Sécurité des Systèmes d'Information

(Vulnérabilité, menace et attaque informatique)

Partie 2: les malwares

université d'Alger 1 -
Benyoucef Benkhedda

Malware

Dark Angel, un créateur de virus,

« *Art de programmation destiné à détruire les systèmes des crétins* »

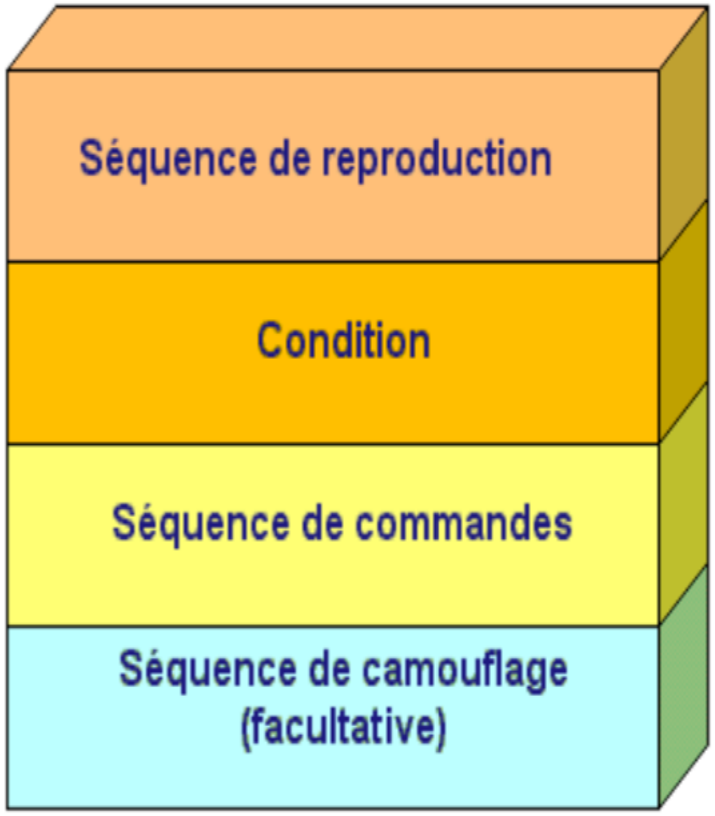
Malwarebytes.com

« *Malware, or "malicious software," is an umbrella term that describes any malicious program or code that is harmful to systems.* »

Définition:

instruction ou suite d'instructions parasites, introduites dans un programme et susceptibles d'entrainer diverses perturbations dans le fonctionnement de l'ordinateur

Structure d’un malware



Séquence de reproduction:

Elle inclut une fonctionnalité de recherche, qui permet de rechercher des fichiers à infecter.

Condition:

Il s'agit tout simplement de la partie qui va conditionner le lancement de l'action qu'est censé accomplir le virus.

Séquence de commandes:

c'est elle qui effectue l'action du virus. Cela peut être détruire des fichiers, formater une partition...

Séquence de camouflage:

Les développeurs de virus ont donc élaboré plusieurs techniques pour cacher le virus.

Types de malwares

Adware:

Des programmes malveillants permet un affichage des pages de publicités sur écran (généralement dans le navigateur web).

Ils s'apparaissent sous forme:

- Les publicités apparaissent dans des endroits où elles ne devraient pas être.
- La page d'accueil de votre navigateur Web a mystérieusement changé sans votre autorisation.
- Les pages Web que vous visitez généralement ne s'affichent pas correctement.
- Les liens de sites Web redirigent vers des sites différents de ce que vous attendiez.
- Votre navigateur Web ralentit à une exploration.
- De nouvelles barres d'outils, extensions ou plugins remplissent soudainement votre navigateur.
- Votre Mac démarre automatiquement l'installation des applications logicielles indésirables.
- Votre navigateur se bloque.

Exemples: xhelper, mtinyapp, fireplo, fireball, DeskAd…etc.

Types de malwares

Spyware:

Des programmes malveillants permet un espionnage sur les activités des utilisateurs et l'envoie des rapports aux adresses ou url spécifiés.

Ils s'apparaissent en quatre (04) types:

- Voleurs de mots de passes (mots de passes stockés dans le cache navigateur, mots de passes systèmes…etc.)
- Chevaux de Troie bancaires permettant le vols des informations de transactions bancaires via des liens ou extensions des navigateurs
- Voleurs d'information permettant un scan de la machine victime pour avoir des différentes informations sur le contenu
- Keyloggers qui sont des enregistreurs de frappes et d'activités pour la sauvegarde des comportements des utilisateurs

exemples: emotet, internet optimazer, coolWebSearch…etc.

Types de malwares

Virus:

Des programmes malveillants permet de s'infiltrer dans le système en infectant des fichiers normaux ou fichiers systèmes afin d'assurer leurs objectifs (arrêt de système, suppression ou cache des fichiers…etc.)

S'apparaissent en plusieurs types

exemples: ILOVEYOU, Slammer, Nimbda, Code Red…etc.

Types de virus

Virus du secteur d'amorçage:

- Attaque le premier secteur lu durant la phase de Boot
- Difficile à déceler car il est chargé avec le démarrage => avant démarrage d'anti-virus

Virus d'application:

- Attaque les fichiers exécutables dans l'ordinateur
- Écrit sous forme de bout de code en assembleur
- Se place dans le 1er segment de la cible et s'exécute d'abord

Virus furtifs:

- Très difficile à détecter
- Il sert à modifier le fonctionnement du système d'exploitation d'une façon permettant à l'anti-virus de croire que le système et sains

Types de virus

Virus polymorphes:

- Change sa signature à chaque nouvelle infection
- Utilise la cryptographie pour re-chiffrer le corps principale à chaque nouvelle infection => requiert des anti-virus très intelligents

Virus de macros :

- Attaque les fichiers Microsoft Office (word, power point, excel…etc.)
- Basé sur le langage VBA
- S'exécute à chaque utilisation de fichier et affecte tout nouveau fichiers créé en basant sur le modèle

Vers:

- Certains documents ne les considère pas comme des virus, d'autres les considèrent comme variété des virus
- Ont le même fonctionnement que le virus sauf qu'ils s'exécutent dans le réseau

Types de virus

Virus flibustiers:

- Leur but est de désactiver l'anti-virus
- Ils sont rares mais diablement efficaces et dangereux, le système devenant totalement vulnérable.

Virus compagnons:

- Un virus à l'ancienne, très aisé à détecter. Sur les systèmes DOS, une priorité d'exécution est accordée aux fichiers portant l'extension .com. En créant un fichier .com portant le même nom que l'exécutable .exe

Virus multi-critères:

- Englobe des différentes caractéristiques des autres virus
- Plus il a de caractéristiques plus il est difficile

Types de malwares

Cheval de Troie:

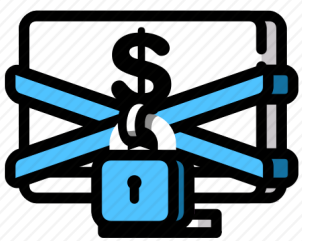
Un programme malveillant qui s'apparaît normal dans le système et permet l'ouverture de certaines portes appelées portes dérobées permettant aux attaquants de s'infiltrer dans le système.

Ils s'apparaissent en cinq (05) types:

- Trojan des portes dérobées qui permet la création des portes de contrôle à distance du système
- Trojan spyware permettant l'écout sur les activités en ligne afin de transmettre des informations confidentielles
- Trojan zombifiants permet la transformation du système cible en esclave (création d'un Botnet)
- Trojan téléchargeur permet le téléchargement des autres malwares
- Trojan de numérotaiton spécialisé dans les smartphones permet de générer des revenus en envoyant des sms premium

exemples: KMSPico, **logiciel de crarck**, Exploit…etc.

Types de malwares



Ransomware:

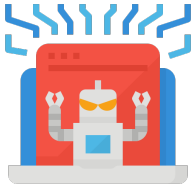
Un programme malveillant qui a le but d'interdire les utilisateurs d'utiliser leur système soit en bloquant l'accès au système soit en chiffrant les données en demandant une rançon.

Ils s'apparaissent en trois (03) types:

- Scareware permet d'inonder le système per une fausse alerte de malware et demander de payer pour le supprimer du système
- Casiers d'écran permet de bloquer l'affichage normale du système par un affichage de message
- Ransomware de chiffrement permet de chiffrer les données de l'utilisateur en demandant un rançon pour avoir la clé de déchiffrement

exemples: wannacry, cryptoLocker, Petya…etc.

Types de malwares



Rootkit:

Un programme malveillant qui permet d'avoir un accès avec privilèges d'administrateur au système à distance.

Cryptomining malveillant:

Un programme malveillant qui permet de transférer la machine victime en une source qu'un attaquant peut l'utiliser pour le mining de la monnaie virtuelle

Types de malwares

Bombe logique:

Un programme malveillant qui permet sous certaines conditions bien définies de détruire tout le système victime ou supprimer toutes les données qui existent

Hoax (Canular):

Les virus font souvent l'objet de fausses alertes que la rumeur propage, encombrant les messageries avec des chaines de mails. Certaines fausses alertes misent également sur l'ignorance des utilisateurs en matière d'informatique pour leur faire supprimer des éléments sains de leur système.

Comment connaître si je suis infecté?

- La machine commence à se ralentir
- Un tas de publicité ennuyeuses qui s'apparaissent souvent
- Votre ordinateur crache tout seul ou affiche la fenêtre bleu de la mort (BSOD)
- Changement bizarre dans l'espace disque utilisé
- Un comportement bizarre de votre appareil (ventilateur du processeur qui commence souvent…etc.)
- Usage des ressource élevé d'une façon anormale
- La page d'accueil de votre navigateur change toute seule
- Des barre d'outils ou des extensions qui s'apparaissent tous seuls dans votre navigateur
- L'antivirus s'arrête de fonctionner et refuse les mises-à-jours
- Même si tout semble bien fonctionner sur votre système, ne soyez pas complaisant, car aucune nouvelle n'est pas nécessairement une bonne nouvelle. => « **FILELESS attacks** »

Comment peut-on avoir un malware?

- Par l'utilisation des **logiciels gratuits** ou **cracké**
- Cliquer sur **les liens dans les emails** et visiter n'importe quel **site web**
- Téléchargement des fichiers de **n'importe quelle source** surtout **les sources piratés**
- Peut s'infiltrer à travers l'installation des applications déjà infectées
- Ne soucions pas de notre sécurité (pas de mise-à-jours des applications, autoriser tout les paquets dans le pare-feu…etc.)

"Malware attacks would not work without the most important ingredient: *you.*"