

PROTEGEZ VOUS DES VIRUS.

Fléau majeur de l'informatique, les virus sont aussi présents sur internet. Qu'ils s'attaquent au secteur d'amorce de vos disques, aux fichiers exécutables ou aux documents incluant des macros, leur but est toujours le même : proliférer en cachette, puis souvent détruire vos données.

Qu'est-ce qu'un virus?

Un virus est un petit programme conçu pour se cacher dans votre ordinateur, puis se multiplier, se répandre de par le monde et enfin déclencher une action (message, destruction, petite musique, etc.). On dénombre plusieurs catégories de virus, en fonction de la cible visée dans l'ordinateur.

Les différentes familles de virus.

La première catégorie regroupe les virus de secteur d'amorce, "boot sector", c'est-à-dire affectant la zone du disque qui est lue en premier au démarrage). Ces virus remplacent le secteur d'amorce du disque infecté par une copie d'eux-mêmes, puis déplacent le secteur original vers une autre portion du disque. Le virus est ainsi chargé en mémoire bien avant que l'utilisateur ou un logiciel ne prenne le contrôle de l'ordinateur.

Les virus d'applications infectent les fichiers exécutables, c'est-à-dire les programmes (.exe, .com ou .sys). Pour simplifier, disons que le virus remplace l'amorce du fichier, de manière à ce qu'il soit exécuté avant le programme infecté, puis il lui rend la main, camouflant ainsi son exécution aux yeux de l'utilisateur.

Les virus macro sont des virus qui infectent uniquement des documents (Word, Excel...), en utilisant le langage Visual Basic pour Application. Ces virus peuvent malheureusement causer de grands dégâts (formatage du disque dur par exemple).

Enfin, il y a les virus de mail, également appelés **vers**. Ces virus se servent des programmes de messagerie (notamment Microsoft Outlook) pour se répandre à grande vitesse, en s'envoyant automatiquement à tout ou partie des personnes présentes dans le carnet d'adresses. Leur premier effet est de saturer les serveurs de messagerie, mais ils peuvent également avoir des actions destructrices pour les ordinateurs contaminés. Ils sont particulièrement redoutables, car le fait de recevoir un mail d'une personne connue diminue la méfiance du destinataire, qui ouvre alors plus facilement le fichier joint contaminé.

La seconde catégorie concerne les troyens. Contrairement à son cousin le virus, qui profite de toute occasion pour se multiplier, le troyen véritable ne se reproduit pas. Ces derniers permettent à votre agresseur de contrôler à distance votre machine, et lui donne tout pouvoir sur les fichiers de votre disque dur (lecture, suppression, vol, etc.). Le meilleur antidote reste la prévention : n'acceptez jamais de télécharger un fichier douteux, même s'il vous est présenté comme indispensable dans vos hobbies!

Par ailleurs, plusieurs vulnérabilités dans les logiciels Internet Explorer / Outlook font que certains virus peuvent infecter votre ordinateur à la simple ouverture du

message ou lors de sa lecture dans la fenêtre de visualisation voire en consultant une page web si Internet Explorer n'a pas été patché contre cette vulnérabilité.

Fonctionnement d'un virus

Pour bien comprendre le mode de fonctionnement d'un virus, on peut faire l'analogie avec le virus biologique. Comme lui, le virus informatique essaie de contaminer tout ce qu'il peut, de se dissimuler aux yeux de l'organisme infecté, et de se répandre le plus largement possible. Les virus infectent un maximum de fichiers puisqu'ils demeurent en mémoire dès le démarrage de l'ordinateur.

Règles générales de protection

- ne téléchargez pas des programmes d'origine douteuse, qui peuvent vous être proposés sur des sites persos ou des chats eux-mêmes plus ou moins douteux;
- méfiez-vous des fichiers joints aux messages que vous recevez : analysez avec un antivirus à jour tout fichier avant de l'ouvrir, et préférez détruire un mail douteux plutôt que d'infecter votre machine, même si l'expéditeur est connu.
- fuyez les disquettes d'origine douteuse (ou ayant transité dans des lieux publics vulnérables comme les salles de cours ou TP des écoles ou universités), et protégez les vôtres en écriture.
- procédez régulièrement à des sauvegardes du contenu important de votre disque dur après avoir vérifié l'absence de virus : cela peut paraître fastidieux, mais en cas d'infection (ou même simplement en cas de crash de disque dur), ça vous sauvera la mise.

En complément de ces règles de prévention, la meilleure protection et le principal remède en cas de contamination consiste à installer un antivirus. Une solution qui reste toute relative, car aucun produit ne détecte 100% des virus, 100% du temps : d'où l'importance de la prévention. Par ailleurs, de nouveaux virus apparaissant chaque jour, il faut veiller à régulièrement actualiser la base de données virales du logiciel.

Comment savoir si mon ordinateur est contaminé ?

Affichage de messages intempestifs, plantage de l'ordinateur, formatage du disque dur, mémoire système disponible inférieure à ce qu'elle devrait être, changement du nom de volume d'un disque, programmes ou fichiers subitement absents, apparition de programmes ou de fichiers inconnus, ou encore comportement anormal de certains programmes ou fichiers sont des signes possibles d'infection.