

Documentation Utilisateur : Virus et sécurité informatique

Sommaire

<u>1. Problèmes de virus et de sécurité informatique en général rencontrés par les utilisateurs des services du Centre de Ressources Informatiques de Haute-Savoie (automne 2002)</u>	1
<u>2. Les virus informatiques</u>	2
<u>3. Les risques d'attaques liés aux connexions permanentes à moyen débit qui ne sont pas correctement protégées</u>	4
<u>4. La position de la société Microsoft dont les produits représentent la principale cible de ces attaques</u>	5
<u>5. Conclusion</u>	6

1. Problèmes de virus et de sécurité informatique en général rencontrés par les utilisateurs des services du Centre de Ressources Informatiques de Haute-Savoie (automne 2002).

Le Centre de Ressources Informatique de Haute-Savoie a largement été sollicité depuis plusieurs mois sur des sujets traitant de sécurité informatique.

Avec l'apparition de très nombreuses formes de dangers liés à la connexion Internet, mais aussi la banalisation de ce sujet dans les médias et la diffusion au grand public de reportages traitant de ces sujets, les utilisateurs sont de plus en plus sensibilisés (c'est une bonne chose) mais aussi de plus en plus touchés de près par ces problèmes.

Les sujets majeurs sont les virus informatiques d'une part (sous toutes leurs formes) mais aussi les problèmes de vulnérabilité des machines des utilisateurs dans le cadre de connexions à Internet par d'autres fournisseurs d'accès Internet (dans le cas des connexions par ADSL et câble notamment). On ne parlera pas ici des "denis de service" dûs aux spams (le fait de voir sa boîte aux lettres électroniques polluée par des mails non désirés et faisant souvent appels à des images situées sur des serveurs distants peut arriver à bloquer l'utilisation d'une machine pendant une durée non négligeable quand on cumule les nuisances de tous ces spams qu'on peut recevoir dans une journée) afin de ne pas surcharger le document (la Question/Réponse 15 de la [FAQ du CRI](#) expose un peu cet aspect des choses).

2. Les virus informatiques

Nous entendons par "virus" toutes les formes d'attaques liées à l'arrivée sur une machine de fichiers infectés qui tentent de nuire au fonctionnement de celle-ci, qui essaient de se propager par tous les moyens à partir de cette même machine, voire qui permettent l'accès à la machine depuis l'extérieur pour d'autres attaques plus violentes (=> virus, vers, "chevaux de Troie", ...).

Depuis novembre 2001, le CRI, saisi par la demande des usagers, a réfléchi et étudié avec plusieurs sociétés spécialisées une réponse possible à ces problèmes avec les impératifs suivants :

- ◆ le système mis en place doit pouvoir être activé ou refusé pour chaque utilisateur des services du CRI de façon individualisée (on ne peut pas imposer à tout le monde ce service). Mettre un système anti-virus sur la messagerie pose des questions déontologiques et juridiques importantes. L'ouverture du courrier sans autorisation préalable de l'utilisateur final (que ce soit à l'envoi ou à la réception) n'est pas correct (à la fois déontologiquement et surtout juridiquement). Ce problème 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.
- ◆ le système mis en place ne peut pas se contenter de scanner les emails en entrée et sortie du réseau du CRI. Tous les trafics réseau (web, ftp, mail notamment) doivent faire l'objet de ce contrôle; sinon, le système se révélerait vite inefficace. En effet, un virus informatique peut se trouver dans n'importe quel fichier échangé sur le web; il n'est pas limité aux transactions de type messagerie électronique.
- ◆ le coût induit par un tel système (licences du logiciel anti-virus, serveurs supplémentaires nécessaires pour ce traitement) doit être économiquement acceptable.
- ◆ tous les aspects légaux et juridiques liés au statut du CRI de Haute-Savoie et à la diversité de ses utilisateurs doivent être pris en compte

Les diverses propositions qui ont été reçues ne répondaient jamais totalement aux impératifs ci-dessus (certaines propositions dépassaient le budget annuel du CRI!), si bien qu'aucune solution n'a pour l'instant pu être retenue et mise en place.

Le CRI n'a donc pas encore de système de protection anti-virus à proposer à ses utilisateurs. Cependant, il continue d'étudier cette question. En attendant, il est donc vivement conseillé à chacun :

- ◆ de se munir d'une protection individuelle tenue à jour fréquemment. Des solutions peu coûteuses existent à titre individuel ou collectif.
- ◆ de mettre à jour régulièrement les logiciels qui révèlent certaines lacunes en terme de sécurité. Le couple Internet Explorer/Outlook Express notamment qui fait très souvent l'objet de patches de mise à niveau pour palier aux trous de sécurité découverts régulièrement et corrigés par Microsoft; <http://www.microsoft.com/downloads/searchdl.asp?LangIDCODE=7%3Bfr&Submit1=GO> et <http://windowsupdate.microsoft.com/> sont 2 adresses à consulter fréquemment pour les personnes qui utilisent ces outils

- ◆ de se méfier de tout mail non attendu, de nature suspecte, dont l'expéditeur peut apparaître comme connu malgré tout 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, ...)
- ◆ de se méfier 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 informations alarmistes où il est demandé de supprimer un fichier ou de propager l'information à l'ensemble du carnet d'adresses. Des sites recensant ces alertes existent et permettent d'éviter la prolifération de ces canulars (exemple : <http://www.foxbuster.com/> ; <http://www.secuser.com/hoax/index.htm> ; <http://www.symantec.com/avcenter/hoax.html>).
- ◆ de limiter les accès en écriture sans mot de passe pour les partages réseau. En effet, un bon nombre 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 une simple protection par mot de passe (même basique) pour les accès en écriture, on évite assez simplement la propagation de ces virus.

Même si un système antivirus est mis en place par le CRI, et pour appuyer l'intérêt d'avoir le système antivirus au plus près de l'utilisateur, on peut aussi estimer qu'un tel outil placé au niveau des serveurs du CRI ne permettrait pas d'éviter l'infection des machines des utilisateurs par des virus présents sur des disquettes par exemple, ou des CD-ROM (tout support amovible en général)... Dans un cas comme ça, le danger de diffusion du virus sur les autres machines du réseau apparaît encore à nouveau par les phénomènes de propagation utilisés par certains de ces virus (partages réseau, serveurs de messagerie internes, ...).

3. Les risques d'attaques liés aux connexions permanentes à moyen débit qui ne sont pas correctement protégées

D'autre part, les internautes utilisant les services du CRI sont de plus en plus tentés, et c'est légitime, par les offres d'accès au réseau à moyen débit qu'offrent des technologies telles que le câble et l'ADSL notamment. Les contraintes économiques et/ou techniques liées à ces technologies ne permettent pas aujourd'hui au CRI de proposer de tels accès à ses usagers. Il semble que certains utilisateurs des services du CRI qui bénéficiaient au préalable d'une connexion par modem RTC ou adaptateur/routeur RNIS aient franchi le pas ou s'apprêtent à le franchir, de prendre un abonnement auprès d'autres fournisseurs d'accès afin de bénéficier de l'accès à ces technologies.

S'il est tout à fait compréhensible que les gros consommateurs en terme de bande passante soient intéressés par ces offres qui permettent sans contestation l'accès à certaines ressources avec un débit plus important, il ne faut pas qu'ils en oublient les aspects de sécurité informatique liés à cette connexion quasi-permanente à Internet et ne bénéficiant en général d'aucune protection par firewall de la part de leur fournisseur d'accès à Internet.

En effet, le fait de bénéficier d'un accès à moyen débit, permanent (ou presque selon les cas), et avec une adresse d'identification sur le réseau (l'adresse IP) qui varie peu sont autant de facteurs augmentant les risques d'attaques de la machine raccordée. Certains internautes mal intentionnés passent leur temps à essayer de pénétrer sur les ordinateurs d'autres internautes qui ne se protègent pas des accès extérieurs. Ainsi, en utilisant des outils simples qui exploitent les "trous de sécurité" des machines attaquées, ils peuvent avoir accès au contenu du disque dur d'un ordinateur et y récupérer des données privées, les détruire, les diffuser, etc. C'est ainsi que des informations confidentielles peuvent échapper au contrôle de leur propriétaire et leur porter préjudice (numéros et/ou codes de carte bancaire par exemple). Pire encore, la pénétration d'un "pirate" informatique sur une machine d'un réseau lui permet d'avoir accès aux autres machines du réseau (partages de fichiers notamment). Cela peut permettre aussi de "rebondir" sur une autre machine en relation plus ou moins directe avec la machine qui a servi de porte d'entrée. Ainsi, sur un réseau où une seule machine a un accès à Internet, toutes les machines, qui semblent pourtant à première vue hors de portée de toute attaque, sont potentiellement en danger.

La mise en place de système "filtrant" et régulant les échanges bi-latéraux à l'entrée des réseaux connectés ainsi devrait être systématique mais les contraintes techniques et financières d'un tel système sont souvent trop importantes et conduisent les utilisateurs à estimer que de telles précautions se sont pas justifiées, ceux-ci partant du principe que "ça arrive toujours aux autres". Dans la mesure où un ordinateur peut servir de relais à une attaque venant d'Internet, toute personne utilisant une machine connectée au "Net" doit être consciente de sa responsabilité vis à vis des autres machines du ou des autres réseaux qui sont en contact avec celle-ci.

4. La position de la société Microsoft dont les produits représentent la principale cible de ces attaques

Les réponses aux questions de sécurité informatique formulées par Microsoft, un des principaux concernés quand on parle de virus informatique, les systèmes d'exploitation MS Windows et les logiciels de cet éditeur étant particulièrement fragiles vis à vis de ce genre d'attaques, sont, à nos yeux, insatisfaisantes (voir <http://www.microsoft.com/France/Internet/ressources/dossiers/securite/default.asp>). La considération des risques y est beaucoup trop faible. Les utilisateurs de ces outils doivent être conscients des risques qu'ils prennent lorsqu'ils utilisent, par exemple, un outil de messagerie tel qu'Outlook Express lorsque celui-ci n'est pas maintenu au "goût du jour". Un simple mail qui arrive dans la "boîte de réception" peut, lorsqu'il est affiché, infecter la machine hôte sans que le moindre attachement ne soit ouvert explicitement par l'utilisateur (cas des virus Klez ou BugBear apparus au cours de la dernière année)!

5. Conclusion

En conclusion, il est donc important que chacun prenne en main sa propre sécurité informatique par des attitudes simples à mettre en place et peu contraignantes. On ne peut pas se contenter de vouloir un accès à Internet sans prendre en considération tous les aspects qui en dépendent et la sécurité en fait largement partie.

Pour finir, voilà quelques URLs de référence sur la sécurité informatique en général, et les virus en particulier :

- ◆ Sécurité informatique

- ◇ <http://www.cnrs.fr/Infosecu/>
- ◇ <http://www.cru.fr/securite/>
- ◇ <http://www.secuser.com/>
- ◇ <http://www.securiteinfo.com/>
- ◇ <http://www.securite.org/index2.html>
- ◇ <http://www.securite-informatique.com/>
- ◇ <http://www.secusys.com/index.htm>

- ◆ Virus et hoax

- ◇ <http://www.aspirine.org/>
- ◇ <http://www.hoaxbuster.com/>
- ◇ <http://www.secuser.com/>