

INFORMATIQUE	LES VIRUS INFORMATIQUES	N.Menu 2000 / DGEO2
CHAPITRE 4		P. 1

Chapitre 4

4.1 Les Virus

4.1.1 Qu'est ce qu'un virus ?

Un virus informatique est un tout petit programme (un bloc de code exécutable) qui s'attache à, écrit par-dessus, ou remplace un autre programme afin de se reproduire sans que l'utilisateur du système en soit conscient.

Certains virus ne causent pas de gros dégâts et peuvent être présents pendant des années sans que l'utilisateur s'en rende compte, d'autres peuvent altérer occasionnellement des fichiers de données (parfois insidieusement, sur de longues périodes) ou essayer de détruire des fichiers ou des disques.

Cependant, même un « gentil » virus n'est pas totalement innocent par le fait de la place grandissante qu'il occupe sur le disque, du temps CPU gaspillé et par le temps et les coûts générés afin de le détecter et de l'anéantir.

4.1.2 Les types de virus

- Un « file virus » s'attache à un fichier, habituellement à une application. En général, les « file virus » n'infectent pas les fichiers de données.
- Les « Boot sector » virus altèrent le programme qui se trouve dans le secteur de boot de toutes disquettes Dos (DOS formatted disk). Généralement un virus de ce type effectue son propre code de manière à contaminer le secteur de boot du disque dur. Par la suite, toutes les disquettes (non protégées physiquement) utilisées sur ce PC seront contaminées.
- Les virus « multi-partite » reprennent un peu des caractéristiques des 2 précédents
- Les « Macro-virus » constituent une catégorie à part. En effet, ces virus ne sont pas spécifiques à un système d'exploitation et infectent indifféremment des ordinateurs tournant sous DOS, Windows (3.x, 95 et NT) ou Macintosh. De plus, ces virus n'infectent pas des programmes mais des documents. Ils utilisent certaines fonctions du langage macro de MS Word pour infecter le modèle de base NORMAL.DOT. Dès qu'un document infecté est ouvert, le virus infectera ce modèle qui est la base de la majorité des autres documents et modèles de MS Word.
- ... une tapée d'autres encore

INFORMATIQUE	LES VIRUS INFORMATIQUES	N.Menu 2000 / DGEO2
CHAPITRE 4		P. 2

4.1.3 Les virus par E-mail, quels dangers ?

Si l'affirmation « ne vous inquiétez pas, un simple E-mail ne peut pas contaminer votre système par le simple fait d'être reçu » pouvait être vraie il y a quelques mois seulement, la situation vient de changer...

Il y a quelques temps, un courrier électronique traditionnel ne contenait que du texte brut. Or le texte brut est simplement affiché, il n'est pas trituré, ni interprété comme une commande dans un programme. Le texte brut est par nature inoffensif. Le virus n'avait pour seule solution que de se planquer dans les fichiers attachés, les programmes ou les documents Word par exemple.

Aujourd'hui cependant, sous l'initiative de Netscape et de Microsoft, le courrier électronique multimédia a tendance à se développer.

Dans le cas de ce nouveau type de courrier, ce n'est plus du texte brut qui circule dans l'e-mail, mais du code HTML, accompagné d'images (jusque là tout va bien) mais aussi parfois de petits programmes conçus pour le Web. Prenons le cas des contrôles ActiveX. Ces programmes sont conçus dans un langage (ActiveX) développé pour le Web par Microsoft. Or ce langage ouvre des brèches de sécurité dans Windows. En clair, en programmant bien, on peut concevoir des virus en ActiveX. Et les diffuser ensuite par courrier électronique, ni vu ni connu. Il importe donc d'être vigilant si votre logiciel de messagerie interprète les contrôles ActiveX. En clair : attention si vous utilisez (entre autres) les logiciels Internet Mail et Outlook Express.

4.1.4 Les messages d'alerte aux virus par E-mails

Bien des fois, vous recevrez des E-mails du style :

ATTENTION !!! ALERTE AU VIRUS !!! Si vous recevez un e-mail intitulé (Voir la liste de ces virus) **NE L'OUVREZ PAS**. Le virus qu'il contient va effacer l'intégralité de votre disque dur. Faites suivre ce message à vos amis. Ceci est un nouveau virus, très nocif et peu de gens connaissent son existence..

Viennent ensuite les références de la personne bien informée qui a identifié ce virus (une personne du département recherche d'IBM, ou du département Vente de Microsoft, etc) afin de donner une plus grande crédibilité à cette alerte.

Ces mails sont généralement des canulars créés par goût de la plaisanterie, mais ils ont une conséquence néfaste sur l'internet. En effet, il vous est conseillé de faire suivre ce courrier à toutes vos connaissances afin de les prévenir du danger qu'ils encourent.

Supposons que ce mail fasse 1 Ko (ce qui est normal pour un petit mail) et que votre carnet d'adresse contienne 100 adresses. En faisant suivre ce mail, vous transférez alors 100 Ko sur le réseau (100 X 1 Ko). Imaginez maintenant que chacun des récipiendaires aient également 100 correspondants dans leurs carnets d'adresses. Ce mail de 1 Ko que vous avez innocemment fait suivre s'est multiplié en 10 000 mails pour un total de 10 Mo. Et il ne s'agit là que du deuxième niveau de cette réaction pyramidale! Au troisième niveau, on atteint le Giga-octet...

INFORMATIQUE	LES VIRUS INFORMATIQUES	N.Menu 2000 / DGEO2
CHAPITRE 4		P. 3

4.1.5 Que faire pour se protéger contre les virus ?

Il n' y a aucun moyen efficace à 100 % néanmoins :

Utilisez un logiciel antivirus régulièrement. Celui-ci doit être bien paramétré...

Achetez vos logiciels chez des revendeurs officiels.

Pour ne pas recevoir de virus par les fichiers attachés...

Passez à l'antivirus tous les fichiers que vous recevez en pièces attachées. Si vous ne possédez pas d'antivirus ou que l'origine vous paraît vraiment douteuse, ne les ouvrez surtout pas. Et jetez-les direct à la poubelle.

Pour ne pas se faire infecter par des virus ActiveX...

Si vous utilisez Internet Mail, Outlook ou Outlook Express, changez de logiciel de messagerie ou réglez bien les paramètres d'Internet Explorer. Choisissez ainsi « niveau de sécurité élevé ».

...Normalement, vous êtes protégé...