Les virus informatiques démystifiés

Virus

Mails

Internet

Appareils mobiles

Sécurité

Annexes

Publié et conçu par Paul Oldfield.

Demande de renseignements : info@sophos.fr
Site web : www.sophos.fr

Table des matières

Le problème des virus

Virus, pirates informatiques, contournement de protections logicielles, délinquance informatique font les gros titres des journaux et nous coûtent des millions, si l'on en croit les médias. Mais les virus et tous les autres désagréments du cyberespace posent-ils problème ? Sont-ils vraiment très néfastes ?

Si vous en doutez, imaginez seulement ce qui pourrait se passer au bureau ou chez vous.

Scénario : personne n'a mis à jour l'antivirus depuis des mois. Vous vous en chargez et vous découvrez que vos tableaux de comptes sont infectés par un nouveau virus qui change les chiffres au hasard. Bien entendu, vous sauvegardez régulièrement vos documents. Mais cela fait peut-être des mois que vous sauvegardez des fichiers infectés. Comment savoir à quels chiffres vous fier ?

Imaginez maintenant qu'un nouveau virus de messagerie vienne de sortir. Votre entreprise reçoit tellement de mails que vous décidez de fermer complètement la passerelle de messagerie… et vous ratez une commande urgente d'un gros client.

Autre hypothèse : vous êtes en train de travailler sur vos dossiers. Vous avez pratiquement terminé votre appel d'offres lorsque l'un de vos enfants installe un nouveau jeu sur le PC et y installe par la même

occasion un virus. Le virus efface tout sur le disque dur… y compris le travail que vous y avez enregistré.

Imaginez un ami qui vous envoie en pièces jointes des fichiers trouvés sur Internet. Vous les ouvrez et déclenchez du même coup un virus qui expédie des documents confidentiels à toutes les personnes figurant dans votre carnet d'adresses… vos concurrents y compris.

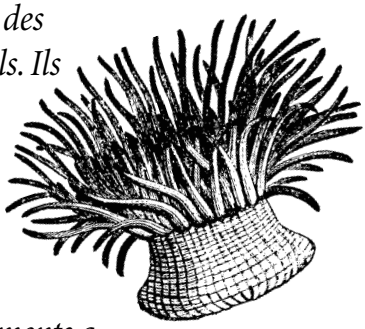
Enfin, imaginez que vous envoyiez malencontreusement à une autre entreprise un rapport contenant un virus. Se sentira-t-elle, par la suite, suffisamment en sécurité pour continuer à faire affaire avec vous ?

Ces incidents vous sont tous arrivés au moins une fois. A chaque fois, de simples précautions, de celles qui ne coûtent rien, auraient pu vous éviter ce souci.

Le but de ce guide est de vous indiquer les risques et comment les éviter.

Virus, chevaux de Troie et vers

Au milieu des années 80, Basit et Amjad ALVI de Lahore s'aperçurent que des personnes pirataient leurs logiciels. Ils réagirent en écrivant le premier virus informatique, programme plaçant sa propre réplique et un message de copyright dans chaque disquette copiée par leurs clients. De ces simples commencements a émergé toute une contre-culture du virus. Aujourd'hui, les nouveaux virus peuvent balayer la planète en quelques heures et les craintes qu'ils suscitent sont amplifiées par les médias. C'est ce qui fascine les gens, souvent mal informés. Lisez la suite, vous y apprendrez comment les virus se propagent et comment vous en protéger.



Qu'est-ce qu'un virus ?

Un virus informatique est un programme qui se répand à travers les ordinateurs et les réseaux en créant ses propres copies, et cela, généralement à l'insu des utilisateurs.

Les virus peuvent avoir des effets secondaires néfastes, qui vont de l'affichage de messages agaçants à la suppression de la totalité des fichiers placés dans votre ordinateur.

Comment le virus infecte-t-il l'ordinateur ?

Pour infecter votre ordinateur, un programme de virus doit au préalable être exécuté.

Les virus ont des moyens pour s'assurer que cela arrive. Ils peuvent se fixer sur d'autres programmes ou se dissimuler au sein d'un code de programmation qui s'exécute automatiquement à l'ouverture de certains types de fichiers.

Vous pouvez recevoir un fichier infecté depuis une disquette, une pièce jointe à un mail, ou le web lors d'un téléchargement.

Pour plus de précisions, reportez-vous aux "Virus du secteur de démarrage", "Virus parasites" et "Virus de macro" définis plus loin dans ce chapitre.

Chevaux de Troie

Les chevaux de Troie sont des programmes réalisant des actions non spécifiées dans leurs caractéristiques.

L'utilisateur lance un programme qu'il croit parfaitement légitime, permettant ainsi à celui-ci de réaliser des fonctions cachées, et souvent néfastes.

Par exemple, *Troj/Zulu* prétend être un programme destiné à corriger le bogue de l'an 2000 alors qu'en fait, il écrase le disque dur.

Les chevaux de Troie sont parfois utilisés comme moyen d'installer un virus chez un utilisateur.

Les chevaux de Troie par porte dérobée sont des programmes qui autorisent d'autres personnes que vous à prendre le contrôle de votre ordinateur au travers d'Internet.

Vers

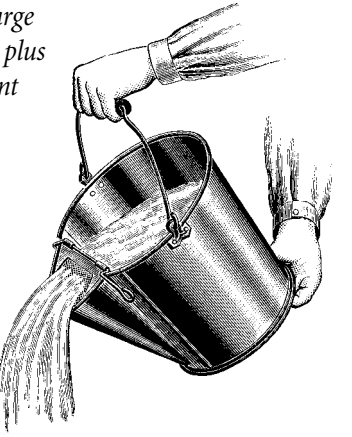
Les vers sont semblables aux virus, mais ne requièrent pas d'hôte (contrairement aux virus de macro ou du secteur de démarrage).

Les vers ne font que créer leur réplique exacte et utilisent les transmissions entre ordinateurs pour se propager.

De nombreux virus, tels *Kakworm* (*VBS/Kakworm*) ou *Love Bug* (*VBS/LoveLet-A*), se comportent comme des vers et s'expédient d'eux-mêmes à d'autres utilisateurs.

De quoi sont capables les virus ?

Les effets secondaires, souvent appelés la "charge virale", sont l'aspect des virus qui intéresse le plus les utilisateurs. Voici certaines des actions dont sont capables les virus.



Afficher un message — *WM97/Jerk* affiche le message "I think (user's name) is a big stupid jerk!".

Faire des farces — *Yankee* joue la chanson "Yankee Doodle Dandy" chaque jour à 17 heures.

Refuser un accès — *WM97/Nightshade* protège, tous les vendredis 13, par un mot de passe le document en cours.

Subtiliser des données — *Troj/Love Let-A* envoie par mail à une adresse aux Philippines des renseignements sur l'utilisateur et sa machine.

Altérer des données — *XM/Compatable* opère des changements dans les données des tableaux Excel.

Effacer des données — *Michelangelo* écrase des portions du disque dur tous les mardis 6.

Rendre le matériel inopérant — *CIH* ou *Chernobyl* (*W95/CIH-10xx*) entreprend d'écraser le BIOS le 26 avril, rendant de ce fait la machine inutilisable.

Les risques d'infection virale

Voici les différentes sources qui peuvent rendre votre ordinateur vulnérable.

Internet

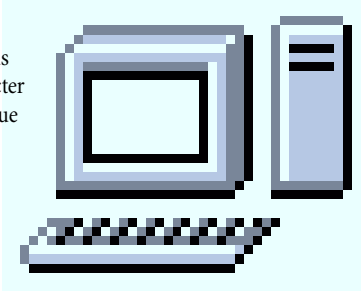
Les programmes ou fichiers documents téléchargés peuvent être infectés.

Documents et feuilles de calcul

Ils peuvent contenir des virus de macro capables d'infecter et d'opérer des changements dans d'autres fichiers documents ou feuilles de calcul.

Programmes

Les programmes transportant un virus sont capables d'infecter votre machine dès que vous les lancez.



Mails

Les mails peuvent inclure une pièce jointe infectée. Si vous double-cliquez dessus, vous risquez de contaminer votre machine. Certains mails contiennent même des scripts malveillants qui s'exécutent dès que vous les affichez en aperçu ou les lisez.

Disquettes et CD-ROM

Les disquettes peuvent contenir un virus dans leur secteur de démarrage ou renfermer des programmes ou des fichiers documents infectés ; tout comme les CD-ROM.

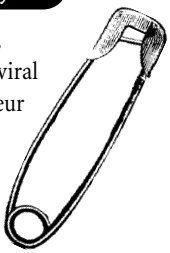
La prévention contre les virus

Il existe de simples mesures à prendre pour éviter l'infection virale ou traiter le virus quand l'infection est déjà là.

Sensibilisez les utilisateurs aux risques

Prévenez tous vos collègues que l'échange de disquettes, le téléchargement de fichiers depuis un site web et l'ouverture de pièces jointes aux mails sont des activités à risque.

Installez un antivirus et mettez-le régulièrement à jour



Les antivirus peuvent détecter les virus et, la plupart du temps, désinfecter leurs cibles. Si votre antivirus propose un contrôle viral sur accès, faites-en usage. Ce mode protège les utilisateurs en leur interdisant l'accès à tout fichier infecté. Voir la section "Les technologies antivirales" dans la suite de ce chapitre.

Sauvegardez toutes vos données

Réalisez des sauvegardes de tous vos programmes et données, y compris les systèmes d'exploitation. Si un virus vous atteint, vous aurez ainsi la possibilité de remplacer vos fichiers et programmes par des copies saines.

Pour plus de précisions, reportez-vous à la section "Dix mesures pour une informatique sécurisée".

Les virus du secteur de démarrage

Les virus du secteur de démarrage ont été les premiers à apparaître. Ils se propagent en modifiant le secteur d'amorçage, dans lequel se situe le programme permettant à l'ordinateur de démarrer.

Lorsque vous allumez votre ordinateur, le BIOS recherche le programme du secteur de démarrage – il se trouve généralement sur le disque dur, mais peut aussi se situer sur une disquette ou un CD-ROM – et l'exécute. Ce programme charge alors en mémoire le reste du système d'exploitation.

Le virus de secteur de démarrage est celui qui substitue sa propre version, modifiée, au secteur de démarrage d'origine (et cache en général l'original à un autre endroit du disque dur). Au démarrage suivant, l'ordinateur utilise le secteur de démarrage infecté et le virus est activé.

L'infection ne se produit que si vous amorcez le démarrage de l'ordinateur à partir d'un disque avec un secteur de démarrage infecté, comme par exemple une disquette.

Nombre de virus du secteur de démarrage sont désormais bien anciens. Généralement, ceux qui ont été programmés pour les machines fonctionnant sous DOS ne se propagent pas dans des ordinateurs sous Windows 95, 98, Me, NT ou 2000, bien qu'ils puissent parfois les empêcher de démarrer correctement.

Form

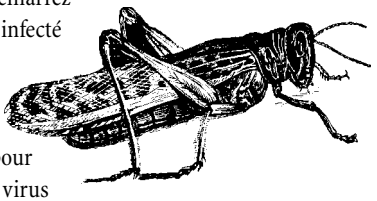
Ce virus est encore largement répandu dix ans après sa première apparition. La version originale produit un clic le 18 de chaque mois lorsqu'une touche de clavier est pressée.

Parity Boot

Ce virus peut afficher, de façon aléatoire, le message "PARITY CHECK" et figer brutalement le système d'exploitation. Le message a l'apparence des véritables messages d'erreur qui s'affichent lorsque la mémoire de l'ordinateur est défaillante.

Les virus parasites (virus de fichiers)

Les virus parasites, appelés aussi virus de fichiers, se fixent d'eux-mêmes sur des programmes (ou fichiers exécutables).



Lorsque vous démarrez un programme infecté par un virus, c'est le virus qui s'exécute en premier. Et pour se camoufler, le virus lance ensuite le programme original.

Le système d'exploitation de votre ordinateur voit le virus comme une partie du programme que vous essayez de lancer et lui donne les mêmes droits d'exécution. Cela permet au virus de se répliquer, de s'installer de lui-même en mémoire ou encore de libérer sa charge virale.

Les virus parasites sont apparus tôt dans l'histoire du virus informatique, mais sont toujours une menace réelle. Internet a plus que jamais facilité la propagation des programmes, donnant aux virus de nouvelles occasions de se répandre.

Jerusalem

Les vendredis 13, il supprime tous les programmes tournant sur l'ordinateur.

CIH (Chernobyl)

Le 26 de certains mois, ce virus écrase une partie du processeur du BIOS, rendant l'ordinateur inutilisable. Il est capable également d'écraser le disque dur.

Remote Explorer

WNT/RemExp (*Remote Explorer*) infecte les fichiers exécutables de Windows NT. Il fut le premier virus à pouvoir s'exécuter en tant que service, c'est à dire tourner sur des systèmes NT sans connexion du profil.

Les virus de macro

Les virus de macro exploitent les macros, qui sont des commandes incorporées aux fichiers, s'exécutant automatiquement.

De nombreuses applications, comme les traitements de texte ou les tableurs, utilisent des macros.

Un virus de macro est une macro qui peut se répliquer et se propager en passant d'un fichier à un autre. Si vous ouvrez un fichier contenant ce type de virus, ce dernier placera sa copie dans les fichiers de démarrage de l'application et l'ordinateur en sera infecté.

La prochaine fois que vous ouvrirez un fichier affecté à la même application, le virus infectera ce fichier. Si votre ordinateur est en réseau, l'infection peut se propager rapidement : quand vous envoyez un fichier, le destinataire peut également être infecté. Par ailleurs, un virus de macro malveillant peut opérer des changements dans vos fichiers documents ou vos paramètres.

Ces virus infectent les fichiers utilisés dans la plupart des entreprises et certains peuvent infecter plusieurs types de fichiers, tels ceux de Word ou Excel. Ils ont aussi la capacité de se répandre sur n'importe quelle plate-forme où tourne l'application. Et surtout, ils peuvent se propager sans difficulté, vu que les fichiers documents s'échangent fréquemment par mail ou téléchargement d'Internet.

WM/Wazzu

Il infecte les documents Word et insère le mot "wazzu", à l'aveuglette, tous les un ou trois mots.

OF97/Crown-B

Il infecte les fichiers Word, Excel et PowerPoint. Déclenché dans un document Word, il désactive la protection contre les macros des autres applications d'Office 97, pour pouvoir aussi les infecter.

Les technologies antivirales

Un moteur d'antivirus a la capacité de détecter les virus, interdire l'accès aux fichiers infectés et souvent éliminer l'infection. Voici une présentation des différents types de technologies antivirales disponibles.

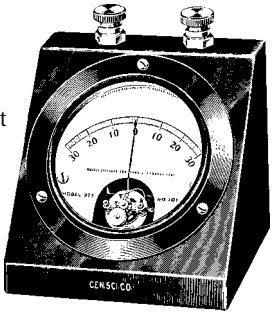
Les scanners

Les *scanners* de virus savent détecter et souvent supprimer les virus, connus à la date où le *scanner* est édité. Les *scanners* sont le type le plus courant d'antivirus mais ils doivent être mis à jour régulièrement si l'on veut qu'ils puissent reconnaître les nouveaux virus.

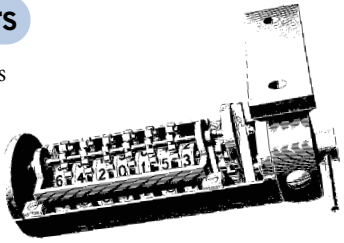
Il existe des *scanners* à la demande et des *scanners* sur accès. Nombre d'antivirus intègrent les deux.

Les *scanners* à la demande vous permettent de démarrer ou de planifier un contrôle sur des fichiers ou lecteurs spécifiques.

Les *scanners* sur accès, eux, restent actifs sur votre machine pendant que vous l'utilisez. Ils vérifient vos fichiers dès que vous tentez de les ouvrir ou de les exécuter.



Les checksummers



Ces programmes peuvent vous indiquer si des fichiers ont été modifiés. Si un virus infecte un fichier, programme ou document, en modifiant sa structure, les *checksummers* sont là pour signaler le changement.

Leur avantage est qu'ils n'ont pas besoin de connaître les caractéristiques d'un virus pour détecter sa présence ; ils ne requièrent donc pas de mise à jour régulière.

Leur inconvénient est qu'ils ne peuvent distinguer un virus de fichier d'une modification normale du fichier et les fausses alertes sont donc possibles. Les *checksummers* rencontrent des difficultés particulières avec les fichiers documents qui sont sujets à des changements fréquents.

En outre, les *checksummers* ne vous alertent qu'après que l'infection a eu lieu, ils ne savent pas identifier un virus et ne permettent pas la désinfection.

Les heuristiques

Les antivirus heuristiques tentent de détecter les virus – connus comme inconnus – en utilisant les règles générales de reconnaissance des virus. Au contraire des *scanners* de virus classiques, ce type d'antivirus ne s'appuie pas sur des mises à jour fréquentes de tous les virus connus.

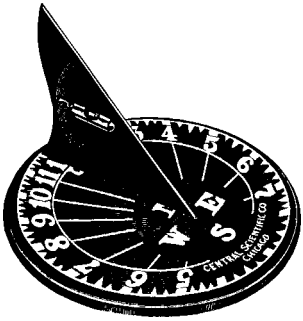
Cependant, si un nouveau type de virus apparaît, le logiciel ne le reconnaîtra pas et aura par conséquent besoin d'être actualisé ou même remplacé.

Les heuristiques sont enclins au déclenchement de fausses alertes.

Un bref historique des virus

1949 Le mathématicien John Von NEUMANN émet l'hypothèse selon laquelle les programmes informatiques pourraient se reproduire.

Années 50 Les laboratoires Bell développent un jeu expérimental où les joueurs utilisent des programmes malveillants pour attaquer leur ordinateur respectif.



1975 L'auteur de science-fiction John BRUNNER imagine un "ver" informatique qui se répandrait à travers les réseaux.

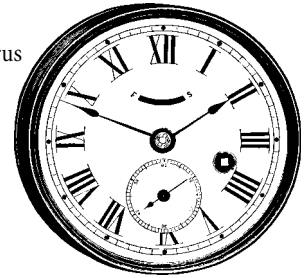
1984 Fred COHEN introduit le terme "virus informatique" dans une thèse portant sur ces programmes.

1986 On prétend que le premier virus informatique, *Brain*, a été écrit par deux frères pakistanais.

1987 Le ver *Christmas tree* paralyse le réseau mondial d'IBM.

1988 Le ver *Internet worm* se propage à travers le réseau internet américain DARPA.

1990 Mark WASHBURN écrit 1260, le premier virus polymorphe, qui mute (change de forme) à chaque nouvelle infection.



1992 Panique mondiale causée par le virus *Michelangelo,* même si, au bout du compte, très peu d'ordinateurs ont été infectés.

1994 Apparition de *Good Times*, premier grand canular de virus.

1995 Apparition du premier virus de macro, *Concept*. La même année, des programmeurs de virus australiens créent le premier virus écrit spécialement pour Windows 95.

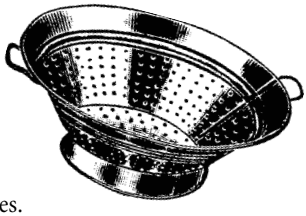
1998 *CIH* ou *Chernobyl* est le premier virus à paralyser le matériel.

1999 Propagation mondiale de *Melissa*, virus qui s'expédie lui-même par mail. Apparition de *Bubbleboy*, le premier à infecter un ordinateur lorsqu'on visualise un mail.

2000 *Love Bug* est devenu le virus de messagerie le plus efficace à ce jour. C'est aussi l'apparition du premier virus infectant le système d'exploitation des Palm, mais les utilisateurs n'en sont pas infectés pour autant.

Le coût caché des virus

En dehors de l'altération ou de la suppression de données, les virus peuvent aussi causer du tort à votre entreprise de façon moins évidente.



Tout le monde sait que les virus ont pour effets de supprimer ou d'altérer des fichiers. Cela est grave, mais vous pouvez rapidement récupérer vos données si, au préalable, vous les avez sauvegardées. Mais, certains effets secondaires, moins visibles eux, sont plus graves.

Des virus peuvent, par exemple, empêcher le fonctionnement des ordinateurs ou vous forcer à arrêter le réseau. Pendant ce temps, de précieuses heures de travail et a fortiori de recettes sont perdues.

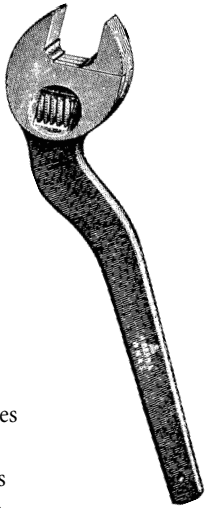
Certains virus interrompent les transmissions de mails, dont les entreprises dépendent. *Melissa* ou *ExploreZip*, qui se propagent par mail, peuvent occasionner tellement de mails que les serveurs tombent en panne. Et même si ce n'est pas le cas, il arrive, de toute façon, que les entreprises réagissent au risque en arrêtant leur serveur de messagerie.

Votre messagerie également est menacée. *Melissa* est capable d'expédier des documents pouvant contenir des informations sensibles, à n'importe quel contact de votre carnet d'adresses.

Les virus peuvent nuire gravement à votre crédibilité sur le marché. Si vous envoyez des documents infectés à vos clients, ils peuvent à l'avenir refuser de faire affaire avec vous et exiger des compensations, ce qui vous mettrait dans l'embarras ou risquerait de compromettre votre réputation sur le marché. Le meilleur exemple est *WM/Polypost,* qui poste des copies de vos documents, sous votre nom, sur les forums de discussion d'alt.sex.

Qui programme les virus ?

Si un virus atteint votre ordinateur ou votre réseau, votre première réaction – en dehors des jurons – serait de vous demander "Pourquoi programmer un virus ?"



A première vue, bien peu de raisons peuvent pousser quelqu'un à écrire un programme de virus. Les programmeurs de virus n'ont rien à gagner en termes d'argent ni de carrière ; ils atteignent rarement la célébrité ; et, contrairement aux pirates informatiques, ne ciblent pas de victimes particulières, les virus se propageant de façon imprévisible.

La programmation de virus se comprend plus facilement si on la compare à certains actes délictueux comme les graffitis ou le vandalisme.

Les programmeurs de virus sont plutôt des hommes, célibataires et âgés de moins de 25 ans. L'estime qu'ils ont d'eux-même est fortement liée à la reconnaissance de leurs pairs, ou tout au moins d'une petite communauté de fanas d'informatique. Leurs exploits, comme dans le graffiti, sont une sorte de performance offrant un statut au vainqueur.

Par ailleurs, les virus donnent à leur auteur des pouvoirs virtuels tels qu'il n'aurait jamais pu les espérer dans le monde réel. C'est sans doute pour cette raison que les programmeurs de virus s'attribuent des noms inspirés du Heavy Metal ou de la littérature fantastique, se nourrissant eux aussi de l'illusion de prouesse et de puissance.

Est-il toujours répréhensible de programmer des virus ?

La plupart d'entre nous considèrent comme un fait établi que les virus ne sont rien d'autre qu'un mal, mais est-ce forcément vrai ?

De nombreux virus sont "inoffensifs" ou revêtent l'apparence d'une blague. D'autres nous alertent sur des défauts dans la sécurité de certains logiciels. Certains soutiennent que les virus pourraient même s'avérer utiles, en prodiguant par exemple des correctifs pour les bogues. Malheureusement, l'innocuité supposée des virus ne résiste pas à un examen plus approfondi.

Premièrement, les virus opèrent des changements au sein des ordinateurs sans le consentement et parfois à l'insu des utilisateurs. C'est amoral – et illégal dans de nombreux pays – que l'intention en fût bonne ou mauvaise. On ne doit pas s'immiscer dans l'ordinateur d'autrui de la même façon qu'on n'irait pas emprunter la voiture de quelqu'un sans le lui dire – même si on a remis de l'essence.

Deuxièmement, les virus ne réalisent pas toujours ce qui était prévu par leur auteur. Si un virus est mal programmé, il peut causer des dégâts imprévisibles. Même s'il est inoffensif pour le système d'exploitation pour lequel il avait été conçu, un virus peut se révéler extrêmement destructeur sur d'autres plates-formes ou sur des systèmes destinés à être développés.

Les virus "proof-of-concept"

Parfois, des virus sont écrits pour prouver qu'on peut toujours en créer de nouveaux. On leur donne le nom de virus "*proof-of-concept*" (la preuve par trois). Ils sont généralement dépourvus d'effets secondaires (charge virale) et n'ont pas vocation à être largués sur d'autres ordinateurs.

De la recherche ?

Les programmeurs de virus aiment affirmer qu'ils font de la recherche. Pourtant, les virus sont des programmes de piètre qualité, lancés à l'aveuglette vers des utilisateurs qui ne s'y attendaient pas, et il n'existe aucun moyen d'en collecter les résultats. Ce n'est guère ce que l'on peut appeler de la recherche.

Les canulars de virus

Si vous avez été prévenu de l'existence de virus du nom de Good Times, Budweiser Frogs ou encore How to give a cat a colonic ("comment administrer un laxatif à votre chat"), c'est que vous avez été victime d'un canular. Les canulars de virus, et plus particulièrement ceux apparaissant dans les mails, sont chose courante et peuvent être tout aussi coûteux pour vous, en termes de temps et d'argent, que les véritables virus.

Qu'est-ce qu'un canular de virus?

Les canulars signalent des virus qui n'existent pas.
Le canular typique est un mail qui :

- Vous avertit de l'existence d'un nouveau virus, indétectable et extrêmement destructeur.
- Vous demande d'éviter la lecture des mails ayant un objet tel que : *Join the Crew* ou *Budweiser Frogs*, par exemple.
- Affirme que l'avertissement a été émis par une grande société informatique, un fournisseur d'accès Internet ou un organisme d'Etat, ex : IBM, Microsoft, AOL ou la FCC (équiv. américain de l'ART, qui régule les télécoms.)
- Affirme que le nouveau virus peut réaliser quelque chose d'improbable. Par exemple, *A moment of silence* annonce qu'il n'est pas nécessaire d'échanger un programme pour infecter un autre ordinateur.
- Emploie un jargon d'informaticien pour décrire les effets du virus, ex : *Good Times* annonce que le virus peut faire rentrer le processeur de votre PC dans "une boucle binaire infinie de complexité[n]".
- Vous conseille vivement de faire suivre l'avertissement aux autres utilisateurs.

Le canular qui n'en était pas un

Un mail intitulé *Rush-Killer virus alert* a commencé à circuler le 1er avril 2000. Il prévenait de l'existence de virus prenant le contrôle de votre modem et composant le 911 (numéro des urgences aux Etats-Unis), en conseillant vivement de faire suivre l'alerte. Le mail présentait tous les signes extérieurs d'un canular. Et pourtant ce virus était réel : c'était l'un des virus *BAT/911* qui se propagent à travers les partages Windows et appellent vraiment le 911. Distinguer un canular d'un vrai virus n'est pas chose facile ; suivez donc les conseils donnés à la fin de ce chapitre, dans "Que faire face aux canulars ?".

Les canulars sont problématiques

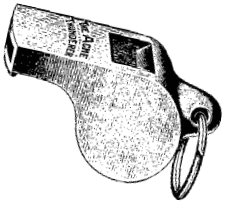
Les canulars peuvent être aussi perturbants et coûter autant qu'un virus authentique.

Si les utilisateurs font vraiment suivre un canular d'alerte à tous leurs amis et collègues, il en résulte un déluge de mails, qui peut submerger les serveurs et les faire tomber en panne. L'effet est le même que pour le vrai virus *Love Bug*, à la différence que l'auteur du canular n'a pas eu besoin de programmer le moindre code.

Les utilisateurs finals ne sont pas les seuls à réagir de façon excessive. Les entreprises, qui reçoivent fréquemment des canulars, prennent des mesures drastiques, telles que fermer leur serveur de messagerie ou couper leur réseau, ce qui paralyse les transmissions plus efficacement que le font beaucoup de virus réels, empêchant l'accès à des mails potentiellement importants.

Les fausses alertes virales détournent aussi les administrateurs réseaux de leur lutte contre les vraies menaces virales.

Par ailleurs, les canulars peuvent s'avérer remarquablement persévérants. Comme les canulars ne sont pas des virus, un antivirus ne peut ni les détecter, ni les désactiver.



Lequel est apparu en premier ?

Un canular peut inspirer une vraie menace virale et vice-versa. Après que le canular *Good Times* a fait les gros titres, certains programmeurs de virus ont attendu que cette rumeur soit entièrement démystifiée pour écrire un **vrai** virus affublé du même nom (les sociétés d'antivirus l'ont appelé *GT-Spoof*).

Que faire face aux canulars ?

Les canulars dépendent, de la même façon que les virus ou les chaînes de courriers, de leur propre capacité à se propager. Si vous parvenez à persuader les utilisateurs de briser la chaîne, vous limitez le mal.

Instaurez une politique d'entreprise sur les alertes virales

Une politique d'entreprise sur les alertes virales peut être la solution. En voici un exemple:

"Ne faites suivre d'alertes virales de quelque type que ce soit à PERSONNE D'AUTRE qu'à *celui ou celle qui est en charge de la sécurité antivirale au sein de l'entreprise*. Il importe peu que l'alerte virale provienne d'une société commercialisant des antivirus ou qu'une grande entreprise d'informatique ou votre meilleur ami l'ait confirmée. TOUTES les alertes virales doivent être réexpédiées à la *personne en charge de ces questions* et à elle seule. Cela fait partie de son métier de notifier à l'ensemble de la société les alertes virales. Celles qui sont issues de toute autre source doivent être ignorées."

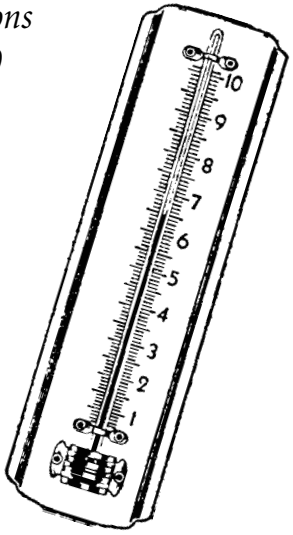
Tant que les utilisateurs suivront cette politique, ils ne seront pas inondés de mails et les personnes référentes de la société pourront décider de la validité du risque, s'il y a lieu.

Informez-vous en permanence sur les canulars

Informez-vous en permanence sur les canulars en consultant les pages Canulars et craintes de notre site web sur : www.sophos.fr/virusinfo/hoaxes

Le Top 10 des virus

Quels virus ont le mieux "réussi" de tous les temps ? Nous avons sélectionné pour vous les 10 virus qui ont parcouru les plus grandes distances, ont infecté le plus grand nombre d'ordinateurs... ou ont eu la plus longue durée de vie.



Love Bug

(VBS/LoveLet-A)

Love Bug est probablement le plus célèbre des virus. En feignant d'être un billet doux, il a joué sur la curiosité des utilisateurs, se propageant en quelques heures sur l'ensemble de la planète.

Première apparition : Mai 2000

Origine : Les Philippines

Alias : Love Letter

Catégorie : Ver Visual Basic Script

Déclenchement : Dès l'infection initiale

Effets : La version originale du virus envoie un mail avec l'objet "I LOVE YOU" et le texte "kindly check the attached love letter coming from me". L'ouverture de la pièce jointe permet au virus de s'exécuter. Si vous avez installé Microsoft Outlook, le virus s'en sert pour tenter de s'expédier lui-même à l'ensemble des contacts de votre carnet d'adresses. Il peut aussi se diffuser tout seul vers d'autres utilisateurs de forums de discussion, subtiliser des renseignements sur l'utilisateur infecté et écraser certains fichiers.

Form

Form figure dans le Top 10 *des virus depuis huit ans et reste encore très répandu. Sous DOS et les premières versions de Windows, il agissait discrètement, et a ainsi pu se propager largement.*

Première apparition : 1991

Origine : La Suisse

Catégorie : Virus du secteur de démarrage

Déclenchement : Le 18 du mois

Effets : Produit un clic chaque fois que vous appuyez sur une touche ; et peut également empêcher le fonctionnement des ordinateurs sous Windows NT.

Kakworm

(VBS/Kakworm)

Kakworm a rendu possible l'infection virale par simple visualisation de mail.

Première apparition : 1999

Catégorie : Ver Visual Basic Script

Déclenchement : Dès l'infection initiale (pour la plupart de ses effets) ou le premier de n'importe quel mois (pour l'effet arrêt de Windows)

Effets : Vous recevez le ver incorporé au message du mail. Si vous utilisez Microsoft Outlook ou Outlook Express avec Internet Explorer 5, il suffit de lire ou d'afficher en aperçu le mail infecté pour infecter votre machine. Le virus change les paramètres d'Outlook Express de façon à ce que le code du virus s'inclue automatiquement dans chaque mail émis. Le 1er de n'importe quel mois après 17h, il affiche le message "Kagou-Anti_Kro$oft says not today" et arrête Windows.

Anticmos

Anticmos est un virus de secteur de démarrage typique. Il était très répandu au milieu des années 90 et est apparu souvent parmi le Top 10 *des virus.*

Première apparition : Janvier 1994

Origine : Détecté la première fois à Hong Kong, mais on pense qu'il est originaire de Chine Populaire

Catégorie : Virus du secteur de démarrage

Déclenchement : Aléatoire

Effets : Tente d'effacer les informations sur le type de lecteurs de disquettes et disques durs installés.

Melissa

(WM97/Melissa)

Melissa est un virus de messagerie qui emploie des subtilités psychologiques pour se propager rapidement. On dirait qu'il provient de quelqu'un qu'on connaît et qu'il inclut un document qu'on doit à tout prix lire. Résultat, Melissa s'est propagé dans le monde entier en une seule journée.

Première apparition : Mars 1999

Origine : Un programmeur américain de 31 ans, David L Smith, a posté un document infecté sur le forum de discussion d'alt.sex

Catégorie : Virus de macro Word 97 ; exploite aussi Word 2000

Déclenchement : Dès l'infection initiale

Effets : Envoie un message aux cinquante premiers contacts de tous les carnets d'adresses accessibles à partir d'Outlook, en mettant le nom de l'utilisateur comme objet et un exemplaire du document infecté comme pièce jointe. Si, à l'ouverture du document, la minute et le quantième du mois sont identiques (ex : à 10h05 le 5 du mois), le virus y ajoute un texte sur le Scrabble.

New Zealand

New Zealand était bien le virus le plus courant au début des années 90.

Première apparition : Fin des années 80

Origine : La Nouvelle Zélande

Alias : Stoned

Catégorie : Virus du secteur de démarrage

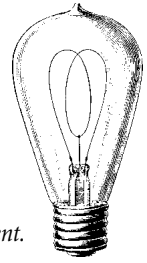
Déclenchement : 1 fois sur 8, si vous démarrez à partir d'une disquette

Effets : Il affiche le message "Your PC is now Stoned!", place une copie du secteur de démarrage d'origine dans le dernier secteur du répertoire racine sur les disquettes de 360 Ko ; mais peut aussi endommager des disquettes de plus grande capacité.

Concept

(WM/Concept)

Concept a remporté un succès instantané en étant accidentellement livré avec un logiciel standard de Microsoft. Ce fut le premier virus de macro découvert dans la nature et l'un des virus les plus courants des années 1996-98. Le virus prend le contrôle de Word au moyen de sa macro AutoOpen qui s'exécute automatiquement, et réalise l'infection au moyen de la macro "Enregistrer le fichier sous", lancée lorsque Word enregistre un document. Il a de nombreuses variantes.



Première apparition : Août 1995

Catégorie : Virus de macro

Déclenchement : Aucun

Effets : Lorsque vous ouvrez un document infecté, apparaît une boîte de dialogue intitulée "Microsoft Word" et contenant le chiffre 1. Le virus inclut le texte "That's enough to prove my point", mais ne l'affiche jamais.

CIH (Chernobyl)

(W95/CIH-10xx)

CIH a été le premier virus à endommager le matériel. Une fois qu'il a écrasé le BIOS, on n'a d'autre choix que de remplacer la puce du BIOS avant de pouvoir réutiliser l'ordinateur.

Première apparition : Juin 1998

Origine : Programmé par le Taïwanais Chen Ing-Hau

Catégorie : Virus parasite s'exécutant dans les ordinateurs sous Windows 95

Déclenchement : Le 26 avril. Ces variantes se déclenchent le 26 juin, ou bien le 26 de n'importe quel mois

Effets : Tente d'écraser le BIOS puis écrase le disque dur.

Parity Boot

Parity Boot se propage dans les secteurs de démarrage des disquettes. Son succès démontre que les virus du secteur de démarrage, qui étaient les plus courants dans les années 80 et au début des années 90, peuvent encore prospérer. Récemment encore (1998), il était encore parmi les virus les plus régulièrement signalés ; et plus particulièrement en Allemagne, où il fut diffusé en 1994 dans un CD-ROM distribué avec des magazines.

Première apparition : Mars 1993

Origine : Peut-être l'Allemagne

Catégorie : Virus du secteur de démarrage

Déclenchement : Aléatoire

Effets : Affiche le message "PARITY CHECK" et gèle d'un seul coup l'ordinateur, en imitant une authentique erreur mémoire. Résultat, les utilisateurs imaginent souvent qu'ils ont un problème avec leur RAM (mémoire vive de l'ordinateur).

Happy99

(W32/Ska-Happy99)

Happy99 a été le premier virus connu à se répandre rapidement par mail.

Première apparition : Janvier 1999

Origine : Posté sur un forum de discussion par le programmeur de virus français "Spanska"

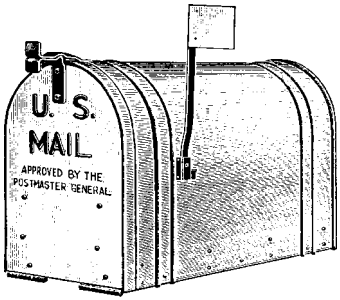
Catégorie : Virus de fichier s'exécutant dans les ordinateurs sous Windows 95/98/Me/NT/2000

Déclenchement : Aucun

Effets : Affiche un feu d'artifice et le message "Happy New Year 1999". Par ailleurs, le virus modifie le fichier wsock32.dll dans le dossier système de Windows de façon à ce que, à chaque fois qu'un mail est envoyé, un second message incluant le virus soit envoyé en même temps.

Les mails

Si vous demandez à des gens de citer un nom de virus, il y a de grandes chances que, pour la plupart, ce soit Love Bug ou Melissa. Ces virus, qui défrayent la chronique, ont en commun de se répandre à travers le monde par mail.



Les mails sont aujourd'hui la plus grande source de virus. Pourquoi en est-il ainsi ?

Tant que les virus étaient transférés par disquette, ils se propageaient avec lenteur. Les entreprises pouvaient interdire l'usage des disquettes ou exiger qu'elles soient examinées pour vérifier leur innocuité avant utilisation. Les mails ont changé tout cela. On peut maintenant échanger des fichiers beaucoup plus rapidement et infecter un PC n'est pas plus compliqué que de cliquer sur une icône – c'est même plus facile. Les virus classiques peuvent se propager plus vite et de nouveaux types de virus exploitent les fonctions des programmes de messagerie.

Peut-on attraper un virus juste en lisant un mail ?

Certains utilisateurs pensent qu'ils ne prennent aucun risque à ouvrir un mail tant qu'ils ne visualisent pas la pièce qui y est jointe. Ceci n'est plus nécessairement vrai aujourd'hui.

Les virus tels que *Kakworm* ou *Bubbleboy* sont capables d'infecter les utilisateurs à la lecture d'un mail. Ils ont l'apparence de n'importe quel autre message, mais contiennent pourtant un script caché qui s'exécute dès que vous ouvrez le mail, ou même le prévisualisez dans le panneau d'aperçu (si tant est que vous utilisiez Outlook avec la version correcte d'Internet Explorer). Ce script peut changer les paramètres de votre système et envoyer le virus à d'autres utilisateurs par mail.

Microsoft a émis un patch qui élimine cette faille dans la securité. Pour le télécharger, rendez-vous à www.microsoft.com/technet/security/bulletin/ms99-032.asp

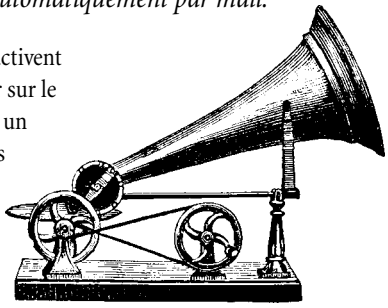
Les mails de canular

Les mails sont un vecteur courant pour les canulars. Ce sont de faux signalements de virus qui vous recommandent vivement de faire suivre le message à toutes les personnes que vous connaissez.

Un canular par mail peut se répandre à travers les réseaux de la même manière qu'un virus et provoquer une avalanche de mails, la différence étant que le canular ne nécessite pas de code viral : il ne repose que sur la crédulité des utilisateurs. Pour plus d'informations, reportez-vous au chapitre "Les canulars de virus".

Les virus qui se propagent automatiquement par mail

Les virus qui parviennent le mieux à se répandre aujourd'hui sont ceux que vous recevez automatiquement par mail.



Ce sont les virus typiques qui s'activent par un simple clic de l'utilisateur sur le document joint. Celui-ci exécute un script qui utilise les programmes de messagerie pour faire suivre les documents infectés à d'autres utilisateurs de mails. *Melissa*, par exemple, envoie un message aux cinquante premiers contacts de tous les carnets d'adresses auxquels Microsoft Outlook peut accéder. D'autres virus s'envoient d'eux-mêmes à tous les contacts du carnet d'adresse.

Qu'est-ce qu'un spam ?

Un *spam* est un mail non sollicité, qui fait souvent la promotion de plans d'enrichissement rapide, d'emplois à domicile, de prêts bancaires ou de sites à caractère pornographique. Les *spams* arrivent souvent avec de fausses références sur l'expéditeur, d'où la difficulté à réagir contre leur auteur. Ces mails doivent simplement être détruits.

Les risques d'une pièce jointe

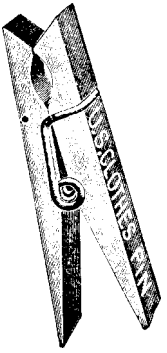
A l'heure actuelle, le plus grand risque pour la sécurité n'est pas le mail lui-même, mais la pièce jointe au mail.

N'importe quel programme, document ou feuille de calcul reçu par mail est susceptible de porter un virus ; le fait de lancer une telle pièce jointe peut infecter votre ordinateur.

Malheureusement, la pièce jointe au mail est un moyen courant d'échanger des informations. De nombreux utilisateurs pensent qu'il est "amusant et inoffensif" de faire circuler des écrans de veille, des cartes de vœux ou des programmes de blagues. Toutefois, ces fichiers sont capables de transporter des virus.

Même une pièce jointe apparaissant comme un type de fichier sûr (ex. : un fichier avec une extension .txt) représente une menace. Ce "fichier texte" peut se révéler être un *VBS script* malveillant avec une extension (.vbs) cachée.

Le ver *VBS/Monopoly* est un exemple de programme malveillant déguisé en divertissement. Il apparaît masqué en "blague sur Bill Gates". Ce qu'il est, puisqu'il affiche un plateau de Monopoly contenant des images de Microsoft. Par ailleurs, il s'expédie de lui-même à d'autres utilisateurs en communiquant les références de votre système à des adresses électroniques spécifiques, menaçant ainsi la confidentialité d'informations sensibles.

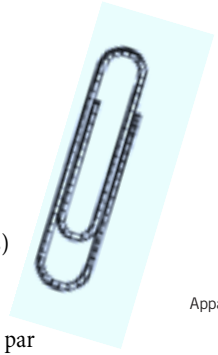


Interception et falsification de mails

L'interception de mails implique que d'autres utilisateurs que vous lisent vos mails en transit. Vous pouvez les protéger par le cryptage.

La falsification de mails correspond à l'envoi d'un mail avec une adresse d'expéditeur falsifiée ou en ayant eu accès à son contenu. Vous pouvez protéger vos mails par l'utilisation de signatures numériques.

Comment arrêter les virus de messagerie ?



Instaurez une politique stricte sur la gestion des pièces jointes

Le fait de modifier votre comportement (et celui des autres utilisateurs) est le moyen le plus simple de lutter contre la menace virale. N'ouvrez aucune pièce jointe, même si elle vient de votre meilleur ami. Ne vous laissez pas tenter par des promesses de plaisirs instantanés ou par ce qui est "amusant et inoffensif". Si vous ignorez si un élément est exempt de virus, traitez-le comme s'il était infecté. Instaurez donc une politique selon laquelle toutes les pièces jointes devront avoir reçu un agrément et été vérifiées par un antivirus avant d'être lancées.

Désactivez l'Exécution de Scripts

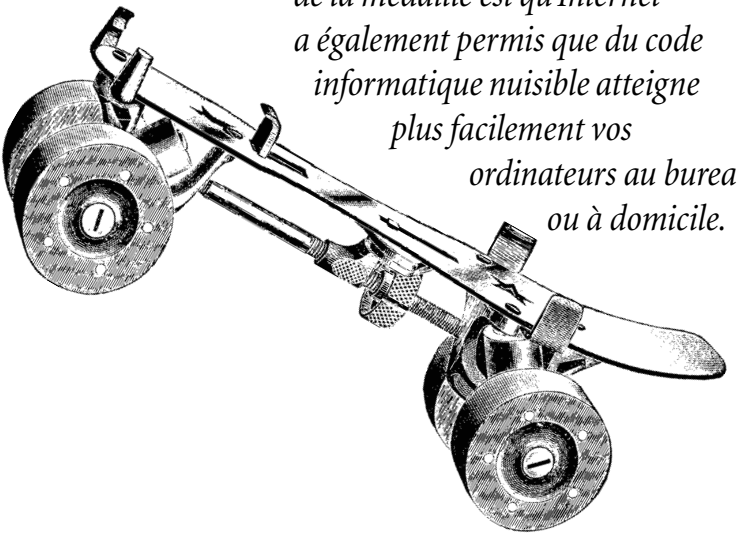
L'Exécution de Scripts(*WSH*) automatise certaines actions, telles que l'exécution de *VBS* ou de script Java sur les ordinateurs sous Windows. En outre, elle permet aussi à des virus comme *Love Bug* de se propager. Vous pouvez sans doute vous passer du *WSH* (mais consultez d'abord votre administrateur réseaux). Pour obtenir des instructions sur le retrait du *WSH* de l'ordinateur, reportez-vous à www.sophos.fr/support/faqs/wsh.html. Et rappelez-vous qu'à chaque fois que vous mettrez à jour Windows ou Internet Explorer, le *WSH* sera réinstallé.

Utilisez un logiciel antivirus

Utilisez un antivirus sur accès sur votre ordinateur de bureau et sur la passerelle de messagerie. Ces deux dispositions vous protégeront des virus envoyés par mail.

Internet

Internet a mis plus d'informations à disposition de plus de gens, et ce plus rapidement que jamais auparavant. Le revers de la médaille est qu'Internet a également permis que du code informatique nuisible atteigne plus facilement vos ordinateurs au bureau ou à domicile.



Un clic et c'est l'infection ?

Internet a augmenté le risque d'infection.

Il y a dix ans, la plupart des virus se répandaient par disquette. La propagation par ce vecteur était lente et dépendait des utilisateurs qui, pour être infectés, devaient exécuter sciemment de nouveaux programmes. Si le virus avait des effets secondaires trop évidents, il était peu susceptible d'affecter de nombreux utilisateurs. Maintenant qu'Internet est si largement utilisé, tout cela a changé.

La mise en commun de logiciels sur le net est facile. D'un clic de souris, vous joignez un programme à un mail et il est aisé de le détacher ensuite pour l'exécuter. Des utilisateurs peuvent tout aussi facilement placer un programme sur une page web, que n'importe qui peut télécharger. C'est ainsi que les virus de fichier (ou "parasites"), qui prennent pour cible les programmes, peuvent se développer sur le net.

Les virus qui bénéficient réellement de cette évolution, cependant, sont les virus de macro, qui affectent les documents ou feuilles de calcul. Les utilisateurs en téléchargent fréquemment, ou se les échangent par mail. Tout ce que vous avez à faire pour infecter votre ordinateur est de cliquer sur un fichier téléchargé ou une pièce jointe à un mail.

Lorsque vous utilisez Internet, ouvrez vos documents téléchargés avec un éditeur de texte qui ignore les macros, et n'exécutez pas les programmes qui ne viennent pas d'une source digne de confiance.

Puis-je être infecté juste en consultant des sites web ?

Consulter un site web est moins périlleux que d'ouvrir des programmes ou des documents inconnus. Les risques existent, néanmoins. La menace dépend du type de code utilisé par le site et des mesures de sécurité mises en place par le fournisseur d'accès et par vous. Voici les principaux types de code que vous rencontrerez.

HTML

Les pages web s'écrivent en HTML (ou *Hypertext Markup Language*). Ce langage permet aux créateurs de sites web de mettre en forme leur texte et de créer des liens vers des images et d'autres pages. Le code HTML ne peut abriter lui-même de virus. Cependant, les pages web peuvent contenir du code qui lance des applications ou ouvre des documents automatiquement. Cela présente le risque de lancer un élément infecté.

ActiveX

ActiveX est une technologie de Microsoft destinée aux développeurs web et utilisée uniquement sur les ordinateurs exécutant Windows.

Les applets ActiveX, utilisées pour créer des visuels sur les pages web, ont un accès total aux ressources de votre ordinateur, ce qui en fait une menace potentielle. Cependant, les signatures numériques, attestant de l'authenticité et de l'intégrité d'une applet, fournissent bel et bien une sécurité limitée.

D'autres types de code utilisés dans les sites web

Java

Si les gens s'inquiètent parfois outre mesure des virus d'Internet écrits en Java, c'est parce qu'ils confondent les applets Java, qui s'utilisent pour créer des effets sur les pages web, avec les applications et les scripts Java.

En général, les **applets** sont sûres. Elles sont exécutés seulement en environnement sécurisé (qu'on appelle la *sandbox*) par le navigateur. Même si une faille de sécurité peut laisser échapper une applet, une applet malveillant ne peut pas se propager aisément. Les applets s'écoulent habituellement d'un serveur vers les ordinateurs des utilisateurs, et non d'un utilisateur à un autre (vous dites à vos amis d'aller consulter un site, vous ne lui envoyez pas une copie de l'applet). De surcroît, les applets ne sont pas sauvegardées sur le disque dur, sauf dans le cache du navigateur web.

Si malgré tout, vous rencontrez une applet néfaste, c'est très probablement un cheval de Troie, c'est à dire un programme malveillant feignant d'être un véritable logiciel.

Les **applications Java** sont simplement des programmes écrits en langage Java. A l'instar de tout autre programme, elles sont capables de porter un virus. Vous devez les traiter avec la même prudence que celle dont vous feriez preuve avec d'autres programmes.

Un **JavaScript** est un script incorporé à du code HTML dans les pages web. Comme n'importe quel autre script, il peut réaliser des opérations de façon automatique, ce qui comporte des risques. Vous pouvez désactiver les scripts actifs (reportez-vous à "La sécurité sur le net" à la fin de ce chapitre).

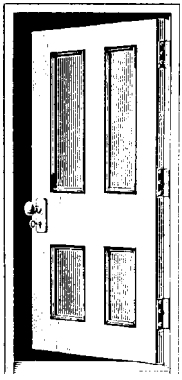
Les scripts VBS

Les VBS (scripts en Visual Basic) peuvent s'exécuter dès qu'une page est visualisée, selon le navigateur utilisé. Vous n'avez rien à faire pour les lancer.

Ces scripts sont utilisés par les vers de messagerie tels *Kakworm* ou *Bubbleboy*, mais peuvent tout aussi bien être exécutés depuis une page web.

Les chevaux de Troie par porte dérobée

Un cheval de Troie par porte dérobée est un programme qui autorise quelqu'un à prendre le contrôle de la machine d'un autre utilisateur par l'intermédiaire d'Internet.



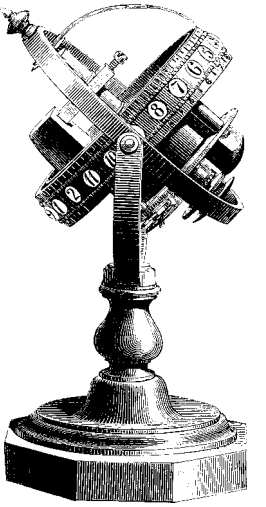
De même que les autres chevaux de Troie, le cheval de Troie par porte dérobée se présente comme un programme légitime qui donne envie d'être utilisé. Lorsqu'il est exécuté (en général, sur un PC sous Windows 95/98), il s'ajoute de lui-même à la routine de démarrage du PC. Le cheval de Troie peut ensuite surveiller le PC jusqu'à ce que ce dernier se connecte à Internet. Une fois que le PC est en ligne, celui qui a envoyé le cheval de Troie peut utiliser les logiciels de son ordinateur pour ouvrir ou fermer des programmes sur l'ordinateur-cible, modifier des fichiers et même envoyer des éléments sur son imprimante. *Subseven* et *BackOrifice* sont parmi les chevaux de Troie par porte dérobée les plus connus.

Les cookies sont-ils un risque ?

Les *cookies* ne représentent pas de menace directe pour votre ordinateur ou les données qui y sont placées. Cependant, ils sont vraiment une menace pour la confidentialité : un cookie permet à un site web de conserver vos références et de suivre à la trace vos visites du site. C'est pourquoi, si vous préférez garder l'anonymat, vous devriez désactiver les *cookies* en utilisant les paramètres de sécurité de votre navigateur.

Les attaques sur les serveurs web

Les utilisateurs ne sont pas les seuls à être menacés sur Internet. Certains pirates informatiques prennent pour cible les serveurs web qui diffusent les sites web que l'on consulte depuis un ordinateur.



Il existe une forme courante d'attaque qui consiste à envoyer tellement de requêtes à un serveur web qu'il ralentit ou tombe en panne. Lorsque cela arrive, les vrais utilisateurs ne peuvent plus consulter sur les sites web hébergés par le serveur.

Les scripts CGI (ou *Common Gateway Interface*) sont un autre point faible. Ces scripts s'exécutent sur les serveurs web pour gérer les moteurs de recherches, avaliser les entrées d'un formulaire, et autres. Les pirates informatiques sont capables de tirer profit de scripts CGI rédigés de façon médiocre pour prendre le contrôle d'un serveur.

La sécurité sur le net

Si vous souhaitez faire usage des paramètres de sécurité d'Internet, voici ce que vous devez faire :

Isolez de votre réseau les machines d'accès à Internet

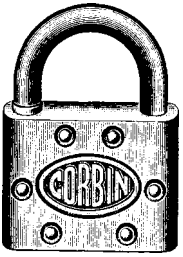
Séparez vos réseaux entre les ordinateurs connectés à Internet et ceux qui n'ont qu'un intranet. Cette manipulation diminue les risques de téléchargement de fichiers infectés et de propagation des virus sur votre réseau principal.

Utilisez des pare-feux et/ou routeurs

Un pare-feu permet au seul trafic autorisé de pénétrer dans votre entreprise. Un routeur, quant à lui, contrôle le flux de paquets de données reçus au travers d'Internet.

Paramétrez la sécurité de votre navigateur Internet

Désactivez les applets Java ou ActiveX, les *cookies*, etc., ou demandez à être averti lorsque ces types de code sont exécutés. Par exemple, dans Internet Explorer de Microsoft, sélectionnez **Outils|Options Internet |Sécurité| Personnalisez le Niveau** et sélectionnez les paramètres de sécurité que vous souhaitez.

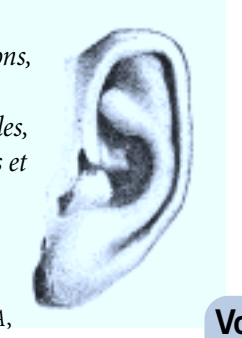


Téléphones mobiles et portables palmtops

La dernière décennie amenait le monde (ou le web mondial) sur votre ordinateur de bureau ; la prochaine l'amènera sur votre téléphone mobile. Vous pouvez déjà accéder à des sites et des services de type internet sur les mobiles de nouvelle génération et la technologie se développe vite. Mais comme il devient plus aisé de transférer des données – même en déplacement – le risque est que de nouvelles menaces à la sécurité émergent elles aussi.

Existe-t-il des virus pour téléphones mobiles ?

Au moment où nous écrivons, il n'existe aucun virus qui infecte les téléphones mobiles, malgré les dires des médias et les canulars.



Il y **a eu** des virus qui envoyaient des messages aux mobiles. Exemple, *VBS/Timo-A*, un ver se propageant de lui-même par mail, utilise également les modems pour envoyer des mini-messages (SMS) à une sélection de numéros de téléphones mobiles. Le virus notoire *Love Bug* a aussi la faculté d'expédier du texte vers des télécopieurs et des mobiles. Cependant, ces virus ne sont pas capables d'infecter ou de porter atteinte à votre téléphone mobile.

Les choses pourraient changer à mesure que les téléphones mobiles se font plus sophistiqués.

Vos données courent-elles des risques ?

Les appareils mobiles ne sont pas un lieu aussi sûr pour placer vos données qu'un PC :

- Ils se perdent ou se volent facilement.
- Les coupures d'alimentation peuvent faire perdre les données qui s'y trouvent.
- Les données n'y sont pas sauvegardées.

A mesure que les appareils mobiles se complexifient, ils pourraient aussi devenir vulnérables aux virus ou aux piratages informatiques.

Mobiles WAP et virus

La nouvelle technologie, dont on parle le plus dans ce domaine, est le WAP (ou Wireless Application Protocol*).*

Le WAP vous apporte des informations et des services de type internet sur votre téléphone mobile ou votre organiseur. Il est basé sur le même modèle que les communications web, c'est à dire qu'un serveur central transmet du code au navigateur de votre téléphone qui l'exécute. Pour l'instant, les possibilités de virus sont donc très limitées.

Un virus pourrait infecter le serveur lui-même, mais les chances qu'il se propage ou qu'il ait un effet sur les utilisateurs seront très faibles.

Premièrement, il n'y a aucun endroit sur un système WAP où un virus pourrait se répliquer ou survivre. Contrairement à un PC, un téléphone WAP ne stocke pas d'applications. Le téléphone télécharge le code dont il a besoin et n'en garde aucune copie, sauf de façon provisoire dans le cache du navigateur.

Deuxièmement, un virus peut d'autant moins se propager d'un utilisateur à un autre qu'il n'y a pas de communications entre deux téléphones clients.

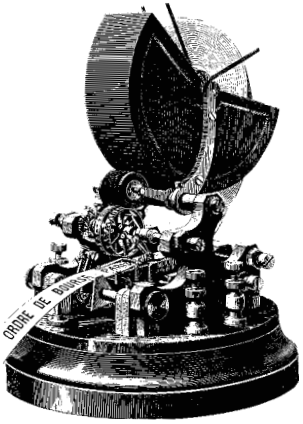
En théorie, un "virus" pourrait diffuser des *liens* vers des sites WAP malveillants, les utilisateurs étant alors tentés d'utiliser des applications néfastes, mais cela implique encore d'exécuter du code depuis le serveur.

Mots à la mode

WAP	*Wireless Application Protocol*
WML	*Wireless Markup Language*
WML Script	C'est un langage de programmation similaire au script Java
Cartes	C'est le nom des pages en WML
Jeu de cartes	C'est un ensemble de pages reliées entre elles, toutes disponibles pour un navigateur WAP sans téléchargement supplémentaire

Les risques à venir du WAP

Le WAP utilise une version du HTTP, le protocole des pages web, qui a la capacité de transmettre des contenus plus complexes que ceux que traitent à présent les navigateurs WAP. Une future génération de navigateurs pourrait être capable de télécharger des fichiers, tels que les documents, qui peuvent héberger des virus de macro.



Sous WAP, les serveurs seront bientôt capables de délivrer de façon automatique et systématique (le *push*) du contenu sur les téléphones mobiles. En dehors du fait d'alerter les utilisateurs sur des informations actualisées (telles que des résultats financiers ou des scores de matchs) ou de nouveaux mails reçus, la technologie *push* a la capacité de télécharger des données dans le cache – sans que vous ayez à agir. Du code malveillant pourrait exploiter ce système pour se diffuser de lui-même.

Il existe encore d'autres problèmes potentiels. Par exemple, des sites WAP malveillants pourraient s'afficher comme pourvoyeurs de services utiles. De tels sites pourraient faire tomber en panne le navigateur de l'utilisateur ou obturer sa mémoire.

Mots à la mode

XML	*eXtensible Markup Language*, recommandé pour l'utilisation sur le *world wide web*
WTLS	*Wireless Transport Layer Security.* Méthode de cryptage utilisée sur les réseaux de téléphonie mobile

Les systèmes d'exploitation des mobiles

Les ordinateurs palmtops *ou les assistants personnels numériques (les* PDA*) sont susceptibles, dans un avenir très proche, de créer de nouvelles opportunités pour les virus.*

Les portables *palmtops* et les *PDA* utilisent des systèmes d'exploitation spécialement écrits pour eux ou réduits à leur échelle, parmi lesquels EPOC, PalmOS ou PocketPC (anciennement Windows CE). Ces systèmes finiront par pouvoir utiliser les versions ordinateur de bureau des applications les plus courantes, ce qui les rendra vulnérables au code malveillant de la même façon que les machines de bureau. Début 2001, il y avait déjà des virus affectant le système des Palm.

Les portables *palmtops* sont par ailleurs régulièrement connectés au PC du domicile ou du bureau pour synchroniser les données sur les deux machines (par ex. : des contacts du carnet d'adresses ou le calendrier). Cette synchronisation de données pourrait permettre aux virus de se propager facilement.

Personne ne sait encore lequel, des ordinateurs mobiles ou des *smart phones*, obtiendra le plus de succès. Que ce soit l'un ou l'autre, les risques pour la sécurité augmenteront à mesure que les ordinateurs mobiles deviendront plus communicants.

Mots à la mode

EPOC	C'est un système d'exploitation pour portables *palmtop*
PDA	*Personal Digital Assistant*
PalmOS	Système d'exploitation pour les ordinateurs Palm
PocketPC	Système d'exploitation de Microsoft pour portables *palmtop*, anciennement Windows CE
UPNP	*Universal Plug and Play*, c'est un système de Microsoft qui permet les connexions entre les ordinateurs mobiles et d'autres appareils

Des virus dans votre frigo ?

Des appareils de plus en plus variés "se parleront" bientôt les uns aux autres en utilisant les liaisons infrarouges ou les ondes radio basse tension, faisant apparaître de nouveaux risques pour la sécurité.

Bluetooth est une norme de transmission de données par ondes radio basse tension de très faible portée, (par ex. : 10 m). Les ordinateurs, téléphones mobiles, télécopieurs et même les appareils domestiques tels que les magnétoscopes ou les réfrigérateurs pourront utiliser *Bluetooth* pour connaître les services fournis par d'autres appareils voisins et établir des liaisons avec eux de façon transparente.

Les logiciels exploitant *Bluetooth* émergent. La technologie *Jini* de Sun, par exemple, permet à des appareils de créer des connexions, d'échanger du code Java de façon automatique et de donner un contrôle des services à distance. Le risque est qu'un utilisateur non autorisé, ou du code malveillant, puisse exploiter *Bluetooth* pour interférer avec ces services.

Bluetooth et *Jini* sont conçus pour veiller à ce que seul du code dans lequel on a confiance et provenant de sources connues puisse réaliser des opérations sensibles. Ces mesures rendent peu probable un accès viral, mais si un virus contourne bel et bien la sécurité, il est possible qu'il n'y ait pas grand chose à faire pour stopper sa propagation.

Mots à la mode

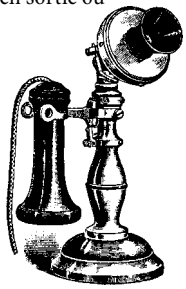
3G	Technologie mobile de "3ème génération"
Bluetooth	Transmission de données par ondes radio de faible portée
Jini	C'est une technologie qui permet à des appareils d'échanger du code Java
MExE	*Mobile station application Execution Environment,* c'est un successeur possible au WAP qui permettrait aux fournisseurs de services de télécharger du code Java vers un mobile

Comment protéger les appareils mobiles ?

A mesure que la technologie des mobiles et des PDA *évolue, les mesures de securité devront être adaptées. Le problème principal étant de savoir où utiliser ces mesures antivirales.*

Le contrôle à la passerelle et durant le transfert des données

Dans un avenir proche, le meilleur moyen de protéger les appareils mobiles pourra être de vérifier les données lors de leur transfert en sortie ou en entrée. Pour les téléphones mobiles, par exemple, la passerelle WAP pourrait être un bon endroit pour installer une protection antivirale. Toutes les transmissions passent par cette passerelle sous une forme non cryptée, et il y aurait ainsi une occasion idéale de réaliser un contrôle antiviral.



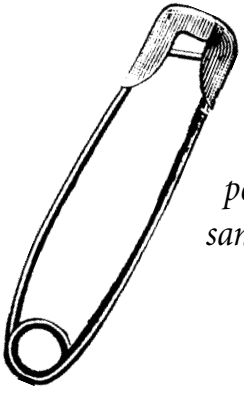
Pour les ordinateurs *palmtops*, on pourrait utiliser une protection antivirale lors de la synchronisation des données du *palmtop* avec un PC ordinaire. Le PC pourrait exécuter la majeure partie du logiciel de vérification virale, et de ce fait, le manque de puissance ou de mémoire du *palmtop* ne serait plus un problème.

Le contrôle antiviral sur les appareils mobiles

Comme les appareils mobiles s'interconnectent de plus en plus, il deviendra difficile de surveiller le transfert de données en un point central. La solution sera de mettre un antivirus dans chaque appareil – une fois qu'ils auront acquis une puissance de traitement et une mémoire suffisantes.

Dix mesures pour une informatique sécurisée

Outre l'utilisation d'un logiciel antivirus, il y a une foule de mesures simples à prendre pour vous aider à vous protéger ainsi que votre entreprise contre les virus. Voici les dix trucs importants pour une informatique sans souci.



Mesures pour une informatique sécurisée

N'utilisez pas de documents au format .doc ou .xls

Enregistrez vos documents Word en RTF (*Rich Text Format*) et vos feuilles de calcul Excel comme fichiers CSV (*Comma Separated Values*). Ces formats ne supportent pas les macros, et par conséquent ne peuvent propager de virus de macros, qui constituent de loin la menace virale la plus courante. Dites aux autres personnes de vous envoyer des fichiers avec respectivement les extensions RTF ou CSV. Attention, cependant ! Certains virus de macros interceptent la macro EnregistrerSous RTF, qui sauvegarde alors le fichier à cette extension, mais en conservant le format DOC. Pour être en totale sécurité, sélectionnez "texte seulement".

Ne lancez pas de programmes ou de documents non sollicités

Si vous ne savez pas si un élément est exempt de virus, partez du principe qu'il ne l'est pas. Dites aux personnes de votre entreprise qu'ils ne doivent pas télécharger de programmes ou de documents non autorisés depuis Internet, y compris des écrans de veille ou des programmes de "blagues". Instaurez une politique selon laquelle tous les programmes doivent recevoir l'agrément du Responsable Informatique et que l'absence de virus doit être vérifiée avant leur utilisation.

Ne faites suivre les avertissements sur les virus qu'à la personne autorisée

Les canulars sont un problème aussi important que les virus eux-mêmes. Dites aux utilisateurs de ne pas faire suivre les avertissements sur les virus à leurs amis, collègues ou à quiconque figurant dans leur carnet d'adresses. Instaurez une politique d'entreprise selon laquelle toutes les alertes virales devront parvenir uniquement à la personne ou au service responsable.

Mesures pour une informatique sécurisée

Si vous n'avez pas besoin de l'Exécution de Scripts, retirez-la

L'Exécution de Scripts (*WSH*) automatise certaines tâches sur les ordinateurs sous Windows, mais elle vous rend également vulnérable aux virus de messagerie comme *Love Bug* ou *Kakworm*. A moins que vous en ayez besoin, désactivez-la. Pour les instructions, consultez la Foire Aux Questions du web sur www.sophos.fr/support/faqs/wsh.html

Suivez les bulletins de securité des autres éditeurs de logiciels

Guettez les dernières infos sur la sécurité et téléchargez des patchs pour vous protéger contre les menaces virales. Voir le chapitre "Liens utiles".

Bloquez les types de fichiers non désirés à la passerelle

De nombreux virus utilisent aujourd'hui les *VBS* (Scripts en Visual Basic) et le type de fichiers *scrap object* (.SHS) de Windows pour se propager. Comme il est peu probable que vous ayez besoin qu'on vous envoie ces types de fichiers de l'extérieur, bloquez-les plutôt à la passerelle de messagerie.

Changez la séquence de démarrage de votre ordinateur

La plupart des ordinateurs essaient de démarrer en premier sur la disquette (souvent le lecteur A:). Il est préférable que votre service informatique change les paramètres du CMOS de manière à ce que l'ordinateur démarre par défaut sur le disque dur. Dans ce cas, même si une disquette infectée est laissée dans l'ordinateur, elle ne pourra infecter le secteur de démarrage du disque. Si, à l'occasion, vous avez besoin de démarrer à nouveau sur une disquette, vous pourrez rétablir les paramètres initiaux.

Mesures pour une informatique sécurisée

Protégez vos disquettes en écriture

Protégez vos disquettes en écriture avant de les donner à d'autres. Une disquette protégée en écriture ne peut pas s'infecter.

Abonnez-vous à un service d'alertes virales par mail

Un service d'alertes virales peut vous avertir de l'apparition de nouveaux virus et vous proposer les identités virales qui permettront à votre antivirus de les détecter. Sophos a un service d'alertes virales gratuit. Pour des précisions, consultez www.sophos.fr/virusinfo/notifications

Sauvegardez régulièrement vos données

Si un virus vous infecte, vous serez ainsi en mesure de restaurer tous les programmes et données perdus.

Liens utiles

Consultez ces sites pour plus d'informations

Analyses virales
http://www.sophos.fr/virusinfo/analyses

Bulletins de Sécurité de Microsoft
http://www.microsoft.com/france/technet/default.asp

Canulars et craintes sur les virus
http://www.sophos.fr/virusinfo/hoaxes
http://www.vmyths.com (en anglais)

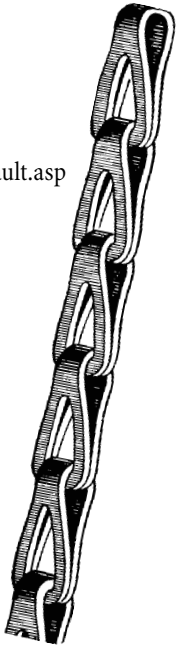
Envoi automatique d'alertes virales par mail
http://www.sophos.fr/virusinfo/notifications

Informations sur la sécurité de Java
http://www.java.sun.com/security (en anglais)

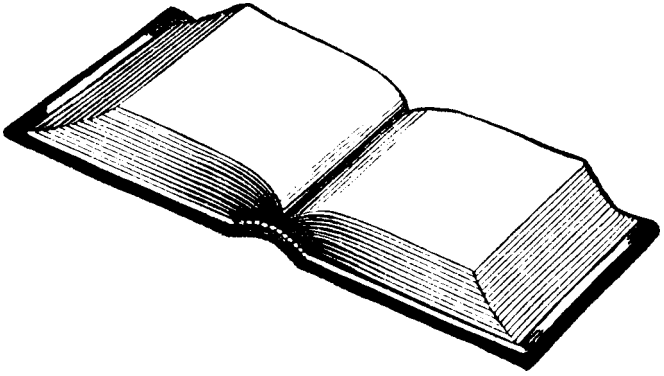
La *WildList Organization*
http://www.wildlist.org (en anglais)

Le *Virus Bulletin*
http://www.virusbtn.com (en anglais)

Netscape Security Center
http://home.netscape.com/fr/security



Lexique



ActiveX	Technologie de Microsoft qui accroît les capacités de votre navigateur web.
Agents doubles (ou *spoof*)	Ils prennent l'identité de quelqu'un ou de quelque chose d'autre (en contrefaisant, par ex., l'adresse de l'expéditeur du mail).
Amorçage	Processus se réalisant lorsqu'on allume un ordinateur, par lequel le système d'exploitation est chargé depuis un disque.
Applet	Une "petite application". On parle habituellement d'applets Java.
Applet Java	Petite application utilisée généralement pour créer des effets dans les pages web. Les applets sont exécutées par le navigateur dans un environnement sain (voir *Sandbox*) et ne peuvent pas opérer de changements dans votre système.
Application Java	Programme basé sur Java qui peut mener à bien les fonctions complètes qu'on attend de lui, comme sauvegarder des fichiers sur un disque.
ASCII	*American Standard Code for Information Interchange*. C'est le système normatif de représentation des lettres et symboles.
BIOS	*Basic Input/Output System* (système de base d'entrées/sorties). C'est le logiciel de la couche inférieure qui fait l'interface avec le matériel.
Canular	Signalement d'un virus qui n'a jamais existé.
CGI	*Common Gateway Interface*. C'est un mécanisme permettant au serveur web d'exécuter des programmes ou des scripts et d'en envoyer le résultat à un navigateur web.
Cheval de Troie	Programme informatique ayant des effets (indésirables) qui ne sont pas décrits dans ses spécifications.

Cheval de Troie par porte dérobée	Programme de cheval de Troie qui donne à un utilisateur distant un accès et un contrôle non autorisés sur un ordinateur.
Cookie	Petit paquet de données qui renferme des renseignements sur l'ordinateur d'un utilisateur. Les *cookies* sont généralement utilisés pour permettre à un site web de suivre à la trace les visites et les caractéristiques des utilisateurs.
CSV	*Comma Separated Values*. C'est un format de fichier dans lequel les valeurs (ex. : celles d'une feuille de calcul Excel) apparaissent – *cf.* son nom – séparées par des virgules. Ce format ne supporte pas les macros, et ne peut donc pas propager de virus de macro.
Disque dur	Disque magnétique, généralement interne à un ordinateur, et utilisé pour stocker des données.
Disquette	Disque magnétique amovible souple utilisé pour stocker des données.
Enregistrement d'amorçage maître	Le *master boot record*, appelé aussi secteur de partition, est le premier secteur physique du disque dur à être chargé et exécuté lorsqu'un PC amorce son démarrage ; et par ailleurs la partie la plus critique dans le code du démarrage.
FTP	*File Transfer Protocol*. C'est le système permettant aux utilisateurs d'Internet de se connecter à des sites distants pour télécharger des fichiers (d'un serveur web au terminal ou dans le sens inverse).
HTML	*Hypertext Markup Language*. C'est le format de la plupart des documents sur le web.
HTTP	*Hypertext Transport Protocol.* C'est le protocole utilisé par les serveurs web pour rendre les documents d'un site disponibles pour les navigateurs.
Hypertexte	Texte lisible par un ordinateur qui permet une création étendue de liens vers des fichiers.

Identité virale	Description des caractéristiques d'un virus que l'on utilise pour sa reconnaissance.
Internet	Signifie un réseau composé de nombreux réseaux interconnectés ; Internet étant de loin le plus vaste d'entre eux.
Java	Langage de programmation indépendant des plates-formes ou du web où il s'utilise, developpé par Sun Microsystems. Les programmes écrits en Java sont soit des applications, soit des applets.
Macro	Ensemble d'instructions au sein de fichiers de données qui peuvent réaliser automatiquement des commandes de programme, ex. : l'ouverture ou la fermeture de fichiers.
Modem	Le MOdulateur/DEModulateur convertit les données informatiques dans une forme adaptée à la transmission par ligne téléphonique, liaison radio ou satellite.
Mot de passe	Suite de caractères donnant accès à un système.
Navigateur web	Programme utilisé pour accéder à des informations sur le web, c'est donc la partie "client" du web.
Ordinateur *palmtop*	Il est suffisamment petit pour tenir sur la paume (*palm*) de votre main.
Par porte dérobée	Moyen dissimulé de contourner le système normal de contrôle d'accès à un ordinateur. Voir Cheval de Troie par porte dérobée.
Pare-feu	Système de sécurité placé entre Internet et le réseau d'une entreprise – ou au sein-même d'un réseau – pour ne laisser passer que le trafic réseau autorisé.
Passerelle	Ordinateur servant au transfert de données (ex. d'une passerelle de messagerie, par laquelle transitent tous les mails parvenant à une entreprise) ; ce peut être aussi un ordinateur qui convertit des données d'un protocole dans un autre (ex. en messagerie : du SMTP en POP3).

PC	*Personal Computer* (ordinateur individuel). C'est un ordinateur autonome, de bureau ou portable.
PDA	*Personal Digital Assistant*. C'est un petit appareil informatique mobile qui s'utilise la plupart du temps pour gérer les données des carnets d'adresses ou des calendriers.
Pièce jointe	Fichier document, feuille de calcul, image, programme ou de tout autre type, qui est greffé sur le message d'un mail.
Pirate informatique	Utilisateur d'ordinateur qui tente de débusquer un accès non autorisé aux systèmes informatiques d'autres utilisateurs.
Portable *laptop*	Ordinateur portatif suffisamment petit pour être utilisé sur les genoux (*on top of the lap*).
Portable *notebook*	Ordinateur encore plus petit qu'un portable *laptop* (*notebook* = carnet) ; appellé aussi "ultra-portable".
Poste de travail	Ordinateur individuel, souvent connecté à un réseau.
Programme	Ensemble d'instructions qui indique à un ordinateur les actions à réaliser.
RAM	*Random Access Memory*, une sorte de mémoire temporaire de l'ordinateur. Cette mémoire vive agit comme l'espace de travail de la machine, mais les données qui y sont stockées sont perdues une fois l'ordinateur éteint.
ROM	*Read Only Memory*, une sorte de mémoire permanente dans l'ordinateur. Cette mémoire morte s'utilise généralement pour stocker le logiciel de démarrage d'un ordinateur.
RTF	*Rich Text Format*. C'est un format de fichier document qui ne supporte pas les macros, et ne peut donc pas propager de virus de macros.
Sandbox	Mécanisme servant à exécuter des programmes en environnement contrôlé, en particulier au moyen d'applets Java.

Sauvegarde	Copie des données d'un ordinateur s'utilisant pour recréer les données qui ont été perdues, égarées, altérées ou effacées.
***Scanner* de virus**	Programme qui détecte les virus. La plupart des *scanners* sont viro-dépendants, c'est à dire qu'ils identifient ceux des virus qu'ils connaissent déjà. Voir aussi *Scanner* heuristique.
***Scanner* heuristique**	Programme qui détecte les virus en utilisant des règles générales sur l'aspect courant et le mode de comportement des virus.
Secteur de démarrage	Partie du système d'exploitation qui est lue en premier par le disque lorsqu'on allume un PC. Le programme stocké dans le secteur de démarrage est ensuite exécuté, ce qui permet au reste du système d'exploitation de se charger.
Secteur de démarrage du DOS	Secteur de démarrage qui charge le DOS dans la mémoire vive d'un PC. C'est par ailleurs, un point d'attaque courant des virus de secteurs de démarrage.
Serveur de fichiers	Ordinateur fournissant un stockage de données centralisé et, souvent, d'autres services aux postes de travail d'un réseau.
Serveur de proxy	Serveur qui envoie des requêtes à Internet de la part d'une autre machine. Il se situe entre l'entreprise et Internet et peut être utilisé dans un but de sécurité.
Serveur web	Ordinateur connecté à Internet qui met à disposition les documents du web, au moyen généralement du HTTP.
SHS	Extension des fichiers *scrap object* de Windows. Les fichiers SHS peuvent renfermer du code de presque tous les types et s'exécutent automatiquement si vous cliquez dessus. Cette extension peut être cachée.
Signature numérique	Moyen de s'assurer que personne n'a touché à votre message et qu'il provient bien de l'expéditeur annoncé.
SMTP	*Simple Mail Transport Protocol*. C'est le système de délivrance des mails d'Internet.

Somme/résultat des contrôles	Valeur calculée à partir d'un (ou des) élément(s) de données pouvant être utilisée pour vérifier que ces données n'ont pas été altérées.
Spam	Courrier électronique non sollicité.
Système d'exploitation	Programme qui contrôle l'utilisation des ressources matérielles de l'ordinateur et effectue des fonctions de base telles que la maintenance des listes de fichiers et l'exécution des programmes.
TCP/IP	*Transmission Control Protocol/Internet Protocol*. C'est le nom collectif des protocoles standards d'internet.
Téléchargement	Transfert de données d'un ordinateur (serveur) vers un autre ordinateur (terminal).
URL	*Uniform Resource Locator*. C'est l'adresse d'un site web.
VBS	Script en Visual Basic. C'est du code incorporé à une application, un document, ou une page web qui peut s'exécuter dès que la page est visualisée.
Ver	Programme qui se diffuse en multiples exemplaires. Au contraire du virus, le ver ne requiert pas de programme hôte.
Virus	Programme qui a la capacité de se répandre à travers les ordinateurs et les réseaux en se greffant sur un autre programme et en créant ses propres répliques.
Virus compagnon	Virus qui exploite le fait que lorsque deux fichiers programme ont le même nom, le système d'exploitation utilise leur extension pour décider lequel exécuter. Par exemple, les ordinateurs sous DOS exécuteront par préférence un fichier .com plutôt qu'un .exe. Le virus crée donc un fichier .com qui contient le code viral et lui donne le même nom que le .exe existant.
Virus de fichier	Voir Virus parasite.

Virus de macro	Virus employant les macros d'un fichier de données pour s'activer et se greffer sur d'autres fichiers de données.
Virus de redirection	Virus qui bouleverse les entrées d'un répertoire de façon à ce qu'elles pointent vers le code du virus, permettant à celui-ci de s'exécuter.
Virus du secteur de démarrage	Type de virus dérèglant le processus d'amorçage.
Virus furtif	Ces virus dissimulent leur présence à l'utilisateur et aux antivirus, en déroutant généralement les services d'interruption.
Virus multipartite	Virus qui infecte à la fois les secteurs de démarrage et les fichiers programme.
Virus parasite	Virus qui se greffe sur un autre programme informatique, et s'active lorsqu'on exécute le programme.
Virus polymorphe	Virus qui se modifie de lui-même. En changeant son propre code, le virus essaie de se rendre plus difficile à détecter.
WAP	*Wireless Application Protocol*. Semblable à l'internet, il apporte des informations consultables sur un téléphone mobile ou un organiseur.
Web	Voir World wide web.
World wide web	Système hypertexte diffusé pour la lecture des documents à travers Internet.
WSH	*Windows Scripting Host* (Exécution de Scripts) ; cet outil automatise certaines actions, comme l'exécution des fichiers VBS ou Java Script, sur les ordinateurs sous Windows.
WWW	Sigle de *WorldWide Web*.

Index

J

M

N

O

P

R

S

T

U

V

W

X

Index des virus