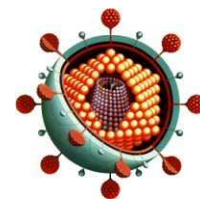




HISTOIRES DE VIRUS

UN PEU DE VOCABULAIRE...

Virus : Parasites informatiques malveillants conçus pour se reproduire, endommager ou récupérer des données. Ils se propagent en se greffant à des programmes véhiculés par mails, CD-Rom ou Disquettes.



Vers : Parasites informatiques qui arrivent depuis Internet et s'installent seuls sur les ordinateurs si le système d'exploitation n'est pas mis à jour. Ils ne se reproduisent pas.

Chevaux de Troie (troyens) : Ce sont des programmes piégés qui ont l'apparence de programmes informatiques sains. Ils arrivent souvent par e-mail et ne se reproduisent pas.

Spyware : Logiciels espions infiltrés, qui, à l'insu de l'utilisateur, enregistrent des données (courriers électroniques documents, mots de passe...) pour les transmettre à un tiers.

Adware : Utilisés dans le domaine de la publicité en ligne, ces logiciels collectent et transmettent des informations sur les habitudes de navigation des internautes. Ils sont également responsables de l'affichage sauvage de publicités.

Spam : Le pourriel ou spam en anglais, désigne les communications électroniques massives, notamment de courriers électroniques, non sollicitées par les destinataires, à des fins publicitaires ou malhonnêtes.

FAUX ET FAUSSES RUMEURS...

Même si les logiciels malveillants ne sont pas à prendre à la légère, il ne faut pas non plus tomber dans la psychose ! Les canulars, les avertissements, et les histoires d'horreur sont presque aussi habituels que les vrais virus. Alors quand vous entendrez une histoire de virus, faites preuve de retenue avant de céder à la panique. Vous ne pouvez pas obtenir de virus par les méthodes suivantes :

- **Lire un courrier électronique** - Le simple fait de lire le texte d'un courrier électronique est totalement inoffensif. Si un message contient un virus, il est placé dans une pièce jointe ou dans une image incorporée au message. Pour être sûr de ne pas contaminer votre ordinateur, le plus simple est de supprimer tout message venant d'une personne que vous ne connaissez pas et dont l'objet est en anglais.
- **Lire une page Web** - Oui, il y a une brèche dans la sécurité du navigateur Internet Explorer: si vous désactivez les fonctions de sécurité du navigateur, des contrôles ActiveX malveillants peuvent réarranger les fichiers de votre disque dur, chercher des informations secrètes et ainsi de suite. Cependant, si vous réalisez régulièrement les mises à jour système (dans le cas de Windows, des nouvelles mises à jour sont mises en ligne tous les mois. Par ailleurs, vous pouvez toujours installer un autre navigateur que Internet Explorer (Mozilla, Netscape...).
- **Télécharger un fichier** - Répétons-le, vous devez exécuter un programme pour contracter un virus. Alors, si vous téléchargez un document, vous pouvez attraper un virus en ouvrant le document téléchargé.

Les virus à travers l'histoire

1949 : John Von Neumann présente les fondements théoriques des logiciels autocopiés.

1960 : Un groupe de jeunes ingénieurs des laboratoires Bell met au point un jeu informatique du nom de Core war,

1984 : Le magazine Scientific American présente un guide pour fabriquer ses propres virus.

1986 : Les frères Alvi, deux Pakistanais, fournissent à des touristes des copies de logiciels pirates infectés du virus Brain. Ce serait le premier virus clairement identifié et connu. Il a causé de sérieux dégâts sur les campus américains.

1988 : Peace/Mac affiche son message de paix universelle sur les écrans de possesseurs de Macintosh II.

1988 : Robert Morris est arrêté pour fraude informatique. Cet étudiant vient de causer 15 millions de dollars de dommage sur Internet à cause de son virus.

1989 : Datacrime : trois virus font trembler les Pays-Bas et la France. La police néerlandaise propose alors un ensemble de programmes informatiques à bas prix pour lutter contre ces virus. C'est à cette époque que la France prend réellement conscience de l'existence des virus.

1991 : Diffusé par une disquette vendue dans la revue Soft et Micro, le virus Frodo/4096 arrive en France. Le Clusif (Club de la sécurité des systèmes d'information français) propose sur son serveur une procédure de détection et de décontamination pour lutter contre Frodo. Le serveur enregistre 8 000 connexions.

1992 : Le virus Michelangelo plonge la planète dans l'effroi. Ses effets restent pourtant limités : 200 000 machines infectées, au lieu des 5 à 15 millions annoncées.

1998 : D'après les chiffres publiés par Dr Salomon's, éditeur d'antivirus, on recensait 17 745 virus différents en 1998, contre 18 en 1989.

2000 : le virus "I Love You" provoque l'effroi sur Internet par sa contagion très rapide.



HISTOIRES DE VIRUS

Vous venez tout juste de recevoir un message urgent d'un ami: il y a un nouveau virus dans les parages, et il est vraiment vilain. Si vous lisez du courrier électronique ou cliquez sur un lien, le virus effacera automatiquement votre disque dur, videra votre compte en banque, et expédiera des messages obscènes à tout votre carnet d'adresse patron. Étant un internaute consciencieux, vous passez le mot à vos amis et au département d'informatique de votre travail.



Attention ! Vous devriez vérifier si l'information que l'on vous a communiquée est bien réelle. En effet, très souvent, nous avons tendance à faire confiance à l'expéditeur. Or celui-ci peut aussi être victime d'une rumeur. Il est essentiel de vérifier une information avant de la faire suivre ! Car c'est grâce à ce genre de messages que des personnes mal intentionnées récoltent votre adresse et peuvent vous envoyer de vrais virus !

Pour vérifier que l'information est une rumeur, vous pouvez aller sur le site www.hoaxbuster.com

SE PROTÉGER...

La première protection consiste à **mettre ses logiciels à jour régulièrement**. Sans ses mises à jour régulières, vous serez quoi qu'il arrive, vulnérable.

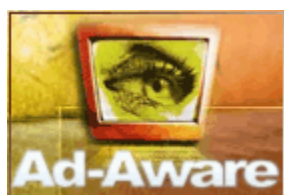
Afin de vous prémunir des failles de votre système d'exploitation, il est préférable de mettre à jour votre système d'exploitation. Dans le cas de Windows XP, vous pouvez cliquer sur Démarrer > Tous les programmes > Windows Update.

En réalisant cette opération, vous allez sur Internet, sur le site de Windows. Pour mettre à jour votre système d'exploitation, suivez les étapes. Attention, certaines mises à jour sont longues à télécharger (cas du service pack 2 par exemple).

Aujourd'hui il est impératif d'avoir un **anti-virus**. Les antivirus sont légion. Du logiciel payant au logiciel gratuit, le choix est varié. Cependant il ne faut pas oublier que votre antivirus doit être **mis à jour régulièrement**. L'antivirus Avast (Edition Familiale) est gratuit, performant, et il se met à jour tout seul. Si vous n'avez pas d'antivirus, vous pouvez le trouver à cette adresse : www.avast.com/index_fre.html



Pour se prémunir faces aux logiciels espions, le meilleur moyen est d'installer un **Firewall**. Ce logiciel met en place un « périmètre de sécurité » autour de l'ordinateur. Il vous demandera ainsi, à chaque fois qu'un programme se lance, si vous autorisez celui-ci à se lancer. Votre ordinateur ne sera alors plus l'objet de programmes malveillants. Windows intègre déjà un firewall et il n'est pas indispensable de le remplacer par un autre.



En complément, il y a des logiciels qui vérifient que vous n'avez pas de **logiciels indésirables** sur votre ordinateur. Le logiciel gratuit **Ad-Aware** vous permettra d'effacer tous les programmes espions et aussi les programmes qui lancent des publicités non désirées.

Attention, aujourd'hui, il est indispensable d'avoir un antivirus et un firewall. Mais il n'en faut qu'un seul de chaque ! Si vous installez plusieurs anti-virus ou firewall en même temps, rien ne fonctionnera plus !



HISTOIRES

DE VIRUS

LA PRÉVENTION EN 5 ÉTAPES SIMPLES.

- 1. Procurez-vous un logiciel antivirus** – Et assurez-vous de le mettre à jour fréquemment, des nouveaux virus apparaissent tous les jours.
- 2. Inspectez tous les disques** – (disquettes, Cd-rom...) A l'aide de votre antivirus, scannez ces supports qui viennent d'un autre système que le votre.
- 3. Téléchargez prudemment** Par prudence, enregistrez tous les fichiers téléchargés dans un répertoire spécial sur votre disque dur, puis inspectez les avec votre antivirus.
- 4. Inspectez les documents annexés aux courriers électroniques** avant de les ouvrir. Le soucis : certains logiciels de courrier électronique vont ouvrir automatiquement certains documents en utilisant l'application appropriée. Désactivez cette fonction de votre logiciel de courrier électronique puis inspectez chaque document annexé.
- 5.** Si vous possédez un graveur ou un autre support de masse, **réalisez régulièrement une sauvegarde** afin de ne pas tout perdre.

COMMENT SE DÉBARRASSER D'UN VIRUS ?

Si vous soupçonnez votre système d'être vérolé, lancez manuellement votre antivirus. Si cependant celui-ci ne repère pas de virus, réalisez une mise à jour puis relancez votre antivirus.

Enfin, si malgré tout rien n'est trouvé, vous pouvez réaliser lancer un antivirus en ligne. Il en existe plusieurs. A l'adresse suivante, vous trouverez votre bonheur <http://www.secuser.com>.

Enfin si rien ne se passe, vous devriez plutôt voir du côté d'un réparateur ou d'un ami doué en informatique.

Ce document est largement inspiré des pages présentes sur le site
<http://membres.lycos.fr/cgiguere/vdn/vdn31.htmf>