SÉCURITÉ INFORMATIQUE

numéro 31 octobre 2000

SÉCURITÉ DES SYSTÈMES D'INFORMATION

Le cap est maintenu …

éditorial

Philippe Schreiber qui, depuis plusieurs années vous proposait des éditoriaux empreints de talent et de pertinence, a quitté ses fonctions au début du mois d'août. Souhaitons-lui une retraite riche en satisfactions.

Les responsables changent, les problèmes demeurent. Il en va ainsi, bien sûr, de ceux liés à la sécurité des systèmes d'information mis en œuvre par les chercheurs, les ingénieurs et les techniciens dans nos laboratoires pour recueillir, traiter et, le moment venu, échanger les données issues de leurs travaux.

Ces systèmes recèlent des connaissances nouvelles qu'il convient de protéger, en tout ou en partie, pour diverses raisons dont la moins importante n'est pas celle consistant à pouvoir disposer, le cas échéant, du délai nécessaire pour valoriser les dites connaissances au bénéfice de notre économie conformément à une des missions du CNRS, avant que d'autres ne le fassent à son détriment.

Par son action, menée en liaison avec ses collaborateurs directs et en sachant solliciter les bonnes compétences, mon prédécesseur a contribué à provoquer l'indispensable prise de conscience face au problème et mis en place les premières mesures concrètes.

Le contexte semble maintenant propice pour définir une politique globale de sécurité des systèmes d'information de nos laboratoires et des réseaux qui les relient entre eux ainsi que pour mettre sur pied l'organisation apte à mettre cette politique en œuvre, à la faire vivre et à évaluer son efficacité. C'est ce à quoi je vais m'attacher.

La route à parcourir sera sans doute longue. Le pilote vient d'être changé. Le cap est néanmoins maintenu.

Alfred Schwenck
Fonctionnaire de Défense

Les nouveautés d'automne…

Avant de présenter ce premier numéro de l'automne, je me dois de souhaiter la bienvenue à notre nouveau « Fonctionnaire de Défense » M. Alfred Schwenck : on pourra trouver un bref résumé de ses activités antérieures sur http://www.sg.cnrs.fr/melwebsg/2000/08/040800.htm.

« Fonctionnaire de Défense » est un titre qui apparaît parfois comme mystérieux. C'est en réalité un agent du CNRS, placé auprès du Directeur Général, dont le rôle premier est d'assurer la protection du patrimoine scientifique, c'est-à-dire la protection de l'ensemble de nos moyens, de nos savoir-faire et des résultats de nos recherches. Il apprécie l'opportunité de leur transfert à l'étranger en fonction des intérêts fondamentaux de la Nation afin qu'une diffusion incontrôlée d'informations scientifiques ne compromette ni la liberté ou la sécurité de nos concitoyens, ni la prospérité de notre économie, ni le respect de l'éthique scientifique, ni la protection de la vie privée qui est garantie par la constitution.

Dans ce nouveau numéro « Spécial virus », Jean-Marc Larré présente l'expérience de déploiement de l'anti-virus « Panda Global Virus Insurance » menée dans son laboratoire. Cette expérience avait pour objectif de vérifier la faisabilité d'une gestion centralisée avec ce type de produit. En lançant « l'opération AVP » en 1995, nous avions voulu favoriser la généralisation de l'utilisation des anti-virus. Puis, avec l'apparition des virus de macros qui rendait nécessaire l'amélioration de la réactivité de nos mises à jour, nous avons proposé la nouvelle version d'AVP qui permettait de télécharger les signatures. Le développement de l'informatique personnelle ayant suivi sa courbe exponentielle, il est encore nécessaire de s'adapter : comment un administrateur système peut-il veiller à la bonne configuration et à la mise à jour – au moins hebdomadaire – d'un antivirus sur un parc de plusieurs centaines de machines ? Impossible, comme le dit Jean-Marc Larré, sans une gestion centralisée ! Son expérience a été concluante et nous souhaitons la généraliser aux laboratoires qui en feraient la demande. À cette fin, nous avons conclu un accord de licence avec le distributeur du logiciel « Panda anti-virus » en remplacement de l'accord avec AVP qui prendra fin en avril 2001. Deux types de licences sont donc proposés gratuitement aux laboratoires du CNRS :

1. Panda Antivirus Platinum pour la protection des postes clients Dos, W3.x, W95/98/Me, Win NT3.51/4.0, Windows2000 Pro.
2. Panda Global Virus Insurance pour la protection des serveurs NT 3.51/4.0, 2000, Novell Netware 3.x, 4.x, 5.x, MS Exchange, Lotus Domino (d'ici novembre 2000) et la protection des stations clientes grâce à Panda Platinum. Ce produit intègre notamment une console d'administration, Panda Administrator.

Pour plus d'informations, consulter : http://www.cnrs.fr/Infosecu/

Robert Longeon

CENTRE NATIONAL DE LA RECHERCHE SCIENTIFIQUE

Panda Software, l'expérience d'un déploiement automatique

Le Centre d'Etude Spatiale des Rayonnements (CESR) est une unité propre du CNRS dans le domaine des sciences de l'univers. Il est impliqué dans de nombreux projets spatiaux en collaboration, entre autres, avec le CNES ou l'ESA. Le CESR se trouve sur le campus universitaire Paul-Sabatier à Toulouse, son personnel de tout statut est composé de 130 personnes. L'implication dans des projets européens (ou plus) de grande envergure avec de nombreuses entités internationales amène le CESR à échanger une grande quantité de données par les réseaux (ou d'autres médias). Pour préserver notre crédibilité et respecter nos engagements dans les collaborations, le CESR doit pouvoir mener une politique de sécurité qui garantit l'intégrité des données entrant ou sortant du laboratoire.

Mai 2000 : une vague de nouveaux types de virus déferle et produit un « raz de marée » sur les sites, ce qui nous amène rapidement à construire « digues » et « jetées ». En amont du serveur de messagerie, nous avons mis en place, depuis 1998, le logiciel « Interscan Virus Wall » de la société Trendmicro. Malheureusement, comme pour les autres logiciels antivirus, un délai de plusieurs heures s'est produit entre les premiers dégâts et la parution d'une véritable signature efficace pour ce nouveau type de virus. **Constat :** nous avons une « jetée », mais pas de « digue », le CESR n'a toujours pas installé d'antivirus sur toutes ses machines (130 PC Windows complètement autonomes).

Les méthodes de détection des virus restent similaires d'un antivirus à l'autre, seuls les algorithmes utilisés diffèrent de façon significative. On recense quatre familles importantes de méthodes de détection :

- la recherche par comparaison avec une base de données comportant la signature des virus ;
- la recherche par une analyse heuristique, vérification qu'un code ne contient pas d'instructions ou de commandes malicieuses afin de lutter contre les nouveaux virus ou les virus polymorphes (virus capable de se régénérer en modifiant leur signature virale) ;
- le contrôle de l'intégrité des fichiers en vérifiant leur empreinte ;
- la mise en place d'une sentinelle qui scrute toutes les opérations d'entrées/sorties sur le système ou qui attend qu'un virus se manifeste ou se réveille.

J'ajouterai un concept très important dans la lutte contre les virus, la **réactivité :** l'aptitude à réagir face à un nouveau virus. La mise en place d'une protection sur toutes les stations dans un délai le plus court possible reste un paramètre important à considérer. Il faut pouvoir automatiser l'installation de l'antivirus (et de sa mise à jour) et la mise à jour de la base de données des signatures sur toutes les stations.
« Panda antivirus » offre la possibilité de déploiement automatique et de contrôle de l'état des différentes stations du parc micro. C'est essentiellement cette dernière fonctionnalité et sa facilité de mise en œuvre que nous avons voulu tester au CESR.

Mais dès qu'une nouvelle version du logiciel sortira, que le responsable de la sécurité changera la stratégie d'analyse des virus, et sachant que pour être efficace dans la lutte contre les virus il faut diminuer les temps de latence entre le moment où un nouveau type de virus arrive et la mise en place d'une protection, je vois mal le service informatique du laboratoire passer une nouvelle semaine à réinstaller tous les postes. Il faut mettre en place des dispositifs automatiques de mise à jour et verrouiller les accès à la configuration pour les utilisateurs, ce que prévoit le logiciel « Panda antivirus local network ».

Échantillon d'une faune nuisible …

Lokky.336 : virus résident de MS/Dos, infectant les fichiers exécutables dotés d'extensions .EXE. Il a deux moyens d'infection pour le moins étranges. Le premier s'appelle Cavity et exploite sa petite taille pour se copier à l'intérieur du fichier infecté. Le deuxième se nomme Full Stealth (Invisibilité maximale) ou « Disinfection on the fly » (Désinfection à la volée) et, tant que « Lokky.336 » est résident dans la mémoire, il s'élimine chaque fois que le fichier est ouvert et le ré-infecte dès qu'il est fermé. La raison de cette action est de rendre la détection plus difficile pendant tout le temps où « Lokky.336 » est résident mémoire.

Deadboot.448 : virus qui affecte les secteurs d'amorce du disque dur (Master Boot) et des disquettes (Boot), ainsi que les fichiers exécutables dotés d'extensions .EXE (on dit qu'il est multivolet). Le virus infecte tout d'abord l'enregistrement d'amorçage principal du disque dur, puis il s'installe en résident mémoire et attend l'opportunité d'infecter les secteurs d'amorce de disquettes consultées. Résultat de l'infection : les répertoires du disque dur sont encodés par le virus et il est impossible d'en retirer une quelconque information, même après la désinfection.

W32/Coke22231.A : virus polymorphe (il modifie sa signature à chaque contamination) multifilière (il utilise plusieurs vecteurs de contamination) lent. Pour mieux échapper aux anti-virus, il utilise plusieurs couches ou niveaux de chiffrement. Il installe tout d'abord sa routine de chiffrement polymorphe dans la section de code des fichiers PE, puis la divise en huit parties. Il a trois manières de se diffuser : l'une d'elle est d'infecter des documents de Microsoft Word 97 ; une autre est d'infecter des fichiers PE (Windows EXE) ; et la troisième est de s'auto-envoyer comme fichier attaché à des messages électroniques. Outre désactiver la protection antivirus que Word établit dans tous les documents qui contiennent des macros définies, « W32/Coke22231.A » essaie de supprimer tous les programmes antivirus installés sur le disque dur.

W97M/Blaster.B : virus de macro (appartenant au groupe W97M et à la famille Marker) qui infecte les documents de Microsoft Word 97, ainsi que le modèle global de documents NORMAL.dot que cette application utilise. Le 17 de chaque mois, il recherche le fichier MINNY.LOG dans le répertoire racine du disque dur. S'il ne le trouve pas, il insère une ligne de commande dans le fichier AUTOEXEC.BAT, qui supprime la totalité des contenus (fichiers et dossiers) des lecteurs C:, D:, E: et F:, lorsque le système est ensuite redémarré. De plus, lorsqu'un quelconque document infecté est exécuté ou ouvert, « W97M/Blaster.B » crée le fichier CONT.DEL dans le répertoire racine du disque dur. RL

Mise en place d'une solution centralisée

130 postes à installer, et environ 15 minutes d'installation par poste (dans le meilleur des cas). Il faut environ une semaine pour faire l'installation complète du parc : pourquoi pas ?

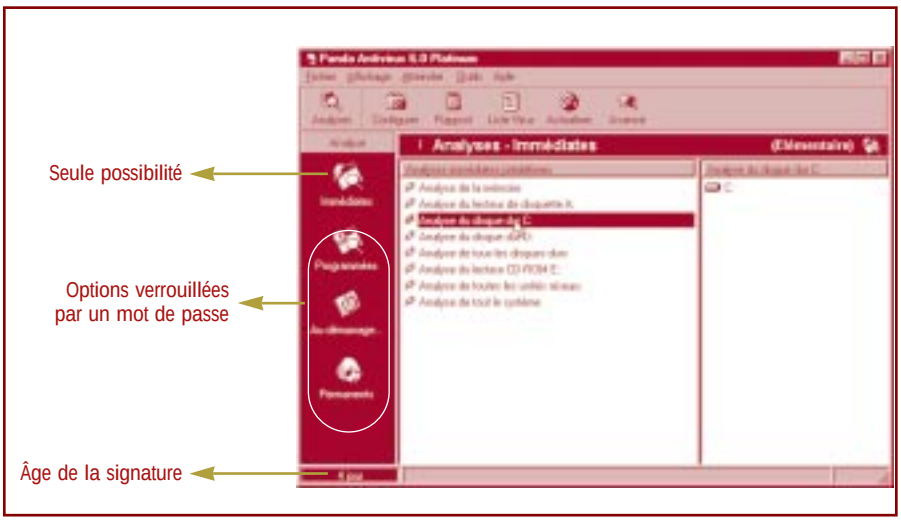
PAVLN (pour Panda antivirus local network) est prévu pour être installé dans une configuration propre : un serveur NT avec un PDC, et tous les utilisateurs se connectent et s'identifient sur le serveur. Dans ce cas, PAVLN est idéal, la procédure d'installation et le déploiement sont relativement faciles et rapides :

- Installation de PAVLN sur le serveur NT.
- Configuration du module serveur, mise en place de la politique de mise à jour des signatures.
- Configuration des modules clients sur le serveur (DOS, Win 95/98/NT...) avec la stratégie d'analyse des virus.
- Affectation d'un script (créé automatiquement par PAVLN) d'installation automatique de « Panda anti-virus » pour chaque utilisateur sur le PDC qui se connecte. Lors de la première connexion, « Panda antivirus » sera installé sur le client NT, puis, pour les autres connexions, une comparaison entre la version installée du logiciel et celle présente sur le serveur sera faite (ainsi que la signature des virus selon la configuration).

PAVLN au CESR est un peu plus complexe à mettre en place. Nous n'avons effectivement pas de serveur NT et donc encore moins de PDC pour distribuer les mots de passe. Chaque poste est totalement autonome et les systèmes d'exploitation sont hétérogènes. J'ai tenté de bluffer PAVLN avec un serveur SAMBA configuré en PDC, mais soit il est plus malin que moi, soit j'ai mal configuré mon serveur SAMBA. Je laisse donc à quelqu'un de plus expérimenté que moi dans ce domaine le soin de faire des investigations plus complexes. J'ai donc installé un PC (Pentium MMX 233 MHz avec 128 Mo de mémoire) avec NT serveur en PDC (important, le PDC : même si vous n'avez pas de domaine à contrôler, PAVLN en a besoin ; donc il faut en créer un !).

Une fois que j'ai bien compris cela, la suite de l'installation s'est relativement bien passée :

- Installation de PAVLN sur le serveur.
- Configuration du module serveur, mise en place de la politique de mise à jour des signatures.
- Configuration des modules clients sur le serveur (DOS, Win 95/98/NT...) avec la stratégie d'analyse des virus.
- Partage des répertoires nécessaires en mode « invités » avec les autorisations en lecture uniquement, c'est-à-dire sans identification à la connexion. Ce mode d'utilisation est à proscrire pour des problèmes importants de sécurité que vous pouvez imaginer mais je n'ai pas trouvé d'alternative.
  Le fichier ..\Pavmon\Wsrpt\Pavmon.dat doit être accessible en écriture.
- Envoi d'un message à l'ensemble des utilisateurs : « Installer dans le démarrage automatique de vos ordinateurs un raccourci vers ce script \\panda\netlogon\script.bat ». L'écriture d'une documentation avec capture d'écran accessible depuis l'intranet du laboratoire permet à quasiment tout le monde de faire cette opération. Le script est une version simplifiée de celui qui pourrait être utilisé dans le cas de la configuration PDC et NT (plus contrôle des autorisations à utiliser l'antivirus). Désormais, lors de la première exécution du script, « Panda antivirus » sera installé sur le poste ; puis, pour les autres exécutions, une comparaison entre la version installée du logiciel et celle présente sur le serveur sera exécutée (ainsi que la signature des virus selon la configuration). PAVLN affiche dans sa fenêtre les postes installés, avec en détail les versions des logiciels et la date de la dernière mise à jour du fichier signature.



Panda antivirus offre de grandes possibilités de configuration, entre autre dans le verrouillage des accès aux menus et au paramétrage. Il faut prendre un peu de temps afin de définir sa politique de mise en place avant de lancer le déploiement sur tous les postes. Voici quelques exemples importants des réflexions que l'on doit mener :

- Analyser tous les fichiers ? ou seulement ceux avec des extensions dites à risque (.exe, .vbs, etc.) ?
- Lancer une analyse totale à chaque démarrage ? une fois par semaine ? seulement le lundi ?
- Le programme permanent doit-il écouter les ports TCP (analyse de port POP, par exemple) ?
- La mise à jour du fichier signature doit-elle se faire à partir du serveur ? ou depuis le serveur de Panda Software par Internet ? et à quelle fréquence ?
- Doit-on réparer automatiquement quand on détecte un virus ? ou poser la question à l'utilisateur ?
- L'utilisateur doit-il avoir accès à ces paramétrages au risque qu'il invalide les analyses au profit des performances de son PC ?
- Etc.

Au CESR, les utilisateurs ne peuvent rien paramétrer. J'ai laissé uniquement la possibilité de lancer à la demande une analyse des disques. Quelques bémols : j'ai pu tester deux versions différentes sur lesquelles quelques corrections ont été apportées, et on peut penser que les problèmes qui persistent – comme la mise à jour programmée – soient résolus dans les versions futures.

Moyennant les autorisations nécessaires (identification et mot de passe), le serveur de Panda Software en Espagne permet de récupérer les documentations, les dernières mises à jour de tous les logiciels et la mise à jour de la signature des virus partielle (seulement les dernières modifications) ou complète. Une version pour MacOS serait à l'étude.

La mise en place de Panda peut être assez simple sur un réseau. Sa liberté de configuration relativement souple ne laisse à peu près rien de côté. Le logiciel et la documentation sont fournis dans plusieurs langues, dont le français. Les tests que j'ai pu faire n'ont jamais concerné les performances tant sur le plan efficacité de détection que sur le plan de la charge CPU du logiciel permanent et du temps d'analyse, car seul un comparatif avec d'autres logiciels anti-virus serait significatif, mais ce n'était pas le but recherché.

Jean-Marc Larré
CNRS/CESR
(Centre d'Etude Spatiale des Rayonnements)
Jean-Marc.Larre@cesr.fr

Les mythes des virus informatiques

Nous allons jeter quelques éclaircissements sur les chemins empruntés par les virus lorsqu'ils envahissent les systèmes informatiques. Nous traiterons également d'autres points les concernant, tels que les types de dossiers qu'ils infectent et la façon de protéger vos disques.

Est-il possible d'être infecté en utilisant un CD-ROM ?

Un CD-ROM étant un dispositif inaltérable, il est impossible d'écrire quoi que ce soit dessus. S'il est indemne de virus, il le restera, même utilisé par un système contaminé. En revanche, si le CD-ROM contient déjà un virus (infiltré dans un fichier exécutable, des archives compressées, etc.), il infectera votre ordinateur lorsque ledit fichier sera exécuté. Il faut être attentif à l'origine du CD-ROM car si, pour la plupart, ils proviennent de sources fiables (magasins, fabricants, etc.), quelques CD-ROM infectés sont en circulation.

Peut-on être infecté par le simple fait de se connecter à un réseau (Internet, connexion modem ou un réseau local) ?

Oui, c'est même aujourd'hui la manière la plus courante pour se faire contaminer. L'action de transférer un programme d'un endroit à un autre est sûre. Le risque d'infection réside dans le fait d'exécuter un programme qui n'a pas été analysé auparavant par un antivirus. On peut se faire aussi contaminer par des documents (Word, Excel, PowerPoint, ...) qu'on reçoit en pièce jointe et qu'on lit sans prendre quelques précautions. On peut enfin se faire contaminer directement par des courriers présentés par des agents de messagerie comme OutLook qui interprètent les scripts à l'ouverture. Des vers, comme Bubbleboy et KAK, sont capables d'infecter des systèmes par simple ouverture du message qui le transporte. Nous vous conseillons vivement de désactiver cette fonctionnalité si vous l'avez sur votre messagerie.

Les cookies constituent-ils un moyen potentiel d'infection ?

Les petits fichiers, connus sous le nom de « cookies », qui vous sont envoyés lors de votre navigation sur l'Internet n'impliquent aucun risque quel qu'il soit. Ils sont désagréables (ils prennent de l'espace sur le disque dur, ils donnent des informations à qui veut bien la prendre sur les pages que vous avez visitées), mais ce ne sont que de simples fichiers de données, vous n'avez donc pas besoin de les vérifier lorsque vous lancez une recherche de virus.

Les images téléchargées peuvent-elles contenir un virus ?

Soyez prudents et notez bien qu'il existe des virus qui se font passer pour des fichiers image JPG ou même pour des archives compressées. En outre, certains fichiers image sont distribués avec des programmes de visualisation qui, eux, par contre, peuvent être infectés.

Néanmoins, presque toutes les pages Web comportent un grand nombre d'images qui sont automatiquement transférées sur l'ordinateur pour être vues à l'écran. Les fichiers image (généralement des fichiers .JPG ou .GIF) peuvent également être transférés pour être regardés ou imprimés. Ces fichiers image ne contiennent pas de programmes, car ce ne sont que les données qu'un programme de lecture d'images interprète pour en afficher une à l'écran. Si un virus était inclus dans ces fichiers, il ne présenterait aucun danger, parce qu'il ne pourrait jamais être exécuté.

Les virus sont-ils capables d'endommager le matériel ?

Il faut être vigilant ! Tous les virus ne sont hélas pas des mythes. Preuve en est la toute dernière génération de virus destructifs, l'infâme CIH/Chernobyl en tête, parfaitement capable de supprimer les données cruciales du BIOS, rendant de ce fait les cartes mères inutilisables.

Néanmoins, bien que des rumeurs fassent croire que certains des virus qui circulent sur cette planète sont capables de « brûler » les écrans des ordinateurs en jouant avec la fréquence du moniteur et les paramètres de rafraîchissement, la vérité est toute autre : aucun type de code malveillant n'est en mesure de produire un tel effet. Il en est de même des rumeurs sans fondements qui affirment l'existence de virus capables de détruire les claviers, les unités de disque et d'autres périphériques : ce n'est pas vrai.

Des archives compressées peuvent-elles contenir un virus ?

En effet, les virus se logent parfois dans des archives compressées, comme dans n'importe quel autre type de programme. Heureusement, la plupart des grands antivirus actuels peuvent procéder à des analyses à l'intérieur des archives, pour rechercher les virus.

Dans de nombreux cas, c'est le manque de connaissance quant à l'existence possible de virus dans des archives compressées qui entraîne les utilisateurs à décompresser des dossiers sans prendre les précautions nécessaires, un geste qui mène inévitablement à l'infection.

Les virus peuvent-ils infecter d'autres types de fichiers que ceux dotés des extensions .COM et .EXE ?

Oui. De nombreux virus infectent également les secteurs d'amorçage des ordinateurs. Ces virus sont très bien cachés, car les secteurs n'apparaissent pas en tant que fichiers. Du coup, ils restent quasiment invisibles aux yeux des utilisateurs.

D'autres virus sont également conçus pour infecter n'importe quel type de fichier potentiellement exécutable, tels certains lecteurs (fichiers .SYS ou .BIN) et fichiers de recouvrement (.OVR).

Enfin, et non des moindres, certains virus seront spécialement écrits et conçus pour infecter les fichiers de traitement par lot (batch) (.BAT) et les macros des traitements de textes Word, des feuilles de calcul et même des programmes de dessin tels que Corel DRAW.

Les virus peuvent-ils infecter la mémoire CMOS ?

Le PC AT (Intel 80286) et les ordinateurs de la génération suivante sont conçus avec une petite zone de mémoire alimentée par pile et utilisée pour stocker les valeurs des paramètres de configuration, ainsi que l'horloge/calendrier interne du système. Cette mémoire est généralement appelée CMOS (Complementary Metal Oxide Semiconductor/semiconducteur complémentaire à oxyde de métal). Cette zone de mémoire ne stocke que des données et, dans le cas hypothétique où elle serait infectée par un virus, le code ne serait jamais exécuté. Cependant, le CMOS peut être endommagé par un virus ou par une défaillance de la pile, ce qui entraînerait alors la modification ou la suppression des données. Ce simple fait rend encore plus vitale la sauvegarde de la configuration du BIOS, si l'on veut être en mesure de restaurer les données perdues le cas échéant.

..... suite page 5 ...

suite de la page 4

Les Chevaux de bataille

Trojan/PSW.Autodel : cheval de Troie qui n'a qu'un seul but : fournir un accès à distance à d'autres systèmes. Pour atteindre son objectif, il va utiliser un fichier de 32768 octets, dont l'icône est identique à celle du format graphique .JPG. Lorsque ce fichier est exécuté, le cheval de Troie s'auto-copie dans le répertoire C:\WINDOWS\System. Il procède également à quelques petits changements dans le registre Windows afin d'être sûr d'être présent chaque fois que le système est démarré (le cheval de Troie est exécuté à chaque démarrage ou redémarrage du système). Dans le même style, on peut citer : Trojan/PSW.StealthD et Trojan/PSW.Pec.B.

Trojan/Varo31 : cheval de Troie qui est prévu pour effacer certains fichiers et répertoires du système. Cependant, en raison de bogues détectés dans son code, il s'avère incapable d'effectuer cette action. Ce cheval de Troie apparaît sur le système qu'il attaque sous la forme d'un fichier appelé QBASIC.EXE. Une fois exécuté, ce dernier supprime le fichier COMMAND.COM (interpréteur de commande) qu'il trouve dans le répertoire Windows.

RL

Virus et fichiers

Les fichiers ne peuvent faire de mal à qui que ce soit tant qu'ils ne sont pas exécutés. Si vous recevez un fichier qui contient un virus, sachez que pour que l'infection se propage, il faudra que vous l'exécutiez. Étant donné que les utilisateurs des applications Word, Excel, PowerPoint ou Corel DRAW, entre autres, peuvent recevoir des virus inclus dans des fichiers documents, l'infection peut donc être déclenchée lors de l'ouverture de tels documents envoyés par messagerie électronique ou téléchargés depuis Internet. C'est la raison pour laquelle, outre posséder la protection antivirus appropriée, il est vital de configurer son navigateur ou lecteur de messagerie de manière à ce qu'il ne lance pas automatiquement ces applications lorsque vous cliquez sur des documents de ce type (DOC, XLS, etc.). Rappelez-vous également que certaines applications malveillantes sont susceptibles d'entrer dans l'ordinateur sous le couvert d'icônes de documents ou de fichiers image parfaitement inoffensifs.

Est-il préférable de cacher COMMAND.COM ?

COMMAND.COM est un programme qui est exécuté à chaque démarrage d'un PC DOS, WIN3.x ou WIN9x. À l'apparition des premiers virus infectant ce fichier, certains eurent l'idée brillante de le cacher. À l'heure actuelle, les virus évitent plutôt d'infecter ce fichier parce que les antivirus analysent toujours ce fichier par défaut. De plus, les virus actuels peuvent aisément retrouver le COMMAND.COM.

Si je change les attributs des fichiers, est-ce que je les protège des virus ?

Par la commande « ATTRIB », sous DOS, nous pourrions mettre l'attribut « Lecture seule » (+R) aux fichiers, mais les virus (ou programmes) ne trouvent pas cet obstacle bien difficile à surmonter et de plus, cela génère parfois d'autres problèmes (surtout dans les réseaux).

Les unités de disque peuvent-elles être protégées en amont, de sorte qu'il ne soit pas possible de les réécrire ?

Il existe de nombreux programmes qui prétendent représenter des solutions efficaces et qui fonctionnent en empêchant les unités d'être réécrites. Cette solution ne protège que de la réécriture accidentelle et de quelques virus. De plus, il est plus facile de protéger les disquettes de 3 pouces 1/2 et de 5 pouces 1/4, bien que ces dernières soient plus vulnérables car elles peuvent perdre l'autocollant qui les protège.

Que certaines unités de disque soient défectueuses et permettent de réécrire sur ces disquettes en dépit de la protection est un risque inexistant. N'importe quel défaut de fonctionnement sera détecté par le système de protection de la disquette qui en empêchera la réécriture.

Existe-t-il des « remèdes simples » contre les virus ?

Malheureusement non. Il est donc important d'être conscient des problèmes que créent les virus et de prendre les mesures appropriées. L'utilisation d'un bon antivirus capable d'être mis à jour quotidiennement et accompagné d'un support technique efficace en est une.

Les codes malveillants ont-ils une caractéristique par laquelle ils peuvent être identifiés ?

La plupart des virus ont leur propre « signature » qui peut être identifiée par le virus lui-même (pour qu'il n'infecte pas constamment le même fichier) et par le logiciel antivirus. Certains virus utilisent un algorithme de signature au lieu d'une signature avec des caractères. Malgré tout, celle-ci est bien reconnaissable. Le virus n'est pas plus difficile à détecter : il faut seulement effectuer plus de calculs.

Les virus représentent-ils la plus grande menace pour les données ?

Non. Si l'antivirus est à jour et que chaque application est vérifiée avant d'être utilisée, il est de plus grandes menaces que les virus : les problèmes de bogues, les vulnérabilités diverses, les conflits de logiciels résidants – surtout les caches des lecteurs – sont infiniment plus dangereux.

On dit que certains virus ne peuvent pas être éliminés des disques durs...

Tous les disques durs ont un espace appelé « MBR » (Master Boot Record / Enregistrement d'amorçage maître) où sont stockées des informations essentielles, telles que, par exemple, les données relatives au nombre réel de cylindres, de têtes et de secteurs du disque, ainsi que la table de partition du disque dur avec toutes les informations sur leur taille et quant à l'endroit où ils commencent.
L'un des plus importants ensemble de données stockées dans le MBR est le programme qui charge les systèmes d'exploitation. En effet, lorsqu'il démarre l'ordinateur et essaie de localiser le système d'exploitation dans la première unité de disque, le MBR est l'endroit où il va chercher les informations quant au lieu où se trouve le système d'exploitation.

Si un virus d'amorçage a modifié le système de chargement du système d'exploitation et y a inscrit son propre code viral, le virus sera chargé à chaque démarrage du système.

Si un virus remplace le MBR par son propre code, son élimination est plus compliquée. En effet, il survit à n'importe quel formatage de disque, parce que le MBR n'est jamais modifié pendant un processus de formatage (ce secteur du disque est uniquement modifié lors de l'exécution de la commande FDISK ; il faut néanmoins signaler que la section concernant le code n'est reconstruite que lorsque la partition est supprimée avec FDISK ; l'exécuter simplement n'est pas suffisant). C'est cette caractéristique du MBR lors de son formatage qui incite l'utilisateur peu informé à croire que certains virus sont impossibles à éliminer.

En conclusion, nous dirons qu'il n'existe aucun virus de disque dur qui ne puisse être éliminé si les tâches de formatage sont correctement effectuées.

Jean-Stéphane Bagoëe
Panda Software France

Internet – le moyen de transmission de virus le plus important

Nous recommandons aux utilisateurs d'être extrêmement vigilants quant à leur utilisation d'Internet, l'agent de diffusion le plus employé actuellement par les virus informatiques. L'épidémie du virus VBS/Loveletter (alias « ILOVEYOU »), qui a infecté plus de 3 millions d'ordinateurs dans le monde entier et causé des dommages pour un montant actuellement évalué à près de 8,7 milliards de dollars américains, est un exemple typique du danger que présente Internet.

Au sein de ce réseau des réseaux, les moyens que les virus utilisent pour diffuser leurs effets sont les suivants :

- **Messagerie électronique :** les utilisateurs n'ont rien à faire de spécial pour recevoir des messages électroniques de n'importe quel endroit de la planète et, dans de nombreux cas, ils en reçoivent même qu'ils n'ont pas demandés. Ces courriers électroniques peuvent contenir des fichiers, des documents ou des objets ActiveX contaminés qui, une fois exécutés, infecteront l'ordinateur. À l'heure actuelle, même un message électronique sans aucune pièce jointe peut infecter un système, par le simple fait d'être ouvert. Ces menaces sont encore exacerbées par la technique qu'utilisent les tout derniers virus ; outre se diffuser à la vitesse de la lumière, ils sont capables, pour trouver leurs prochaines victimes, de se servir des adresses inscrites dans le « carnet d'adresses » des utilisateurs infectés.

- **Protocole IRC/Chats :** les applications de discussions sur Internet, telles que les messageries en temps réel (ICQ, AOL Instant Messenger, etc.) ou les services Internet Relay Chat (IRC) offrent un moyen de communication rapide, anonyme, facile et efficace. Cependant, elles peuvent également être dangereuses, car les environnements de discussion facilitent la transmission de fichiers, d'URL, etc., susceptibles de faire courir des risques sérieux aux paramètres du réseau. Certains virus sont en mesure d'envoyer automatiquement des fichiers infectés à tous les utilisateurs qui sont connectés à la même chaîne que l'ordinateur qu'ils viennent d'infecter.

- **Pages Web :** lorsqu'un utilisateur se connecte à une page Web, les fichiers qu'il télécharge peuvent être infectés, de même que les contrôles ActiveX et les Java Applets ; ces derniers endommageront donc tous les systèmes sur lesquels ils seront exécutés par la suite.

- **Transferts de fichiers** (FTP) : il est tout à fait possible de placer des fichiers infectés sur un site Web ou de les télécharger depuis Internet sur un ordinateur par ailleurs libre de virus.

- **Newsgroups :** des messages et des fichiers de données peuvent être infectés et, par conséquent, contaminer les ordinateurs des utilisateurs qui participent à ces groupes.

Outre Internet, les virus utilisent les moyens suivants pour se propager :

- **Connexions du bureau au réseau :** en raison de leur énorme capacité à communiquer avec le monde extérieur – par lignes téléphoniques, unités de disques, Internet et autres réseaux –, les ordinateurs de bureau sont un vecteur à haut risque de virus.

- **Disquettes et disques amovibles :** à l'instar de n'importe quel autre type de disque, les disquettes peuvent contenir des fichiers contaminés. Quand il s'agit d'un virus d'amorçage, la disquette est particulièrement dangereuse car, laissée dans l'unité de disque, elle infectera automatiquement l'ordinateur de l'utilisateur lorsque ce dernier l'allumera et que le système tentera de se lancer à partir de la disquette infectée. Les disques durs amovibles présentent des problèmes similaires.

- **Connexions téléphoniques directes *via* modem :** ce type de connexion permet à un ordinateur de se raccorder à toute autre machine n'importe où dans le monde, avec en corollaire le risque de transmettre des fichiers et des messages électroniques infectés. Il en est de même des serveurs qui peuvent se connecter à des modems afin de permettre l'accès à distance à des réseaux.

Jean-Stéphane Bagoëe
Panda Software France

Ce n'est pas drôle du tout !

• LES VIRUS LES PLUS DANGEREUX DU POINT DE VUE de la sécurité ne sont pas ceux qui manifestent leur présence intempestivement. Ceux qui, tapis dans l'ombre du disque dur, ont pour mission de créer une vulnérabilité « cachée » et de signaler le « client » à des programmes de scrutation réseau spécialisés, le sont infiniment plus.

• LE VER APPELÉ « FUNNYSTORY » EN EST UN EXEMPLE. Il envoie de lui-même un courrier à des adresses puisées – à l'insu du propriétaire – dans le carnet d'Outlook. Ce courrier contient une pièce jointe présentée comme des « histoires drôles » : c'est un cheval de Troie dont l'objectif est de voler des données sensibles, telles que des noms et des mots de passe de systèmes, des codes cachés et des mots de passe de connexion à Internet. En outre, le ver envoie périodiquement à une adresse électronique préétablie les données rassemblées depuis ce PC infecté. Celui-ci est littéralement siphonné par ces messages électroniques. « FunnyStory » crée également un registre où il inscrit la date, l'heure, le nom de l'utilisateur et le nom du PC infecté. Au moment de l'infection et pour éviter d'être détecté, le ver se détruit lui-même après avoir modifié le système afin d'être lancé à chaque démarrage. Il n'est évidemment pas visible depuis la barre des tâches de Windows.

• SOCKET23 (SOCKETS DE TROIE V2.5) EST UN autre exemple de code pernicieux qui cherche à rester silencieux. Il se transmet comme un virus et est capable d'infecter un environnement WINDOWS-95 ou NT. Il permet la prise de contrôle à distance de toute machine infectée. RL

SÉCURITÉ INFORMATIQUE
numéro 31 octobre 2000
SÉCURITÉ DES SYSTÈMES D'INFORMATION

Sujets traités : tout ce qui concerne la sécurité informatique. Gratuit.
Périodicité : 5 numéros par an.
Lectorat : toutes les formations CNRS.

Responsable de la publication :
ROBERT LONGEON
Centre national de la recherche scientifique
Service du Fonctionnaire de Défense
c/o IDRIS - BP 167. 91403 Orsay Cedex
Tél. 01 69 35 84 87
Courriel : robert.longeon@cnrs-dir.fr
http://www.cnrs.fr/Infosecu

ISSN 1257-8819
Commission paritaire n° 3105 ADEP

Conseil et coordination : CNRS - DIST - Jacqueline Leclère • Conception et réalisation : La Souris 01 45 21 09 61