Les virus

Le virus est à la mode ! Particuliers, industriels, partis politiques, commerces,… tout le monde est touché par ce fléau, telle la ville de Baltimore qui en a récemment fait les frais *(encadré)*. Pour être – un peu moins ignorant – il est important de connaître les principaux mode de virus existants pour savoir s'en préserver et… s'en débarasser au cas où.

La bombe logique est un programme installé dans le système en attendant un événement (date, action, données particulières…) pour s'exécuter. Elle est généralement utilisée dans le but de paralyser temporairement des serveurs afin de nuire à leur fonctionnement.

Le spyware est un mouchard qui peut enregistrer différents types de données : sites visités, requêtes tapées dans les moteurs de recherche, données personnelles, type de produits achetés, informations bancaires. Ces informations sont exploitées à des fins de profilage pour l'envoi de publicités ciblées sur les centres d'intérêt de la personne qui a été espionnée.

Le keylogger espionne les frappes de clavier de l'ordinateur qui l'héberge afin de les transmettre à un pirate. Ce système permet ainsi de recueillir les mots de passe, codes de carte bancaire, intitulés sous lequel vous ouvrez une session…

Le backdoor est un cheval de Troie caché dans un logiciel, un service en ligne ou un système informatique afin de surveiller, copier ou détruire des données, de prendre le contrôle d'un ordinateur et de pouvoir l'utiliser pour mener des actions malfaisantes…

Le trojan (cheval de Troie) est un programme informatique utilisé pour voler des informations personnelles, propager des virus ou perturber les performances de

votre ordinateur. Il permet également un accès à distance.

Le ver informatique est un virus réseau qui s'auto-reproduit et se déplace sans avoir besoin de support physique. Il recherche les fichiers contenant des adresses de messagerie et les utilise pour envoyer des messages électroniques infectés en usurpant les adresses des expéditeurs dans les derniers messages afin que les messages infectés semblent provenir de quelqu'un que vous connaissez.

Le ransomware empêche l'utilisateur d'accéder à son système ou ses fichiers et exige le paiement d'une rançon en échange du rétablissement de l'accès. Il utilise couramment les e-mails indésirables (malspams) pour livrer des malwares. Ces e-mails peuvent inclure des pièces jointes piégées ou des liens vers des sites Web malveillants.

Le phishing est un envoi d'e-mail qui prend l'apparence de banques, de services de paiements… Vous êtes invités à remplir un formulaire en ligne ou à cliquer sur un lien qui mène vers un faux portail de connexion. L'objectif de ce procédé est l'accès, entre autres, à vos mots de passe et noms d'utilisateur.

Vérifiez si votre adresse mail est hackée sur :
have i been pwned?