Communautique

VIRUS ET ANTI-VIRUS

- La protection contre les virus, texte de référence du Centre National de Recherche Scientifique (CNRS)
- Quelques antivirus
- Communautique, soutien aux formations: page référence sur la protection contre les virus informatiques
- Quelques règles de prévention face à la contamination par virus

www.communautique.qc.ca **info@communautique.qc.ca**

5225, rue Berri, bureau 304, Montréal, H2J 2S4,
Tél.: (514) 948-6644 ; Fax. : (514) 948-2046

LA PROTECTION CONTRE LES VIRUS

Richard Longeon
Tiré du site du Centre National de Recherche Scientifique
(http://www.cnrs.fr/Infosecu/Virus.html)

QU'EST-CE QU'UN VIRUS

Pour le commun des utilisateurs, un virus est un programme qui, à son insu, exerce une action nuisible à son environnement : modification ou destruction de fichiers, effacement du disque dur, allongement des temps de traitement, manifestations visuelles ou sonores plus ou moins inquiétantes, etc. Cette action peut être continue, sporadique, périodique, ou n'avoir lieu qu'à une date précise ou selon la conjonction d'événements extérieurs fortuits. Le virus Michelangelo, par exemple, ne se déclenche que le 6 mars.
Mais on sait moins que les virus peuvent aussi servir à crocheter les systèmes les plus secrets en créant des vulnérabilités "cachées" qu'un autre processus exploitera ultérieurement. Ces virus ont pour mission de se disséminer afin de propager ces vulnérabilités et "marquer" les systèmes atteints pour qu'ils puissent être détectés par des programmes de balayage de l'Internet. Ils doivent rester le plus silencieux possible pour ne pas se faire repérer. Contrairement aux autres virus, ils ne perturbent pas le système et ne détruisent pas de données. Ces virus là sont les plus dangereux, même s'ils paraissent ne pas gêner. Sur une machine ainsi contaminée, votre système d'information est un livre ouvert. Il n'est plus question alors de parler de sécurité !
On voit ici que les virus s'attaquent à tous les aspects de la sécurité définie dans la trilogie : confidentialité, intégrité, continuité de service. On les caractérisera donc par leur mode de propagation, plutôt que par leur capacité de malfaisance, trop générale.

Le vocabulaire des informaticiens est souvent très imagé. C'est ainsi, qu'outre les virus, on peut parler de vers, de bombes logiques ou de chevaux de Troie. Derrière chacun de ces termes se cachent des actions malveillantes précises qu'il n'est pas sans intérêt de connaître.

QU'EST-CE QU'UN VER

Un ver est un programme qui possède la faculté de s'auto-reproduire et de se déplacer au travers d'un réseau (cf. le ver Internet de Robert Morris de 1988). Les vers n'ont pas forcément besoin d'un support physique ou logique (disque, autre programme hôte, fichier). Ils se déplacent de manière autonome en exploitant des mécanismes système ou réseau (rpc, rlogin, etc.). Un ver est un virus réseau.

QU'EST-CE QU'UNE BOMBE LOGIQUE

Les bombes logiques sont des dispositifs programmés insidieux qui contiennent généralement un mode de déclenchement différé. Ce mode exploite principalement des informations comme la date système, le lancement d'une procédure, une commande du shell, un appel système. Les mécanismes utilisés sont, dans certains cas, conçus de manière à répondre à une commande télé programmée (RTC, accès à un PAVI, à un PAD…).

QU'EST-CE QU'UN CHEVAL DE TROIE

Les chevaux de Troie se présentent généralement sous la forme de programmes à caractère utilitaire ou d'un jeu. Ces programmes comportent, en plus des fonctions déclarées, une partie

insidieuse (mécanisme caché qui s'exécute de façon illicite en parallèle des actions connues de l'utilisateur). Par exemple, un cheval de Troie, en plus de ses fonctions normales, enverra des informations à un site "warez" ou créera dans le système une entrée secrète ou d'autres types de vulnérabilité.

LES VIRUS TRANS-APPLICATIFS

Avec l'arrivée d'Office 97, les divers langages macro ont convergé vers Visual Basic 5 (VB5), ouvrant théoriquement la porte à des virus trans-applicatifs. Ce n'est qu'une question de temps : de plus en plus de produits indépendants supportent VB5. Il est donc envisageable d'imaginer des macro-virus sur ces autres plates-formes.
La caractéristique principale d'un virus est sa capacité à se propager. Un macro-virus Word se propage aisément lorsqu'il utilise les procédures d'exécution automatiques prédéfinies via une ou plusieurs macros AUTO de Word ou lorsqu'il supplante une entrée d'un menu. Il intègre ainsi l'environnement global en mettant à jour le fichier NORMAL.DOT.

LA PREVENTION CONTRE LES VIRUS

Nous recommandons, pour se protéger des virus:

1. de contrôler toutes les nouvelles applications à installer
2. de verrouiller les supports de stockage quand ils n'ont pas besoin d'être en écriture
3. d'avoir un antivirus à jour

Les unités du CNRS ont à leur disposition des aides et des outils afin de les encourager à améliorer l'efficacité de leur protection anti-virus :

- La liste de diffusion "sos-virus" permet d'échanger les questions et les expériences.
- Un site de téléchargement de mises à jour de logiciels F-Prot, Sam, AVP, TBAV,
- La distribution gratuite de ces logiciels.

LA PREVENTION CONTRE LES FAUX VIRUS

Les canulars ("myths, hoaxes, urban legends") se présentent faussement comme un avis de sécurité. Ils ont un double objectif :

- créer la confusion et de la désinformation en matière de sécurité ;
- provoquer des envois de courrier électronique en cascade afin d'inonder les boîtes aux lettres ("spamming" en américain).

Cette pratique a été inaugurée avec la fausse annonce d'un prétendu "nouveau virus" "GOOD TIME", présenté comme très dangereux. Cette fausse annonce continue, plusieurs années après son baptême, à circuler sur l'Internet, parfois avec quelques variantes (Penpal Greetings, AOL4FREE, PKZIP300, etc.). Elle a toujours autant de succès ! Plus généralement, des manipulations de ce genre affectent de nombreux thèmes couvrant la sécurité des systèmes et des réseaux ce qui a amené les organismes de sécurité comme le CERT à signer leurs messages.

Il est facile de vérifier qu'une alerte virus est un canular en consultant au choix les sites suivants :
http://ciac.llnl.gov/ciac/CIACHoaxes.html
http://www.symantec.com/avcenter/hoax.html
http://www.stiller.com/hoaxes.htm
http://kumite.com/myths/
http://www.nai.com/services/support/hoax/hoax.asp
http://urbanlegends.miningco.com/msubvir.htm?pid=3D2733&cob=3Dhome

On trouve également aux adresses ci-dessous les archives des canulars et autres mythes qui courent sur Internet

(en anglais)
http://www.snopes.com/
http://snopes.simplenet.com/message/
http://www.urbanlegends.com/

(en francais)
http://www.trendmicro.fr/infovirus/canulars.htm

En règle générale il ne faut faire confiance qu'aux sources " authentifiées " et ne jamais prendre pour " argent comptant " des informations qui vous arrivent par le courrier électronique. Dans tous les cas, vérifier l'information avant de propager le message, surtout dans une liste de diffusion. Si vous êtes crédule, vous participez à votre insu à la malveillance**.**

LES MACROS VIRUS : UN DANGER PERMANENT !

Il est possible de rencontrer des macro virus chaque fois qu'un produit offre à l'utilisateur la possibilité d'écrire des macro-commandes permettant une écriture sur disque. La plate-forme qui comporte le plus de macro virus est Microsoft Word pour Windows. Les virus se propagent facilement dans cet environnement car les fichiers .DOC contiennent à la fois le texte et toutes les macros associées. Microsoft Excel est également touché.
La fabrication d'un macro virus, contrairement aux souches anciennes où il fallait maîtriser la programmation système, est à la portée d'un néophyte. Cette facilité attire les vocations malsaines et il se crée une quantité innombrable de nouveaux macro virus tous les jours. La procédure ancienne, de rafraîchissement tous les six mois du fichier des "signatures virus " sur l'antivirus, ne suffit donc plus. Faites donc régulièrement des mises à jour (au minimum une mensuelle) et rappelez-vous qu'un macro virus peut bloquer partiellement un laboratoire pendant plusieurs jours

LA PREVENTION (de contamination par Word)

1. Empêcher la modification NORMAL.DOT
   Une première méthode de lutte contre la propagation des macro-virus, consiste à empêcher la modification du fichier NORMAL.DOT. Vous pouvez l'empêcher,
   Soit en protégeant le fichier en écriture
   Soit en forçant l'option " confirmer l'enregistrement de NORMAL.DOT " de Word.
   Cliquez sur " Outil ", puis sur " Options ". Choisissez ensuite l'onglet " Enregistrement ". Parmi les options d'enregistrement affichées, sélectionnez " Confirmer l'enregistrement de NORMAL.DOT "
   Cette méthode constitue une première ligne de défense mais il faut savoir que beaucoup de virus actuels savent très bien la contourner.

2. Désactivation des macros de type AUTO.
   On peut aussi désactiver le lancement des macros au démarrage,
   Lancez Word ou ouvrez un document en gardant la touche <majuscule> enfoncée. Cette opération permet d'empêcher l'exécution des macros automatiques de type AUTO ce qui interdit aux virus l'utilisation des "AutoOpen" ou "AutoExec" pour se propager. D'une manière similaire l'activation de ce contrôle à la sortie de Word fait obstacle à l'exécution de la macro "AutoClose".

3. Si vous n'utilisez jamais les macros, préférez la fonction de Word "DésactiverMacroAuto " qui a exactement le même rôle que la technique précédente, mais opère une désactivation globale et automatique (plus sûre …). ***Cliquez sur " Outils, Macro ", entrez autoexec. Cliquez sur " Créer ". La nouvelle macro est éditée, insérez la commande " DésactverMacroAuto "***
   Sub MAIN

DésactivezMacroAuto 1
End Sub

Malheureusement, il y existe d'autres macros que celles de type AUTO. Cette méthode n'est efficace que dans la mesure où les macro-virus ont " l'amabilité de bien vouloir n'utiliser que celles-là "

Décontamination de vos documents

4. Sur Mac vous pouvez toujours utiliser Word5.1 qui n'interprète pas les macros. On trouve de nombreux utilitaires sur Internet qui permettent de convertir un document Word (6, 98) en Word5.1. Un document converti en Word5.1 n'a plus de macros et donc n'est plus contaminé.

5. Sur PC, utilisez l'utilitaire WordPad . Puis faites du copier/coller pour récupérer vos documents sous un nouveau nom. Quand vous avez achevé cette opération, jeter vos originaux et videz la poubelle.

Si malgré tout cela, vous n'avez pas pu vous débarrasser de votre macro-virus, cela signifie que vous avez oublié un document contaminé. Recommencez au début, en vous débarrassant cette fois, de TOUS les documents susceptibles d'être contaminés.

Quelques Antivirus

Par la Puce Communautaire

Il existe à ce jour une panoplie d'antivirus aussi performants les uns que les autres, quelques-uns uns se démarquent des autres avec des caractéristiques supplémentaires, certains sont plus conviviaux, d'autres sont plus efficaces, d'autres sont plus versatiles et certains sont moins dispendieux. C'est pourquoi il peut être difficile de s'y retrouver. Vous allez voir dans cette présentation un bon nombre d'antivirus (soit version serveur ou version individuelle) ; leurs caractéristiques, avantages, inconvénients prix etc.

Il existe une grande diversité de produits disponibles, par conséquent on ne traitera que de cinq anti-virus version individuelle et version serveurs. Les versions serveurs gèrent le trafic de données possiblement infectées sur un réseau. Par conséquent, dans la présentation on traitera des deux versions pour chaque antivirus.

NORTON Antivirus 5 de SYMANTEC version individuelle et serveur

Norton AntiVirus 5.0 version individuelle pour Windows fonctionne dans les environnements Windows95, Windows98 et WindowsNT 4.0

Voici comment Norton Antivirus se démarque des autres logiciels d'anti-virus. Il peut soit supprimer les fichiers contaminés, réparer les fichiers contaminés ou mettre en quarantaine les fichiers contaminés. Il vérifie au démarrage que votre ordinateur soit exempt de virus. Il recherche les virus chaque fois que vous utilisez des programmes de votre ordinateur, des disquettes ou des documents que vous recevez ou créez. Il contrôle votre ordinateur pour détecter toute activité inhabituelle qui pourrait signaler la présence de virus. Il exécute automatiquement une analyse programmée, pour vérifier que vos disques locaux n' ont pas de virus. Il offre une protection contre les virus transportés par Internet en analysant automatiquement tous les fichiers lors de leur téléchargement. Il offre aussi une très bonne protection contre les virus de macro Microsoft Word. Il est aussi capable d'analyser le contenu de nombreux fichiers compressés. Parmi toutes ces fonctions, une fonction se distingue des autres, elle est assez répandue parmi tous les producteurs d'antivirus: c'est la mise à jour en ligne, vous pouvez en quelques *clics* mettre à jour votre antivirus pour la dernière version avec l'aide de LIVE UPDATE, programme qui est fourni avec NORTON antivirus. Vous pouvez aussi programmer l'exécution automatique de LIVE UPDATE.

En conclusion, NORTON antivirus est un programme très convivial, efficace, peu dispendieux. Il requiert un ordinateur de 25 Méga Hertz avec Windows95, 8 Méga octets de mémoire, lecteur de cédéroms ainsi que 24 méga octets d'espace disque disponible. IL en coûte environs 40 à 65$ pour se procurer ce logiciel, une version d'essai de 30 jours est disponible sur le site web de la compagnie Symantec.

NORTON antivirus version serveur est disponible en version pour WindowsNT 3.51 ou 4.

Il possède sensiblement les mêmes caractéristiques que la version individuelle. Il permet de faire l'administration réseau au point de vue de la vérification des virus ; il vérifie toute information transigée sur le réseau et permet de prévenir une grande propagation des virus.

Pour terminer, la version serveur demeure plus dispendieuse, mais très versatile et performante autant pour des petits ou gros réseaux. Il requiert un processeur d'Intel, 16 méga octets de mémoire et 24 méga octets d'espace disque disponible.
http://www.symantec.com/

PC-CILLIN 6 de Trend Micro version individuelle et version serveur

PC-CILLIN version individuelle existe en 2 versions ; pour Windows 95/98 et WindowsNT 4.0

PC-CILLIN est un antivirus performant et convivial mais limité au niveau des caractéristiques. Il vous offre l'aide en ligne avec un expert pour vous aider à bien optimiser les performances de votre antivirus. Son interface est simple et conviviale, et un assistant vous guide étape par étape pour la vérification de vos disques durs. Il possède aussi l'option de quarantaine qui permet d'isoler les fichiers contaminés des autres fichiers afin d'éliminer tout risque de propagation. Il offre aussi une protection contre les attaques provenant des sites web avec ActiveX et JAVA. Un seul inconvénient qui le rabaisse par rapport à ses compétiteurs, c'est le fait qu'il ne possède pas de programme de mise à jour en ligne, par conséquent vous devez aller sur le site web de la compagnie télécharger les dernières mises à jour de virus.

Pour terminer, à moins de 40$ il demeure un très bon antivirus même si certains de ses principaux concurrents offrent quelques caractéristiques plutôt alléchantes comme la mise à jour en ligne et la version française. Mais il se distingue des autres de par sa convivialité de par son assistant de réalisation de tâches. Une version d'essai de 30 jours est disponible sur le site web de la compagnie Trend-Micro. À noter que PC-CILLIN est disponible seulement en anglais.

La version serveur qui se nomme SERVERPROTECT est disponible pour WindowsNT 3.51, WindowsNt 4 et Novell Netware 3,4 et 5.

La version serveur est beaucoup plus complète que la version individuelle, car il peut mettre à jour automatiquement les définitions d'antivirus. Il peut aussi être programmé pour vérifier automatiquement les possibilités d'infection. Il vérifie toute
activité qui pourrait s'apparenter à un virus et si c'est le cas il peut vous le signifier par un message en Windows, un courriel etc. Dépendant de votre configuration personnelle. De plus, il fait des rapports quotidiens de toute activité suspecte. Et comme toute version serveur il gère la vérification automatique de tout fichier transigé le réseau.

La version serveur requiert un processeur Pentium 166 méga hertz et plus, 32 méga octets de mémoire ainsi que 32 méga octets d'espace disque disponible. Un cédérom d'essai est disponible sur commande à partir du site de TREND MICRO.
Il est disponible de 600 à 2100$ dépendant du nombre de licences (25 à 100).

http://www.antivirus.com

MCAFEE VirusScan 4.0 de Network Associates version individuelle et version serveur

McAFEE VirusScan version individuelle est disponible pour Windows95, Windows98 et WindowsNT.

Mcafee VirusScan est un *leader* sur le marché des antivirus grâce à ses nombreuses caractéristiques et sa simplicité d'interface. Il offre la mise à jour en ligne, tout en vous indiquant le nombre de jour depuis la dernière mise à jour. Vous pouvez aussi programmer des mises à jour automatiques. Il permet de programmer des vérifications contrôlées des disques durs. De plus, il protège aussi votre courrier électronique en vérifiant toute entrée ou sortie de messages de votre boîte aux lettres. Il vérifie aussi tous les fichiers visualisés ou téléchargés depuis Internet, alors vous pouvez bloquer une adresse Internet qui est habituellement contaminée. Lorsque MCAFFE Viruscan trouve un virus il vous offre le choix entre exclure, effacer ou réparer le fichier contaminé. Il possède une console principale avec les options principales et vous affiche un statut de votre système.

Finalement, McAFEE VirusScan est un antivirus très simple, performant, mis à jour régulièrement, versatile et peu coûteux. Il en coûte environ 45$ et une version d'essai est aussi disponible sur le site de la compagnie Network Associates. Une version française est disponible.

La version serveur nommée NETSHIELD, existe pour WindowsNT 3.51 et 4 ainsi que Novell Netware 3 à 5.

La version serveur est plus complète que la version individuelle, elle offre les principales caractéristiques d'un antivirus version serveur comme la vérification de tous les fichiers qui passent par le serveur sur le réseau. Il met automatiquement en quarantaine les éléments infectés, ce qui évite une perte de temps et aussi une propagation de l'infection. Il s'intègre parfaitement aux outils d'administration du serveur. Vous pouvez programmer la vérification des disques locaux. Les mises à jours sont téléchargées automatiquement.

Enfin, une version d'essai est disponible sur le site web de la compagnie Network Ascociates. Il est requis un processeur Intel ainsi que 6.5 méga octets d'espace disque disponible.

http://www.mcafee.com/

SOPHOS Antivirus de SOPHOS version individuelle

SOPHOS version individuelle est disponible pour Windows3.11, 95, 98 et en version WindowsNT.

SOPHOS est un antivirus très simple d'utilisation, facile à utiliser, à configurer ou pour planifier des vérifications. Il répare les fichiers infectés sur-le-champ et produit un rapport de toutes ses activités. Toutes ses commandes principales sont centralisées dans un programme très convivial. Il ne possède pas de programme de mise à jour en ligne, par conséquent vous devez aller sur le site web de la compagnie télécharger les dernières mises à jour de virus. Il est mis à jour une fois par mois et aussi lorsque des nouveaux virus deviennent critiques.

Pour terminer, SOPHOS est un antivirus performant et simple, mais quelques bonnes caractéristiques lui manquent, dont la mise à jour en ligne, la vérification des courriels et la quarantaine. Il est disponible en plusieurs langues et une version d'essai de 30 jours est disponible sur le site de SOPHOS.

http://www.sophos.com/

F-SECURE de DATAFELLOWS version individuelle et serveur

F-SECURE version individuelle est disponible en version Windows95 et 98 et en version WindowsNT.

Il possède une interface simple et il s'intègre à Windows en vous offrant la possibilité de vérifier un document en un simple *clic*, les principaux antivirus tels McAFEE et NORTON antivirus possèdent aussi cette fonction. Il permet aussi de planifier des tâches comme des vérifications de disques. Le programme GATEKEAPER, inclus avec F-SECURE, vérifie tous les fichiers transigés sur Internet et sur vos lecteurs disquette et disques durs. Il permet aussi l'utilisation réseau du logiciel, que ce soit pour vérifier tous les ordinateurs d'un réseau à partir d'un ordinateur ou bien pour produire un rapport de toute activité sur chaque ordinateur et peu importe le système d'exploitation sur les systèmes.

En conclusion, F-SECURE est un antivirus très convivial et très performant, que se soit sur un simple ordinateur ou sur un réseau. Il requiert un processeur de Pentium, 32 méga octets de mémoire et 15 méga octets de disque dur. Il est disponible à environ 125-500$ dépendant du nombre de licences (1-10). Une version d'essai est aussi disponible sur le site de la compagnie DATAFELLOWS.

La version serveur est disponible seulement pour WindowsNT

La version serveur demeure très semblable à la version individuelle exceptée la gestion réseau. Il effectue des rapports quotidiens de toute activité suspecte.

La version serveur est disponible pour WindowsNT 4 et requiert un processeur de Pentium, 64 méga octets de mémoire et 15 méga octets de d'espace disque disponible. Il se vend environ 375$.Il n' y a pas de version d'essai disponible.

http://www.datafellows.com/

INOCULATE/*IT* de COMPUTER ASSOCIATES version Serveur

INOCULATE/*IT* est offert en version WindowsNT pour WindowsNT 3.51 et 4

INOCULATE/*IT* est un des meilleurs antivirus en version serveur, il possède toutes les principales caractéristiques intéressantes pour un administrateur réseau. Il peut vérifier tous les disques durs locaux ou réseaux et même les serveurs de messagerie. Il éradique automatiquement tout virus trouvé en temps réel sur tout le réseau. Il met à jour automatiquement ses définitions de virus une fois par mois. Il peut aussi vérifier les fichiers compressés tels les ZIP, ARJ et Microsoft, il vérifie aussi tous les fichiers téléchargés par Internet ou par courrier électronique. Tout fichier infecté qui est modifié, déplacé sur le réseau est automatiquement mis en quarantaine.

Finalement, INOCULATE/*IT* est un très bon atout à l'obtention d'une excellente sécurité sur un serveur de type WindowsNT. Pour plus d'information référez-vous au site web de la compagnie COMPUTER ASSOCIATES.

http://www.cai.com/

NOTE: Une version gratuite pour un usage personnel est également disponible sur le site (http://www.antivirus.cai.com). Il est possible de télécharger les mises à jours des signatures de virus. Malheureusement, le logiciel n' est disponible qu' en version anglaise et pour les systèmes d' exploitations Windows..

Document crée par l'équipe de La Puce Communautaire
Janvier 2000

Virus informatiques : ressources disponibles sur le Web

- **http://www.cnrs.fr/Infosecu/Virus.html**

On retrouve sur le site du Centre national de recherche scientifique une foule d'informations concernant les différents formes de virus, des stratégies face à la protection contre les virus ainsi qu'une méthode pour contrer les macros-virus souvent transmis par l'intermédiaire des fichiers Word ou Excel..

- **http://www2.nb.sympatico.ca/Aidez/Logiciels/Virus/comment.html**

Comment mon ordinateur peut-il contracter un virus? ; Comment protéger mon ordinateur des virus? Où puis-je me procurer des logiciels antivirus? ; Comment savoir s'il s'agit d'un virus ou d'un canular?
Cette section du site de Sympatico apporte des réponses aux questions concernant les virus informatiques.

- **http://www.netsurf.ch/archives/1999/99_11/991122nt.html**

Article de Francis Pisani sur les faux virus du magazine électronique NetSurf. On y retrouve des liens vers des sites qui traite des principaux canulars ou «légendes virtuelles» circulant dans le village global Internet.

- **http://www.megagiciel.com/117.html**

Section du site mégagiciel permettant de télécharger des versions d'essais ou gratuites des logiciels anti-virus les plus populaires.

- **http://www.geocities.com/siliconvalley/hills/4227**

Les différentes techniques utilisées par les virus et les antivirus pour infecter et nettoyer les disques durs.

Quelques règles de prévention face à la contamination par virus

- Contrôler toutes les nouvelles applications à installer
- Verrouiller les disquettes et autres supports de stockage quand ils n'ont pas besoin d'être en écriture
- Utiliser un antivirus à jour (Actualisation régulière des signatures virus)
- Balayer systématiquement les fichiers téléchargés par Internet, les fichiers attachées aux messages de courriel et les disquettes de source inconnue ou de l'extérieur de l'organisme
- Prévention de contamination par macro virus
  - Utiliser la touche SHIFT avant de double-cliquer sur le document afin d'annuler l'ouverture des macros de type AUTO
  - Désactiver l'exécution des macros commandes (voir les options du logiciel)