Virus informatiques

Qu'est-ce qu'un virus?

C'est un petit programme qui a la faculté de se répliquer (reproduire) automatiquement. Il va recopier son propre code tel quel , ou en le modifiant, dans des éléments qui sont déjà dans l'ordinateur. Le plus souvent son but est de nuire.

D'où viennent les virus?

Le principe des virus date de 1949. lorsque Johanes Von Neuman, mathématicien hongrois, réussit à mettre au point une machine capable de mémoriser les instructions d'un programme.
A l'époque le but n'est pas de nuire.
Dans les années 60, un jeu le Core War utilise ce principe des virus et le fait connaître.
Dans les années 80, avec l'arrivée de la micro informatique les premiers virus nuisibles débarquent et se propagent via les disquettes.
Aujourd'hui, c'est l'invasion de virus destinés le plus souvent à nuire et personne n'est à l'abri.
Pourquoi?

- Par jeu,
- Par vengeance
- Par mal-être pour être reconnu
- Par cupidité, pour récolter des mots de passe ou des no de cartes de crédit….
- Pour "ennuyer Microsoft"…

Comment agissent les virus

Ils s'installent toujours au sein d'un programme existant sur l'ordinateur. Ils laissent donc dans le fichier infecté une trace particulière à chaque virus qu'on appelle sa signature. (quelques octets)
Les virus informatiques, comme les autres, ont un cycle de vie

La naissance ou création

Un humain, le programmeur, va créer un petit programme capable de se reproduire (éventuellement en se modifiant) pour nuire au plus grand nombre. L'imagination est sans limite et va du simple affichage d'un texte sur l'écran à la destruction de données, à l'arrêt de l'ordinateur.

L'enfance ou gestation ou exécution

Le programmeur va introduire son virus dans le système. Il copie ce programme sur le serveur d'une entreprise, d'une école, d'un grand distributeur de courrier électronique…le but étant de le diffuser le plus largement possible sans se faire remarquer.

La reproduction ou propagation

Le virus par définition va se reproduire. (il a été créé pour ça) donc il va se multiplier. C'est à dire le programme va se recopier indéfiniment, soit à l'identique comme un clone, soit en se modifiant légèrement pour brouiller les pistes. C'est la période pendant laquelle il va infecter le maximum d'ordinateurs, via internet, le courrier électronique, les disquettes, …
Tant qu'il ne fait rien d'autre, il est difficile de le détecter.

L'âge adulte ou activation ou action

C'est le moment où il va entrer en action et exécuter la partie du programme issue de l'imagination du programmeur. C'est la période pendant laquelle il va commettre des dégâts.
Pour qu'un virus s'active, il faut certaines conditions (écrites dans son programme). Par exemple une date, un compteur…

C'est le plus souvent à ce moment, qu'on s'aperçoit que son ordinateur est contaminé. Encore faut-il être capable d'isoler le virus. Quand le nouveau virus est identifié il est transmis aux sociétés qui développent les antivirus, souvent via le NCSA (National Computer Security Association)
http://www.ncsa.com/

Le déclin ou l'éradication

On ne peut pas parler vraiment de mort d'un virus informatique. Tout au plus on peut le neutraliser si les utilisateurs pensent à mettre à jour leurs logiciels antivirus. Ce virus ne disparaît pas mais il cesse de représenter un danger réel.

Différents types de virus

Différents classements possibles, selon leurs agissements, leurs cibles, la manière dont ils se propagent, où ils se localisent.
Un virus peut être multiforme c'est à dire à la fois un ver et un cheval de Troie
Les **spyware**[1] et les **spam**[2] peuvent facilement contenir des virus.

Les vers (worm)

Ils représentaient 83% des virus en 2003 et ont la particularité de pouvoir se reproduire très facilement sans avoir besoin de se greffer sur un programme. Ce sont eux qui infectent le plus souvent les messageries. A l'insu de l'internaute, il se propage en utilisant le carnet d'adresses.

Les chevaux de Troie (troyens)

Ils permettent à un utilisateur extérieur de profiter d'une faille pour vulnérabiliser le système de sécurité en le "marquant" c'est –à-dire en laissant un code qui permettra à cet utilisateur extérieur éventuellement de prendre le contrôle de votre ordinateur. Ils s'infiltrent sur le disque dur, souvent via des fichiers utilitaires ou des macros cachées dans des documents word ou excel….et s'activent dès qu'on ouvre le fichier: vols de mots de passe, destructions de données….

Les virus polymorphes

Ils peuvent modifier automatiquement leur code de façon à ne pas être reconnu par les antivirus. On dit qu'ils changent d'apparence, comme les caméléons

Les virus flibustiers

Ils ont la capacité de modifier les signatures des antivirus pour les neutraliser.

---

[1] **Spyware =** petit programme qui s'introduit, via internet, dans un ordinateur à l'insu de l'utilisateur dans le but de collecter des informations.

[2] **SPAM** = Acronyme de "Spiced Pork And Meat". En français: pourriel
Courrier non sollicité, posté en masse qui envahit les boîtes aux lettres.

Comment se protéger?

Mettre à jour régulièrement les correcteurs de sécurité des logiciels.

Les logiciels vendus comportent souvent des failles de sécurité. Pour pallier à ces failles, il est nécessaire de télécharger les patchs de sécurité régulièrement mis à jour par les fabricants.

- Fermer toutes les applications et **aller dans Windows Update**
  - En cas de gros problème, vous trouverez un message vous disant quoi faire.
  - Ex. pour Sasser, installer la mise à jour KB835732 pour xp.
- Cliquer sur "Rechercher des mises à jours".
  - Si KB835732, n'apparaît pas dans la liste, tant mieux. Cela signifie que cette mise à jour est déjà installée dans votre ordinateur. (configuration automatique)
  - Sinon, téléchargez-la.
- Regarder si d'autres mises à jour vous sont nécessaires.
- Installer les patchs concernant Outlook express et MS Explorer.

Attention certaines mises à jour doivent se faire seules. Elles sont indiquées ainsi:

- doit être installé séparément des autres mises à jour.

Certaines mises à jour nécessitent un redémarrage de l'ordinateur.

Installer un antivirus et le tenir à jour.

Absolument indispensable, l'antivirus permet de neutraliser la plupart des virus connus. Mais il n'agit pas sur les nouveaux virus. Comme de nouveaux virus apparaissent chaque jour, il faut naturellement **mettre son antivirus à jour** très régulièrement.
Cela signifie télécharger la signature des nouveaux virus. En général on configure son antivirus pour que cette mise à jour s'effectue automatiquement.
Un conseil: vérifier (scanner) régulièrement la totalité de votre disque dur et des systèmes, d'amorçage, la mémoire et tous les logiciels susceptibles d'être infectés.

Installer un pare-feu ou firewall ou garde-barrière.

Le pare-feu contrôle l'accès à votre ordinateur et affiche un message d'alerte dès qu'un intrus essaie d'y pénétrer .

Installer un logiciel anti-espion

Il vous protégera des logiciels espions, (les spywares). Ce sont des logiciels qu'un "cyberpirate" installe sur votre ordinateur sans vous en informer. Son but: récolter des informations intéressantes (mots de passe, no de carte de crédit…) Attention, ces spywares sont rarement détectés par de simples antivirus.

Contrôler son courrier avant de l'ouvrir

Ne pas communiquer son adresse E-mail partout. Donner de préférence une adresse webmail dans les forums ou lors des téléchargements.
Pièces jointes = danger potentiel.
Supprimer sans les ouvrir toutes les pièces jointes douteuses, surtout si vous ne connaissez pas l'expéditeur.
Attention, même vos meilleurs amis peuvent vous infecter à leur insu, donc vérifier s'ils ont une bonne raison de vous envoyer cette pièce jointe. S'il y a le moindre doute, demandez-leur de confirmer.
Vider la poubelle.

Sauvegarder ses données sur des supports extérieurs.

Simplement parce que si votre disque dur est endommagé, vos fichiers ne seront pas perdus.

Nettoyer son disque dur après le surf

Supprimer les traces de votre passage, surtout si vous êtes allé dans un site sensible ou si vous avez communiqué des données confidentielles.

Actuellement, on trouve des logiciels qui agissent à la fois comme pare-feu, antivirus, anti-spam et anti espion. Ils ne protègent pas totalement mais diminuent considérablement les risques. Certains sont gratuits d'autres payants.

Conclusion

S'il convient d'éviter la paranoïa, il faut également éviter de croire que les virus ne touchent que les autres !

Un ordinateur non protégé = un appartement avec une porte grande ouverte.

Rester vigilant, s'informer, se protéger

- avec un antivirus régulièrement mis à jour, un pare-feu et un anti-espion
- mettre à jour les patchs des systèmes d'exploitation,
- trier son courrier avant de l'ouvrir,
- sauvegarder ses données sur un support externe.

Mais rappelons-nous toujours que le risque 0 n'existe pas.

Sources

http://www.secuser.com/
http://www.secuser.com/faq/virus/
http://www.chez.com/faqvirus/def_virus.html
http://www.geocities.com/siliconvalley/hills/4227/virus1.html
http://www.reseaunance.com/dossiers/virus/quoivirus.shtml
http://www.cyberacadie.com/virus.htm
http://www.lesmordus.com/dossierv.htm