

Les virus : quelle plaie!

La seule parade vraiment efficace pour contrer les virus est la déconnexion du Net, ou encore l'utilisation d'une plate-forme exotique comme un BeOS, Linux ou Mac OS. Et si malgré ces recommandations vous continuez à préférer le PC et ses Windows, dotez-vous d'un antivirus remis à jour régulièrement

Nous allons tenter de décrire ce qu'est un virus et l'étendue des dommages causés par ces petites bêtes qui galopent et se propagent à une allure vertigineuse. Afin de rester professionnel, nous traduisons ici un document écrit en anglais provenant de *Mikko Hermanni Hyppönen*, manager de l'entreprise finlandaise *F-Secure Corporation*. Il s'agit là d'informations de première main puisque cette entreprise est spécialisée dans la recherche d'antivirus et la vente de parades informatiques à cette plaie mondiale.

Cette entreprise qui emploie 350 personnes réalise aussi des logiciels de cryptage, des gestionnaires de sécurité ainsi que des applicatifs de désinfection dédiés aux palmtops et autres appareils portables.

Qu'est-ce qu'un virus?

Toujours écrits par la main d'un humain, les virus ont une fâcheuse tendance à se propager. Ils se répandent habituellement via le courrier électronique. Les virus ram-

pants de type *Worm* n'ont besoin d'aucune aide extérieure pour étendre « leurs bienfaits », ils sont totalement autonomes. Le virus peut receler diverses fonctions maléfiques, l'annonce d'un message humoristique, la modification ou perte de données par effacement partiel ou total d'un disque dur, ou encore la création dans le PC d'une porte dérobée autorisant l'accès à distance.

Trois grandes catégories de virus existent : les virus binaires, les macros et les scripts. De 1986 à 2001, la progression a été exponentielle. Entre 1993 et 1995, elle augmentait de un à deux milliers de virus par an alors que de 2000 à 2001, sont apparus 10'000 nouveaux virus.

Passons en revue ces différentes familles de virus. Aujourd'hui, les virus binaires dépassent les 55'000 alors que le nombre de virus évoluant dans le DOS des PC est d'environ 45'000, Windows 9x/Me n'en connaît que 500 et 300 pour l'environnement Windows NT/2000.

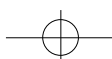
Pour ce qui est des macrovirus, plus de 8000 sont connus à ce jour. Ceux-ci ne peuvent vivre qu'aux dépens d'une application spécifique. Il y a 7000 macrovirus qui apprécient particulièrement le traitement de texte Microsoft Word, il y en a 1400 qui sévissent dans le tableur Excel et une centaine dans le logiciel de présentation Powerpoint. Signalons au passage que les macros sont en fait des mégafonctions destinées, à l'origine, à simplifier le travail répétitif de l'utilisateur. Ce sont des mini-programmes simples à réaliser, permettant d'automatiser certaines tâches. Ils sont transmis généralement par fichier attaché, incorporé à un fichier Word de type [.doc]. Et côté scripts, *F-Secure* en a dénombré 650 à ce jour.

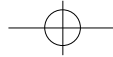
Les épargnés ou presque...

Mais dans le monde informatique, il n'existe pas uniquement des PC, avec ses déclinaisons DOS, Win, etc. D'autres plates-formes plus exotiques permettent presque d'échapper au fléau des virus. Ainsi ces autres ordinateurs ne peuvent être infectés que par une centaine de virus soit 50 pour les Macintosh, 25 pour les systèmes d'exploitation Linux et 6 « chevaux de Troie » pour les « EPOC ». Il s'agit là du DOS des *Psions* de l'éditeur *Symbian*. L'un de ces 6 virus, qui se fait appeler *Alarme*, provoque des sonneries impromptues et consomme de ce fait trop rapidement la puissance de la batterie.



Cette encyclopédie on-line permet de comprendre la signification de plus de 20'000 termes anglophones et abréviations issus des nouvelles technologies. Ici, la définition anglaise de « cheval de Troie »





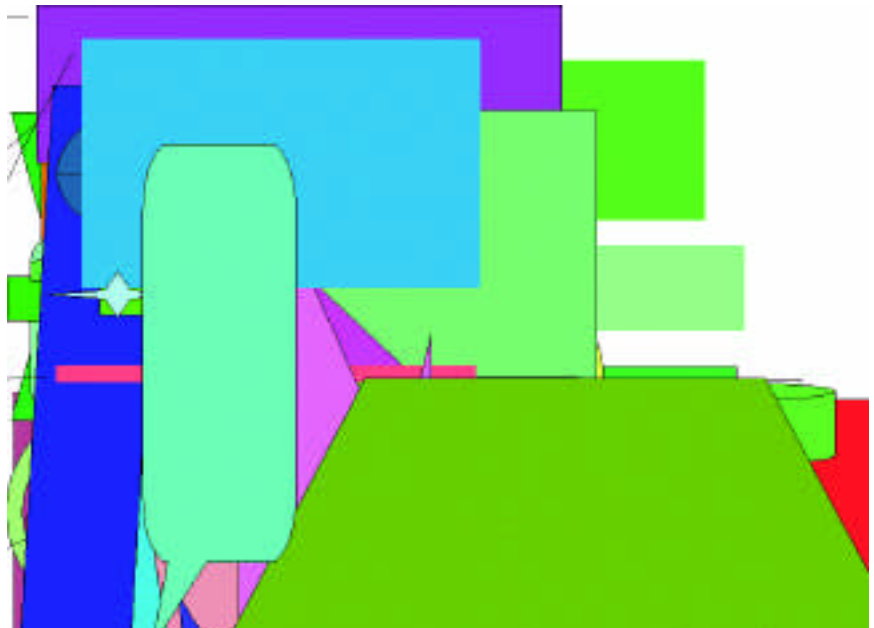
Le *Palm OS* n'est pas totalement épargné puisqu'un virus existe déjà, ainsi qu'un second de type «cheval de Troie». Voici en quelques lignes les virus les plus graves qui ont sévi ces dernières années, avec les coûts qu'ils ont engendrés:

- 1998: CIH
- 1999: ExplorerZip (1020 mio \$), Melissa (1100 mio \$)
- 2000: LoveLetter (875 mio \$)
- 2001: Sircam (1050 mio \$), Anna Kournikova, Code Red (2620 mio \$), Nimda (590 mio \$), BadTrans, Goner.

Que font donc ces virus dans un PC?

Sircam est un virus connu pour son aptitude à voler des données. En effet, lorsqu'il est confortablement installé dans un PC, il localise les documents les plus récemment utilisés et les envoie aux adresses électroniques découvertes dans le logiciel de messagerie.

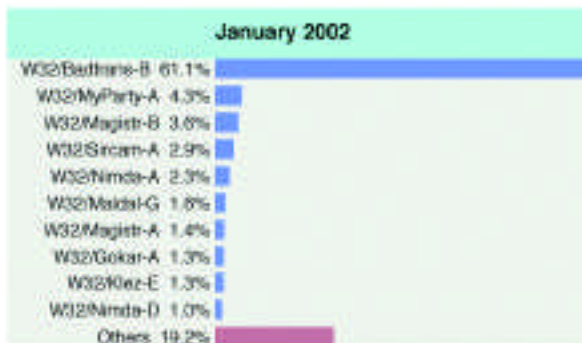
Code Red est le premier virus de type «ver» à avoir vu le jour. Son habitat naturel est la toile de l'Internet. C'est aussi le premier de type *DDoS* et sa particularité est de sauter de site en site. Sa vie se décompose en trois phases. La première,



Résultats hauts en couleur après l'infection du virus «wm97» appelé également Melissa

assimilable à la reproduction, lui permet de se répliquer et de s'étendre, la seconde est l'attaque et la dernière est la mise en

sommeil. En juillet 2001, *Code Red* a infecté 340'000 machines et 170'000 machines en août.

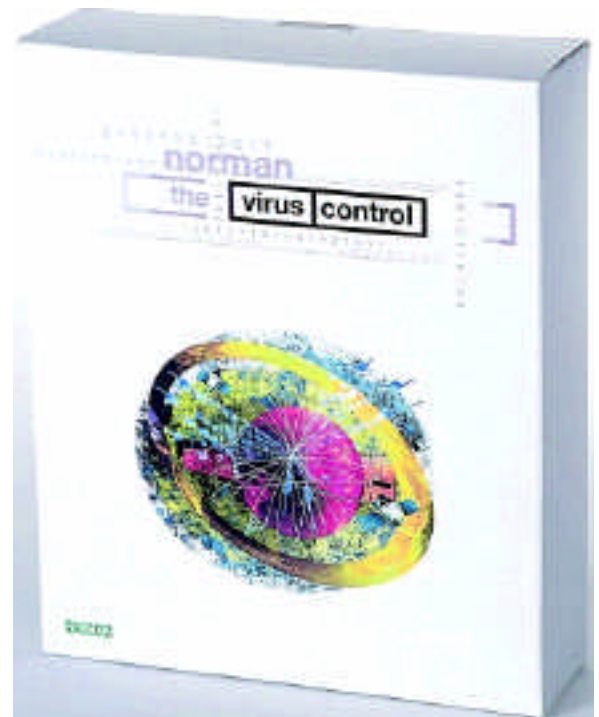


Source : Sophos.com

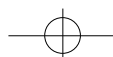


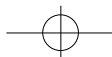
Source : Sophos.com

Evolution de l'invasion des virus de janvier à février 2002.



L'un des nombreux anti-virus disponible sur le marché





MSM Web News

Nimda, un nom bien étrange correspondant au «verlan» du mot Admin est aussi surnommé *W32.Nimda.A@mm*. Ce virus a plusieurs cordes à son arc, en l'occurrence quatre moyens d'infection différents: via les serveurs Web, au sein d'un réseau local et propagation par courrier électronique. Mais ce n'est pas tout: il est capable de créer un compte local avec des privilèges d'administrateur au sein de la machine infectée permettant à un intrus de s'y faufiler. Son pouvoir est dévastateur puisqu'en un seul jour 2,2 millions de machines ont été infectées.

BadTrans est tout aussi mauvais que le précédent. Il se perpétue grâce aux adresses du logiciel de messagerie et envoi à ces destinataires des réponses débutant par *Re: [titre du mail]* afin de ne pas éveiller de méfiance. Mais ce qu'il y a de plus grave c'est qu'il est capable de dénicher les mots de passe tapés au clavier, proches de mots clés tels que log, pass, rem... Il les rassemble dans un fichier puis envoi celui-ci périodiquement à une liste d'adresses e-mails.

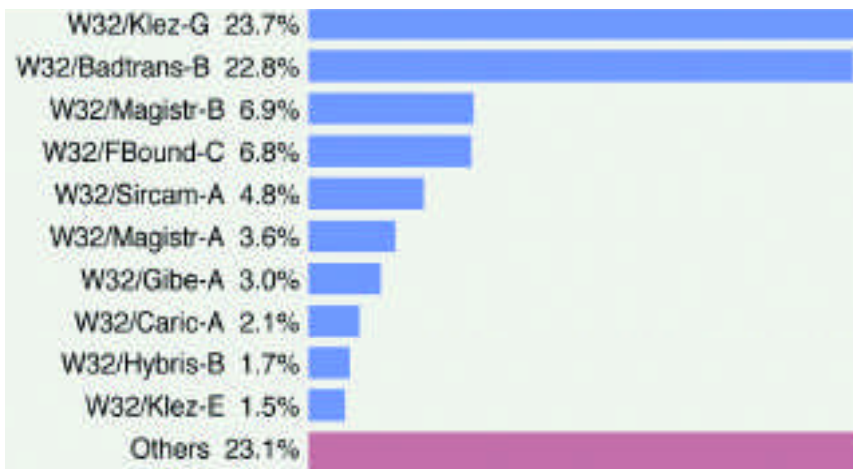
Pourquoi les virus sont-ils créés? Les raisons en sont multiples: par curiosité, par défi, par soif de pouvoir, ou encore pour assoir sa renommée. A titre d'exemple, *David L. Smith* créateur de *Melissa* est un américain de 30 ans. Sa peine, selon *Symantec.com*, pour cet acte malveillant est de 4 à 5 ans de prison et une amende de 150'000\$. Et *Christopher Pile*, âgé de 27 ans, créateur du virus appelé *Smeg*, a purgé une peine de 18 mois de prison. Et finalement le citoyen de Taiwan *Chen Ing-Hau*, 27 ans également, n'a eu aucune condamnation malgré la création du diabolique *CIH*.

La vitesse de réaction est primordiale

En effet, les éditeurs d'antivirus qui conservent chacun un zoo de ces virus doivent intensément communiquer entre eux afin de délivrer à leurs clients des parades aussi rapides que possible. La dangerosité de chaque nouveau virus détecté est évidemment évaluée afin, d'une part, d'avertir le public et d'autre part, de réagir rapidement. Voici les temps de réaction face aux derniers virus d'importance:

- Melissa 1999: 3h 15 min
- Loveletter 2000: 1h 40 min
- Anna Kournikova 2001: 2h 5 min
- Sircam 2001: 1h 50 min
- Nimda 2001: 1h 47 min

Et comme nous l'avons vu plus haut, les



Voici la liste du «Top ten» des virus recensés durant le mois de mars de l'année 2002 par le site Sophos.com

virus s'infiltrèrent partout même sur les Palms et les Psions... A quand la prise d'assaut des autres mobiles tels que les Natels? En tout état de cause, l'auteur de cet article *Mikko H. Hyppönen*, manager de F-Secure Corporation, fait déjà de la promotion pour un antivirus dédié aux appareils sans fils tels que téléphones portables, iPaq, Palm et autres mobiles.

Source de cet article:
Mikko Hermanni Hyppönen
mikko.hypponen.com
mikko.hypponen@f-secure.com
www.f-secure.com
 Traduction et adaptation :
Jean-René Gonthier, jrgonthier@msm.ch

Des références en matière de virus

Afin de parfaire cet article avec des sources similaires mais complémentaires, je vous propose ici quelques sites d'éditeurs de virus ou d'éditorialistes sur le thème de ces petites bêtes qui s'insinuent sournoisement dans nos machines branchées.

Une Newsletter pour rester vigilant

Secuser ou l'actualité de la sécurité informatique, c'est aussi le déploiement d'un antivirus gratuit. Sur ce site, le surfeur apprend également tout sur les nouvelles attaques de virus et leurs parades ainsi que la possibilité de s'abonner gratuitement à une Newsletter «Alerte» intégrant

une synthèse hebdomadaire. C'est en effet essentiel d'être immédiatement prévenu lors d'une propagation d'un nouveau virus. *Secuser* traite encore du spamming, du mailbombing et des moyens techniques et juridiques pour y faire face. www.secuser.com

Du shareware à la désinfection

Le serveur web *Megagiciel* bien connu des amateurs de la Toile du Québec expose notamment ce qu'est un virus et fait le tour des parades possibles par une rubrique «Bien choisir son antivirus» comportant des liens vers presque tous les éditeurs d'AV. C'est aussi un répertoire de partageables et de forums. www.megagiciel.com

Un des nombreux éditeurs d'AV

Editeur de *MailMonitor*, *Sophos* a notamment à cœur de renforcer la sécurité des messageries électroniques. Cette société propose également le logiciel *Anti-Virus* ainsi qu'une interface *SAVI*, permettant à des applications tierces d'intégrer le moteur antiviral de *Sophos*. www.sophos.fr

JEAN-RENÉ GONTHIER
 Rédacteur MSM
jrgonthier@msm.ch

