponsables* ». Ross Greenberg, auteur de antivirus **Flushot+,** qui mène une véritable croisade jusque dans les couloirs du Congrès américain, est encore plus sévère : « *En ce qui concerne les concepteurs de virus, de vers, il s'agit sans doute d'adolescents impuissants, incapables de rapports sociaux normaux, qui cherchent à s'affirmer à travers ce genre de pratiques terroristes* ».

En règle générale, les auteurs classent les manipulateurs de virus dans une typologie manichéenne : les adolescents asociaux, et les doctes chercheurs de réputation intergalactique. Et dans tous les cas, le virus est abordé sous son angle malsain et nuisible. Exception à cette règle, Mark Ludwig, un des trois créateurs de Core War. Il condamne également les diffuseurs malveillants de virus, mais voit la création de « *codes autopropageables* » comme une inspiration philosophique nouvelle. Pour lui, les virus ne sont pas une nouvelle menace sur l'humanité, mais un nouveau champs de connaissance à explorer, au même titre que l'astronomie héliocentrique du XVIème siècle, ou que la route des Indes par l'Ouest du siècle précédent.

Selon **Mark Ludwig**, c'est la première fois que l'homme a créé *une « sorte de nouvelle forme de vie* » autonome, doté de sa stratégie de reproduction, avec ses besoins et ses contraintes (son biotope ? les machines informatiques). Il réclame l'abolition du terme virus, empreint de trop de connotations péjoratives, suremployé à mauvais escient par les médias, de surcroît au cours des années SIDA.

Les tentatives de reproduire le monde vivant par des machines ont échoué. Les codes autopropageables constituent une nouvelle voie d'exploration : l'opportunité se présente de tenter à nouveau le développement d'entités en prenant pour point de départ l'équivalent informatique du micro-organisme le plus simple.

Mark Ludwig fustige tous ceux qui condamnent jusqu'à l'existence même de ces programmes. Avec la modestie de celui qui a atteint les limites actuelles du savoir dans sa spécialité, il pose un regard plein d'espoir quand à la recherche sur le sujet. Il admet ne pouvoir en apprécier l'horizon, encore trop flou et brouillé par la morale, mais « *Une chose est sûre : nous ne saurons jamais si personne n'y va voir* ». Il termine ainsi l'introduction de son ouvrage **Naissance des virus informatiques** : « *Aussi, je voudrais vous inviter à monter à bord de ce petit radeau que j'ai construit et partir ensemble à l'aventure...* »

Moi, je veux bien, mais j'avoue que je suis imperméable à ce genre de poésie. Cette forme de vie, si c'est est une, ce dont je doute, est comparable aux Indiens, tels que les décrivaient jadis certains colons des plaines américaines, à la « belle » époque de la rue vers l'or : *« un bon indien, c'est un indien mort »*[51]. Pour moi, comme pour beaucoup d'autres utilisateurs de l'informatique, cette « forme de vie » présentée par Mark Ludwig ne sera intéressante que lorsqu'elle aura été complètement éradiquée...

[51] - Phrase attribuée d'abord au général Custer, puis à beaucoup d'autres...

Annexes

Annexes :

Programmer des (anti) virus ?
Sites Internet dédiés à la lutte antivirus
Le syndrome de la suffisance

Programmer des (anti)virus ?

Auteurs de virus, développeurs d'antivirus. Tout semble les séparer, et pourtant, les derniers ressemblent aux premiers. Ils sont animés par les mêmes passions : le programmation et la mise au point de nouvelles techniques.

Dépeint tantôt comme un adolescent bidouilleur en quête de reconaissance, tantôt comme un programmeur bulgare de génie sous payé, le **créateur de virus** est difficillement définissable. En réalité, celui-ci est souvent quelqu'un de très expérimenté. Car, pour développer un programme capable de se reproduire à l'intérieur d'un autre, il faut avoir de solides bases en assembleur et maîtriser nécessairement les aspects techniques du système d'exploitation. Il est, en revanche, certain qu'avec les langages de script tels que **VBA** (Visual Basic for Application), cette thèse risque de devenir caduque. Ces derniers offrent, en effet, la possibilité aux débutants de concevoir très rapidement des vers destructeurs

Les motivations du programmeur de virus ne sont pas toutes les mêmes. Si certains sont animés part le sens du défi technique, d'autres désirent simplement faire parler d'eux. Pour préserver son anonymat, le programmeur de virus signe ses créations de son pseudonyme : Mental Driller, Metabolis, Darkman, Qyuantum, etc. Il agit ainsi en pleine discrétion, tout en s'assurant d'être reconnu par ses pairs.

Afin de progresser et d'échanger leur savoir, les auteurs de virus ont décidé de s'associer et de former des groupes. Le but de ces dernier est de trouver de nouvelles méthodes d'infection et de les communiquer. Parmi les plus connus, citons Immortal Riot, Vlad, Codebreakers ou 29A. Certains, tels Vlad, à l'origine du virus Boza, premier infecteur de fichiers exécutables 32 bits sous Windows 95, ont cessé leur activité. Mais d'autres continuent à agir. Ainsi, plusieurs groupes diffusent encore de manière régulière leurs création au travers de magazines zélectroniques. La dernière édition de 29A, une publication parue sur le Web à la fin de l'année 1998, met plus de 40 sources de virus commentées à la disposition de ses lecteurs. De nouvelles méthodes pour tromper les différents antivirus sont évoquées.

Sur Internet, de nombreux sites sont dédiés aux amateurs de virus informatiquess. Seulement, depuis l'affaire **Melissa**[52], un véritable climat de psychose s'est installé aux États-Unis. Le FBI s'est, en effet, employé à fermer plusieurs de ces sites. Le fameux site House of Kaos a été parmi les premiers à en faire les frais. Depuis, les hébergeurs tremblent : de peur de voir arriver les forces de l'ordre dans leurs locaux, ils pratiquent l'autocensure et effacent les sites comportant ne serait-ce qu'une seule trace de virus informatique.

Les **auteurs d'antivirus** sont surtout d'habiles programmeurs. Leur tâche consiste à recueillir les échantillons qu'on leur envoie, les analyser, déterminer si le code présent comporte une activité virale et, le cas échéant, réaliser rapidement un antidote. A l'instar des auteurs de virus, ils doivent connaître sur le bout des doigts les fonctionnalités cachées des systèmes d'exploitation. En outre, la même soif de defi et de connaissance les anime. A chaque instant, ils s'efforcent d'innover en concevant de nouvelles parades destinées à piéger les virus. Seules différences avec leurs homologues concepteur de virus, les créateurs d'antivirus sont généralement plus âgés et agissent dans un but lucratif.

Généralement, les programmateur d'antivirus se font la course : c'est à celui qui identifiera le premier la nouvelle espèce polymorphe, ou bien celui qui disposera d'une solution d'éradication eficace avant les autres. Car ici, des sommes extrèmement importantes sont en jeu. Et c'est surtout la réputation de chacun qui est engagée.

[52] L'affaire du virus nommé Mélissa...

Une véritable rivalité existe entre les auteurs de virus et ceux d'antivirus. Ces derniers ne cessent de se mettre au défi. Ainsi, il n'est pas rare que les programmeurs de virus glissent à l'intérieur de leurs création quelques messages de provocation à l'intention des concepteurs d'antivirus. Une illustration de cet antagonisme : le cas du virux **Boza**. Décelé par un spécialiste, Vesselin Bonchev, l'exécutable contenait le chaîne de caractère BIZATCH qui s'avérait être le nom officiel du virus. Mauis, malgré cela, les auteurs d'antivirus ont décidé de le baptiser Boza. Mécontent, l'auteur, Guantum, s'est très rapidement manifesté pour que sa création soit référencée comme il l'avait décidé. Sans doute pour l'énerver, les auteurs d'antivirus n'ont jamais voulu en démordre et ont gardé Boza.

En surface, les éditeurs d'antivirus présentent l'image d'une communauté soudée de chercheurs. On nous les montre en blouse blanche, en train de disséquer des morceaux de code informatique. Afin de protéger les utilisateurs, ces chercheurs s'échangent les signatures des dernieres spécimens identifiés et les intègrent à leur logiciel. Ces règles déontologiques sont généralement respectées. On comprend, dans cette mesure, pourquoi l'affaire Remote Explorer a tant agité les consciences.

En Décembre 1988, MacAfee, l'éditeur de VirusScan, met la main sur le premier virus NT résident, baptisé **Remote Explorer**. Il conçoit rapidement une solution d'éradication et l'annonce. Comme cela se fait habituellement, les autres compagnies d'antivirus réclament l'épreinte du spécimen. Ils devront finalement patienter plus d'une semaine avant de récupérer la bête en question. Explication officielle : la personne responsable du laboratoire était partie en vacances... Le paysage des auteurs d'antivirus est loin d'être idylique.

Dans un autre registre, le **calendrier des virus** est un beau coup marketing des éditeurs d'antivirus. Pour inciter les utilisateurs à acheter leur produit, ils répertorient les noms des virus qui entrent en action chaque jour. C'est ainsi qu'il les effraient. Le problème est qu'en vérité, tout cela ne veut rien dire. En effet, l'utilisateur peut très bien être victime d'un virus inconnu disposant d'une mise à feu qui s'actionnera avant qu'un antivirus ne le détecte. En outre, quel est l'utilité de ce calendrier ? Doit-on le consulter chaque matin et prier, les bras croisés, que rien ne se passe ? Ou bien ne faut-il pas mieux faire de la prévention, en permanence ?

Quelques sites dédiés à la lutte antivirale

Remarque préliminaire :

Toutes ces adresses ont été testées lors de leur introduction dans cette section (pour la plupart en 1998/99). Elles étaient donc valables à cette époque, sous réserve d'une faute d'orthographe. A présent, il n'est pas impossible qu'elles n'existent plus ! Internet est un monde mouvant...

Les adresses peuvent correspondre à des sites (pour la plupart **anglophones**, hélas...) ou pointer directement sur des pages jugées intéressantes. Bien évidemment, cette liste est loin d'être exhaustive, vous pourrez trouver beaucoup d'autres sites, ou pages, sur ce sujet. N'hésitez pas à me communiquer les adresses correspondantes.

Alwil Software
http://www.anet.cz/alwill/viruses.htm

Amplitude (The productivity & security group)
http://www.cti.fr

Command AntiVirus Software
http://www.commandcom.com/html/rirus/virus.html

Computer Incident Advisory Capability Virus Database
http://ciac.llnl.gov/ciac/CIACVirusDatabase.html

CTI Informatique
http://www.cti.fr

Datafellows Virus Information Center
http://www.datafellows.com/vir-info/

Dr Solomon Virus Central
http://www.drsolomon.com/vircen/

Eliashim Antivirus Center
http://www.eliashim.com/valert.html

IBM AntiVirus Online Virus Alerts
http;//www.av.ibm.com/BreakingNews/VirusAlert/

Institut européen pour la recherche sur les virus
http://eicar.org

Kaspersky Labv (éditeur du logiciel AVP)
http://www.avp.ru
http://www.avpve.ru
http://www.evpve.ru/avp_ve.eng/infex.htm
(encyclopédie en ligne des virus informatiques)
http://www.kasperskylab.ru/eng/virus.default.html
(une présentation historique des virus informatiques)

McAfee Virus Pages
http://vil.mcafee.com/villib/alpha.asp

Scientif American

http://www.sciam.com/1197issue/1197kephart.htm
(les enseignements de la biologie dans la lute contre les virus informatiques)

Stiller Research Virus Information

http://www.stiller.com
http://www.stiller.com/hoaxes.htm
(pages consacrées aux faux virus)

Symantec (AntiVirus Research Center)

http://www.symantec.fr
http://www.symantec.com
http://www.symantec.com/avcenter/sarcman/
(la protection antivirus sous la forme d'une bande dessinée...)

The WildList

http://wildlist.org/WildList/wildlist.htm

Thunderbyte

http://thunderbyte.com

Trend Micro (Technologies antivirales pour l'entreprise)

http://www.antivirus.com/vinfo/index.htm
http://www.trendmicro.fr

Vet Virus Control Center

http://www.cybec.com.au/html/vvcc/antivirus/zoo/index.html

Virus Bulletin

http://www.virusbtn.com/
(publication internationale sur les virus)

D'autres adresses sur les « faux virus »

http://members.aol.com/virushoax/
http://kumite.com/myths
http://www.stiller.com/hoaxes.htm

Table des matières