

Virus/Anti-Virus - 1/2

Virus/Anti-virus : la guerre est interminable. Les virus : leurs dangers où se placent-ils, sont ils capables de tout détruire ? Les anti-virus : sont-ils fiables à 100% ?

Les virus

Un virus est un petit programme, situé dans le corps d'un autre, qui, lorsqu'on l'exécute, se met dans la mémoire et exécute les instructions que son auteur lui a donné.

La définition d'un virus est : "tout programme d'ordinateur capable d'infecter un autre programme d'ordinateur en le modifiant de façon à ce qu'il puisse à son tour se reproduire". Ils se multiplient pour la plupart, c'est-à-dire qu'il s'insèrent dans les fichiers que vous exécutez après qu'il soit résident en mémoire.

Les virus ont des formes très différentes, et des conséquences aussi diverses, cela va de la balle de ping-pong qui traverse l'écran au virus destructeur de données. Quelques rares virus sont également capables de détériorer le matériel, par exemple de flasher le BIOS (chose possible sur certains BIOS, c'est notamment le cas du virus Win95 CIH alias Chernobyl), détériorer le disque-dur (en faisant repasser physiquement la tête du disque des millions de fois sur le même secteur), abîmer l'écran (possible en appliquant matériellement des changements de fréquence pouvant causer la mort du moniteur...).

Les virus utilisent différentes voies pour infecter les systèmes, une simple disquette, une méthode qui a été longtemps la presque la seule employée, un réseau local et l'échange de fichiers par son intermédiaire, Internet avec le téléchargement de fichiers et les emails, particulièrement les fichiers qui y sont joints.

Les anti-virus

Les antivirus possèdent deux fonctions principales, ce sont des programmes résidents dans la mémoire vive de l'ordinateur ce qui leur permet d'analyser les fichiers utilisés et prévenir lorsqu'un fichier suspect est détecté, l'autre fonction des antivirus est de scanner le disque dur par exemple chaque semaine et de vérifier plus attentivement si l'ordinateur n'est pas infecté par un virus.

Ainsi, chaque fichier est vérifié avant toute utilisation (lecture, écriture). Cette vérification consiste en une comparaison du fichier avec une banque de données reprenant les signatures des virus connus. Les signatures des virus sont des suites de caractères, propre à chaque virus informatique. C'est leur caractère, c'est ce qui les définit. Si la recherche est fructueuse, si un virus est trouvé, alors l'antivirus stoppe l'action en cours (lecture ou écriture) et demande que l'utilisateur intervienne. Les attaques des virus peuvent être parer également en utilisant leur signature, à travers leurs signes distinctifs pour les reconnaître mais aussi par analogie de certains programmes avec des routines (c'est à dire des suites d'instructions) connues, ceci empêche ainsi de voir de nombreux virus se propagés alors qui possèdent les mêmes fonctions. Ainsi les antivirus contrôlent les faits et gestes des programmes sur les ordinateurs et permettent de détecter les problèmes qui peuvent survenir. Alors, l'antivirus va tenter de stopper les effets du virus et surtout de restaurer les programmes endommagés. Cependant ce genre de système ralentit la machine. De plus, il faut une mise à jour fréquente de la base de donnée de signatures pour conserver une efficacité maximale, une fréquence de 15 jours semble être un bon compromis.

Concernant l'adoption d'un antivirus, celle-ci ne doit pas se faire au hasard, il faut privilégier les logiciels émanant des compagnies reconnus, ce qui est généralement aisé sauf lorsqu'un produit performant n'est pas connu en France.

Aussi, l'antivirus InoculateIT Personal Edition est un bon choix, surtout au vue de sa gratuité pour un usage

Virus/Anti-Virus - 2/2

dans un but non lucratif, en effet des mises à jour très régulière sont disponibles (chaque semaine) et point important il permet d'éradiquer les troyens qui représentent maintenant une menace très importante. Son interface est simple et intuitive bien qu'en anglais, une fois l'installation effectuée (sans problème), il se compose de trois fenêtres, celles de haut servant à sélectionner soit un dossier soit des fichiers, puis il suffit cliquer sur "GO" pour commencer l'analyse et les résultats s'affichent dans la fenêtre du bas. Les options par défaut sont bien adaptés à une utilisation normale. Seul défaut, apparemment il n'existe pas de fonction de programmation.

Les logiciels du type de Norton et McAfee sont également d'un bon niveau de détection de virus mais pêche largement en ce qui concerne les troyens. A préciser, que Panda Antivirus ne présente pas cette lacune et offre, pour un utilisateur enregistré, des mises à jour très fréquentes mais surtout prévient l'utilisateur dans le cas d'un risque important qui peut être supprimé par une mise à jour. Cependant ces logiciels présentent le désavantage d'être lourd et de nécessiter une configuration récente pour être efficace à leur maximum.