FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

Les Virus

- La définition
- L'historique
- La propagation
- Les types
- La détection
- Comment se protéger

Les virus

- Définition

  Un virus informatique est un programme malveillant qui se réplique automatiquement en se copiant dans un autre programme. Il se propage par lui-même dans d'autre code ou document exécutable dans le but d'infecter les systèmes vulnérables, prendre le contrôle de l'administrateur et de voler les données des utilisateurs. (Ils sont conçues pour piéger)

- Autre référence - des vers, Cheveaux de Troie, ramsonware, spyware, adware, scarewares, rootkits, hameçonnage, logiciels malveillants, bootkits, backdoors, enregistreur de frappes, déni de service, etc.

Les virus

- Historique
  - 1971 Robert Thomas ingénieur chez BBN Technologies à développé le premier virus baptisé “Creeper” sur les réseau “ARPANET”, type télétype.
  - ARPANET (Advanced Research Project Agency Network) ceci faisait parti de DND - le Département Nationale de la Défense des États Unis.
  - Plus récent, le premier virus informatique d’origine sauvage découvert c’est “Elk Cloner” sur le système d’exploitation Apple par un adolescent appelé Richard Skrenta en 1982, la propagation c’est fait via disquette.

Les virus

- Propagation
  - Les e-mails
  - Ouvrir pieces jointe dans un e-mail
  - Visiter un site Web infecté
  - Cliquer sur un fichier exécutable
  - Afficher une annonce infecté peut provoquer la propagation du virus
  - Connection à des périphérique de stockage amovibles (clés USB et autre)

Les virus

- Méthode de propagation (2)
  - Le virus se reproduit immédiatement une fois qu'il atterri sur un ordinateur
  - Le virus dormant, jusqu'à ce qu'il déclenche le code malveillant. (programme infecté doit être exécuté)

→ Mais plus alarmant c'est;

  - Apparition de virus plus sophistiqué - doté de fonctionnalités d'évasion contournant les logiciels anti-virus
  - Enregistrement des frappes de clavier
  - Changement de code durant sa propagation

Les virus

- Types de virus informatiques
  - Virus du secteur de démarrage - infecte l'enregistrement du démarrage principal. Complexe et souvent nécessite le formatage du sytème d'exploitation.
  - Virus d'action directe - reste masqué dans la mémoire de l'ordinateur, s'attache au type spécifique de fichier qu'il infecte, aucune effet sur l'utilisateur ou performance. Souvent appelé un virus non-résident.

Les virus

- Types de virus informatiques (suite)
  - Virus résident - installé sur l'ordinateur et difficile d'identifier et d'éliminer.
  - Virus multipartite - se portage de plusieurs manières et infecte le secteur de démarrage et les fichiers exécutables en mème temps.
  - Virus polymorphe - difficile à identifier avec un programme anti-virus et modifie sa signature chaque fois qu'il se réplique.
  - Écraser le virus - suprême tous les fichiers qu'il infecte. Façon de les supprimer est de supprimer les fichiers infectés. (e-mail)

Les virus

- Types de virus informatiques (suite)
  - Virus spacefiller - remplissent les espaces vides entre le code, n'endommage pas le fichier.
  - Virus #Infecteurs de fichiers - peu d'association avec les fichiers de programme tel que .exe et .com. Certain infectent tout programme sur lequel l'exécution est demandé, types de fichiers .sys, .ovl, .prg, et .mnu. Quand le programme est chargé, le virus est également chargé. (piece jointe à un e-mail)

Les virus

- Types de virus informatiques (suite)
  - Virus #Macro - vise en particulier les commandes du language macro dans les applications telles que Microsoft Word. Les macros sont des séquences de touches incorporées dans les documents ou des séquences enregistrés pour des commendes. Ils ajoutent leurs code malveillants.
  - Virus de #Overwrite - conception pour détruire les données d'un fichier ou d'une application. Écrasent les fichiers avec son propre code, propagation via son propre code pour attaquer autre fichiers, applications, et sytème supplémentaire.

Les virus

- Types de virus informatiques (suite)
  - Virus #Polymorphes - plus en plus utilisé par les cybercriminels, capable de modifier ou muter son code lui mème. Évite bien la détection et change sa signature une fois détecté.
  - Virus #Résident - s'implante dans la mémoire de l'ordinateur et mème quand il est supprimer , la version stocké peut être activée quand on charge certaines applications et programmes. Ils peuvent être ignorées par certain logiciel ant-virus.

Les virus

- Types de virus informatiques (suite)
  - Virus de Rootkit -s'installe en secrets sur un système infecté, il ouvre la porte aux attaquants et leur donne contrôle total du système. Capable désactive fondamentalement des fonctions et des programmes. Créer pour contourner les anti-virus et anti-malware incluant l'analyse du rotait.
  - Virus #Infecteurs de système ou d'enregistrement de démarrage - modifie le code exécutable trouvé dans les zones spécifiques d'un disque (boot-up sequence). Il est moins courant de nos jour.

Les virus

- Détection
  - Ralentissement des performances
  - Pop-Ups bombardant l'écran
  - Programme s'exécutant seuls
  - Multiplication/duplication des fichiers par eux-même
  - Nouveaux fichiers ou programmes sur l'ordinateur
  - Fichiers/dossiers/programmes supprimés ou corrompus
  - Son d'un disques dur (thrashing)

Les virus

- Comment se protéger
  - Voir la présentation de jeudi le 10/03/19 - accéder le lien suivant

    https://formatio.info/automne-2019-1.html

  - La facture - reportage sur les fraudeurs en Inde

    https://ici.tou.tv/la-facture

  - Sources et informations - pour plus d'information voir les sites suivant

    https://en.wikipedia.org/wiki/Malware

    https://antivirus.comodo.com/blog/computer-safety/what-is-virus-and-its-definition/

    https://www.voipshield.com/20-common-types-of-viruses-affecting-your-computer/

    https://www.makeuseof.com/tag/types-computer-viruses-watch/

    https://www.geeksforgeeks.org/types-of-virus/

Courriel indésirable

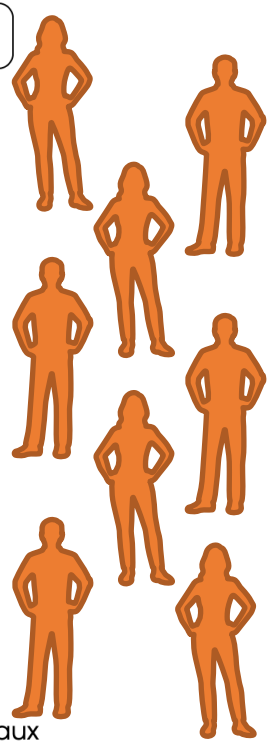
- Comment se protéger
- Il y a plusieurs moyens
  - L'installation de logiciel anti-pourriel/antivirus
  - Coupe feu procure une protection additionnelle
  - Utilisation d'un VPN
  - Garder vos applications à jour
  - Si vous ne reconnaissez pas ne pas ouvrir
  - Éviter les accès non sécurisés
  - Éviter de prêter votre ordinateur
  - Pas sur - téléphoné pour confirmer l'envoie
  - Se servir d'un bon jugement, doute - oublier

Les virus

O - FORMATIO

FORMATIO | RESSOURCE INFORMATIQUE BUREAUTIQUE

Accueil | Nos services | Calendrier | Qui sommes-nous ? | Le club informatique | Nous joindre



VOUS NE MAÎTRISEZ PAS LES NOUVELLES TECHNOLOGIES ?

Vous souhaitez augmenter vos chances de réussite, postuler ou obtenir un meilleur emploi, utiliser de nouveaux logiciels, naviguer sur les réseaux sociaux ou simplement clavarder avec vos amis branchés ?

Oui, c'est possible avec nous

Nous offrons des formations diversifiées accessibles à tous en tenant compte des parcours de chacun.

Nos formations étoiles