Virus, la petite galerie des horreurs

Cheval de Troie, virus de démarrage... les vrais virus informatiques, tout comme leurs cousins biologiques, se répartissent en familles. Rappelons qu'un virus est une séquence de code possédant deux caractéristiques principales : elle s'introduit dans un programme récepteur et elle est capable de se dupliquer et d'infecter d'autres utilisateurs. En voici les principales familles.

- **Cheval de Troie** : souvent assimilé à un virus à cause de ses conséquences, il n'en est pas un, puisqu'il ne se duplique pas. Il se loge en général dans un fichier système (souvent dans les instructions de copie de fichiers) et s'exécute après lui, provoquant de nombreux dommages.

- **Virus parasite** : il adopte le même principe que le cheval de Troie, mais en profite aussi pour se dupliquer. Il en existe deux sortes : les résidents qui infectent un programme lui-même résidant, et les non-résidents qui se lient à n'importe quel programme de la machine. Dans tous les cas, le virus s'exécute juste après (ou juste avant, cela dépend de la manière dont il a infecté le code du receveur) le programme du fichier infecté.

- **Virus de démarrage** : il se loge dans les premiers secteurs du disque dur. Ainsi, il est exécuté et se place en mémoire avant les fichiers système eux-mêmes. Il se signale uniquement en empêchant le chargement d'un programme résident, l'espace mémoire venant à manquer. Form est l'un de ces redoutables virus.

- **Virus segmenté** : il s'agit d'un virus en plusieurs morceaux, à la fois virus de démarrage et virus parasite, par exemple. Très virulent, il est en outre difficile à combattre par les antivirus qui n'ont pas sa référence précise dans leurs tables. En effet, ces derniers trouvent et détruisent souvent la partie démarrage mais ne repèrent pas la partie parasite, ce qui rend la décontamination inefficace.

- **Virus furtif** : tels les nouveaux bombardiers américains, ils arrivent à échapper à bon nombre d'antivirus. Comment ? En intervenant directement au niveau des interruptions utilisées par les antivirus, notamment pour calculer la signature d'un fichier (un nombre caractéristique des octets qui composent ce fichier), ils empêchent la détection de leurs propres octets. Frodo est l'un des plus illustres. Terrible.

- **Virus polymorphe** : tout comme le virus de la grippe qui change d'année en année, certains virus informatiques connaissent une mutation, rendant ainsi certains antivirus inopérants. En fait, ils s'écrivent sous une forme codée à chaque duplication, induisant simultanément les variantes nécessaires au décodage pour l'exécution. Un groupe d'individus, nommé Dark Avenger, a même rendu public sur plusieurs serveurs un moteur de mutation qui permet de transformer un vulgaire virus parasite en un redoutable polymorphe !

- **Virus anti-antivirus** : quelques virus ont été conçus spécialement pour éliminer un antivirus précis. Encore très rare (heureusement !), ce genre de code pourrait devenir extrêmement dangereux s'il s'agit en outre, d'un produit segmenté : l'anti-antivirus préparerait alors le terrain pou le virus véritablement actif !

- **Virus réseau** : comme son nom l'indique, il s'agit d'un virus conçu pour se développer sur un réseau et pour exploiter toutes les facilités. Ils sont généralement destinés à Netware mais, avec la récente percée de Windows NT Server, nul doute que Microsoft ne doivent à son tour affronter ce genre de parasite.

- **Virus macro** : il ne prend pas place dans un code exécutable, mais dans un document prévu pour un logiciel disposant de macros. Actuellement, Word et dans une moindre mesure, Excel, sont seuls touchés par ce type de virus. Le principe consiste à insérer une macro (généralement d'initialisation) dans un fichier de données, ce qui permet ensuite de prendre le contrôle de la machine et de faire ce que l'on veut. Wazzu est le plus connu en France.