Les différents types de virus et malware qui peuvent nuire à l'utilisation d'un ordinateur ou d'un réseau

Compétences Numériques

Bastien Verge, Jeremy Couturet, Noe Matuszenski, Oscar Plaisant, Yanis Dezzaz

- Les Trojan
  - Les origines
- Les Trojan
  - Aujourd'hui
- Les Trojan
  - Origines fréquentes des Trojan
- Les Trojan
  - Symptômes possibles d'une infection
- Les Spywares
  - Définition
- Les Spywares
- Conclusion
  - Stratégies pour éviter les virus
- Conclusion
- Remerciements

- Introduction
- Définitions
  - Virus

- Les types de virus
- Les Vers informatiques
  - Définition
  - Fonctionnement et actions
  - Exemples
    - ILOVEYOU (2000)
    - WannaCry (2018)
- Les Ransomware
  - Définitions
  - Types de Ransomware
    - Les Scareware
    - Les Ransomware de chiffrement
- Les Trojan
  - Les origines
  - Aujourd'hui
  - Origines fréquentes des Trojan
  - Symptômes possibles d'une infection
- Les Spywares
  - Définition

. . .

Dans cette présentation, nous aborderont les différents types de Virus informatique qui peuvent infecter un ordinateur ou un réseau ainsi que leur effets et conséquences.

. . .

L'ensemble de notre travail (détails supplémentaires, sources et bibliographie. . .) ainsi que les autres document à produire (CV et lettres de motivation) sont en ligne, sur le repository gitHub : OsKaR31415/CN-travail-en-groupe

---

. . .

Messagerie instantanée : Discord

. . .

Calendrier partagé : Events Discord

. . .

Repository : gitHub

. . .

Versionning et fonctionnalités de Remote programming : git

. . .

Document principalement écrits au format *markdown* (format simple, léger, portable, convertible façilement, et bien intégré avec gitHub)

. . .

Un virus est un logiciel qui :

. . .

- S'autoréplique pour se propager

. . .

- Utilise un autre logiciel comme "hôte"
- Utilisé à des fins malveillantes

. . .

- les Trojan
- les Vers informatiques
- les Ransomware
- les Spyware

. . .

. . .

Un malware est tout simplement un logiciel malveillant : il cherche à soutirer de l'argent ou des informations à une victime, par diverses méthodes.

. . .

Un virus informatique est un Malware particulier (qui se cache dans une autre application).

. . .

. . .

Virus qui à pour but d'infecter le plus d'appareils possible.

. . .

Il lui suffit d'infecter un appareil connecté à un réseau pour pouvoir se dupliquer et infecter le réseau entier.

. . .

Ce genre programmes sont très difficiles à remarquer, même pour un anti-virus.

. . .

Peut infecter un ordinateur si celui-ci appartient à un réseau infecté.

. . .

Quand il à infecté un ordinateur, le ver se multiplie en utilisant un "quine" (programme capable d'écrire son propre code), pour créer

ensuite une “backdoor” anfin de pouvoir utiliser l’ordinateur infecté comme faisant partie intégrante du réseau d’ordinateurs “zombie” appelé “botnet”.

. . .

Un ver informatique peut avoir un grand nombre de buts : dérober des données, détruire des données, espionner, prendre le contrôle d’ordinateurs. . .

. . .

Il peut se propager comme n’importe quel virus : par des mails ou autres messageries, par des téléchargements, notamment en utilisant le protocole Peer-to-Peer (P2P), par des clef USB ou des CD-ROM. . .

. . .

. . .

. . .

Concu pour éffacer aléatoirement des fichiers sur l'ordinateur infecté.

. . .

À débuté aux Philippines, mais c'est propagé dans le monde entier.

. . .

Il à ainsi causé des milliards de dollars de dommages dans le monde entier, ce qui à fait de lui l'un des virus les plus connus.

. . .

. . .

Utilise une vulnérabilité de Windows 8.

. . .

À réussi à infecter 230 000 PCs en une journée (dont notamment le système de santé publique du Royaume Uni).

. . .

Complété par un Ransomware, il chiffrait les données de la victime et demandait une rançon avant de les redonner.

. . .

. . .

“ransomware”, en Francais, “rançongiciel”, ou “logiciel de rançon”.

. . .

Malware qui “prends en otage” des données personnelles, en empêchant l’utilisateur d’accéder à ses fichiers tant qu’il n’à pas payé une raçon.

. . .

. . .

Vient de l’anglais “Scare” (faire peur).

. . .

Fait peur à l'utilisateur en lui faisant croire que son ordinateur est infecté par un virus, et l'encourage à payer pour un faux antivirus.

. . .

Dans ce cas, la raçon se fait par le paiement de l'utilisateur.

. . .

. . .

Plus difficile à éviter.

. . .

Peut s'injecter de beaucoup de manières différentes

. . .

Le Ransomware de chiffrement entre dans le système de la victime et chiffre (rend illisible) tous ses fichiers. Il exige alors une raçon pour que l'utilisateur puisse récupérer ses fichiers.

. . .

Dans ce cas, la raçon est explicitée comme telle, et non masquée comme pour le Scareware.

. . .

“Trojan”, “Trojan horse”, ou “Cheval de Troie”

. . .

Logiciel

. . .

- fonctionnalité malveillante

. . .

- but de s’installer **à l’insu** de l’utilisateur

. . .

Terme inventé en 1970 par Daniel J. Edwards.

. . .

Fait référence à la mythologie Grecque antique.

. . .

Un programme en apparence inoffensif, mais contenant du code malveillant.

. . .

L'utilisateur ne se doute pas qu'il installe lui-même un virus.

. . .

- Téléchargement sur des sites non-officiels

. . .

- Téléchargement via le protocole P2P

. . .

- Visite de sites web contenant un exécutable (contrôles ActiveX ou applications Java)

. . .

- Utilisation d'applications obsolètes (exploitation de failles) (navigateurs, messageries, lecteurs multimédias)

. . .

- Ingéniérie sociale (par exemple, envoi du cheval dirrectement à la victime par messagerie)

. . .

- Pièces jointes de messages envoyés

. . .

- Mise à jour d'un logiciel

. . .

- Absence de logiciel de protection

. . .

- Lecture d'une clef USB d'origine inconnue

. . .

Les symptômes les plus probables sont :

. . .

- activité anormale de la carte réseau / du disque dur

. . .

- curseur de souris qui bouge anormalement

. . .

- ouverture non planifiées de programmes

. . .

- système qui plante régulièrement

. . .

- supression, blocage, modifications de certaines données

. . .

. . .

Forme de malware qui se cache sur un appareil pour surveiller les activités de la victime.

. . .

Peut voler des données telles que des données banquaires ou des mots de passe.

. . .

- Une des menaces les plus anciennes et les plus courantes sur internet

. . .

- Peut infecter un système de la même manière qu'un malware quelqonque

. . .

- Le but est de cacher ce virus pour que la victime ne le remarque pas

. . .

- Les attaques peuvent aussi se propager depuis un utilisateur à une entreprise par exemple

. . .

- Les attaques ne sont pas ciblées : le but est d'infecter le plus grand nombre de personnes

. . .

- Il existe de nombreux types de virus informatiques

. . .

- Leurs buts peuvent être très différents

. . .

mais on peut remarquer des stratégies simples pour éviter d'être infecté par grand nombre de ces virus :

. . .

. . .

- Faire attention aux mails que l'on ouvre, notamment aux pièces jointes

. . .

- Faire attention aux sources des applications que l'on installe

. . .

- Faire attention à ce que l'on télécharge (surtout pour des téléchargements en P2P)

. . .

- Faire attention à ne pas lire de clef USB ou autres moyens de stockage d'origine étrangère

---

. . .

Important : Ces conseils sont valables pour le système d'exploitation *Microsoft Windows*.

. . .

Les systèmes basés ou inspirés de Unix éliminent beaucoup de problèmes de sécurité.

. . .

Le facteur du nombre d'utilisateurs joue un rôle dans cette grande différence de fiabilité, car faire un virus pour windows est souvent plus rentable.

. . .

- Les clefs USB ne sont plus dangeureuses si on n'éxécute pas soi même un fichier qui est contenu dedans

. . .

- Les mails ne sont plus dangeureux, sauf encore une fois si l'on éxécute une pièce jointe

. . .

- Des fichiers classiques (texte, texte enrichi ou hypertexte) ne sont probablement pas non plus dangeureux

. . .

- Les failles sont plus rares et trouvées plus rapidement, surtout pour les systèmes qui sont en *open source* et qui bénéficie

d'une grande communauté

. . .

Merci pour votre écoute !