Les trois grandes familles de VIRUS - 1/1

Ces Virus qui pourrissent notre PC. Cette article présente les trois grandes familles de virus : Bombe logique, Vers et Trojans. Mieux les connaître permet de s'y intéresser d'avantage pour mieux y faire face...

Le virus est un programme informatique capable de se propager sur d'autres machines via un support physique (Disque dur, Disquette) ou via un support logique (un réseau, Internet). Un virus n'endommage pas forcement un ordinateur comme on le croit souvent. Un virus peut ne rien faire que de se propager. Mais ils en sont pas moins nuisibles : il peuvent surcharger un réseau et ralentir les applications réseaux (messageries, applications clients-serveur...) en prenant une partie de la bande passante pouvant ainsi créer des bouchons sur un réseau. Mais en générale, les virus altèrent plus ou moins le bon fonctionnement de la machine.

Les trois grands types de virus :

Les Cheveaux de troie

Les chevaux de troie (ou Trojans, ou encore nommés Troyens) ont pour but d'utiliser la machine à distance à de fin malhonnêtes : Prise de contrôle de la souris et du clavier, copie de fichiers, repérer les frappes au clavier lors d'une connexion https (afin par exemple de connaître votre numéro de compte bancaire lors d'achat en ligne) etc... Les Trojans sont en générales cachés à l'intérieur d'un autre programme "inoffensif" que vous téléchargez et installez sur votre machine.

Les bombes logiques

Les bombes logiques sont également cachées à l'intérieur d'un autre programme. Ceux-ci s'activent lors d'un événement précis (ex : combinaison de touches). Une fois cette événement réalisé, ils font ceux pourquoi ils sont programmés (ex : détérioration de fichiers systèmes...). Exemple de bombe logique : le virus "Tchernobyl"

Les vers

Le Vers fait aujourd'hui partie de la famille des virus. Mais contrairement aux "virus classiques", ils n'ont pas besoin de supports physiques ou de programmes pour se propager. Ils ne se propagent uniquement sur une autre machine que celle déjà infectée si bien qu'il ne peut y avoir qu'une copie du ver par machine. La principale nuisance d'un ver est de saturer la bande passante à cause de sa rapidité de propagation sur un réseau.

Les Mass-mailer

Les mass-mailer sont des vers qui récupèrent les adresses du carnet d'adresses ou des fichiers temporaires pour s'auto-distribuer via la messagerie électronique (exemple de mass-mailer : "I love you")