

Edito

Le vocabulaire des informaticiens est parfois très imagé... Ainsi, lorsque vous entendez parler de vers, de bombes logiques ou de chevaux de Troie, sachez qu'il est en fait question de virus informatiques, et que derrière chacun de ces termes se cachent des actions malveillantes précises qu'il n'est pas sans intérêt de connaître.

Les utilisateurs du CRI sont nombreux à se plaindre de ce qui est devenu le fléau majeur de l'informatique. Ce CRI Pratique n°2 vous propose un petit aperçu destiné à vous faire comprendre ce qu'est un virus, comment il agit, et comment l'on peut essayer de s'en prémunir. Malheureusement, vous verrez qu'il n'existe aucune solution « miracle », et que la meilleure protection reste la prévention ...

Ce sujet complexe et important nécessiterait beaucoup plus que ces quelques pages. Une documentation complète est disponible sur le site web du CRI, dans la rubrique "Documentation". N'hésitez pas à la consulter, elle vous permettra d'augmenter votre sécurité ainsi que celle des autres : http://www.cri74.org/actualites/virus/securete_info_virus.html

Bonne lecture !

Entre "vers" et "chevaux de Troie", un bêtisier de l'informatique pas très amusant...

Pour la plupart des utilisateurs, un virus est un programme qui 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.

Mais on sait moins que les virus peuvent aussi servir à percer les systèmes les plus secrets en créant des vulnérabilités "cachées" qu'un autre processus exploitera ultérieurement. Ces virus propagent ces vulnérabilités et "marquent" 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 et c'est pourquoi ils ne perturbent pas le système et ne détruisent pas de données. Ces virus, contrairement aux apparences, sont les plus dangereux. En effet, sur une machine ainsi contaminée, votre système d'information devient un livre ouvert, et l'intégrité même de votre système et de vos données est en danger.

Quelques définitions

ver	Programme qui possède la faculté de s'auto-reproduire et de se déplacer au travers d'un réseau. Il s'installe sur l'ordinateur et agit comme un programme. Il utilise le réseau local, les mails, les cédéroms et les disquettes pour se propager.
bombe logique	Dispositif programmé qui contient un mode de déclenchement différé.
cheval de Troie	Se présente généralement sous la forme de programmes à caractère utilitaire ou de jeux. 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). C'est par un cheval de Troie que se créera par exemple une entrée secrète ou d'autres types de vulnérabilité dans le système.

Les applications "critiques"

Toutes les applications informatiques, quelles qu'elles soient, sont susceptibles de présenter des failles sécuritaires. Ces failles peuvent alors être utilisées par des personnes mal intentionnées pour s'introduire dans votre ordinateur, en prendre le contrôle et lui faire exécuter n'importe quelle application ou des actions spécifiques sur le système.

Il est donc impossible de dresser une liste exhaustive de ces « applications critiques ». Cependant, parce que les créateurs de virus cherchent à infecter le plus grand nombre d'ordinateurs, ils s'attaquent aux applications les plus utilisées. Et ce sont donc, très logiquement, les différentes versions du système d'exploitation Microsoft Windows, le navigateur web Microsoft Internet Explorer ou encore les différentes versions des outils messagerie Microsoft Outlook et Outlook Express, utilisées en majorité, qui sont victimes de ces attaques. Mais cela n'empêche pas l'existence de failles sur d'autres applications comme Mozilla ou Eudora.

Détecter un virus

La liste suivante contient des problèmes logiciels et matériels qui pourraient indiquer la présence de virus. Attention, le conditionnel est de rigueur, puisqu'aucun de ces symptômes n'est une preuve définitive de la présence d'un virus !

Symptômes Logiciels

- Le système ralentit
- Le système d'exploitation ou les applications affichent des messages d'erreurs inhabituels
- Des messages étranges apparaissent
- Des fichiers système disparaissent
- Vos applications se bloquent fréquemment
- Le système d'exploitation ou des logiciels de base ne peuvent être lancés
- De nouveaux programmes apparaissent dans la liste des programmes en cours
- De nouvelles lignes sont ajoutées sans raison aux fichiers de configuration communs
- L'ordinateur cherche à se connecter à Internet à chaque démarrage ou de manière inopinée, sans aucune action de votre part
- Votre première page, à l'ouverture du navigateur, a changé
- Il y a de nouvelles entrées dans la base des registres

Symptômes Matériels

- Le disque dur semble constamment en activité ou semble effectuer une opération fastidieuse
- Des messages d'erreurs apparaissent indiquant un manque de ressources système alors que vous n'avez aucune application ouverte
- Le lecteur de disquettes cherche à écrire constamment sur la disquette alors qu'il n'y en a pas dans le lecteur
- Un message d'erreur inhabituel apparaît avant le chargement de Windows

En règle générale :

-Méfiez-vous de tout mail non attendu, de nature suspecte, dont l'expéditeur peut paraître connu mais qui aurait un contenu louche (texte incomplet, fichier attaché non mentionné dans le mail, adresse de l'émetteur proche d'une adresse valide mais légèrement différente, ...)

-Méfiez-vous des annonces concernant des virus qui ne précisent pas une adresse de site « de confiance » (éditeur anti-virus, organismes de référence) où vérifier la véracité des propos. Il est très fréquent que des canulars (ou « hoax ») ou autres « chaînes de l'amitié » polluent les boîtes aux lettres électroniques avec des messages alarmistes où il est demandé de supprimer un fichier ou de propager l'information à l'ensemble du carnet d'adresses.

-Limitez les accès en écriture sans mot de passe pour les partages réseau. En effet, beaucoup de virus ont la possibilité de se transmettre aux autres machines d'un réseau dans lequel une machine est infectée, en pénétrant sur les disques durs dont un accès est autorisé sans authentification. Avec un simple mot de passe (même basique) pour les accès en écriture, on évite assez simplement la propagation de ces virus.

Mais surtout, mettez à jour de manière régulière votre antivirus, et tenez-vous au courant tout aussi régulièrement des dernières mises à jour, des correctifs et autres avis officiels émis par les éditeurs et les structures spécialisées concernant vos applications : les failles de sécurité récemment découvertes sont ainsi déclarées et sécurisées.

Comment se prémunir des virus ?

Il n'y a pas de solution « miracle », et mettre à jour votre logiciel antivirus ne suffit pas. Cependant, la prévention paie toujours, et quelques règles simples peuvent être appliquées :

-Ne téléchargez pas des programmes d'origine douteuse, qui peuvent vous être proposés sur des sites personnels ou des forums de discussion ("chats") eux-mêmes plus ou moins douteux.

-Méfiez-vous des fichiers joints aux messages que vous recevez : analysez avec un antivirus à jour tout fichier avant de l'ouvrir, et préférez détruire un mail douteux plutôt que d'infecter votre machine, même si l'expéditeur est connu.

-Fuyez les disquettes d'origine inconnue (ou ayant transitées dans des lieux publics vulnérables comme les salles de cours des écoles), et protégez les vôtres en écriture.

-Créez dès maintenant, si ce n'est pas déjà fait, une disquette de démarrage saine contenant un antivirus (la plupart des antivirus le proposent) pour une désinfection d'urgence.

-Procédez régulièrement à des sauvegardes du contenu important de votre disque dur après avoir vérifié l'absence de virus : cela peut paraître fastidieux, mais en cas d'infection (ou même simplement en cas de "crash" de disque dur), vous serez heureux de l'avoir fait.

Attention cependant ! Veillez à ne pas "backuper" un virus !

Que peut faire le CRI pour protéger ses utilisateurs ?

Vous l'avez compris, aucun système n'est entièrement fiable. Le CRI étudie différentes solutions pour préserver au maximum ses utilisateurs, mais ces solutions restent pour la plupart compliquées à mettre en place et très coûteuses en général.

Le CRI pourrait installer un antivirus sur son propre serveur mail. Mais cette solution présente beaucoup d'inconvénients. Le premier vous concerne directement : ce système doit pouvoir être activé ou refusé par chaque utilisateur de manière individualisée. Cette procédure pose donc des questions déontologiques et juridiques importantes. L'ouverture du courrier sans autorisation préalable de l'utilisateur final n'est pas correcte. De plus, elle implique la mise en place d'un système de filtrage personnalisé et individuel par utilisateur, qui n'est en général pas disponible sur les systèmes antivirus commerciaux, et nécessite donc des développements particuliers.

D'autre part, un antivirus placé sur le serveur mail du CRI ne pourrait détecter que les virus transitant par ce serveur mail. Si l'utilisateur possède une messagerie, hébergée chez un autre fournisseur d'accès (dumont@yahoo.com, durant@voila.fr, etc.), l'antivirus placé au CRI ne sera d'aucun secours lorsque cette personne ira « récupérer » un message sur cette boîte aux lettres depuis son poste informatique, le message en question empruntant un autre chemin que le serveur mail du CRI.

Enfin, la messagerie n'est pas le seul vecteur de virus. Vous pouvez par exemple contaminer votre ordinateur en téléchargeant un fichier sur le web, et c'est pourquoi tous les trafics réseau faisant transiter des fichiers (web, ftp, etc.) doivent faire l'objet d'un contrôle pour une garantie d'efficacité évidente.

À l'heure actuelle, le CRI ne peut donc que mettre en garde ses utilisateurs des risques liés aux virus, et leur rappeler qu'à l'instar de la conduite automobile, l'informatique exige une certaine responsabilisation de la part de ceux qui l'utilisent. Alors restez vigilants, pensez à mettre à jour de façon régulière vos antivirus, méfiez-vous de tout ce qui peut vous sembler anormal, et surtout, en cas de doute, n'hésitez pas à faire appel au CRI : mieux vaut prévenir que guérir !

Agenda

Le 18 juin 2003, le CRI organise la première édition de LinuxEdu, Solutions Libres et TICE, réservée aux acteurs de l'Éducation Nationale. [Toutes les informations sur le site web du CRI : http://www.cri74.org/](http://www.cri74.org/)

Dans le prochain numéro...

de CRI Pratique (juin 2003) : [Entre sécurité et économie, quel Fournisseur d'Accès Internet choisir ?](#)