UNIVERSITE DE LIMOGES

Service Commun Informatique

Fiche Pratique

juin 2004

Virus, hoax etc...

SERVICE COMMUN INFORMATIQUE

Qu'est-ce qu'un virus ?

Un virus est un programme, transmis par courrier, fichier, ou de façon indépendante (réseau) qui se charge en mémoire et exécute les instructions que son auteur a programmées.
On distingue ainsi différents types de virus :

les vers : capables de se propager à travers un réseau (local ou internet)
Voir http://www.commentcamarche.net/virus/worms.php3

les troyens (chevaux de Troie) : permettant de créer une faille dans un système pour permettre à son concepteur de s'introduire dans le système infecté afin d'en prendre le contrôle.
Voir http://www.commentcamarche.net/virus/trojan.php3

les bombes logiques : capables de se déclencher suite à un événement particulier (date système, activation distante, ...)
Voir http://www.commentcamarche.net/virus/bomblogi.php3

Qu'est-ce qu'un antivirus ?

Les antivirus sont des programmes capables de détecter et de nettoyer le cas échéant un virus sur l'ordinateur.
Les antivirus s'appuient, entre autres, sur la « **signature virale** » propre à chaque virus pour les détecter. Cette méthode n'est fiable que si l'antivirus possède une **base virale à jour**.
On appelle "rétrovirus" ou "virus flibustier" (en anglais *bounty hunters*) un virus ayant la capacité de modifier les signatures des antivirus afin de les rendre inopérants.

Qu'est ce qu'un hoax ?

On appelle **hoax** (en français *canular*) un courrier électronique propageant une fausse information (alerte virale, demande humanitaire…) et poussant le destinataire à diffuser la fausse nouvelle à tous ses proches ou collègues.
Le but des hoax est simple :

- contribuer à engorger inutilement les réseaux, en véhiculant de la désinformation.
- encombrer inutilement les boîtes aux lettres déjà chargées.
- nuire à l'image de la personne qui redirige cette fausse information.

Comment se prémunir contre les virus

Pour renforcer la sécurité de votre ordinateur et favoriser une meilleure protection contre les derniers virus connus et ceux à venir, il suffit de quelques gestes simples qui devraient devenir des automatismes :

- **Installez un antivirus et mettez-le à jour quotidiennement**

Les logiciels suivants, négociés globalement par le Ministère de l'Education Nationale, sont disponibles sur le serveur FTP de l'Université :
voir sur le site du S.C.I. : http://www.unilim.fr/sci/ à la rubrique "**Distribution de logiciels**".
PC : Pour un nouveau pc (poste ajouté au parc informatique depuis décembre 2003) :
VirusScan Enterprise 7.1 (dossier : Viruscan_Enterprise_7.1/VSE710FR.zip)
NB : on ne doit pas installer Norton Anti-Virus (celui du serveur de l'Université) sur un nouveau poste.
Cette installation n'est possible qu'en cas de renouvellement d'un poste.
Pour les inconditionnels de Norton, il suffit :
soit d'acheter le logiciel en dehors du contrat de l'Université,
soit de libérer une licence d'un autre poste, afin de bénéficier de celle-ci pour l'installer sur le nouveau poste.
MAC : Virex 7 (dossier : Mcafee/Virex/Virex7.gz)

Pour confirmer une alerte ou scanner ponctuellement votre disque dur, vous pouvez aussi utiliser un antivirus gratuit en ligne, par exemple : http://www.secuser.com/outils/antivirus.htm

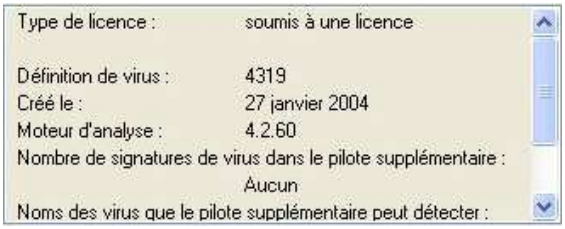
Virus…

- **Programmez la mise à jour de votre antivirus quotidiennement**

Comment vérifier la dernière date de mise à jour ?

Pour Norton AV : au lancement du logiciel, affichage de la version de mise à jour

Pour MacAfee (Viruscan) : console Viruscan, cliquez sur "à propos de…"

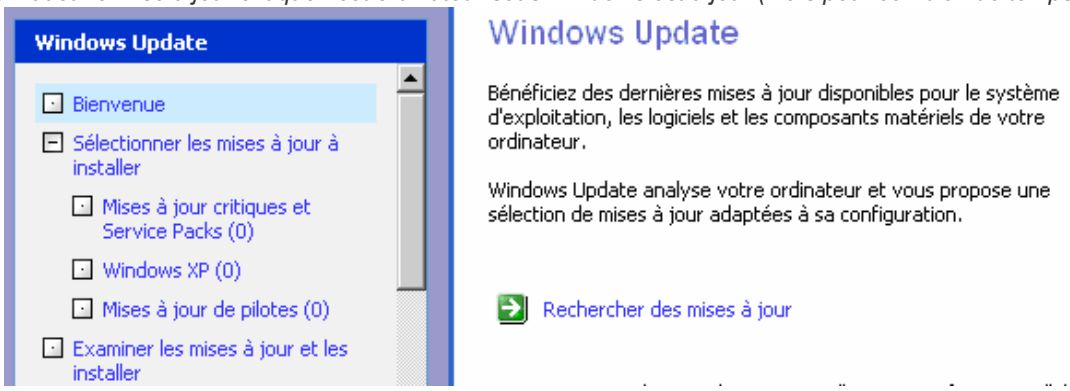


- **Appliquez régulièrement les correctifs de sécurité**

en particulier dans le cas des produits Microsoft (Internet Explorer, Outlook (Express), Word, etc.), très répandus et fréquemment pris pour cible.
Plusieurs outils existent afin de faciliter cette mise à jour, comme WindowsUpdate, OfficeUpdate. Ces correctifs permettent de combler les failles utilisées par les virus (par exemple l'exécution automatique à l'ouverture d'un courriel).
Windows Update (**http://windowsupdate.microsoft.com**) est le service en ligne de mises à jour de Windows et du navigateur Internet Explorer (choisissez "Rechercher des mises à jour", puis téléchargez et installez les "Mises à jour critiques et Service Packs" et, si besoin, les "Mises à jour recommandées").

Exemple 1, ci-dessous : 6 mises à jour critiques : votre ordinateur (sous Windows) est en danger !

Ici : aucune mise à jour critique : cet ordinateur sous Windows est à jour (mais pour combien de temps ?)



Vous pouvez aussi utiliser la fonctionnalité « Mises à jour automatiques » de Windows afin de télécharger et d'installer les mises à jour de sécurité importantes de Microsoft, de manière transparente.

Menu Démarrer / Panneau de configuration / icône Système / onglet « Mises à jour automatiques »

Office Update (**http://office.microsoft.com/home**)
C'est le service en ligne de mises à jour des logiciels de la suite Microsoft Office (Word, Excel, Access, Outlook, etc.). Cliquez sur "Rechercher des mises à jour".

- ***Méfiez vous des pièces jointes dans un mail***

En effet une pièce jointe n'est jamais anodine, même si elle provient d'une personne connue :
cette dernière peut avoir été victime d'un virus qui a utilisé son carnet d'adresses pour infecter tous ses correspondants.
Prenez également le temps de lire le contenu des messages qui vous sont adressés avant d'ouvrir un fichier joint : si un collègue qui ne parle pas anglais vous envoie soudain un mail dans la langue de Shakespeare ou si votre tante Cécile vous adresse un message composé de phrases (encore plus) incompréhensibles (que d'habitude), il y a lieu de se méfier et de demander confirmation à l'expéditeur. Dans le pire des cas, il peut s'agir d'un virus inconnu, non détecté ou encore imparfaitement détecté par votre antivirus.
Attention, contrairement à la quasi-totalité des autres, le virus **NetSky** apparu en avril 2004 se propage dans un message écrit en **français**. En fait, il s'adapte à l'origine géographique du destinataire !
Si votre adresse de messagerie se termine par .fr, le titre du message et son contenu seront en français, avec une phrase comme « Cliquez ici pour lire ce document » .
Un simple clic sur le lien, et vous êtes infecté !

Un dernier conseil

Si vous travaillez sous Windows 2000 ou Windows XP, activez-en le pare-feu intégré, ce qui devrait vous protéger de nombreux virus.
Pensez aussi à visiter http://www.symantec.fr et http://www.macafee.com