LES VIRUS

INFORMATIQUES

Décembre 2005

Espace Menaces - Groupe Virus

CLUB DE LA SECURITE DES SYSTEMES D'INFORMATION FRANÇAIS
30, rue Pierre Semard, 75009 PARIS
Tél. : +33 153 25 08 80 – Fax : +33 1 53 25 08 88
e-mail : clusif@clusif.asso.fr - Web : http://www.clusif.asso.fr

REMERCIEMENTS

Le CLUSIF tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Michel	**BERTIN**	
Olivier	**GUERIN**	*CLUSIF*
Olivier	**ITEANU**	*ITEANU & ASSOCIES*
Pascal	**LOINTIER**	*ACE INSURANCE*
François	**PAGET**	*McAfee*
Jean-Charles	**SIMON**	*MICHELIN*

Nous remercions aussi les membres ayant participé à la relecture.

TABLE DES MATIÈRES

1. HISTORIQUE

1940 -1949 - La théorie

Le mathématicien John Von Neumann développe le principe théorique des automates et des machines reproductrices. Sa théorie se fonde sur les principes de la machine de Turing où le concept de machine à calculer est étendu à celui de machine à construire.

1960 - 1980 - Les premiers vers

Dans un but ludique, divers informaticiens développent un nouveau concept de jeu informatique (Core War). Pour chacun d'entre eux, il s'agit d'écrire un programme (qu'ils appellent « organisme ») capable de créer des copies de lui-même tout en cherchant à éliminer les programmes adverses.

D'autres chercheurs mettent au point des programmes de démonstration et des utilitaires capables de réaliser des tâches répétitives sur diverses machines d'un même réseau. Ces programmes n'ont rien de malveillant. Certains experts redoutent cependant une mauvaise utilisation ou un dysfonctionnement. Les prédictions se réalisent, elles marquent la fin des expériences.

1980 -1988 - La genèse des virus

A partir de 1981, quelques exemples de diffusion de codes auto-reproducteurs sont signalés sur APPLE-II. A cette époque, il n'est pas fait mention du terme « virus informatique ». Dans le contexte qui nous intéresse, celui-ci est utilisé pour la première fois par Fred Cohen en 1984.

En 1986, les premiers cas d'infections font leur apparition dans le monde PC. Certains auteurs sont identifiés : Basit et Amjad Farooq Alvi pour le virus Brain, Ralf Burger pour Virdem. Les universités sont en première ligne avec l'apparition de Lehigh à Lehigh (USA), Jérusalem à Technion (Israël), Stoned à Wellington (Nouvelle-Zélande), Ping-Pong à Turin (Italie).

A cette même période, apparaissent les premiers vers spécifiquement malveillants. Le plus fameux d'entre eux atteint Internet le 2 novembre 1988 et porte les initiales de son créateur : RTM (Robert Tappan Morris). 5% des machines du réseau sont touchées, et l'incident est à l'origine de la création des CERT (Computer Emergency Response Team).

1989 -1992 - Les choses sérieuses commencent

Alors qu'apparaissent les premiers anti-virus, aucune région du monde n'est épargnée par le phénomène. La propagation se fait principalement par l'entremise de disquettes, c'est une propagation lente.

Le printemps 1989 est marqué par l'alerte au virus Datacrime et sa forte résonance médiatique. Aux Pays-Bas, la police prend le problème au sérieux, l'action de Datacrime est considérée comme un acte criminel. Elle demande à un programmeur d'écrire un détecteur et le met ensuite à la disposition du public dans les commissariats contre une somme minime.

Cette année là, on recense une cinquantaine de virus. En Bulgarie, un inconnu se faisant appeler Dark Avenger en imagine de nouveaux. Les procédés qu'il met au point augmentent la capacité de propagation et la difficulté de détection. Certains de ses outils sont qualifiés

de « révolutionnaires ». Ils sont toujours source d'inspiration pour de nombreux auteurs de virus actuels.

La seule recherche d'une signature n'est plus efficace, certains virus, comme la série des V2Px de Mark Washburn possèdent un algorithme de chiffrement qui rend leur apparence différente sur chacune de leur copie. Ces virus polymorphes rendront la vie difficile à nombre de produits anti-virus. Ils devront mettre au point des outils de décryptage génériques.

En 1991, les grands éditeurs, Symantec, McAfee, Docteur Solomon proposent déjà leurs produits. Le nombre de virus passe de 250 à 1000. Parmi eux, on retiendra les noms de Flip, Tequila et Maltese Amoeba.

Des serveurs dédiés à l'échange de virus voient le jour dans le monde entier. Le premier d'entre eux est Bulgare, il participera fortement à la notoriété des auteurs de l'Est de l'Europe. Dark Avenger l'utilisera pour diffuser le premier générateur de chiffrement qui permet de rendre polymorphe un virus créé par ailleurs.
On découvre en Australie une nouvelle variante de Stoned. Elle est destructrice le 6 mars de chaque année, jour anniversaire de la naissance de Michelangelo (1475). Ce virus provoquera en 1992 le principal événement médiatique du domaine.

1992 – 1995 – Générateurs et sophistication

Le premier virus ciblant Windows est diffusé en septembre 1992. Il n'est pas performant mais tient compte de la structure segmentée des fichiers.

D'autres virus se dotent de fonctionnalités de protection contre les logiciels anti-virus (anti-debug, greffe sans point d'entrée en début de programme, contamination lente...). On assiste à la multiplication des groupes d'auteurs de virus, des générateurs de virus, générateurs de chiffrement et des sources.

Les virus ne cessent de se complexifier. Natas, One-Half, Tremor et Monkey en sont quelques exemples.

Ce sont cependant les virus système qui se propagent le plus en représentant 80% des infections recensées. Les principaux portent les noms de Form, Jumper.B et Antiexe.

1995 – 1999 - Les virus de macros

Avec WM/Concept, les virus de macros font leur apparition en août 1995. L'idée n'est pas nouvelle, mais cette mise en circulation contraint les entreprises à réviser leur politique de sécurité. En effet, le virus ne se propage plus exclusivement via un programme exécutable mais aussi par le biais d'un fichier bureautique que l'on avait tendance à considérer comme un simple fichier de données.

Un an plus tard, XM/Laroux est le premier virus opérationnel sous Excel. Toute la suite Office de Microsoft sera bientôt atteinte dans ses différentes versions. Malgré quelques tentatives, les autres plates-formes telles que Lotus AmiPro/WordPro, Corel 7-9 ou Visio 5 ne seront jamais une véritable cible. Les auteurs de virus préfèrent s'acharner sur le leader mondial.

En 1996, Boza est le premier virus spécifiquement créé pour Windows 95. Issu du même groupe d'auteurs, Staog sera le premier virus ciblant Linux.

Les langages de macro font de nombreux adeptes. On compte plus de 1000 macro-virus en juin 1997. En un an, le nombre total de virus connus passe de 15000 à 40000.

Alors qu'apparaissent en 1998 les premiers virus de script, les virus système disparaissent et 80% des alertes virales concernent des macro-virus.

Les systèmes d'exploitation Windows redeviennent petit à petit le terrain de prédilection des auteurs de virus. Toutes les techniques de furtivité et de cryptage qui s'appliquaient à la plate-forme DOS sont actualisées pour fonctionner aussi bien en environnement 16 bits que 32 bits.

1999 – 2000 – L'invasion des « mass-mailers »

L'utilisation des disquettes se raréfie. Les échanges informatiques par e-mail prennent le relais. Le premier virus mondialement connu qui exploite la messagerie électronique apparaît en janvier 1999. Il s'agit de W32/Ska@M. Il ne cible qu'un destinataire à chaque activation. Il lui faudra plus de 6 mois pour faire son premier tour du monde.

En mars 1999, 2 jours auront suffit à W97M/Melissa@MM. Il cible d'un coup 50 destinataires.

Les macro-virus sont toujours d'actualité ; ils laissent cependant de plus en plus la place à des virus utilisant des langages de script (VBScript et JavaScript) ou la programmation en assembleur 32 bits.

Avec VBS/Loveletter@MM, la vitesse de propagation s'accélère encore. S'attaquant à chaque activation à l'ensemble des destinataires des divers carnets d'adresses, il ne mit que quelques heures pour envahir la planète (mai 2000).

Ces nouveaux venus que l'on nomme aujourd'hui des « mass-mailers » se propagent par l'entremise d'une pièce jointe. En octobre 1999 JS/Kak@M démontre qu'un virus peut s'en affranchir. Au format HTML, une simple prévisualisation suffit à infecter la machine.

Au 1er janvier 2000, on recense plus de 56000 virus.

Les équipements nomades, tels que les assistants numériques (PDA, *Personal digital Assistant*) et les téléphones portables, offrent de nouvelles plates-formes de recherche. Une vingtaine de virus ou chevaux de Troie, *Proof of Concept (PoC)*, sont conçus pour les systèmes d'exploitation des organiseurs de l'époque : *PoC* correspond à la faisabilité technique même si, ensuite, le programme malveillant n'est pas répandu. En juin 2000, VBS/Timofonica@MM n'est qu'un mass-mailer de plus. Il retient cependant l'attention du public, car il est capable d'envoyer des messages SMS aux utilisateurs du service de portable espagnol Telefonica. En août apparaît Liberty, le premier Cheval de Troie dédié aux assistants Palm. Les systèmes d'exploitation de ces nouveaux équipements ne sont pas encore suffisamment sophistiqués mais les auteurs de virus cherchent de nouvelles voies.

Parmi les « mass-mailers », les virus programmes (W32) vont petit à petit s'imposer. Les techniques de détection générique et heuristique sont de plus en plus efficaces face aux virus de macro et de script. Plus complexes, les virus programmes peuvent mettre en œuvre des processus rendant plus difficile la détection. Au travers d'un même fichier, ils peuvent élargir leurs techniques de propagation.

Chaque mois, de nouvelles vulnérabilités sont mises à jour. S'ils ne les découvrent eux-même, les auteurs de virus s'empressent de les utiliser pour augmenter les capacités de propagation.

2001 – 2002 – Le vrai retour des vers

Plus de 80% des virus recensés sont des mass-mailers, ce sont aussi des virus programmes. La frontière entre auteurs de virus et hackers s'amenuise. De nombreux virus, tels que W32/Sircam@MM et W32/Bugbear@MM, transportent des portes dérobées et des outils de collecte d'information.

En septembre 2001, W32/Nimda@MM est le premier virus pouvant se prévaloir du titre de « virus Internet ». Ses multiples modes de propagation lui permettent une propagation optimale via la messagerie, les serveurs IIS, les partages réseaux et les consultations Web. Il infecte les serveurs mais également les stations de travail.

Les virus cherchent à utiliser Internet pour se mettre à jour. W32/Babylonia@M et W32/Hybris@MM en sont deux exemples.

W32/CodeRed.A voit le jour en juillet 2001, c'est un véritable ver, uniquement en mémoire dans sa version initiale, il infecte 350.000 machines autour du monde en 24 heures. C'est beaucoup plus que Loveletter !

2003 – 2004 - De nouveaux moyens de propagation et de nouveaux objectifs

Le nombre total de virus et autres programmes malveillants dépasse maintenant les 100 000.

Un an et demi après CodeRed, le 25 janvier 2003, apparaît W32/SQLSlammer.worm. Les leçons apprises n'ont pas vraiment servi. Le correctif de sécurité bloquant la faille utilisée par le virus était connu depuis juillet 2002, mais de nombreuses machines étaient toujours vulnérables à cette attaque. En 10 minutes, 90% des machines vulnérables étaient atteintes. Selon les sources c'est entre 75.000 et 350.000 machines qui furent infectées. Le chiffre le plus élevé est sans doute le plus probable.

Les mass-mailers continuent d'envahir nos boîtes aux lettres. Ceux de la famille W32/Klez@MM sont particulièrement persistants.

L'échange de fichiers musicaux et vidéo est une pratique de plus en plus courante sur le Net. Divers logiciels gratuits permettent ces échanges de fichiers entre les internautes. Le nombre de virus utilisant comme moyen de propagation cette technologie d'échange, dite poste à poste, augmente très rapidement. On en compte plus de 300 au début de 2003 et plusieurs milliers à la fin de cette même année. Ciblant plus particulièrement le grand public, cette nouvelle technique de propagation se rajoute aux autres. Associée aux précédentes, elle offre à un même virus une meilleure capacité de propagation.

Des liens s'établissent entre les auteurs de virus et les autres acteurs liés à la criminalité informatique. Les virus diffusent toutes sortes d'outils d'attaque qui exploitent au mieux les ressources de l'Internet. La mise en place de serveurs relais parasites permet la diffusion massive et anonyme de courriers non sollicités. Des robots, programmes malveillants permettant une prise de contrôle à distance de machines vulnérables se propagent et forment des réseaux d'attaque cachés (ou botnet). Diverses tentatives de capture de code confidentiels liés, entre autre, aux activités bancaires sont expérimentées (W32/Bugbear@MM, W32/Sobig@MM, W32/Mimail@MM). Même si les résultats semblent peu concluants, ils révèlent le changement de cap qui s'amorce : le virus quitte le monde ludique pour servir des intérêts frauduleux.

En janvier 2004 apparaît W32/Mydoom@MM. Se propageant principalement au travers de la messagerie électronique, il est aussi capable d'investir le réseau d'échange de fichiers KaZaA. Depuis cette date bien d'autres virus ont suscité le trouble. Les mémoires

retiendront entre autre les batailles que se livrèrent les auteurs de Netsky et Bagle durant le premier semestre 2004. On notera aussi l'apparition du ver Witty dès le lendemain de la publication de la faille qu'il utilise. On s'approche ainsi de l'exploitation immédiate des vulnérabilités publiées (*zero day attack*).

Très logiquement, les concepteurs de virus *PoC* s'attaquent à des modèles très répandus afin d'augmenter les opportunités de propagation. Le système d'exploitation des téléphones Nokia devient une cible privilégiée. Il existe deux modes opératoires pour la contamination et la propagation :

- S'appuyer sur la technologie Bluetooth et solliciter du possesseur du téléphone l'installation d'un logiciel. La démarche est identique à celle qui incitait au double-clic pour exécuter un programme sur un PC. Toutefois, les messages ne sont encore très « attractifs » : « Install Kill Saddam », « Install CommWarrior », etc.
- Utiliser la technologie MMS pour transporter puis faire installer un programme exécutable malveillant.

Résultat de l'infection d'un téléphone portable par le virus SymbOS.Skull2

2. TYPOLOGIE DES INFECTIONS INFORMATIQUES

2.1 Introduction

Les infections informatiques sont des programmes ou des sous-ensembles de programmes malveillants qui, à l'insu de l'utilisateur, sont destinées à perturber, à modifier ou à détruire tout ou partie des éléments indispensables au fonctionnement normal de l'ordinateur. On différencie les programmes simples et les programmes auto-reproducteurs.

L'organisation de l'activité et le bon fonctionnement du système d'information peuvent également être perturbés par la diffusion de courriers ou d'éléments non sollicités tels que :

- des farces, en anglais *jokes* : programmes inoffensifs et dédiés, le plus souvent, à l'amusement,
- des courriers non sollicités, plouriels, en anglais *spam* : messages à caractère commercial s'appuyant éventuellement sur une usurpation d'adresse électronique,
- des arnaques financières tel que le *scam* : messages vous proposant un montage financier attractif derrière lequel se cache une escroquerie qui s'articule autour d'une demande d'avance de fonds de la part de la victime,
- des rumeurs, en anglais *hoaxes* : informations malveillantes et non fondées qui sont diffusées pour inquiéter les destinataires ou discréditer une personne ou un organisme,
- des lettres chaînes : messages s'appuyant sur la crédulité des destinataires faisant appel à la piété, la générosité et/ou la superstition et proposant éventuellement un enrichissement personnel,

Nous verrons plus loin que ces attaques ont de nombreux points communs avec certains chevaux de Troie ou virus.

2.2 Les grandes familles d'infections

2.2.1 Programmes simples

Un programme simple contient une fonctionnalité malveillante (*payload*) cachée qui se déclenche ou s'initialise lors de son exécution. Il n'y a pas propagation. En un seul exemplaire, ce programme doit être introduit dans l'ordinateur ciblé. C'est souvent l'utilisateur lui-même qui, par manque de discernement, introduit le programme. Ce processus peut également être le travail d'un virus.

L'action induite peut avoir un caractère destructif ou simplement perturbateur. Elle peut être immédiate ou retardée dans le temps. Dans de nombreux cas, le programme appelé s'installe à l'insu de l'utilisateur et modifie les paramètres du système pour ensuite s'exécuter à chaque démarrage de la machine. Il agit alors de manière discrète et continue.

On retrouve dans cette catégorie :

- les bombes logiques,

- les chevaux de Troie,
- les portes dérobées,
- les outils de capture d'information,
- les outils d'attaque réseau,
- les outils d'appropriation de ressource.

2.2.1.1 Bombe logique

C'est un programme contenant une fonction destructrice cachée et généralement associée à un déclenchement différé. Cette fonction a été rajoutée de façon illicite à un programme hôte qui conservera son apparence anodine et son fonctionnement correct jusqu'au moment choisi par le programmeur malveillant. Elle peut être conçue pour frapper au hasard ou de manière ciblée.

Exemple de bombe logique ciblée : un programmeur insère dans le programme de paie de l'entreprise qui l'emploie une fonction de destruction dont l'exécution est déclenchée si son nom disparaît du fichier du personnel.

Exemple de bombe logique aveugle : un programmeur insère dans un logiciel public distribué gratuitement sur Internet une routine de destruction qui se déclenche chaque 1er avril.

2.2.1.2 Chevaux de Troie et portes dérobées (en anglais *backdoors*)

Ces programmes permettent d'obtenir un accès non autorisé sur les équipements qui les contiennent.

On utilise le terme de cheval de Troie lorsqu'il s'agit d'une fonction cachée et rajoutée au sein d'un programme légitime quelconque. Le terme de porte dérobée s'applique à tout programme malveillant spécifiquement dédié à cet effet.

Il s'agit en fait de l'un des éléments d'une application client/serveur permettant la prise de contrôle à distance d'un PC. Deux ordinateurs entrent en jeu. Le premier contient l'élément client, il pilotera le processus. Le second est la machine cible ; il contient l'élément serveur – le cheval de Troie ou la porte dérobée. Il devra être actif sur la machine pour pouvoir initier la connexion avec le client. Le pirate interroge le réseau, au travers d'une adresse IP. Si celle-ci est joignable, la connexion s'effectue.

Une telle prise de contrôle à distance peut être légitime (opération de télémaintenance) ou non. Dans le cas d'un acte malveillant, le propriétaire de la machine visitée a exécuté à son insu l'élément serveur ; il ignore que son poste peut être visité.

Avant 1998, ces programmes ne faisaient guère parler d'eux. Cette année là, toute une série d'outils furtifs de prise de main à distance ont été mis à disposition sur le Web. Les plus connus furent Back Orifice et Socket23.

Back Orifice (en référence à "Back Office" de Microsoft) fut créé par un groupe de hackers baptisé *le culte de la vache morte* (The cult of the Dead cow - cDc). Voici les premières lignes d'un texte qui fut disponible sur leur site :

> *« Back Orifice is a remote administration system which allows a user to control a computer across a tcpip connection using a simple console or GUI application. On a local LAN or across the internet, BO gives its user more control of the remote Windows machine than the person at the keyboard of the remote machine has. »*

Avec de tels outils, un pirate est à même de prendre le contrôle total de sa cible. A titre d'exemple, notons qu'il peut :

- analyser la configuration de la machine et du réseau s'y rattachant,
- modifier la base de registre,
- naviguer dans les répertoires,
- envoyer/recevoir des fichiers,
- exécuter un programme sur la machine,
- rebooter, verrouiller l'ordinateur,
- visualiser l'affichage et surveiller les frappes au clavier,
- émettre des sons.

2.2.1.3 Outils de capture d'information

Les techniques de collecte d'information sont diverses. Il est possible de classifier les outils utilisés en fonction de l'information recherchée.

2.2.1.3.1 Renifleur de clavier et de mots de passe

Un renifleur de clavier (en anglais *keylogger*) est un programme permettant d'enregistrer les frappes au clavier. Son rôle ne se limite pas à l'enregistrement d'éventuels mots de passe. Il peut être sélectif ou enregistrer l'intégralité des informations qui transitent sur le périphérique de saisie. Les outils spécifiquement dédiés à la capture de mots de passe prennent souvent la dénomination anglaise de *Password-Stealer* (PWS).

La plupart de ces dispositifs sont invisibles. Les frappes clavier sont généralement écrites dans un fichier temporaire chiffré et envoyé automatiquement, par courrier électronique, à l'espion.

Beaucoup de virus actuels diffusent ces différents outils. Ils profitent du mode de propagation viral pour s'installer plus aisément sur de nombreuses machines qui deviennent ainsi vulnérables à ce type d'attaque.

Certains *keyloggers* sont en vente libre (exemple: Ghost Keylogger ou Keylogger pro).

2.2.1.3.2 Publiciel et espiogiciel

Au fil de la navigation sur le Web, divers programmes sont installés sur l'ordinateur à l'insu de l'utilisateur. Ils sont plus communément connus sous leurs terminologies anglaises d'*adware* et de spyware.

Un *adware* (*Advertising Supported Software*) est un logiciel qui permet d'afficher des bannières publicitaires. La plupart des annonceurs sont juridiquement légitimes et leur société commerciale reconnue. Les programmes ne diffusent pas d'information vers l'extérieur mais permettent la planification ciblée de messages d'accroche.

Les *spywares* sont des adwares qui installent sur le poste de l'utilisateur un logiciel espion et envoient régulièrement et, sans accord préalable, des informations statistiques sur les habitudes de celui-ci. Certains spywares ne se contentent pas de diffuser de l'information. Ils modifient les paramètres système à leur avantage pour imposer, à l'utilisateur qui en est la victime, un certain

mode de navigation sur le Web. Ces logiciels peuvent aussi capturer vos habitudes en consultation hors ligne. Ils expédient les résultats de leur collecte à chaque ouverture du navigateur.

Certaines rumeurs font état d'une utilisation de la carte son à des fins d'écoute. Cette technique est tout à fait envisageable mais aucun cas concret n'a pu être établi.

Pour contrer tout cela, il existe aujourd'hui des solutions spécifiques de détection-éradication, mais les nouvelles versions des logiciels antivirus prennent aussi en compte les spywares. Plus que jamais, la mise à jour de la base de « signatures » est nécesaire.

2.2.1.4 Outils d'attaque réseau

2.2.1.4.1 Attaque en Déni de Service (DoS, Denial of Service)

En terme de serveur et, plus rarement de poste client, une attaque de type DoS est une activité consistant à empêcher quelqu'un d'utiliser un service. Pour ce faire, l'attaquant utilise un programme qui cherche à rendre le système ciblé indisponible en le faisant se suspendre ou en le surchargeant.

En terme de réseau, une attaque de type DoS consiste à submerger la victime d'un flot de trafic supérieur à sa capacité de traitement. La bande passante est alors saturée et le réseau devient indisponible.

2.2.1.4.2 Attaque en Déni de Service Distribué (DDoS)

Il s'agit d'une attaque de type DoS qui utilise un grand nombre de machines simultanément.

Ce type d'attaque se déroule généralement en deux temps. L'attaquant tente d'abord d'installer son outil sur le plus grand nombre de machines possibles. Celui-ci est programmé pour se déclencher soit sur commande (cas des *botnets*), soit à un instant prédéfini. Il doit ainsi provoquer une surcharge bien plus importante que dans le cas d'une attaque unique.

2.2.1.5 Outils d'appropriation de ressources

2.2.1.5.1 Numéroteur furtif

Un numéroteur furtif (en anglais *dialer*) est un programme gérant une connexion réseau à distance. Il s'agit souvent de faciliter une liaison vers un site au contenu licite par le biais d'un numéro téléphonique surtaxé. Ces programmes s'installent généralement de manière silencieuse lors de la navigation Web.

Dans certains cas, le programme *dialer* démarre en même temps que l'ordinateur sans que l'utilisateur en ait la connaissance. Il établit la liaison automatiquement et reste en ligne aussi longtemps que la session est ouverte. Ils concernent essentiellement les connexions en bas débit *via* la ligne téléphonique, l'ADSL impliquant un autre mode d'accès à Internet.

2.2.1.5.2 Relais de spam

Installés sur la machine à l'insu de son propriétaire, ces mini-serveurs permettent l'émission du courrier non-sollicité (spam) vers les victimes de spammeurs. Cette technique leur évite de se faire eux-mêmes détecter et bloquer directement par leur fournisseur d'accès. Cette pratique équivaut à un détournement de ressources.

2.2.2 Programmes auto-reproducteurs

La finalité d'un programme auto-reproducteur est identique à celle d'un programme simple. Il s'agit d'exploiter, de perturber ou de détruire.

A sa première exécution, le programme cherche à se reproduire. Il sera donc généralement résident en mémoire et, dans un premier temps, discret.

Si elle existe, la fonctionnalité malveillante (*payload*) s'effectuera dans un délai plus ou moins court et sur un critère quelconque prédéfini (*trigger*).

Pour de nombreux virus la perturbation se limite à la reproduction et à tous les ennuis qu'elle engendre. Il n'y a pas à proprement parler de fonction malveillante (absence de *payload*).

Les vers et les virus forment à eux seuls la famille des programmes auto-reproducteurs, on les retrouve au premier rang des infections informatiques.

A l'époque du ver RTM (du nom de son auteur: Robert Tappan Morris), la distinction entre ver et virus est généralement acquise même si elle apparaît parfois des plus fines :

- Un ver (d'après la définition de Peter Denning en 1990) est un programme capable de fonctionner de manière indépendante. Il se propage de machine en machine au travers des connexions réseau. Un ver ne modifie aucun programme, il peut cependant transporter avec lui des portions de code qui pourront, par la suite, effectuer une telle activité (virus par exemple).
    - La terminologie anglaise « worm » est dérivée du mot « tapeworm » imaginé par John Brunner dans une de ses œuvres de science-fiction « Sur l'onde de choc ».
- Un virus (d'après Fred Cohen en 1984/87) est un programme capable d'infecter d'autres programmes en les modifiant pour y inclure une copie de lui-même qui pourra avoir légèrement évolué. Le virus ne peut pas fonctionner d'une manière indépendante. L'exécution du programme hôte est nécessaire à son activation. Par analogie avec son cousin biologique, il se multiplie au sein de l'environnement qu'il cible et entraîne corruption, perturbation, et/ou destruction.

Tout code malveillant à même de se propager est souvent considéré comme un virus. Selon cette théorie, les vers ne sont alors qu'un sous-ensemble dans la famille des virus. C'est le parti pris que nous prendrons dans la suite de ce document. Notons cependant qu'il n'existe pas de consensus à ce sujet dans la communauté anti-virale et diverses autres définitions circulent.

2.3 Classement par cible

Il existe quatre catégories principales de virus. Elles ont chacune une cible bien précise :

- Les virus programme, dont le vecteur de contamination principal est constitué par les exécutables,
- Les virus système, dont le vecteur de contamination est le secteur de partition ou le secteur de démarrage (*Boot Sector*),
- Les virus interprétés qui regroupent les virus de macro sur les documents et les virus de Script utilisant un langage de programmation particulier qui se rapprochent de la programmation par lot (*batch*),

- Les vers qui, comme nous l'avons vu, sont les infections typique des réseaux.

De nombreux virus cumulent les cibles et renforcent ainsi leur capacité de contamination. Ils prennent alors les noms de virus multipartites ou multifonction.

Une nouvelle classe de programmes malveillants se développe depuis 2003 : il s'agit des robots. Ils cumulent souvent une fonctionnalité de type « ver » et une activité d'appropriation de ressources, d'attaque réseau et/ou d'espionnage.

2.3.1 Virus programme

Les virus programme cherchent à infecter les exécutables binaires compilés. Le principe de fonctionnement est le suivant :

1) le virus est présent dans un fichier exécutable,
2) lorsque celui-ci est exécuté, le virus choisit et contamine un ou plusieurs autres fichiers,
3) il agit généralement par ajout entraînant une augmentation de taille,
4) s'il se maintient résident en mémoire, il infecte d'autres fichiers à l'exécution, ou simplement lors d'une manipulation.

Il existe plusieurs types de programmes, et chacun d'eux peut faire l'objet d'une attaque virale spécifique :

Programmes DOS. Jusqu'en 1999, la majorité des virus programmes fonctionnaient sous DOS et ciblaient les fichiers exécutables par ce système d'exploitation. Déjà limitée à cette époque, la proportion des infections dues à ces virus DOS n'a cessé de diminuer pour être presque inexistante aujourd'hui. Les plus courants d'entre eux étaient résidents en mémoire et utilisaient la technologie "par ajout". Ils étaient souvent furtifs, cryptés et polymorphes.

Application *Windows* 16 bits. Ces programmes sont aussi appelés « New Executable » (NE EXE). On les rencontre dans les environnements *Windows 3.x*. Une trentaine de virus ciblant cette plate-forme ont été recensés. Leur diffusion a été quasi nulle.

Application *Windows* 32 bits. Ces programmes sont aussi appelés « Portable Executable » (PE EXE). Les fichiers VxD sont appelés « Linear Executable » (LE). On les rencontre dans les environnements Windows actuels. En forte expansion, certains utilisent des fonctions non documentées du noyau de Windows et tout comme leurs prédécesseurs, ils peuvent présenter des caractéristiques de furtivité, et de polymorphisme. Ils pourront être - ou non - résidents en mémoire.

A l'origine, des CD-ROM de jeu furent le principal vecteur de leur diffusion. Cette nouvelle technique représentant un nouveau « challenge » pour les auteurs de virus, de nombreux sites Internet les proposaient au téléchargement à grand renfort de publicité.

Aujourd'hui, leur diffusion se fait par la messagerie électronique, les disques partagés et les échanges de fichiers sur le modèle « poste à poste ». L'infection locale des fichiers sur le poste de travail n'est qu'une fonctionnalité complémentaire aidant à la propagation du virus au travers du réseau.

Pour être complet, il nous faut citer les applicatifs OS/2 (NE – « New Executables » - LX) et Linux (ELF Internal Format). Quelques virus existent également dans ces domaines.

2.3.2 Virus système

Préalablement à l'apparition des macro-virus, les virus systèmes étaient -de loin- les plus répandus. Ils infectent les zones systèmes des disques durs ou des disquettes :

- secteur de partitions (MBR, *Master Boot Record*) pour les disques durs,
- secteur d'amorce (*Boot, Dos Boot Record*) pour les disques durs et les disquettes.

Pour s'approprier l'un de ces 2 secteurs, le virus peut être introduit *via* un programme spécifique (dropper ou virus multipartite). Les auteurs ont cependant immédiatement compris qu'il était beaucoup plus simple de concevoir un virus directement sous la forme d'un secteur de démarrage de disquette. Le principe de fonctionnement adopté est le suivant :

1) le virus est présent dans le secteur de démarrage d'une disquette,
2) il contamine le PC lorsque le BIOS exécute le code,
3) il déplace ou écrase le code original du BOOT ou du MBR du disque dur,
4) il remplace ce code par lui-même,
5) il sauvegarde éventuellement le code excédent (code complémentaire du virus) dans d'autres secteurs, libres ou occupés,
6) dès lors et à chaque nouveau démarrage, il sera résident en mémoire et capable d'infecter d'autres disquettes sur un simple accès.

Exemples d'infection du MBR : Jumper.B, Antiexe.

Exemple d'infection du BOOT : Form.

2.3.3 Virus multipartites

Un virus multipartite cherche à infecter les zones systèmes des disques durs ou des disquettes et les fichiers exécutables. Selon des critères propres à chaque virus, l'une ou l'autre des techniques d'infection est mise en œuvre à un instant donné. Le but recherché est une plus grande propagation.

De tels virus infectent, par exemple, le secteur de partition du système puis, une fois résidant en mémoire vive, infectent les fichiers exécutables situés sur des unités logiques.

Exemples : Tequila, One-Half.

2.3.4 Virus interprétés

2.3.4.1 Virus de macro

Les virus interprétés regroupent principalement les virus de macro et les virus de script. Du fait de la sophistication des outils de bureautique actuels, tout fichier de données doit être considéré comme potentiellement dangereux. Même si aujourd'hui de nombreux standards de fichier n'acceptent pas l'encapsulation de routines automatisables (macros ou scripts), cette technique tend à se développer. Un type de fichier aujourd'hui inoffensif pourra ainsi rapidement devenir dangereux.

Jusqu'à l'arrivée de WM/Concept en 1995, le grand public était persuadé qu'un virus, considéré à juste titre comme un programme, ne pouvait être véhiculé et introduit dans un ordinateur qu'avec

l'aide éventuelle d'un autre programme. En clair, seuls les fichiers exécutables ou les zones systèmes des disquettes pouvaient, après infection, propager à leur tour le virus. A contrario, les fichiers ne contenant que des données étaient sans danger.

La sophistication des outils bureautiques avec l'apparition des langages de macro a bouleversé la donne. Sans toujours en imaginer les conséquences, les fichiers de données contenant textes ou feuilles de calcul se sont trouvés enrichis de routines automatisables et programmables. Par là même, ils devenaient un nouveau terrain de jeu pour les auteurs de virus.

Lorsque apparaît le virus « Concept », de nombreuses sources annoncèrent que les chercheurs anti-virus l'avaient depuis longtemps envisagé. Certains en soupçonnaient même l'existence en Europe dès le milieu de l'année 1988. Un article fut publié à ce sujet en août 1989, dans la revue « Computers & Security ».

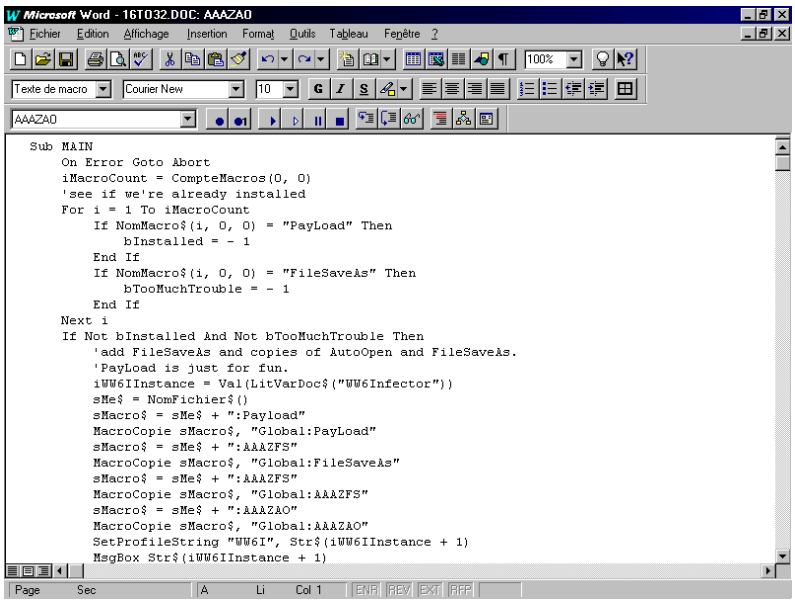
Ciblant Word 6 de Microsoft, *WM/Concept* (*WinWord.Concept*) fut cependant, en Août 1995, le premier macro-virus *« in-the-wild »* (dans la nature). Deux ans après (août 1997), on en comptait plus de 1300.

Se propageant rapidement, les virus de macro ont vite retenu l'attention. Avant leur apparition (1994), les virus système représentaient environ 80 % des cas de contaminations signalés, et moins d'une dizaine de virus représentait également environ 60 % des cas signalés. Ces statistiques ont été bouleversées en quelques mois. Ainsi, les virus *WM/Concept, WM/Npad, WM/Mdma, WM/Wazzu* et leurs variantes représentèrent en 1998 la majorité des infections recensées.

Deux ans après, la très grande majorité des virus de macro infectait les différentes versions du traitement de texte MS-Word et du tableur MS-Excel (depuis les versions Office-95, jusqu'à celles incluses dans le pack Office-2000). Des virus existaient cependant sous MS-Access et MS-PowerPoint. Pour mieux atteindre ces cibles qui ne faisaient pas l'objet d'échanges incessants entre utilisateurs, le concept de « multi–applications » fut remis à la mode.

Potentiellement, tout programme utilisant des macro-commandes ou un macro-langage peut faire l'objet d'une attaque par un virus créé pour cet environnement. On a ainsi détecté quelques virus contaminant les plates-formes Lotus AmiPro/WordPro, Lotus 1-2-3, Corel 7-9 et Visio 5.

Après avoir été rudimentaires, les modes de reproduction des virus de macro se sont sophistiqués. Ils firent appel à d'autres langages de programmation de haut niveau et non plus seulement au langage machine « assembleur ». Le but de cet artifice fut souvent l'activation d'une fonction malveillante (*payload*) ou le contournement d'une sécurité. VBScript est un parfait exemple de ces techniques. Il permet la création de script FTP (W97M/GROOV) ou encore une interaction avec des outils de messagerie (W97M/COLDAPE.A). Les techniques de chiffrement et de polymorphie devinrent de plus en plus courantes.



Plus besoin de connaître l'assembleur ! Une telle simplicité se traduisit, à l'époque, par l'apparition de plusieurs dizaines de virus de macro par mois.

Considérant que la grande majorité des virus de macro en circulation infecte Microsoft Word, une sage précaution consiste à mettre en lecture seule le fichier *NORMAL.DOT* et à en conserver un exemplaire sain. Selon le virus présent, la procédure de restauration s'en trouvera facilitée.

Les variations autour du concept de virus de macro sont nombreuses. Les modifications peuvent porter sur l'environnement : menus, barres d'outils, raccourcis clavier, boutons. Les effets de la charge virale peuvent être similaires à ceux des virus d'exécutables : modification d'environnement, modification de contenu, effacement de fichiers, etc.

Exemples : WM/Concept, W97M/Class, X97M/Laroux, O97M/Tristate, W97M/Melissa@MM.

2.3.4.2 Virus de script

Un langage de script est un langage de programmation spécialisé destiné à contrôler l'environnement d'un logiciel. Interprété, il peut donc être exécuté sur toute machine disposant de l'interpréteur approprié. Deux des plus utilisées sont VBScript et JavaScript.

Pour s'exécuter correctement, les fichiers de scripts font appel à Windows Scripting Host (WSH). Absent d'une configuration standard Windows 95 ou Windows NT4, ce logiciel est aujourd'hui installé par défaut avec les versions actuelles de Windows.

2.3.4.2.1 VBScript

VBScript a été créé à partir de VBA et de Visual Basic. Il repose sur du code source en clair et non sur du code compilé tel que celui des applets. Tout un chacun peut donc voir et modifier le code des scripts qu'il rencontre.

VBScript doit être aussi considéré comme un langage autonome. Il détrône les fichiers de traitement par lots composés d'une série de commande DOS (fichiers batch).

Les premiers virus purement VBScript datent d'octobre 1998. En raison de leurs capacités de propagation hors du commun, l'un des alias donné au premier né de la famille fut "rabbit" (traduction, lapin). Leur nombre a ensuite augmenté parallèlement à la généralisation de ce nouveau langage.

Leur apogée fut atteinte en 2000 en utilisant la messagerie électronique comme vecteur de propagation. Les précurseurs apparurent en juillet 1999. Il s'agissait de VBS/Freelink@MM, VBS/Monopoly@MM et VBS/Triplesix@MM.

2.3.4.2.2 Java

JAVA est un langage créé par Sun Microsystems. Il est comparable au C++ et orienté objet. Il est indépendant de toute plate-forme. Son exécution ne nécessite que la présence du processeur virtuel « Java Virtual Machine ». Java permet de réaliser deux types de programmes : des applets et des applications. Alors qu'un applet n'est qu'une forme hybride de programme incorporé à un document HTML, Java permet aussi la réalisation d'applications intégrées complètes et autonomes qui peuvent avoir le contrôle total du système.

Le virus JV/Strange Brew est apparu en Août 1998. Il s'agit du premier virus natif Java. Il est capable d'infecter aussi bien les applets que les applications.

Cependant ses capacités d'infection sont limitées, un applet infecté n'infectera pas un autre applet ni une application. L'infection et la propagation ne peuvent avoir lieu au travers du Web. Il ne peut se propager que depuis une application locale infectée en utilisant *JAVA.EXE* (kit JDK – Java Developper's Kit) ou l'un de ses équivalents.

JV/Strange Brew est parfois considéré comme étant le premier virus véritablement multi plates-formes car il est capable de sévir sur n'importe quel environnement exécutant une machine virtuelle Java : depuis les PC Windows jusqu'aux serveurs Unix et aux super calculateurs Cray.

2.3.4.2.3 JavaScript

JavaScript n'est PAS Java ! En effet, si Java est un langage compilé, JavaScript, développé par la société Netscape, est interprété. Le code est inclus soit dans une page HTML, soit dans un fichier à l'extension standard « .js ».

Du point de vue viral, notez bien la distinction faite au niveau du préfixe (JV pour Java, JS pour JavaScript). A titre d'exemple, JS/TheFly@MM est un ver JavaScript. Il est contenu dans un fichier attaché the_fly.chm (Compiled HTML Help File).

En novembre 1998, certains parlèrent de virus HTML. Il s'agissait en fait de code VBScript capable de se propager via des fichiers HTML sur une machine locale.

Exemple : JS/Kak@M.

2.3.4.2.4 Traitement par lot

Bien avant l'apparition des langages interprétés modernes, certains auteurs se sont appliqués à créer des virus utilisant les commandes DOS au sein de fichiers batch (extension .bat). Même s'ils sont peu courants, certains d'entre eux sont très sophistiqués et peuvent être résidents en mémoire.

Exemple : BatMan.

2.3.5 Les vers

Il est possible de séparer les vers en deux grands groupes selon qu'ils utilisent les réseaux locaux ou qu'ils s'appuient sur Internet. A ces deux groupes, et de par la définition des vers, il faut rajouter à cette famille les vers de disquettes qui ne font que se recopier de répertoires en répertoires en passant par le lecteur A:

2.3.5.1 Vers de réseaux locaux

Il est facile de franchir le pas entre disques locaux (physiques ou logiques) et disques réseaux et la technique des vers de disquettes s'est très vite étendue à l'ensemble des disques partagés ou partageables. L'infection se déroule généralement de la manière suivante :

1) Recherche de disques accessibles .
2) Affectation de noms de lecteurs (*mapping*).
3) Copie du ver.
4) Exécution.

Dans de nombreux cas l'exécution est différée. Le ver cherche par exemple à se recopier dans un répertoire de démarrage et attend son heure. De ce point de vue, VBS/Netlog découvert en février 2002 en est un intéressant exemple.

2.3.5.2 Vers de messagerie (mass-mailers)

On retrouve dans cette famille, des virus programme, des macro-virus et des virus de Script. Le point commun est l'utilisation de la messagerie électronique comme moyen privilégié de propagation.

La notion de « mass-mailer » apparaît en 1999 avec W97M/Melissa@MM. Dans une courte période de temps, les virus de ce type qui apparaissent expédient un nombre impressionnant de mails. Il a fallu plus de six mois à W32/Ska.A@M pour faire le tour du monde, Melissa n'a mis que deux jours ; quelques heures suffirent à VBS/LoveLetter.A@MM (virus de script).

Pour ces nouveaux venus, il fallait un signe de reconnaissance qui alerte le public. Sous l'impulsion de Vesselin Bontchev et de François Paget, le CARO (Computer Anti-virus Research Organization) adopta l'utilisation du suffixe « @MM » puis celui du suffixe « @M » :

A) Le suffixe « @M » est dédié aux virus/vers qui possèdent un processus opérationnel de propagation par messagerie et qui ciblent une seule boîte aux lettres à chacune de leur activation.

B) Le suffixe « @MM » est dédié aux virus/vers qui possèdent un processus opérationnel de propagation par messagerie et qui ciblent plusieurs boîtes aux lettres à chacune de leur activation.

Même si pour d'obscures raisons le caractère « - » remplace « @ », à compter de septembre 2000, la WildList[1] utilise ce standard.

2.3.5.3 Vers de l'Internet

Créés grâce à une parfaite connaissance de l'environnement réseau et l'utilisation de nouvelles failles de sécurité, ces nouveaux venus sont répertoriés parmi les plus dangereux. L'attaque touche ici les serveurs et non plus les stations de travail.

Tout débute par l'exploitation d'une vulnérabilité. Celle-ci est généralement connue, mais comme les correctifs n'ont pas été appliqués sur de nombreuses machines, le nombre des serveurs vulnérables est suffisant pour une forte propagation.

[1] Organisme international qui a pour but de recenser l'ensemble des virus dans la nature (In-The-Wild) au niveau mondial. La collecte s'effectue grâce à de nombreux chercheurs répartis sur les cinq continents. Les statistiques sont mensuelles. Site internet : http://www.wildlist.org/

Avec W32/Codered.A.worm il s'agit d'un problème de dépassement de capacité de la mémoire tampon pour lequel Microsoft proposa un correctif intitulé « MS01-033 ». Il en est de même avec W32/SQLSlammer.worm, le patch de sécurité « MS02-039 » était connu depuis juillet 2002.

Aucun code viral n'est écrit sur le disque dur. La propagation se fait exclusivement en mémoire vive et sa rapidité en est le point fort :

- W32/CodeRed.A.worm transmettait des paquets *TCP-SYN* : sa propagation était limitée par le temps de latence nécessaire avant que n'arrivent les réponses de la cible.
- W32/SQLSlammer.worm ne transmet qu'un seul paquet *UDP* sans rien attendre en retour. C'est la bande passante disponible qui limite sa vitesse de propagation.

2.3.5.4 Vers « poste à poste »

Illégal lorsque non libres de droits, l'échange de fichiers musicaux et vidéo est une pratique de plus en plus courante sur le Web. Plusieurs logiciels gratuits permettent ces échanges de fichiers entre les internautes.

Depuis mai 2002 de nombreux virus utilisent les réseaux poste à poste (*P2P - PEER TO PEER*) d'échanges de fichiers. Le virus se copie généralement dans l'un des répertoires système de Windows, modifie la base de registre pour pouvoir s'exécuter à chaque démarrage et place de nombreuses autres copies de lui-même dans le dossier de téléchargement utilisé par le logiciel d'échange. Afin d'attirer l'attention, les noms retenus correspondaient à des titres de chansons, de films à des jeux informatiques ou des fichiers à caractère sexuel.

Aujourd'hui, plusieurs centaines de vers ciblant KaZaA et/ou Morpheus sont connus.

Exemple : W32/Benjamin.worm, W32/Kazmor.worm.

2.3.5.5 Vers mIRC

Une de ces premières formes d'attaque est apparue en décembre 1997 sur Internet, et notamment sur IRC (*« INTERNET RELAY CHAT »*). L'une des plus connues, cible le fichier de configuration *SCRIPT.INI* du logiciel mIRC (prononciation « murk »).

Par défaut, ce fichier se situe dans le répertoire dédié au téléchargement. De plus, un exécutable listé dans ce fichier s'exécutera lors de la fermeture du logiciel.

Dans les versions mIRC inférieures à V5.3, il est alors possible d'écraser discrètement le fichier *SCRIPT.INI* original par une version infectée. Une fois cette manipulation faite, lorsque l'utilisateur rejoint le canal de discussion, il envoie à son tour le virus à toute personne qui rejoint ce même canal.

Tout comme les *SCRIPT.INI*, les nombreuses variantes de *DMSETUP.EXE* se propagent par « DCC Send » en infectant entre autres *MIRC.INI*.

De très nombreux « mass-mailers » possèdent également une fonction « vers mIRC »

2.3.5.6 Autres vers

Le ver UNIX/Admw0rm est apparu en Russie en mars 1998. Il est capable de se propager d'un environnement Linux à un autre en utilisant une faille des serveurs BIND (Berkeley Internet Name Domain). Dans son environnement original et sa version actuelle, ce ver contient diverses limitations. Une adaptation à un environnement de type INTEL n'est cependant pas à écarter.

2.3.6 Les robots

L'année 2003 a été celle de la naissance des robots. Parmi les plus connus, citons les familles *Gaobot, Spybot* et *Randex*. Pour s'implanter, ils utilisent des méthodes classiques : s'ils ne sont pas eux même autoreproducteurs, ils s'installent sur les machines non protégées qu'ils rencontrent par le biais du courrier électronique (spam) ou d'une vulnérabilité exploitée à l'occasion d'une visite sur un site Internet qui les diffuse.

Ce sont souvent des vers à propagation lente. Chaque variante est créée dans un but précis. La diffusion se limite parfois à une entreprise ce qui rend la détection parfois difficile. Une fois sur la machine, le robot attend des ordres venant d'un serveur distant. Il peut alors capturer de l'information, participer à des attaques groupées (DDoS) et servir de relais de spamming, de phishing et d'émission de mails infectés.

Leur durée de vie est courte, c'est leur nombre qui fait leur force. Ils sont créés, distribués afin de créer un réseau de robots *(botnet*) et rapidement utilisés. Ils attendent d'être sollicités par leur concepteur ou par ceux qui louent leurs services. Certains outils commerciaux douteux s'en servent comme intermédiaires.

2.4 Fonctionnalités

2.4.1 Modes d'infection

Les différentes techniques décrites ci-dessous s'appliquent principalement aux virus programmes.

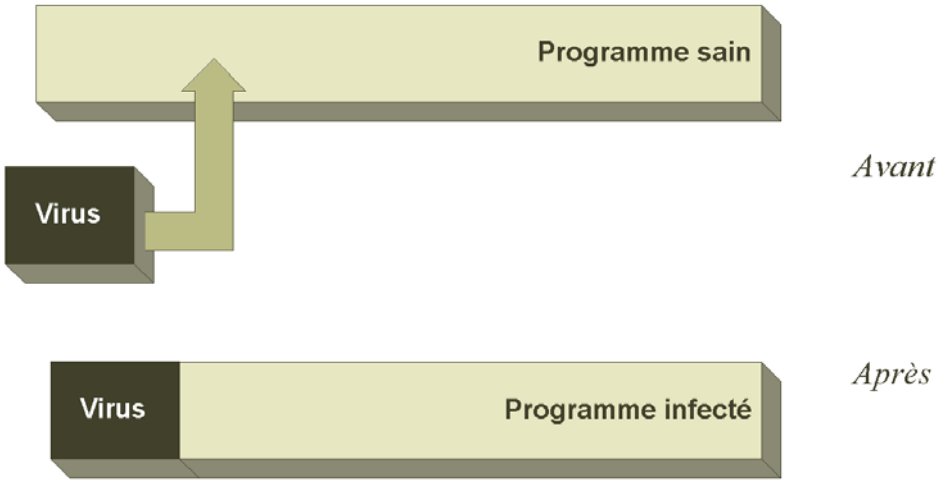
Certaines d'entre elles s'appliquent néanmoins aux virus interprétés. Il existe en effet des virus « par recouvrement » et « par ajout » parmi les macro-virus et les virus de script.

2.4.1.1 Recouvrement

Un virus par recouvrement se contente d'écraser partiellement ou en totalité le programme qu'il infecte. En conséquence, il le détruit au moins partiellement et rend son éradication impossible. Dans certains cas, la taille du programme infecté n'est pas modifiée ; dans les cas contraires, celle-ci s'ajuste à la taille du code viral et devient identique pour tout fichier infecté.

La destruction, même partielle, du code originel fait que celui-ci ne peut plus fonctionner correctement. Ces virus ne sont généralement pas résident en mémoire. Ne réalisant plus la fonction souhaitée, l'utilisateur les détecte rapidement. Les virus agissant par recouvrement ne réussissent jamais à se disséminer largement.

Exemple : BadGuy, W32/HLL.ow.Jetto, LINUX/Radix.ow, VBS/Entice.ow.

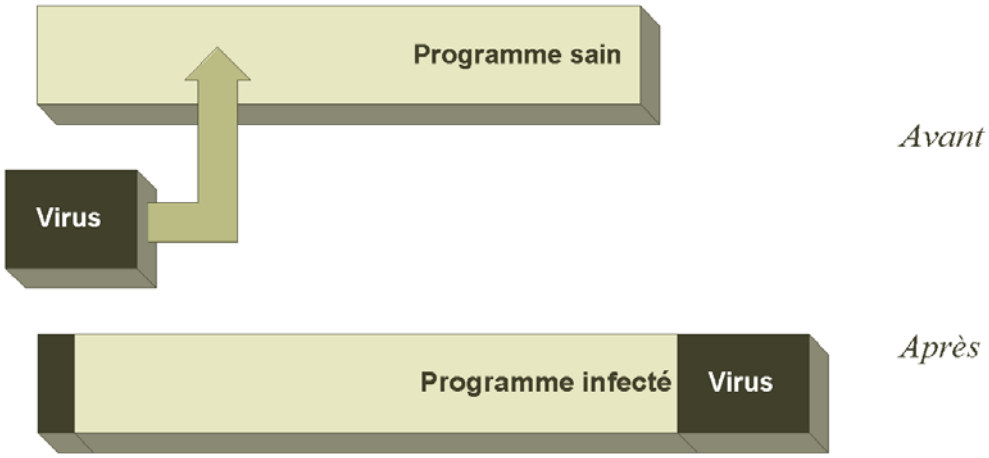


Le virus écrase une partie du code du programme hôte

2.4.1.2 Ajout

Un virus par ajout modifie un programme sans le détruire. Ayant altéré le point d'entrée, le virus s'exécute chaque fois que le programme est lancé, puis lui « rend la main ». Celui-ci fonctionne alors de façon normale. La force d'un virus par ajout est que le programme infecté semble fonctionner correctement ce qui peut retarder la détection du virus. La faiblesse d'un virus par ajout est que la taille du programme est augmentée de la taille du virus, ce qui rend un repérage fondé sur la variation de la taille des programmes possible.

Exemples: Cascade, Jérusalem, W95/Anxiety, W32/Chiton, VBS/Daydream.

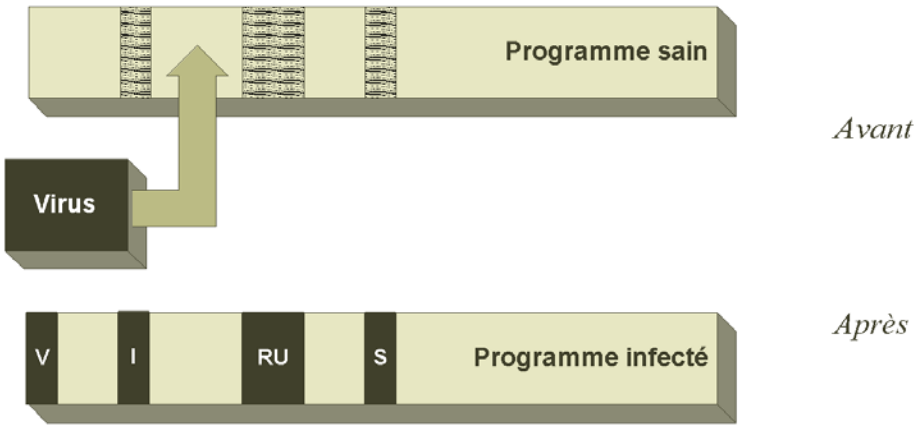


Le virus greffe son code sur le programme hôte

2.4.1.3 Cavité

Connaissant la structure spécifique du type des programmes à contaminer, le virus modifie le point d'entrée du programme et insère tout ou partie de son code dans différentes zones non utilisées. Le fichier *COMMAND.COM* fut longtemps la cible privilégiée de ce genre de virus ; dans ce cas, le code viral pouvait se situer entre le bloc de code, le bloc des données, le bloc de pile « *stack* ». Cette technique est maintenant régulièrement rencontrée dans les environnements Windows.

Exemple : W95/Caw.



Le virus morcelle son code en modules insérés dans les espaces inoccupés du programme hôte

2.4.1.4 Point d'entrée obscur

Avant infection, l'analyse du programme cible permet un positionnement du point d'entrée du code viral en un lieu variable au sein du fichier. Le point d'entrée du programme et les instructions qui s'y situent sont inchangés. Lorsque cette technique est associée à une infection par cavité et à un codage polymorphique, la détection devient très problématique. Cette technique est maintenant régulièrement rencontrée dans les environnements Windows. Elle est très pénalisante pour les anti-virus qui doivent parfois élargir fortement leur zone de recherche.

Exemple : W95/Orez.

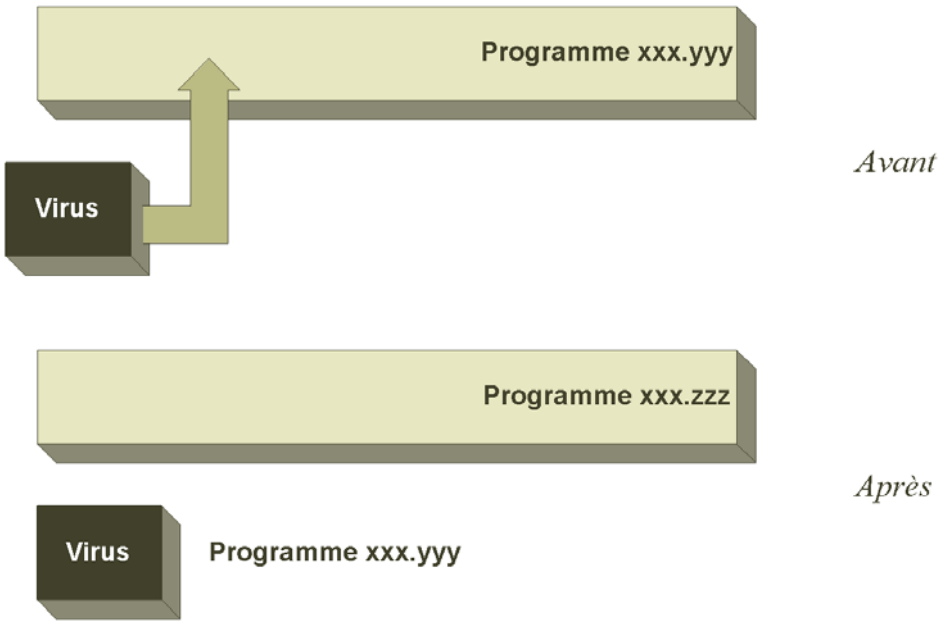
Le virus place son point d'entrée dans un endroit variable du programme hôte

2.4.1.5 Par virus compagnon

Il existe une préséance d'exécution pour les fichiers exécutables : les *.BAT*, puis les *.COM*, puis les *.EXE*. Le virus compagnon va donc créer de toute pièce un fichier du même nom que le programme choisi pour cible mais avec une extension différente. Si, lors de son appel à exécution, le nom seul est utilisé (ce qui est généralement le cas), ce sera le code viral qui s'exécutera en premier. Il donnera ensuite la main au programme original pour ne pas risquer d'alerter l'utilisateur.

Pour durcir son éventuelle détection, certains virus placent leur code dans un autre répertoire, prioritaire au sein de la variable système *PATH*.

Exemple : BAT/bx.cmp, W95/Spawn.cmp.



Le programme hôte est inchangé, un programme de même nom est ajouté sur le disque

2.4.1.6 Par virus délocalisé

Le virus exploite le principe de fonctionnement de la table d'allocation des fichiers pour faire pointer tous les fichiers exécutables contaminés vers le groupe (ou « cluster ») contenant le code du virus. Une fois le code exécuté, celui-ci rend la main au programme initial.

Ces virus sont peu nombreux mais peuvent s'avérer dangereux pour l'intégrité des supports qu'ils infectent. En effet, les utilitaires testant l'intégrité d'un disque découvriront des anomalies (fichiers croisés) et se proposeront de les corriger en entraînant des destructions irrémédiables.

Exemple : Dir-II.

2.4.2 Gâchette de déclenchement

De nombreux virus n'ont aucun module de déclenchement. Ils ne font que se propager en induisant des perturbations que d'aucuns pourraient considérer trop rapidement comme mineures. D'autres mettent immédiatement en œuvre une fonctionnalité perturbatrice ou destructrice. Il serait très dangereux de considérer les seules éphémérides comme moment de déclenchement de la charge virale. Il existe une grande variété de gâchettes, voire la combinaison de plusieurs ou un déclenchement aléatoire !

- date (anniversaire, mensuelle, hebdomadaire),
- heure,
- comptage (nième duplication),
- délai écoulé depuis l'infection initiale sur le système,
- présence d'un matériel ou d'un logiciel,
- combinaison de touches frappées au clavier.

2.4.3 Charge virale

L'époque des animations graphiques et des actions de reformatage rudimentaire est révolue. On observe aujourd'hui des effacements de fichiers ciblés et des désactivations sournoises de logiciels de sécurité (anti-virus non à jour, firewall…).

L'utilisation du virus pour l'installation de portes dérobées, l'atteinte à la confidentialité des données et la collecte de mots de passe sont de nos jours de pratique courante. Les auteurs de virus se rapprochent des pirates informatiques isolés ou organisés.

Remarquons tout de suite qu'*il n'existe pas aujourd'hui de virus inoffensif*. De par son caractère non désiré, le virus coûte de l'argent pour sa désinfection (achat et mise en exploitation de logiciels de sécurité, temps-homme en sensibilisation et intervention). De plus, il y a toujours le risque d'un sur-accident lorsqu'une désinfection est effectuée sans les compétences requises ; ou encore de générer un dysfonctionnement en fonction d'une spécificité des applications ou des équipements installés. Un virus système anodin conçu pour un environnement FAT/DOS peut s'avérer éminemment destructeur sous NTFS ou Linux.

2.4.4 Fonctionnalités supplémentaires

Les fonctionnalités décrites dans ce paragraphe sont généralement mises en œuvre pour tenter de contrecarrer l'action des logiciels anti-virus.

Ainsi, un virus polymorphe rend plus délicat l'emploi d'un logiciel de détection par signature. Un virus utilisant la technique du point d'entrée obscur risquera de passer au travers d'un contrôle seulement effectué sur le début et la fin du programme surveillé. Un virus défensif désactivera un anti-virus actif en mémoire vive et non à jour.

Fort heureusement, il existe toujours des solutions.

2.4.4.1 Anti-debug

Qualificatif appliqué aux virus utilisant des séries d'instructions ou algorithmes rendant impossible un désassemblage via les outils dédiés à cet effet. Le chercheur devra neutraliser ces fonctions avant de pouvoir entreprendre sa recherche.

2.4.4.2 Crypté

Le terme *crypté* est historiquement utilisé de manière impropre en lieu et place du terme chiffré. Dans tout ce document, nous avons pris le parti de ne pas déroger à cette habitude. Un tel virus se décompose donc en 2 parties : un programme de *décryptage* et une suite d'instructions *cryptées* qui forment le corps du virus. L'algorithme utilisé est stable mais peut rendre le désassemblage plus délicat.

2.4.4.3 Défensif

Qualificatif s'appliquant aux virus ayant des fonctions de protection, voire d'attaque, contre les logiciels anti-virus non à jour au moment de leur apparition.

2.4.4.4 Furtif

Qualificatif s'appliquant aux virus camouflant leur présence en renvoyant à chaque requête du système d'exploitation une information erronée mais conforme à celle qui serait retournée dans un environnement sain.

2.4.4.5 Générateur de chiffrement

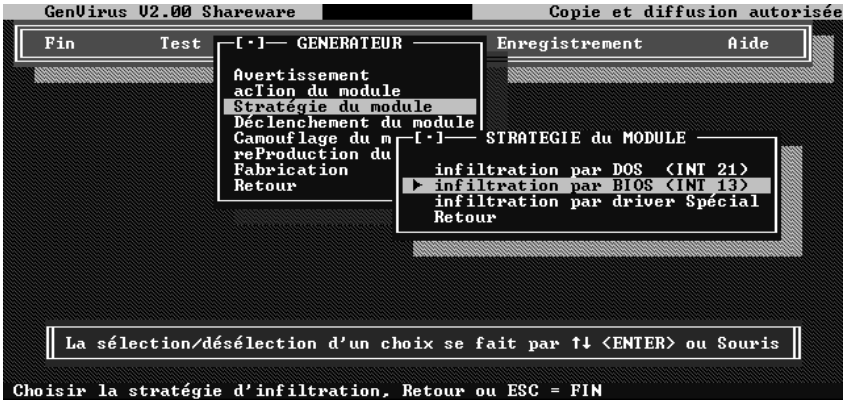
Programme permettant de rajouter une fonction de cryptage, plus ou moins évoluée, au sein d'un virus ne possédant pas cette fonction. Il existe aujourd'hui de nombreux programmes de la sorte. Même s'il est considéré comme simpliste aujourd'hui, le plus médiatique d'entre eux fut écrit par « Dark Avenger » en 1991.

```
MuTation Engine <tm>

Version 0.90ß (17-08-91)

(C) 1991 CrazySoft, Inc. written by Mad Maniac.

1.  License

You are free to include this Engine in viruses. Using it in another ways is
prohibited. You are free to give it to people that will only use it in this way.
MuTaion engine is free.

2.  How it works

Please read the whole document before trying to do something with the Engine.

If you have never written a virus in Assembler, DON'T start with the Engine.

First do this, then return back to the Engine.

MuTation Engine is an object module that could be linked to any virus.It has been
written in Assembler and assembled under Turbo Assembler 2.5. We recommend that you
use this assembler to compile the viruses that will carry the Engine.

Linking it to an object file produced by other assemblers, or high-level languages
compilers is theoretically possible, but we never tried and do not recommend it.
We decided NOT to give up the Engine's source code at this time.

The Engine will encrypt your code each time with a different encryption key. It
will also generate a routine to decrypt it, which will also differ each time. Both
the decryption routine and the encrypted code will have variable lengths.

Thus your virus will be hardly detectable.  The Engine's code is about 2KB; we
believe this is not too big.


8. Final Notes

Well, that's for now.  No time for more. Look at the demo virus and other sample
files included here to get an idea how can you use it. After you include it in your
virus, please check carefully if the Engine does what you expect it to do. Feel
free to experiment with it. If you have problems using it, or have any comments or
suggestions about it, write a message to Dark Avenger at the:

Virus eXchange BBS in Sofia

Phone number: (+359)-2-??-????

Working hours: 20:00 - 06:00 GMT (in the winter)

               19:00 - 05:00 GMT (in the summer)

The latest release of the Engine should also be available at that BBS.

Pass the Engine (all files together in an archive) to virus programmers only.

Greetings to all virus programmers

CrazySoft, Inc.

Bulgaria
```

Extrait de la documentation du Mutation Engine

2.4.4.6 Générateur de virus

Programme permettant la fabrication de virus sans avoir de connaissances particulières. Ces applicatifs sont souvent conviviaux (souris et menus déroulants). Ils ne représentent pas une véritable menace, car une signature du générateur est généralement décelable sur chaque infection créée. Il existe aujourd'hui de nombreux générateurs.



Genvirus

2.4.4.7 Infecteur rapide (*fast infector*)

Virus qui n'attend pas l'exécution d'un programme pour le contaminer. En mémoire, une simple opération d'ouverture d'un fichier sain (exemple de la commande DIR) suffit pour qu'il puisse être infecté.

2.4.4.8 Polymorphe

Qualificatif appliqué aux virus changeant leurs instructions ou simplement leur ordre à chaque infection. Il correspond en fait à un virus crypté ayant intégré dans son programme de décryptage un algorithme de mutation. Il devient ainsi difficile de détecter le virus par une chaîne d'octets sans avoir préalablement *décrypté* son code.

2.4.5 Principes d'identification

Malgré les efforts du CARO (Computer Antivirus Research organization), il n'existe pas aujourd'hui d'organisme centralisateur unique pour l'identification de nouveaux virus. Le chercheur qui détecte une infection essaye de trouver un nom significatif, sans toujours suivre des règles précises.

2.4.5.1 Les différents critères

On utilise couramment la taille en octets *(4096)*, un extrait du message qui apparaît soit à l'écran *(Stoned)*, soit dans le corps du virus *(Tequila)*, un nom rappelant l'effet principal du virus *(Disk Killer)* ou encore un numéro associé à un nom lorsqu'il existe de nombreuses variantes *(V2P6)*.

Cette anarchie est parfois source de confusion lorsque deux éditeurs anti-virus appellent différemment un même virus *(Jerusalem = Israelian = PLO = Friday the 13th*), ou lorsqu'un même virus est appelé différemment d'une version à l'autre d'un même produit anti-virus.

2.4.5.2 Essai de normalisation du CARO

Le CARO est une association internationale informelle regroupant un certain nombre de chercheurs anti-virus. C'est un lieu d'échanges privés entre spécialistes. L'un de ses rôles est l'unification des noms des virus ; il permet aussi aux spécialistes des échanges rapides et sécurisés. Il n'a aucune ouverture vers le public et les médias.

Le CARO a édité en 1991 un document explicitant cette normalisation dans le choix et la forme du nom des virus. Ce document a été remis à jour en 1993 (il est disponible sur demande auprès du CLUSIF). En 1996, le CARO, et plus particulièrement Vesselin Bontchev, proposèrent la normalisation du nom des macros virus. C'est cette règle qui est généralement utilisée par la profession.

Le dernier document public du CARO fut établi avant l'apparition des macro-virus, des virus de Script, des vers, etc. Certains membres de cette association militent aujourd'hui pour sa mise à jour qui interviendra peut-être en 2005.

2.5 Les autres environnements

2.5.1 Virus sur Macintosh

Il existe moins d'une centaine de virus sous l'environnement Macintosh. Les virus du monde Windows sont sans effet sous cet environnement à l'exception de certains virus de macro.

Les raisons généralement invoquées pour expliquer ce faible nombre sont :

- La sécurisation de l'installation des applications sur OS X,
- Un développement en *open source*,
- Un intérêt moindre pour les auteurs de virus par rapport au nombre beaucoup plus important de machines installées sous Windows.

On notera que les systèmes d'exploitation Macintosh font plus l'objet d'attaques de type cheval de Troie ou exploitation d'une faille de sécurité au niveau système d'exploitation ou au niveau applicatif.

Parmi les virus Macintosh, on peut citer : MacMag, nVIR, Hpat et Init29.

2.5.2 Linux et les systèmes d'exploitation Unix

La grande nouveauté offerte par le système Linux fût la stabilité du système d'exploitation. Toutefois, il n'est pas intrinsèquement sécurisé et encore moins de manière permanente. De nombreuses failles, parfois critiques, sont rendues publiques mais l'environnement du logiciel libre permet une grande réactivité au niveau mondial dans la mise à disposition de correctifs de sécurité.

Le mythe qui consiste à dire qu'Unix est insensible aux virus persiste toujours. Signalons tout d'abord que les virus système dédiés au DOS peuvent tout à fait affecter une machine fonctionnant sous Unix. Il n'y aura pas propagation mais activation éventuelle de la charge virale (si elle existe) ou corruption du processus de démarrage.

Les projecteurs sont souvent braqués sur Linux, quelques virus existent cependant dans les environnements BSD et SunOS. Les virus possédant dans leur intitulé le préfixe Unix sont multi plates-formes.

Les virus Unix existent depuis longtemps. Le premier d'entre eux date de 1997 et se nomme Linux/Bliss. Dans un premier temps ils furent simples et non-résidents en mémoire. Ils sont maintenant aussi performants que les virus 32bits Windows. Ils mettent en œuvre des techniques pointues de polymorphie et utilisent, pour certains, la technique du point d'entrée obscur qui rend leur détection plus difficile que par le passé.

En juin 2002, exploitant sans imperfection ces dernières techniques, apparaît {W32, Linux}/Etap.D. Cette notation indique que ce virus, premier du genre, est à même d'infecter aussi bien les machines Windows que les machines Linux. Egalement connu sous le nom de {Win32, Linux}/Simile.D, il vérifie, à sa première exécution, la date du jour. S'il s'agit du 17 mars ou du 17 septembre (sous

Windows) ou du 17 mars ou du 17 mai (sous Linux), il affiche une boîte de dialogue précisant son créateur : un certain Mental Driller, du groupe 29A (concepteurs de virus).

2.6 Les autres éléments perturbateurs

2.6.1 Farces

Comme leur nom l'indique, les canulars ou les farces (*jokes* en anglais) sont conçus pour faire rire. Ils ne se reproduisent pas et ne sont donc pas des virus. Ils n'ont aucune activité destructrice.

Certains sont cependant difficiles à désactiver, d'autres n'hésitent pas à modifier la configuration de l'ordinateur. La limite entre « farce » et programme indésirable ou malveillant est donc étroite. Tout le monde ne possède pas la même dose d'humour et la classification peut varier d'un éditeur à l'autre. Lorsqu'il peut s'avérer perturbateur, le canular est généralement détecté par l'anti-virus. Il y aura parfois lieu d'activer certaines options particulières de recherche.

Les principaux effets des canulars sont :

- affichage d'un message, une image ou une animation,
- manipulation du lecteur de CD-ROM,
- simulation de l'effacement de fichiers ou du formatage du disque,
- retournement de l'écran ou perturbation de l'affichage,
- perturbation de la souris ou de l'usage du clavier,
- simulation d'un programme valide,
- ouverture d'une multitude de fenêtres.

2.6.2 Rumeurs (hoaxes)

Un *hoax* est une rumeur malveillante et non fondée qui est diffusée dans le but de leurrer ou de nuire. Dans la vie courante, les rumeurs ont toujours existé dans différents contextes sociaux, militaires, politiques ou économiques.

Dans le domaine de la propagande, le réseau Internet est un vecteur de choix. La malveillance et la naïveté ont entraîné depuis 1997 une multiplication des rumeurs. L'introduction massive des messageries a fait le reste.

Les rumeurs qui perturbent le monde de l'informatique annoncent généralement l'apparition de nouvelles menaces imminentes et hautement destructrices qu'aucun outil de sécurité ne peut intercepter.

Certaines sont bien connues maintenant mais continuent néanmoins à circuler. Notons par exemples :

- Join The Crew
- A Moment Of Silence
- Bud Frogs Screen Saver

- Buddylst.zip
- Deeyenda
- Good Times
- Guts to Say Jesus
- Irina
- Penpal Greetings
- Win a Holiday

Elles sont souvent d'origine anglo-saxonne mais, pour la plupart, elles ont été traduites en français pour une meilleure (!) diffusion dans l'hexagone.

On retrouve dans l'exemple ci-après la plupart des critères qu'une rumeur doit remplir pour réussir à leurrer son monde :

- Existence d'un enjeu ou intérêt significatif.
- Sensationnalisme. La rumeur est de nature à « appâter » les médias qui en sont avides (recherche de scoop), l'opinion publique qui y est sensible ou une communauté Internet particulière. La présentation est « accrocheuse ».
- Accréditation effective de la rumeur par ces médias ou à travers des internautes (imitation de styles ou de dialectiques crédibilisant la rumeur aux yeux de la communauté visée). Les relais sont connus et dignes de foi.
- Existence d'embryons de « preuve » pour que la rumeur ne soit pas rejetée d'emblée mais, dans le doute, bien prise en compte.
- Incitation à la propagation.

```
MISE EN GARDE ..... URGENT ..... URGENT... URGENT


ATTENTION VIRUS !!! - ATTENTION!

Si vous recevez un e-mail intitule "  WIN A HOLIDAY "

NE L'OUVREZ PAS.  !!!!!!!!!!!

Le virus qu'il contient va effacer l'intégralité de votre disque
dur. Faites suivre ce message a autant de personnes de votre
connaissance. Ceci est un nouveau virus, très nocif et peu de
gens connaissent son existence. Cette information a été rendue
publique par Microsoft.

A titre de prévention, échangez cette information avec tous ceux
qui peuvent avoir accès a Internet.

Nous vous conseillons très fortement d'adresser une copie de ce
message a tous les correspondants inscrits dans votre carnet
d'adresses, de telle sorte que le virus ne s'étende pas.

De même, n'ouvrez pas ou ne regardez pas tout  message intitulé

"  RETOURNE ou IMPOSSIBLE a DELIVRER " .

Ce virus se répandra dans les composantes de votre ordinateur et
les empêchera de fonctionner.

Détruisez immédiatement tout message portant ces mentions.

Par ailleurs, AOL signale qu'il s'agit d'un virus extrêmement
dangereux et qu'il n'y a aucun remède connu a ce jour.

Prenez des mesures de précaution et faites passer le message à
tous vos amis.
```

De nombreuses rumeurs peuvent être regardées *a posteriori*, comme de simples farces. Cependant, propagées à grande échelle au travers des messageries à l'aide de listes de diffusion, elles peuvent perturber, voire bloquer temporairement le système de communication. Elles entraînent aussi un surcroît de travail conséquent des équipes du centre d'assistance technique (*help desk*) qui doivent traiter les appels des utilisateurs inquiets.

Jusqu'à présent, la plupart de ces rumeurs sont identifiables à leur caractère excessif. Elles visent toutes à faire croire à la présence de faux virus sous une forme ou une autre. Il faut néanmoins s'attendre pour l'avenir à des morphologies de rumeurs beaucoup plus perverses et agressives. Plus difficiles à appréhender, certaines rumeurs d'aujourd'hui peuvent devenir demain des réalités.

Dans tous les cas, il convient de garder une attitude autocritique, lucide et de bon sens. Ne transférez pas ces messages à votre entourage sans avoir au préalable consulté le service informatique de votre entreprise ou des institutions compétentes telles que le CIAC, le CERT-IST ou le site www.hoaxbuster.com

2.6.3 Le courrier non sollicité (spam)

La Commission Nationale de l'Informatique et des Libertés (CNIL) donne du spam la définition suivante : *il s'agit de l'envoi massif et parfois répété de courriers électroniques non sollicités à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact, et dont il a capté l'adresse électronique de façon irrégulière.*

Nous savons tous qu'il est extrêmement facile et peu coûteux d'atteindre des centaines d'individus au travers du courrier électronique. Cela n'a pas échappé aux publicitaires et à divers individus peu recommandables qui se cachent souvent derrière une adresse falsifiée pour inonder nos boîtes aux lettres. L'expéditeur ne connaît pas les destinataires, il ne cible ni ses relations personnelles, ni ses relations professionnelles. Les adresses ont été collectées à grande échelle. On retrouve principalement dans ces courriers :

- des messages à caractère commercial,
- des incitations à la visite de site Web,
- des incitations à la prise de contact (pornographie).

2.6.4 Les arnaques financières

Cet aspect de la malveillance informatique n'est pas précisément à classer dans la famille des rumeurs ou du courrier non sollicité. Il tient directement de la fraude financière.

Le courrier électronique en question prétend provenir du fils d'un haut fonctionnaire, du frère d'un industriel ou encore de la femme d'un ex-chef d'état africain. Il vous explique qu'une importante somme d'argent est bloquée quelque part. Avec votre aide, et en utilisant votre surface financière pour le transfert de fond, votre contact vous explique qu'il serait possible de débloquer ces sommes, et une récompense substantielle vous est proposée si vous acceptez ce contrat.

Si vous répondez à ces mails, votre correspondant vous demandera sans doute d'ouvrir un compte sur une banque africaine en y versant des liquidités pour payer des taxes, des frais d'avocats ou encore des bakchichs qui pourront aider au bon déroulement de l'affaire. Il vous interrogera également sur votre environnement financier en vous en demandant les détails. Il est donc important de ne jamais répondre à ce type de message.

Le *phishing* est une autre technique liée au monde de la finance. Il s'agit d'obtenir des données sensibles afin de commettre des impostures à l'identité et des escroqueries financières. L'imposture débute souvent par la réception d'un courrier non sollicité, l'escroc la réalise en 3 étapes :

1) il se fait passer pour qui il n'est pas (une entreprise connue) pour solliciter les données convoitées auprès des internautes.

2) Il présente des contenus fallacieux qui font illusion (motifs évoqués, faux liens, fausses pages web, etc.).

3) Une fois les données convoitées recueillies, il se fait passer pour qui il n'est pas (les internautes escroqués) afin de se procurer des services ou des biens (argent, marchandises, papiers d'identité et autres documents administratifs).

Des courriels s'annonçant en provenance d'eBay (site d'enchères sur Internet), circulent en avisant les personnes que leur compte semble avoir été piraté. Les utilisateurs du site doivent suivre le lien dans le message s'ils ne veulent pas que leur compte soit suspendu. Ils sont alors re-dirigés vers une page web qui porte le logo d'eBay. Cette page demande tout d'abord le pseudo et le mot de passe. Une fois ceux-ci renseignés, un long questionnaire est proposé et de nombreuses données privées sont demandées.

2.6.5 Les lettres chaînes

Par le passé, des lettres chaînes circulaient par la poste. Elles étaient souvent connues sous le nom de chaîne de Saint Antoine. Elles présentaient un texte de prière à Saint-Antoine qu'il fallait transmettre à ses amis. Dans les pays anglo-saxons, elles se sont aussi nommées chaîne de Saint Jude, en référence au patron des désespérés.

Le courrier électronique est aujourd'hui mieux adapté à cette forme de propagation avec l'instantanéité des échanges, son faible coût et sa capacité d'expédition à des destinataires multiples.

L'expéditeur est souvent l'une de nos relations, proche ou lointaine, qui a retrouvé nos coordonnées dans son carnet d'adresses.

L'appel à la solidarité est le principal objet de ce type de message. Une situation dramatique vous est par exemple exposée. Le message vous encourage à le réexpédier car des fournisseurs d'accès Internet sont censés les comptabiliser pour reverser une somme proportionnelle aux personnes en difficulté.

D'autres chaînes utilisent la crédulité des gens face à l'approche de malheurs annoncés ou de bonheurs futurs selon le renvoi ou non du message en quantité. Là aussi, la meilleure solution est la suppression immédiate du message.

3. ORGANISATION D'UNE DÉFENSE EN PROFONDEUR

L'organisation de la lutte anti-virale passe par la mise en place d'outils de détection et de prévention depuis le poste de travail jusqu'à la passerelle Internet. Il est possible d'identifier 4 niveaux concentriques de risque :

1) le poste de travail et les ressources propres à l'utilisateur,
2) les ressources partagées,
3) les passerelles (réseau et messagerie),
4) le monde extérieur, hors du périmètre de l'entreprise.

L'anti-virus comme seule parade aux virus informatiques actuels ne suffit plus. Certains virus/vers utilisent de nouvelles méthodes de propagation et d'action :

- ils ne résident qu'en mémoire vive et se propagent via le flux Internet,
- ils exploitent des failles liées au système d'exploitation et au réseau,
- ils s'associent à des outils de piratage,
- ils utilisent la technique du « spam » pour initialiser leur propagation.

Les particuliers et les entreprises doivent diversifier leurs dispositifs et améliorer ainsi leur niveau de sécurité. Ces autres outils sécuritaires deviennent au fil du temps indispensables. Cette défense en profondeur est aussi une opportunité pour :

- Une variété dans les ressources de sécurité avec des antivirus de « moteurs » différents entre ceux installés sur les postes de travail, les serveurs, les passerelles Internet quand la taille de l'entreprise devient conséquente ou que sont activité en ligne est critique.
- Le déploiement d'une politique de correctifs qui intègre une phase de test, la surveillance des failles au niveau systèmes d'exploitation et applications mais aussi, qui prend en compte l'ensemble des équipements et ressources présents sur le réseau… routeurs, imprimantes, solutions de sécurité (antivirus, parefeu).

L'aspect humain entre également en jeu ; l'information et la sensibilisation des utilisateurs ne sont pas à négliger. Une fois expliquées et comprises, les règles de base doivent être formalisées dans un document reprenant les points clés de la réglementation interne. Le fait de désactiver l'anti-virus doit être présenté comme une faute grave.

Les tableaux suivants nous montrent aussi que les moyens de prévention et de protection diffèrent selon le niveau concentrique choisi. Une fois ceux-ci activés, la responsabilité des divers acteurs n'en est pas pour autant évacuée. Ceux-ci doivent rester conscients des risques qu'un acte inconsidéré pourrait occasionner à quelque niveau que ce soit.

3.1 Les ressources propres à l'utilisateur

Le poste de travail et les ressources propres à l'utilisateur		
Equipements	**Solutions/Mesures**	**Contraintes/Problématiques**
Poste utilisateur fixe, poste utilisateur nomade, organiseur et téléphone IP	Anti-Virus et Pare-Feu (personnels ou implantés depuis le réseau de l'entreprise) Politique de correctifs	Déploiement des produits et des mises à jour Verrouillage de configuration Responsabilité de l'entreprise suite à un acte engagé par un membre de son personnel. Responsabilité de chaque utilisateur face aux actes qu'il commet.

La protection du poste de travail est déterminante. Chaque poste de travail doit être muni de son anti-virus. Même si le virus pénètre la passerelle Internet dans un format non reconnu, même s'il n'est pas détecté sur le serveur, il doit être intercepté avant que l'utilisateur n'ait son poste infecté.

Maintenir à jour le logiciel anti-virus de la station de travail est l'une des tâches les plus ardues de l'administrateur système. Ceci est spécialement le cas sur les équipements nomades qui ne sont pas connectés en permanence au réseau. Les sociétés développant des anti-virus offrent leurs propres outils de déploiement. Dès qu'un parc informatique devient moindrement important, leur utilisation devient indispensable.

Il est aussi impératif de pouvoir verrouiller la configuration choisie afin d'éviter une modification de la configuration ou une désactivation volontaire ou involontaire de l'anti-virus.

Associé à l'anti-virus, le pare-feu personnel est indispensable sur un poste portable. Il permet le passage sélectif des flux d'information entre la machine et le réseau interne et/ou public. On le trouve également sur des postes d'exploitation (*process*) qui sont interfacés avec les automates ou les applications de fabrication industrielle ; et pour lesquels, le déploiement de correctifs est délicat de façon automatique en raison des conditions d'exploitation.

Le pare-feu personnel s'installe directement sur la machine de l'utilisateur, qu'il soit un particulier ou un employé « nomade » de l'entreprise.

Les mises à jour critiques qui s'appliquent au système d'exploitation doivent être appliquées de manière rigoureuse. Il faut aussi en apprécier les criticités :

- Celle intrinsèque à la faille rendue publique,
- Celle par rapport à l'usage de la ressource qui en fait dans l'entreprise. L'analyse de risque dans l'entreprise, pour prendre en compte ces nouvelles menaces à peine caractérisées doit donc s'appuyer une action de veille.

Pour le poste de travail, l'automatisation de l'installation des correctifs de sécurité demeure l'option recommandée. Les personnes ayant une connexion lente peuvent demander à Microsoft l'envoi d'un kit qui contient l'ensemble des mises à jour critiques pour Microsoft Windows.

Des offres de sécurité existent aujourd'hui pour les PDA. Elles protègent ces équipements contre les quelques virus et chevaux de Troie actuels mais ne s'attaquent pas aux menaces émergentes.

3.2 Les ressources partagées

Les ressources partagées		
Equipements	**Solutions /Mesures**	**Contraintes/Problématiques**
Le serveur de données, le serveur de fichiers, l'imprimante, le photocopieur numérique et le PABX (autommutateur téléphonique	Antivirus Politique de correctifs	Outil de déploiement Dégradation de la bande passante interne Certains virus induisent des dysfonctionnements d'imprimante réseau (W32/Codered)

L'application des mises à jours critiques, des correctifs (« patchs ») et des mises à jour applicatives ou systèmes s'étendent aussi aux ressources partagées. Les administrateurs devront de préférence utiliser des outils dédiés qui en gèreront le déploiement. Ces gestionnaires de correctif et de configuration aideront et superviseront tous les processus de mise en place.

Rappelons qu'il est très fortement déconseillé de naviguer sur Internet à partir d'un serveur. Ce procédé semble très pratique pour récupérer un correctif, consulter une base de connaissances, mais il vaut mieux le faire d'une autre station, et obliger les intervenants extérieurs à faire de même.

Même si l'anti-virus risque d'induire une dégradation dans la vitesse du trafic, celui-ci est fortement conseillé en entrée/sortie des serveurs de données.

Les périphériques modernes et les PABX actuels peuvent contenir un système d'exploitation vulnérable et faire l'objet d'attaques de tous ordres, y compris virales.

3.3 Les passerelles

Les passerelles		
Equipements	**Solutions/Mesures**	**Contraintes/Problématiques**
La passerelle Internet, le serveur de messagerie et le routeur	Anti-virus, pare-feu, anti-spam, IDS/IPS et filtrage de contenu, d'URL, de port… Politique de correctifs	Responsabilité de l'entreprise en cas de pollution extérieure.

Nous sommes à la porte d'un monde qui peut s'avérer hostile. La mise en place d'un anti-virus et d'un architecture de pare-feu est ici de la plus grande importance. Ces équipements complèteront les dispositifs précédemment décrits en protégeant le réseau interne de l'entreprise lorsque celui-ci débouche vers l'extérieur.

Les anti-virus pour passerelles devront traiter le plus grand nombre de types de trafic (FTP, HTTP, SMTP…) et savoir analyser un large panel de formats de documents. Ils devront aujourd'hui prendre en compte les flux de messagerie instantanée ou ceux des téléchargements poste à poste ou encore de la téléphonie sur IP

Le contrôle de contenu est une solution de surveillance dédiée à la messagerie électronique et à la navigation Internet (HTTP, FTP…). Outre le fait que certains de ces outils savent détecter les virus et autres codes malveillants, ils permettent une analyse lexicale par mots clés dans les mails ou dans les URL.

L'installation d'un logiciel anti-spam permettra de bloquer ou de limiter la prolifération des messages non-sollicités ou les phénomènes de *mailbombing*.

Fonctionnant comme des solutions anti-virus ou anti-spam, les systèmes de détection d'intrusions (IDS, *Intrusion Detection System*) se réfèrent à une base de signatures d'attaques connues. Elles ne peuvent détecter que celles dont elles possèdent la signature.

Afin de donner à leur solution plus de réactivité lorsqu'une attaque surgit, certains éditeurs ont décidé de transformer leur offre en IPS (*Intrusion Prevention System*) et axent leur technologie vers la prévention proactive, capable de réagir en temps réel lorsqu'une anomalie est détectée ou qu'une intrusion est avérée. L'équipement fonctionne selon des règles de comportement et de signatures d'attaques : il surveille les attaques en dépassement de tampon (*buffer overflow*), les élévations de privilèges, les chargements en mémoire, les modifications critiques du système d'exploitation, l'utilisation excessive du CPU, la diminution soudaine de la bande passante, etc.

Les équipements signalent des divergences par rapport au fonctionnement normal des éléments surveillés. Contrairement au pare-feu, qui traite des requêtes et les interdit, de tels systèmes les analysent de façon continue et ne réagissent qu'en cas d'anomalie.

3.4 Le monde extérieur

Le monde extérieur		
Equipements	**Solutions/Mesures**	**Contraintes/Problématiques**
Le poste domestique, les fournisseurs d'accès à l'Internet (FAI), les autres entreprises et leurs réseaux	Scanner de vulnérabilité	Responsabilité « d'un inconnu » à l'entreprise suite à un acte qu'il engage volontairement ou non.

Une fois l'entreprise sécurisée, le monde extérieur n'a pas disparu.

Tout ordinateur domestique est une source potentielle d'attaque au regard du virus qu'il est susceptible de contenir :

- le virus peut contenir un module d'attaque ciblant votre entreprise,
- le virus peut retrouver sur la machine des URL et adresses de messagerie qui vous correspondent.

Des scanners de vulnérabilité peuvent permettre de faire un audit en évaluant la résistance des machines au sein d'un réseau protégé. Un outil efficace doit savoir détecter les failles et préconiser des solutions.

Au delà des dispositifs techniques de sécurité, il faut aussi utiliser toutes les dispositions contractuelles ou légales disponibles : des lois récentes précisent les responsabilités des acteurs, accroissent les obligations des fournisseurs en matière de traçabilité. On peut enfin noter un renforcement du nombre de policiers ou de gendarmes spécialisés dans la lutte contre la cybercriminalité.

3.5 La dimension humaine

En temps qu'utilisateur ou administrateur système, l'homme se retrouve acteur et responsable à tous les niveaux. La formation et l'information doivent être au cœur du dispositif organisationnel. La sensibilisation n'est jamais définitivement acquise, elle doit faire l'objet de rappels périodiques et adaptés. Ces dispositions doivent se concrétiser dans :

- une politique de charte,
- un règlement intérieur.

Il est possible de nommer des correspondants sécurité qui pourront servir de relais bidirectionnels dans leur environnement proche.

En prise directe avec les utilisateurs, le centre d'assistance (*help desk*) doit travailler en lien étroit avec l'équipe sécurité. Celle-ci doit savoir comment réagir face aux interrogations des utilisateurs et évaluer la pertinence d'une mise à jour forcée et anticipée des outils de protection. Elle doit aussi pouvoir évaluer un risque ponctuel imposant un changement temporaire du niveau de sécurité appliqué (blocage d'une nouvelle extension de fichier, passage au mode d'analyse heuristique, etc.).

Les fiches d'intervention ou de procédures seront adaptées pour prendre en compte la spécificité de traitement pour l'alerte en cours de traitement.

Selon l'importance de l'entreprise on envisagera ou non, la mise en place d'équipes d'astreinte (pour la veille technologique et l'intervention) pouvant aller jusqu'au 24/24 – 7 jours sur 7.

3.6 La politique de mises à jour

Nous recommandons la mise en place de procédures automatiques qui se calquent sur la périodicité des mises à disposition de mises à jour par le fournisseur de l'anti-virus installé. Seule cette acceptation peut permettre une réactivité suffisante face aux menaces actuelles.

Ces mises à jour automatiques pourront se faire de manière ordonnancée en privilégiant le périmètre et les serveurs vitaux. Encore une fois, en prenant en compte le systèmes d'exploitation, les applications et tous les équipements critiques présents : routeurs, imprimantes, antivirus, pare-feux, etc. Comme pour tout déploiement logiciel, une procédure de test incluant la non régression vis-à-vis de l'environnement d'exploitation permettra d'éviter le sur-accident d'un dysfonctionnement bloquant une ressource ou le réseau.

On n'oubliera pas d'appliquer de manière régulière les correctifs (*patches*) liés aux systèmes d'exploitation. Il est souhaitable d'envisager des mises à jour mensuelles ou plus rapprochées en fonction de la criticité avérée.

3.7 La politique de paramétrage

Les virus s'attaquent souvent à des logiciels ou à leurs failles, ils s'introduisent parfois par le biais de fonctionnalités inutilisées en environnement professionnel. D'une manière générale, les installations « standards » des OS sont singulièrement vulnérables. Retirer certaines fonctionnalités « grand public » telles que le partage de fichier ou le partage de bureau « Netmeeting » permet d'obtenir des postes plus performants et moins sensibles aux virus. Par ailleurs, les correctifs à appliquer en sont d'autant moins nombreux et la gestion du parc s'en retrouve affermie.

Le paramétrage des applications, en particulier la navigation Internet et la messagerie, doit faire l'objet de procédures scrupuleuses. Le navigateur de Microsoft est particulièrement visé par les virus, au delà des correctifs à appliquer régulièrement, il faut renforcer la sécurité en modifiant les paramètres de navigation par défaut qui sont parfois très permissifs (exemple : ouverture automatique de contenus actifs). Rappelons que dans les premières heures d'apparition d'un virus, les anti-virus sont parfois inefficaces. Ne pas ouvrir *automatiquement* les pièces jointes est donc la meilleure des parades. Le principe de prudence serait de rendre « passive » une navigation sur Internet, et de n'accepter que le contenu actif (Java™, scripts, ActiveX®, cookies) de sites choisis. Ce paramétrage pouvant être bloquant sur certains sites mal développés, l'utilisateur doit être formé comme cela a déjà été indiqué plus haut.

Le client de messagerie standard Microsoft étant basé sur le paramétrage de sécurité du navigateur, on voit bien l'importance de ce type d'action.

4. TYPOLOGIE DES PRODUITS ANTIVIRUS

La plupart des anti-virus ne mettent pas en œuvre une seule méthode de détection, mais un « panachage » de celles-ci. Ce sont la qualité des méthodes et le dosage de l'une par rapport à l'autre qui font la différence.

4.1 Les méthodes de détection

Au nombre de 5, elles ont chacune leurs particularités et leurs limites.

A l'exception du monitoring de programme, ces méthodes peuvent être mises en œuvre « à la demande » de l'utilisateur ou s'activer automatiquement « sur accès » à un fichier ou une ressource. Ces modes sont aussi appelés statique et dynamique.

Chaque méthode a ses limites. Les auteurs de virus en connaissent parfaitement le fonctionnement. Au fil du temps, ils découvrent de nouvelles techniques qui peuvent leurrer les scanners heuristiques, génériques ou comportementaux. Ces moteurs « intelligents » sont, eux aussi, régulièrement mis à jour et l'utilisateur doit suivre ces évolutions.

Ces méthodes sont également sujettes à des fausses alertes que les mises à jour corrigent au fil du temps.

4.1.1 La recherche par signature

Voici l'un des premiers procédés mis en œuvre dès l'origine des virus. C'est la technique du « scanner » basée sur la recherche d'une chaîne de caractères. Le procédé est fiable mais nécessite des mises à jour fréquentes. Face aux virus polymorphes et aux fichiers compressés, il requiert souvent la mise en place d'algorithmes spécifiques, dont l'efficacité a parfois été contestée.

Pour limiter les temps d'analyse, seules les zones sensibles sont parcourues par le scanner. Elles sont déterminées en fonction de la nature du fichier à analyser et du virus à rechercher.

La recherche par signature ne se limite pas à celle d'une chaîne de caractère stable. Elle s'adapte à la complexité du virus à découvrir. Associée à des processus de décryptage et de décompactage, elle est généralement efficace. En 20 ans, moins d'une trentaine de virus l'ont mise en échec. Pour ces derniers, il a été nécessaire d'inclure des programmes spécifiques comme complément de détection. L'adjonction de telles routines et le perfectionnement des techniques d'émulation et de décompression font qu'il est périodiquement nécessaire de mettre à jour « le moteur » et non pas seulement les bases de signatures.

4.1.2 La recherche générique

En mode résident ou à la demande, la recherche générique peut être considérée comme une recherche par signature que l'on qualifiera de « floue ». Pour une même famille de virus, il est généralement possible d'isoler des séquences de code à la structure identique. Elles sont souvent liées au processus d'infection ou de camouflage (cryptage, polymorphie, *anti-debug*). Ces séquences peuvent correspondre à du code compilé ou à des bribes d'instructions spécifiques rencontrées dans un langage interprété quelconque.

Un travail d'analyse permet d'isoler ces éléments constants. Le résultat se présente sous la forme d'une ou plusieurs chaînes hexadécimales accompagnées, ou non, de jokers (méta caractères tels que « * »). Celles-ci ne sont pas recherchées à un endroit précis mais au sein d'un intervalle que le chercheur doit également définir. La seule localisation de ces indices dans une zone adéquate du fichier indiquera la présence du virus. Il pourra alors s'agir d'une variante connue ou encore inconnue. Les souches détectées sont alors annoncées sous un nom général du type : VBS/LoveLetter.gen@MM ou W32/Gara.gen@MM.

La recherche générique est également très efficace dans la recherche de programmes non-auto reproducteurs inconnus.

4.1.3 Le contrôle d'intégrité

Tout comme les méthodes précédentes, le contrôle d'intégrité est un procédé capable de fonctionner en mode statique ou dynamique. Sachant que toute action virale s'accompagne d'une modification (des fichiers sont modifiés, ou d'autres sont créés) la surveillance débute par l'établissement d'une « photographie de référence » (« code checksum », « CRC : code de redondance cyclique »). Celle-ci s'opère dans un environnement réputé sain. Les données sont ensuite comparées au fil du temps. Si le résultat du CRC a changé (fichier modifié) ou s'il est absent (fichier ajouté), une alerte est émise.

Cette méthode est en théorie infaillible. Des expériences ont cependant été menées par le passé démontrant qu'il était possible d'automatiser la création de couples de fichiers (avant et après modification) répondant au même checksum. Il a ainsi été possible de tromper certains contrôleurs d'intégrité pour peu qu'on en découvre la loi mathématique interne.

Le procédé a néanmoins été fréquemment utilisé dans les environnements MS-DOS et son abandon n'a rien à voir avec une éventuelle fragilité. Celui-ci peut être durci par renforcement de l'algorithme (CRC 32bits, CRC 64bits). Les raisons de la perte d'intérêt de la méthode sont multiples.

En premier lieu, la technique suppose que le poste de travail ne soit pas infecté à l'initialisation de la base de référence. De nombreuses stations avec un virus système ou un ver firent ainsi l'objet d'une « vaccination ». Il fallut attendre plusieurs mois, et l'utilisation d'un scanner à jour pour s'apercevoir de l'infection.

En second lieu, elle ne peut efficacement s'appliquer que sur des équipements stabilisés, exempts de modifications, d'ajouts et de suppressions fréquentes de logiciels. Si ce n'est pas le cas, seules les zones systèmes et quelques répertoires pourront bénéficier de la protection. Il faudra par ailleurs la désactiver à chaque mise à jour, et s'assurer de la provenance et de la qualité des nouveaux fichiers qui seront considérés comme sain.

Les ordinateurs sont aujourd'hui interconnectés, leurs utilisateurs téléchargent chaque jour des dizaines de fichiers et installent de fréquentes mises à jour. L'espace stabilisé au sein d'une machine s'amenuise inexorablement et explique la disparition de la méthode comme procédé de lutte anti-virale.

Plutôt que de créer une base de référence, certains logiciels « marquent les fichiers » en leur ajoutant, comme le font de nombreux virus, quelques octets. Cette méthode est dangereuse à plus d'un titre : le retour en arrière n'est pas toujours optimal et la modification du code exécutable d'un programme peut réserver un jour ou l'autre des surprises…

4.1.4 La recherche heuristique

La recherche heuristique s'apparente à une recherche de singularités au sein des fichiers analysés. Elle ne s'appuie pas sur la connaissance particulière de l'ensemble des variantes d'un même virus, mais sur la structure des fichiers analysés et sur la présence en nombre plus ou moins conséquent d'instructions essentielles à l'ensemble d'une famille virale (macro-virus, exécutables W32, etc.).

La méthode est aujourd'hui fiable malgré quelques fausses alertes qui continuent parfois d'apparaître. La parade consiste à reconnaître ces programmes légitimes dont l'exécution est souhaitée ou normale pour les éliminer d'office avant, après ou pendant l'analyse.

Alors que la méthode générique semble suffisante pour la majorité des virus écrits en langage interprété, la recherche heuristique est particulièrement utile face aux virus programmes. Pour des fichiers exécutables Windows (W32/PE), il est possible de rechercher :

- un point d'entrée dans la dernière section,
- un point d'entrée avant la première section,
- un saut inter-section,
- des caractéristiques de sections inattendues,
- un nom de section inattendu,
- une boucle de décryptage simple ou polymorphe au point d'entrée,
- des instructions inattendues (fonctionnalités d'émission de mails, instructions liées à des « exploits » connus, séquences *anti-debug*, etc.).

Tous les anti-virus modernes utilisent fortement cette méthode en complément de la détection par signature.

4.1.5 Le monitoring de programmes

Il s'agit ici d'analyse comportementale. Elle repose sur l'analyse dynamique des opérations de lecture et d'écriture en mémoire ou sur un support physique. Citons simplement à titre d'exemple trois évènements majeurs qu'il semble bon de surveiller :

- l'écriture en mode physique sur un disque dur,
- la recopie de fichiers entrants dans un répertoire système,
- la modification de la base de registres par un programme non autorisé.

Par le passé, cette méthode était parfois directement couplée à l'anti-virus. Son principal défaut était le déclenchement d'alertes intempestives qu'un utilisateur non averti n'était pas toujours à même d'interpréter : s'agissait-il d'une manifestation d'un virus inconnu ou d'un fonctionnement normal ?

Aujourd'hui, ce procédé est mis en œuvre au sein de produits spécifiques à ce mode de détection. La phase d'installation de ces logiciels dédiés débute par un apprentissage et une reconnaissance des opérations légitimes. La détection qui en résulte dépasse largement la sphère anti-virale pour s'attacher à prévenir tout type d'intrusion. Ces nouveaux produits deviennent indispensables alors que la frontière entre auteurs de virus et criminels informatiques de tout bord s'amenuise de jour en jour.

4.2 L'éradication

Lorsqu'un virus a réussi à traverser les défenses placées sur son chemin, l'entreprise contaminée doit avoir à sa disposition des procédures efficaces pour contenir l'infection et restaurer les équipements infectés pour rétablir leur configuration d'origine sans perte de données.

Face à une infection, et d'un point de vue théorique, un anti-virus doit savoir éliminer tous les virus qu'il rencontre. Les théoriciens indiquent qu'un virus fonctionnel doit être capable d'infecter successivement 2 environnements ou 2 fichiers. Si c'est le cas, le virus est viable : il a su sauvegarder les données qui permettent à l'élément infecté de fonctionner. C'est à l'anti-virus de savoir les restituer.

Pour obtenir l'éradication l'anti-virus doit lancer un processus automatisé inverse. Le succès s'obtiendra après :

1) étude du code viral,
2) comparaison des fichiers sains et infectés,
3) localisation des données déplacées et sauvegardées,
4) marquage des fichiers nouvellement créés,
5) recherche des modifications annexes induites sur le système (par exemple la modification de la base de registres).

En l'absence d'infection locale sur des fichiers préexistants, l'éradication se limite à la destruction du processus en mémoire, l'effacement des fichiers superflus et la suppression des clés de lancement automatique.

Le travail se complique lorsque des fichiers sains ont été modifiés pour accueillir le code viral. Si ces fichiers sont encore opérationnels une fois infectés, il est bon de répéter que l'éradication est toujours techniquement possible. Elle est directement liée à la compétence du chercheur qui doit mettre au point la parade.

De nombreux virus endommagent des fichiers sans pour autant se propager correctement. Les collections virales contiennent des milliers de codes de ce type. Leur exécution entraîne parfois une erreur système qui stoppe l'infection avant qu'elle n'aboutisse. Le système rend généralement la main et rien d'anormal ne semble s'être produit. En anglais, ces virus supposés sont qualifiés d'*intended*.

Si les premières étapes de l'infection virale ont lieu, les fichiers atteints sont généralement corrompus et le retour en arrière par éradication devient impossible.

D'autres virus ne savent pas correctement différencier les fichiers qu'ils sauront infecter de ceux qu'ils détérioreront. Pour les distinguer, certains anti-virus utilisent le suffixe « dam » ou « cor » (en anglais, *damaged* ou *corrupted*) et effacent les souches qu'ils ne peuvent restaurer. L'un des exemples récent est W32/Magistr@MM dont la dénomination W32/Magistr.dam s'applique à de nombreux fichiers définitivement perdus.

5. L'ASPECT JURIDIQUE

5.1 Les actions juridiques possibles

La cybercriminalité recouvre deux types d'infractions :

- les infractions directement liées aux technologies de l'information et de la communication dans lesquelles l'informatique est l'objet même du délit,
- les infractions dont la réalisation est liée ou facilitée par les technologies de l'information et de la communication et pour lesquelles l'informatique n'est qu'un moyen.

L'expérience semble montrer que les délits liés au Système d'Information et réalisés dans un but académique ou ludique sont souvent traités au civil. Les délits facilités par le Système d'Information (délit de droit commun, vol, escroquerie, attaque de site commerciaux, DDoS (déni de service distribué)…) se retrouvent plutôt au pénal.

La responsabilité civile désigne l'ensemble des règles qui obligent l'auteur d'un dommage causé à autrui à réparer ce préjudice en offrant à la victime une compensation. Elle se divise en deux branches selon que les protagonistes sont unis ou non par un lien contractuel. La responsabilité contractuelle est l'obligation de réparer le dommage résultant de l'inexécution d'un contrat ; la responsabilité délictuelle suppose la réparation du dommage causé en dehors de toute relation contractuelle.

La responsabilité civile s'oppose à la responsabilité pénale qui vise à sanctionner l'auteur d'une infraction pénale portant atteinte à l'ordre social. L'auteur d'une infraction pénale et son complice sont condamnés à des peines pécuniaires au profit de l'Etat (l'amende) et / ou à des peines privatives de liberté (prison et droits civiques), tandis qu'au civil les condamnations pécuniaires sont du ressort de la réparation (dommages et intérêts).

5.2 Prise en charge de l'attaque

Si l'on soupçonne une attaque, sa prise en charge passe par :

- l'identification de la victime. C'est l'entité responsable hiérarchique ou fonctionnelle de celle-ci qui décide d'intenter, ou non, d'éventuelles poursuites.
- l'identification du bien altéré :
    - un système d'exploitation ou un logiciel,
    - un site Web,
    - l'image de marque de l'entreprise,
    - une série d'informations confidentielles ou non (SGBD, information financière ou intellectuelle…),
    - une autre cible. Face à la technique du rebond, l'entreprise intermédiaire se retrouve dans le rôle de l'attaquant (involontaire). Elle doit pouvoir faire preuve de sa bonne foi en démontrant qu'elle avait correctement protégé son système. Les vers

informatiques (*@MM* ou *.worm*) peuvent être assimilés à des programmes utilisant la technique du rebond.

- l'analyse de l'impact. C'est au regard de cette évaluation que se décideront les éventuelles poursuites (civil ou pénal).

5.3 L'arsenal juridique en France

L'arsenal juridique destiné à lutter contre les menaces informatiques s'est enrichi de diverses dispositions au cours des vingt dernières années. En effet, il a fallu créer de nouvelles incriminations, celles existantes ne permettant pas d'appréhender les faits qui devaient être réprimés ou le régime des peines associées aux incriminations traditionnelles s'avérant inadapté. Il a fallu en outre mettre à la disposition des services de police et de justice des moyens permettant de poursuivre efficacement le travail d'identification des auteurs des faits incriminés.

Tout comme le reste de ce document, ce paragraphe est le résultat d'un travail collectif réalisé au sein du groupe virus du CLUSIF. Nous nous devons cependant d'indiquer qu'il contient quelques reprises de deux mémoires DESS qu'il nous a été possible de consulter sur Internet :

- Sophie Revol, *les logiciels espions*, DESS Droit du multimédia et de l'informatique,
- Frédéric Duflot, *les infections informatiques bénéfiques : chroniques d'un anathème*, Droit du numérique et des nouvelles techniques.

5.3.1 La responsabilité civile

Suivant que les protagonistes sont unis ou non par un lien contractuel, l'introduction d'un virus peut engager la responsabilité délictueuse ou contractuelle de l'entreprise ou du particulier.

5.3.1.1 Responsabilité civile délictuelle

Un virus pouvant être considéré comme un logiciel, sa mise en place doit être signalée. Elle nécessite l'accord préalable de l'utilisateur du système informatique qui va le recevoir.

L'article 1382 du code civil précise que la mise en œuvre de la responsabilité délictuelle nécessite une faute, un dommage et un lien de causalité entre les deux. Il est envisageable de retenir la responsabilité délictuelle d'une personne qui introduit un virus à l'insu d'un utilisateur dans son système. Dans ce cas, la faute s'apparente à une intrusion dans un système informatique à l'insu de son utilisateur ou à une installation de logiciel sans autorisation. Le dommage consiste en la perte et/ ou l'altération de données personnelles. Il peut entraîner l'octroi de dommages et intérêts dès lors que cette faute est rapportée, qu'un préjudice est prouvé et qu'un lien de causalité est admis entre cette faute et ce préjudice.

5.3.1.2 Responsabilité civile contractuelle

La mise à disposition par un fournisseur d'un logiciel contenant un virus peut entraîner son dysfonctionnement. La responsabilité civile du prestataire peut ainsi être envisagée.

L'introduction du virus peut s'être faite à l'insu de l'utilisateur qui s'est procuré le logiciel chez son fournisseur. L'acquéreur peut engager la responsabilité contractuelle de l'éditeur en raison du non-respect des obligations contractuelles.

Les propriétaires de sites Internet à accès payant peuvent aussi voir leur responsabilité engagée si un virus présent sur leur site a pu s'introduire sur l'ordinateur de leur client.

5.3.2 La responsabilité pénale

Au milieu des années 80, les seuls textes qui ont pour objet la protection des systèmes d'information sont la loi informatique et libertés (6 janvier 1978) et la loi sur la protection du droit d'auteur (3 juillet 1985).

Ces deux lois ne prévoient, ni ne permettent une répression pénale spécifique des menaces informatiques. La prise en compte de la problématique virale et de la cybercriminalité apparaît avec :

- la loi Godfrain relative à la fraude informatique (loi n°88-19 du 5 janvier 1988 relative à la fraude informatique,
- la loi relative à la sécurité quotidienne (loi n° 2001-1062 du 15 novembre 2001),
- la loi pour la sécurité intérieure (loi 2003-239 du 18 mars 2003),
- la loi pour la confiance dans l'économie numérique (loi n°2004-575 du 21 juin 2004),
- la loi relative aux communications électroniques et aux services de communication audiovisuelle (loi n° 2004-669 du 9 juillet 2004),

Ce dispositif législatif est complété par des textes règlementaires en cours d'élaboration, qu'il s'agisse du projet de décret sur la conservation des données de communications électroniques ou du projet de décret sur la conservation des données relatives aux contenus des services en ligne.

5.3.2.1 Prescriptions traditionnelles

La responsabilité pénale peut être engagée en raison d'atteintes aux droits de la personne ou d'atteintes aux systèmes informatiques eux-mêmes. Le Livre III du Code Pénal *« Des crimes et délits contre les biens »* étudie notamment le vol, l'escroquerie et l'abus de confiance.

Le vol d'information n'existe pas en droit pénal. Seul subsiste le vol d'un objet, en l'occurrence un support physique. Le vol ne s'applique donc qu'à une chose *« matérielle susceptible d'appréhension* [physique] *par l'auteur du vol »*. Ni le « vol » de temps machine, ni le « vol » de bande passante ne peuvent être appréhendés par les articles 311-1 et suivants du Code Pénal.

Une escroquerie peut avoir pour objet une chose immatérielle. On peut donc admettre qu'un programme infectieux permettant de se faire remettre une donnée ou facilitant sa remise entre dans le champ de l'article L313-1.

Les biens immatériels semblent exclus des prescriptions liées à l'abus de confiance. En matière de détournement d'une chose remise volontairement, l'article 314-1 s'applique cependant à un bien quelconque et pas seulement à un bien corporel. Il cite certaines valeurs mobilières au titre d'un écrit constitué par l'inscription en compte, et les numéros de carte bancaire. Il apparaît donc qu'en dehors d'hypothèses marginales où une donnée a été confiée à un tiers et que celle-ci se trouve détruite par un organisme informatique viral, les interactions entre l'abus de confiance et les virus sont inexistantes. Signalons cependant une tendance en jurisprudence qui commence à s'affirmer en cas de fraude interne. Dans le cas où un salarié, dépositaire des matériels, logiciels et accès Internet mis à sa disposition par son employeur, les détourne abusivement et, semble-t-il, massivement, pour la collecte de contenus pouvant créer un risque juridique pour son employeur (exemple type : la visualisation voire le téléchargement d'images pédophiles), la Cour de Cassation vient, par deux fois, d'admettre la condamnation du salarié au titre du délit d'abus de confiance.

5.3.2.2 Loi informatique et libertés

Elle instaure des droits pour les personnes fichées et des obligations pour les responsables de traitements automatisés. Elle sanctionne non l'auteur d'une attaque mais l'exploitant qui en est la victime s'il peut lui être reproché *« le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés »*. Les délits ainsi institués figurent au livre II, titre II, chapitre VI, section V du code pénal sous l'intitulé *« Des atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques »*. La législation établit des délits relatifs à l'information des personnes subissant le traitement nominatif et la collecte illicite de données nominatives.

Proches des virus, les logiciels espions et les robots peuvent permettre la captation d'informations nominatives. L'article 25 de la loi précise que *« la collecte de données opérée par tout moyen frauduleux, déloyal ou illicite est interdit »*.

La Commission Nationale de l'Informatique et des Libertés considère, en se basant sur la directive du 24 octobre 1995 et sur la loi de 1978 qui encadrent la collecte des informations personnelles, que l'adresse IP, à savoir le numéro d'identification d'un système sur le réseau Internet via le protocole TCP/IP, est une donnée personnelle. Dès lors, un mécanisme viral qui collecterait ou scannerait et utiliserait ces adresses IP afin d'y installer, par exemple, un serveur proxy destiné à lui permettre une propagation plus rapide ou à favoriser l'envoi de courriers électroniques non sollicités pourrait être appréhendé par les articles 6 et suivants de la loi. Par ailleurs, on peut penser que les adresses MAC (Media Access Control) des périphériques réseaux se verront appliquer la même solution.

Cette notion est cependant contestée par certains experts qui considèrent que l'adresse IP est avant tout une donnée technique au même titre que le nom d'une rue et le numéro dans la dite rue. En effet, une adresse IP sans un minimum de datation n'est souvent d'aucune valeur dans le cadre d'une enquête de police.

5.3.2.3 Loi sur la protection du droit d'auteur

Elle comporte un chapitre sur la protection des logiciels. A ce titre, les mécanismes viraux peuvent être appréhendés comme des programmes entraînant la contrefaçon du logiciel qu'ils pénètrent et modifient.

5.3.2.4 Loi Godfrain

Elle traite des dispositions du Livre III du Code Pénal *« Des crimes et délits contre les biens »*. Elle introduit un Chapitre III relatif aux atteintes aux systèmes de traitement automatisé de données (acronyme : STAD). La loi ajoute les articles 323-1 et suivants qui érigent désormais en délit la réalisation d'un certain nombre de faits ou leur tentative par des personnes physiques ou par des personnes morales.

La loi cite, en premier lieu, *« le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données »* ; elle précise que les peines encourues sont aggravées *« lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système »*.

Le fait de se brancher sans droits sur un réseau et d'en intercepter le trafic grâce à un programme malveillant non autoreproducteur (un programme de type « sniffer » ou « keylogger » par exemple), un code viral le véhiculant ou visant à son insertion peut emporter une telle qualification pénale. Il n'est alors plus nécessaire de démontrer un quelconque préjudice lié à cet accès.

Le dépôt ou l'activation d'un code malicieux sur un serveur public peut ainsi entrer dans le champ du maintien si l'acte ne résulte pas d'une simple erreur mais que son auteur a conscience de l'irrégularité de son acte.

Le simple maintien dans un système, s'il est frauduleux, est susceptible de constituer une infraction même s'il résulte d'un accès régulier antérieur, même s'il n'y a pas intention de nuire.

En second lieu, elle mentionne *« le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données »* ou encore, en troisième lieu, *« le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient »*. Les mêmes peines sont en outre prévues pour *« la participation à un groupement formé ou à une entente établie en vue de la préparation, caractérisée par un ou plusieurs faits matériels, d'une ou plusieurs des infractions prévues* (par la présente loi) *»*.

Conçu pour réprimer le sabotage informatique, ce second point sanctionne aussi bien le fait d'entraver que celui de fausser le système. L'entrave réside dans le fait d'empêcher le fonctionnement logiciel ou matériel du système en provoquant une gêne ou une paralysie partielle ou totale, progressive ou instantanée, temporaire ou définitive, ponctuelle ou permanente et enfin simple ou récurrente. L'étendue de cette disposition permet de couvrir les conséquences de certains virus mettant en œuvre une charge virale (payload) entraînant la consommation excessive des ressources du système ou le dysfonctionnement d'un logiciel.

Le fait de fausser un système revient à l'altérer, à dénaturer son comportement de manière insidieuse ou sournoise et à lui faire produire un résultat non attendu . Dès lors, toute activité non désirée d'un programme, sans exception, semble entrer dans le champ de cet article.

En troisième lieu, l'article 323-3 du Code Pénal incrimine les atteintes aux données d'une manière autonome. L'ajout d'un virus au sein d'un système d'information, même sans destruction constitue une altération de l'ensemble des données de ce système. Il apparaît donc qu'un virus non activé, constitue une altération des données du système. Il peut être considéré comme une donnée fausse qui n'a pas lieu d'exister dans le système d'information.

Par ailleurs, la loi Godfrain sanctionne l'association de malfaiteur en matière informatique. Elle vise ainsi les clubs de piratage et les clubs des codeurs de programmes malveillants. Il est précisé qu'il y a groupement de malfaiteur dès lors qu'il y a concours de deux volontés ou plus, conscience des infractions et concrétisation par un ou plusieurs faits matériels. La loi réprime la simple tentative ; l'incitation à l'entrave d'un système n'est cependant pas réprimée .

5.3.2.5 Loi relative à la sécurité quotidienne

Elle prévoit la conservation par les opérateurs de télécommunication, pendant une période d'un an, des données relatives à une communication *« pour les besoins de la recherche, de la constatation et de la poursuite des infractions pénales »*. Il est précisé que ces données ne peuvent *« en aucun cas, porter sur le contenu des correspondances échangées ou des informations consultées sous quelque forme que ce soit »*. Elles concernent seulement l'identité des utilisateurs et les caractéristiques techniques des services fournis par les prestataires de communication (comme par exemple les adresses IP, les adresses électroniques envoyées ou reçues, ainsi que les adresses de sites visités). La loi modifie, par ailleurs, le code de procédure pénale en y insérant diverses dispositions concernant la mise en clair des données chiffrées nécessaires à la manifestation de la vérité. Elle met donc pratiquement à la charge des fournisseurs des prestations de cryptologie et des éditeurs de logiciels de chiffrement l'obligation de prévoir les moyens de procéder au déchiffrement quand cela leur est demandé par les autorités compétentes.

5.3.2.6 La loi pour la sécurité intérieure

Dans le domaine qui nous intéresse, elle vient compléter la loi relative à la sécurité quotidienne (LSQ). En effet, le texte prévoit que les fournisseurs d'accès à Internet doivent mettre à la disposition de l'officier de police judiciaire, sur demande de celui-ci, les informations utiles à la manifestation de la vérité, à l'exception de celles protégées par un secret prévu par la loi, contenues dans le ou les systèmes informatiques ou traitements de données nominatives qu'ils administrent et ce par voie télématique ou informatique dans les meilleurs délais (art. 8.1).

L'officier de police judiciaire peut, en outre, intervenant sur réquisition du procureur de la République préalablement autorisé par ordonnance du juge des libertés et de la détention, requérir des opérateurs de télécommunications de prendre, sans délai, toutes mesures propres à assurer la préservation, pour une durée ne pouvant excéder un an, du contenu des informations consultées par les personnes utilisatrices des services fournis par les opérateurs.

Cette disposition vient compléter l'article 29 de la LSQ qui prévoyait que la conservation des données ne peut, en aucun cas, porter sur le contenu des communications.

Enfin, l'article 8 bis de la LSI permet aux officiers de police judiciaire de procéder à la perquisition en ligne, en accédant « *par un système informatique implanté sur les lieux où se déroule la perquisition à des données intéressant l'enquête en cours et stockées dans ledit système ou dans un autre système informatique, dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial* ».

Dans le cas où les données accessibles seraient situées en dehors du territoire national, les autorités doivent se conformer aux engagements internationaux existants.

5.3.2.7 Loi pour la confiance dans l'économie numérique

Elle complète le dispositif mis en place par la loi Godfrain en insérant dans le code Pénal un article 323-3-1 qui réprime *« le fait, sans motif légitime, d'importer, de détenir, d'offrir, de céder ou de mettre à disposition un équipement, un instrument, un programme informatique ou toute donnée conçus spécialement adaptés pour commettre une ou plusieurs des infractions »*.

La loi sanctionne donc le fait de détenir un virus et plus seulement le fait de faire entrer le virus dans le système d'information. Un programme viral installé en connaissance de cause sur sa propre machine pour réaliser certaines tâches semble ainsi de facto illégal car susceptible, s'il était transmis à un autre système, de l'entraver ou le fausser.

La loi, qui aggrave également les peines encourues, a aussi pour but de favoriser le développement de la société de l'information par le commerce par Internet. Elle précise les règles pour les consommateurs et les prestataires aussi bien techniques que commerciales. La loi s'inspire de diverses directives européennes dont la convention de Budapest.

Les hébergeurs de sites Internet doivent assurer *« un minimum de surveillance »* sur les pages qu'ils stockent, afin d'empêcher la diffusion d'informations *« faisant l'apologie des crimes de guerre ou des crimes contre l'humanité, incitant à la haine raciale, ou ayant un caractère pédophile »*.

Pour le commerce électronique, le marchand en ligne assume *« une responsabilité globale »* sur l'ensemble de la vente, de la passation de commande à la fourniture de biens, ou de prestations de services.

La publicité non sollicitée (le spamming) par messagerie électronique, sans avoir obtenu le consentement préalable des destinataires est interdite.

5.3.2.8 Loi relative aux communications électroniques et aux services de communication audiovisuelle

Ce texte s'articule autour de 3 principes essentiels :

- la convergence entre les télécommunications et l'audiovisuel, qui sont regroupés sous l'appellation de réseaux de communications électroniques,
- l'adaptation du cadre de régulation de ces réseaux de communication entre l'ART (Autorité de régulation des télécommunications, devenue ARCEP, Autorité de régulation des Communications Electroniques et des Postes) et le CSA (Conseil supérieur de l'audiovisuel). Ce dernier a désormais une compétence élargie à tous les modes de diffusion de la radio et de la télévision (hertzien, câble, satellite, ADSL, Internet).
- La mise en place d'un régime favorisant la concurrence (assouplissement ou suppression des obligations pesant sur les opérateurs de communications électroniques).

5.3.2.9 Intérêts fondamentaux de la nation

Quelques textes très spécifiques régissent l'atteinte aux intérêts fondamentaux de la nation. Il s'agit des articles L. 410-1 et suivants du Code Pénal. Ils ne couvrent que des hypothèses marginales où les éléments viraux ne pourraient être appréciés qu'eu égard à un de leurs effets particuliers. Ils ne font pas l'objet d'une appréhension globale comme lors de la réforme de 1988 .

Citons néanmoins l'article 421-1. Il édicte que *« les vols, les extorsions, les destructions, dégradations et détériorations, ainsi que les infractions en matière informatique »* […] *« constituent des actes de terrorisme, lorsqu'elles sont intentionnellement en relation avec une entreprise individuelle ou collective ayant pour but de troubler gravement l'ordre public par l'intimidation ou la terreur ».*

5.3.2.10 Secrets de la correspondance

Certains virus réémettent d'eux même des courriers électroniques personnels. Ils violent ainsi le secret des correspondances appliqué depuis novembre 2000 au dit courrier électronique tel qu'il est précisé par la convention européenne des droits de l'homme dans son article 8.

5.4 Regard sur l'international

La criminalité informatique ne se cantonne pas à un seul pays. La communauté internationale en a pris conscience. Les enjeux liés au développement des technologies numériques sont abordés à un niveau international. Il nous est possible de citer :

- la Convention du Conseil de l'Europe sur la cybercriminalité (Convention de Budapest - 23 novembre 2001) et de son protocole additionnel relatif à l'incrimination d'actes de nature raciste et xénophobe commis par le biais de systèmes informatiques (7 novembre 2002),
- la directive européenne relative à certains aspects juridiques des services de la société de l'information, et notamment du commerce électronique, dans le marché intérieur (directive 2000/31 du 8 juin 2000),
- l'ensemble des travaux accomplis au sein du G8, d'EUROPOL ou du groupe de travail sur la criminalité liée aux technologies de l'information d'INTERPOL.

5.4.1 Convention du Conseil de l'Europe sur la cybercriminalité

La répression des infractions sur des réseaux transnationaux est entravée par la difficulté à identifier les fraudeurs et la preuve en général. C'est dans l'optique d'une harmonisation que fut adoptée la

convention dite « de Budapest ». Son objectif est d'harmoniser les infractions au niveau européen notamment concernant les infractions en matière de confidentialité et d'intégrité des données des systèmes informatiques et de fraude informatique au sens large. A terme, tous les pays de l'Union européenne devraient ainsi avoir le même système répressif en matière de criminalité informatique. Ce résultat permettrait une lutte plus efficace.

La Convention détermine trois principaux axes de réglementation :

- l'harmonisation des législations nationales concernant les incriminations,
- la définition des moyens d'enquêtes et de poursuites pénales adaptés à la mondialisation des réseaux,
- la mise en place d'un système rapide et efficace de coopération internationale.

La convention oblige tout d'abord les Etats qui l'ont ratifiée à prendre des mesures propres pour ériger en infraction pénale un certain nombre de comportements et en particulier :

- *« le fait intentionnel et sans droit, d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données informatiques »* (article 4 – Atteinte à l'intégrité des données),
- *« l'entrave grave, intentionnelle et sans droit, au fonctionnement d'un système informatique, par l'introduction, la transmission, l'endommagement, l'effacement, la détérioration, l'altération ou la suppression de données informatiques »* (article 5 – Atteinte à l'intégrité des systèmes),
- *« la production, la vente, l'obtention pour utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition, »* […] *« la possession i) d'un dispositif, y compris un programme informatique, principalement conçu ou adapté pour permettre la commission de l'une des infractions (précédentes), ii) d'un mot de passe, d'un code d'accès ou de données informatiques similaires permettant d'accéder à tout ou partie d'un système informatique, »* […] *« dans l'intention qu'ils soient utilisées afin de commettre l'une ou l'autre des infractions (précédentes) »* (article 6 – Abus de dispositifs),
- *« l'introduction, l'altération, l'effacement ou la suppression intentionnels et sans droit de données informatiques, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales comme si elles étaient authentiques, qu'elles soient directement lisibles ou intelligibles »* (article 7 – Falsification informatique),
- *« le fait intentionnel et sans droit de causer un préjudice à autrui i) par toute introduction, altération, effacement ou suppression de données informatiques ii) par toute forme d'atteinte au fonctionnement d'un système informatique, »* […] *« dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui »* (article 8 – Fraude informatique).

Chaque Etat est tenu d'adopter les mesures législatives et autres qui se révèlent nécessaires pour habiliter ses autorités compétentes :

- *« à ordonner ou à imposer d'une autre manière la conservation rapide de données électroniques spécifiées, y compris des données relatives au trafic, stockées au moyen d'un système informatique, notamment lorsqu'il y a des raisons de penser que celles-ci sont particulièrement susceptibles de perte ou de modification »* (article 16 – Conservation rapide de données informatiques stockées),
- *« à ordonner : i) à une personne présente sur son territoire de communiquer les données informatiques spécifiées, en sa possession ou sous son contrôle, qui sont stockées dans un*

système informatique ; et ii) à un fournisseur de services offrant des prestations sur le territoire, de communiquer les données en sa possession ou sous son contrôle relatives aux abonnés et concernant de tels services » (article 18 – Injonction de produire),

- *« à perquisitionner ou à accéder d'une façon similaire : i) à un système informatique ou à une partie de celui-ci ainsi qu'aux données informatiques qui y sont stockées ; et ii) à un support du stockage permettant de stocker des données informatiques »* […] *« sur son territoire, »* […] *« à saisir ou à obtenir d'une façon similaire les données informatiques pour lesquelles l'accès a été réalisé »* (article 19 – Perquisition et saisie de données informatiques stockées),

- *« à collecter ou enregistrer par l'application de moyens techniques existant sur son territoire »* […] *« les données relatives au trafic associées à des communications spécifiques transmises sur son territoire au moyen d'un système informatique »* ou à obliger un fournisseur de services à le faire ou à prêter son concours et son assistance pour le faire (article 20 – Collecte en temps réel des données relatives au trafic),

- *« en ce qui concerne un éventail d'infractions graves »* […] *« à collecter ou à enregistrer, en temps réel, les données relatives au contenu de communications spécifiques sur son territoire, transmises au moyen d'un système informatique »* ou à obliger un fournisseur de services à le faire ou à prêter son concours ou son assistance pour le faire (article 21 – Interception de données relatives au contenu).

A côté des formes traditionnelles de coopération pénale internationale prévues notamment par les conventions européennes d'extradition et d'entraide judiciaire en matière pénale, la Convention de Budapest exige des formes d'entraide correspondant aux pouvoirs définis préalablement par celle-ci. En conséquence, les autorités judiciaires et les services de police d'un Etat doivent pouvoir agir pour le compte d'un autre Etat dans la recherche de preuves électroniques, sans toutefois mener d'enquêtes, ni de perquisitions transfrontalières. Les informations devront être ensuite rapidement communiquées.

Un réseau de contacts disponibles vingt-quatre heures sur vingt-quatre et sept jours sur sept est mis sur pied afin de fournir une assistance immédiate aux investigations en cours.

5.4.2 Directive européenne 2000/31

Ses dispositions sont transposées dans le droit français par la loi pour la confiance dans l'économie numérique. La directive précise notamment la responsabilité des hébergeurs.

5.5 Quelques Conseils

Il est important de se pré constituer des indices ou des éléments d'information :

- Gravure de CD.
- Listing journaux,
- Recherche de témoins,
- PV d'huissiers avec courriers recommandés.
- …

Tous ces éléments seront, le moment venu, recevables ou non recevables par les instances concernées. Ces dernières valideront la recevabilité des éléments collectés.

Dans le cas du déclenchement d'une instance judiciaire, seules les constatations effectuées le plus tôt possible par un enquêteur, avec ou sans l'appui d'un homme de l'art, auront valeur. Elles sont primordiales dès le début de l'enquête.

Pensez à faire un audit de votre contrat d'assurance en vérifiant si les faits générateurs et les types d'indemnisation sont cités (matériel, perte d'usage….).

Dans une démarche de plainte simple, il est possible de contacter des organismes suivants :

- La BEFTI : Brigade d'Enquêtes sur les Fraudes aux Technologies de l'Information. Anciennement SEFTI, elle a été créée en 1994. Elle est rattachée à la Sous-Direction des Affaires Economiques et Financières de la Direction de la Police Judiciaire de la Préfecture de Police de Paris. Son champ d'action se situe uniquement à Paris et en petite couronne.

  Sa mission première consiste à enquêter sur les affaires d'intrusion et d'atteinte au SI. Elle peut également intervenir en matière de contrefaçon logicielle ou de violation des droits de propriété intellectuelle.

  Elle a également une mission de formation et d'information en interne ou à l'extérieur sur le thème des fraudes électroniques. Elle dispense une assistance technique aux autres services de police.

  BEFTI : 122/126 rue du Château des Rentiers. 75013 Paris. tel : 01.55 75 26 19

- L'OCLCTIC : Office Central de la Lutte contre la Cybercriminalité liée au Technologies de l'Information et de la Communication.

  Remplaçant de la BRCI, cet office appartient à la Direction Générale de la Police Nationale et dépend de Direction Centrale de la Police Judiciaire. Il a été créé en 2000 afin de lutter contre la délinquance liée aux nouvelles technologies à l'échelle nationale et internationale.

  Il est investi d'une double mission :

  - La première est liée à l'activité opérationnelle proprement dite et répond à deux objectifs essentiels :
    - la réalisation d'enquêtes judiciaires de haut niveau technique menées à son initiative ou à la demande des Magistrats de l'appareil judiciaire,
    - l'assistance technique à l'occasion d'enquêtes judiciaires menées par d'autres services tels que les services de police, de gendarmerie, de la Douane ou de la DGCCRF (Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes).
  - La seconde mission est en relation avec l'activité stratégique. Il s'agit de :
    - la formation, l'animation et la coordination au niveau national de l'action des autres services répressifs, compétents en matière d'infractions liées aux technologies de l'information et de la communication ;
    - la coopération internationale : l'OCLCTIC est point de contact national pour la France pour les échanges et la coopération policière internationale (Europol, Interpol, G8) ;

- la documentation opérationnelle : banque de données pour permettre le rapprochement des affaires, statistiques annuelles sur les infractions liées aux nouvelles technologies.

http://www.interieur.gouv.fr/rubriques/c/c3_police_nationale/c3312_oclctic/index_html

- Le Ministère de l'Intérieur : DST - Direction de la Surveillance du Territoire

  La Direction de la Surveillance du Territoire est un service de renseignement de sécurité disposant de pouvoirs de police judiciaire spécialisée. Ces missions sont traditionnellement de trois types : contre-espionnage, contre-terrorisme, protection du patrimoine économique et scientifique. De nouvelles menaces de niveau stratégique apparaissent et sont d'ores et déjà prises en compte, il s'agit de la prolifération des armes nucléaires, bactériologiques, chimiques et balistiques ou de la grande criminalité organisée.

- La gendarmerie

  Au niveau central, la gendarmerie possède plusieurs structures de lutte contre les nouvelles formes de criminalité en rapport notamment avec l'utilisation d'Internet :

  - Le département cybercriminalité du service technique de recherches judiciaires et de documentation (STRJD). Il assure la surveillance du réseau en recherchant les infractions portant atteinte aux personnes et aux biens et relatives à la transmission de données à caractère illicite sur Internet, les newsgroups et les réseaux poste à poste.

  - Le département informatique et électronique de l'IRCGN (Institut de Recherche Criminelle de la Gendarmerie Nationale). Il développe des méthodes, des outils et des logiciels permettant de détecter automatiquement des images pédophiles connues ou d'extraire des données.

  - Le centre national d'images pédopornographiques (en collaboration avec la police nationale).

  - Le centre national de formation de police judiciaire. Il propose une formation spécifique, dénommée N-TECH, dans le domaine des nouvelles technologies au profit d'enquêteurs spécialisés affectés en unités de recherches.

  http://www.defense.gouv.fr/sites/gendarmerie/

  judiciaire@gendarmerie.defense.gouv.fr

6. L'ASSURANCE CONTRE LES VIRUS

Nous présenterons tout d'abord les principes qui régissent l'assurance des biens de l'assuré pour ensuite détailler les critères de souscription, puis le déroulement d'un appel en garantie (demande d'indemnisation). Enfin, nous préciserons quelques tendances relatives à l'assurance des systèmes d'information contre la malveillance informatique et plus particulièrement les virus informatiques. Pour rappel, le deuxième grand volet d'assurance est la responsabilité civile : dommage accidentel causé à un tiers.

6.1 Principes d'assurance

Dans le domaine de l'assurance des biens, il y a lieu de distinguer une assurance informatique de l'assurance des informations. Dans le premier cas, il s'agit d'assurer le matériel (serveurs, postes de travail, connectique, etc.) qui sera remboursé en cas de sinistre en valeur à neuf ou vétusté déduite. Dans le second cas, il est difficile d'estimer la valeur financière d'une information ; par contre, on peut quantifier le coût de remise en état d'une information ou d'un système d'information.

Avant de présenter les options possibles, il existe quelques grands principes en matière d'assurance :

- Existence d'un aléa, il doit exister une part de hasard dans la survenance de l'événement.
- Le fait générateur doit être connu et partie intégrante du contrat. Si par exemple, le fait virus n'est pas défini (ou est exclu) alors la garantie ne peut s'activer.
- En raison du principe indemnitaire, il ne doit pas y avoir d'enrichissement de l'indemnisé. Le remboursement des frais ou le rachat d'équipement ne doit pas constituer un gain.

6.2 Souscription d'un contrat

Assurer un système d'information, c'est établir un accord consensuel pour un montant de remboursement et des options d'assurance entre l'assuré et l'assureur.

Les systèmes d'information étant extrêmement variés dans leurs emplois ou dans leur dynamique d'évolution, il est difficile d'établir une métrique du montant à assurer en fonction d'une architecture donnée. C'est donc plus la stratégie d'aversion aux risques et la capacité financière de l'entreprise qui vont déterminer la politique d'assurance.

En matière d'assurance des systèmes d'information, il existe un module de base - la reconstitution de l'information - à laquelle peuvent s'ajouter différentes options de garantie :

- les frais supplémentaires comme par exemple les heures supplémentaires,
- les pertes d'exploitation ou pertes d'activité bancaire, dans le cas présent les charges fixes et le bénéfice non réalisé,
- la carence de fournisseur ou la déficience de fourniture en moyens tels que l'électricité,
- la fraude financière,
- le racket ou l'extorsion,
- la gestion de crise et la reconstitution d'image,

- etc.

Au moment de la souscription, les éléments suivant sont donc discutés :

- le périmètre de garantie, c'est à dire les structures juridiques intégrées dans le contrat ou encore l'existence de limitations géographiques,
- les faits générateurs couverts,
- les options telles que sus nommées,
- Le montant assuré (montant total d'indemnisation),
- La prime à payer pour cette garantie,
- La franchise exprimée en euro ou en jours d'exploitation,
- Les sous limites pour certains faits générateurs (virus, hackers, etc.),
- Les exclusions, soit du fait du marché de l'assurance, soit du fait de la compagnie,
- Et enfin, les obligations contractuelles de l'assuré. Elles sont le plus souvent peu contraignantes... et presque « naturelles » : réalisation de sauvegardes conservées hors site, emploi d'un anti-virus opérationnel (mise à jour de la base de signatures quand elle existe).

Pour terminer cette partie, rappelons que la garantie virus est bien souvent une option par rapport à une garantie plus globale, « malveillance informatique » qui couvre les préjudices des intrusions ou le fait des employés .

6.3 Appel en garantie

Lorsque survient un incident, c'est à l'assuré - éventuellement conseillé par son courtier - de déterminer s'il y a lieu de faire un appel en garantie. En fonction des contrats et des compagnies les exigences peuvent être diverses quant aux délais ou aux pièces à fournir.

D'une manière générale, il s'agira d'identifier le fait générateur et son impact financier au regard des options d'assurance souscrites. En fonction de la complexité ou de l'importance des montants engagés, un expert d'assurance pourrait être diligenté pour apprécier ces éléments. Un expert d'assuré, représentant donc la dite personne pourra également donner son appréciation sur les faits.

Concrètement il s'agira :

- d'identifier le fait générateur et son appartenance aux faits garanties,
- d'historiser le déroulement de l'incident,
- de quantifier l'impact en terme de préjudice ou de frais engagés pour la remise en état du système.

Comme le système d'information est un monde dynamique et volatile, la remise en état doit être faite au plus tôt et charge à l'assuré de conserver les traces et éléments permettant de caractériser le préjudice.

6.4 Evolution de la garantie

Depuis les années 80, les assureurs ont proposé des garanties informatiques, notamment contre les virus informatiques. Toutefois, l'offre du marché a considérablement varié avec le temps. En effet, il y a quelques années, le marché de Londres (qui influe sur les grandes orientations en matière d'assurance) a défini une clause « cyber-data » qui permettait l'exclusion du virus du périmètre de

garantie. Cette politique a notamment été suivie par les assureurs d'origine française. Cette démarche avait pour objet de limiter les conséquences du risque sériel que représenterait une contamination virale informatique à l'échelle mondiale et donc potentiellement chez tous les assurés. Cette crainte, essentiellement fondée sur l'hypermédiatisation de virus « catastrophe » (Datacrime, Michelangelo, Loveletter, Tchernobyl, etc.), étant renforcée par l'absence de maîtrise du portefeuille d'engagement, à savoir si le fait « virus » pouvait être appelé en garantie dans une assurance « tout risque informatique » (c'est-à-dire le matériel) voire une assurance « multirisques bureau ».

Néanmoins, des assureurs américains ont continué à proposer une garantie « virus » y compris sur le marché français. Et aujourd'hui, la tendance est à l'accroissement de cette offre considérant que les réassureurs investissent à nouveau dans ce type de garantie. Toutefois, l'indemnisation au titre du virus est généralement sous limitée dans une garantie de type malveillance informatique.

La confiance revenant ou en raison d'une nouvelle appréciation technique, on trouve même aujourd'hui une garantie virus en responsabilité civile pour Internaute, c'est-à-dire l'indemnisation de dommages causés à des tiers.

7. CONCLUSION

Au milieu des années 1980, le grand public découvrait le phénomène virus. Alors que les concepteurs d'anti-virus mettaient au point leurs premiers produits, de jeunes créateurs s'appliquaient à concevoir, pour se distraire ou par esprit de compétition, des nouveautés qu'ils diffusaient avec le secret espoir de se faire un surnom. A l'approche de l'an 2000, c'était encore le jeu et la recherche d'une reconnaissance qui primaient. Après la mainmise des virus sur les outils bureautiques, la messagerie électronique devint, avec les *mass-mailers*, la cible à atteindre.

En 2005, la donne a changé, l'appât du gain et l'argent facile sont le moteur des attaques actuelles. On parle maintenant de cybercriminalité. Ce terme à la mode couvre à fois les crimes particuliers faisant intervenir des ordinateurs et des réseaux (comme dans le cas du piratage), et la contribution à l'aboutissement de crimes traditionnels grâce à l'utilisation d'ordinateurs (pornographie, racket, détournement d'informations financières). Internet offre l'anonymat, l'instantanéité et la multiplicité des contacts. Pour les criminels, l'attrait du crime assisté par ordinateur est de plus en plus séduisant.

Les nombreux programmes malveillants qui circulent ne sont plus uniquement autoreproducteurs et il existe maintenant des programmes commerciaux indésirables.

Nous retrouvons donc aujourd'hui à côté des vers et des virus :

- Des chevaux de Troie : programmes malveillants en apparence inoffensif contenant une fonction illicite cachée et connue de l'attaquant seul.
- Des adwares : programmes indésirables d'origine commerciale chargés de gérer l'affichage des publicités en fonction du profil de la cible,
- Des spywares : programmes indésirables d'origine commerciale chargés de capturer de l'information à des fins de publicité ou d'espionnage. Ils agissent silencieusement sans le consentement de l'utilisateur.

Pour mieux atteindre leurs buts, tous ces programmes :

- gagnent en sophistication ;
- visent les particuliers, les administrations et les entreprises ;
- récupèrent informations personnelles, financières ou commerciales.

Ils assistent toute une cohorte d'individus qui souhaitent gagner – légalement ou non - un maximum d'argent en un minimum de temps.

Cette évolution laisse présager un avenir durable pour ces logiciels.