Décrire les programmes malveillants
Formation Microsoft Learn

Vous avez sans doute entendu parler de termes comme logiciels malveillants, virus, vers, etc.
Mais qu'est-ce que ces concepts signifient ?
Un virus est-il un ver ?
Que fait un programme malveillant, exactement ?
Ce ne sont que quelques exemples des concepts de base que vous découvrirez dans cette unité.

Qu'est-ce qu'un programme malveillant ?

Les logiciels malveillants sont utilisés par les cybercriminels pour infecter les systèmes et effectuer des actions qui peuvent nuire.
Cela peut inclure le vol de données ou l'interruption de l'utilisation et des processus normaux.

Les logiciels malveillants ont deux composants principaux :

- Un mécanisme de propagation
- Payload

Qu'est-ce qu'un mécanisme de propagation ?

La propagation est la façon dont le logiciel malveillant se propage sur un ou plusieurs systèmes.
Voici quelques exemples de techniques de propagation courantes :

La plupart d'entre nous sont déjà familiers avec ce terme.
Mais que signifie-t-il réellement ?
Tout d'abord, penchons-nous sur les virus en termes non techniques.
En biologie, par exemple, un virus pénètre dans le corps humain et, une fois à l'intérieur, peut se répandre et causer des dégâts.
Les virus basés sur la technologie dépendent de certains moyens d'entrée, en particulier une action de l'utilisateur, pour accéder à un système.
Par exemple, un utilisateur peut télécharger un fichier ou brancher un périphérique USB qui contient le virus et contamine le système.
Vous avez maintenant une violation de sécurité.

Ver informatique

Contrairement à un virus, un ver n'a pas besoin d'une action de l'utilisateur pour se propager à travers les systèmes.
Au lieu de cela, un ver provoque des dégâts en détectant les systèmes vulnérables qu'il peut exploiter.
Une fois à l'intérieur, le ver peut se propager vers d'autres systèmes connectés.
Par exemple, un ver peut infecter un appareil en exploitant une vulnérabilité dans une application qui y est

exécutée.
Le ver peut ensuite se répandre sur d'autres appareils du même réseau et sur d'autres réseaux connectés.

Trojan

L'attaque par cheval de Troie tire son nom de l'histoire classique, dans laquelle des soldats se cachent à l'intérieur d'un cheval de bois présenté comme cadeau aux Troyens. Lorsque les Troyens ont apporté le cheval dans leur ville, les soldats sont sortis et les ont attaqués.
Dans le contexte de la cybersécurité, un cheval de Troie est un type de programme malveillant qui prétend être un logiciel authentique.
Lorsqu'un utilisateur installe le programme, il peut prétendre fonctionner comme annoncé, mais il effectue également des actions malveillantes secrètes, telles que le vol d'informations.

Qu'est-ce qu'une charge utile ?

La charge utile est l'action effectuée par un logiciel malveillant sur un appareil ou un système infecté.
Voici quelques types courants de charge utile :

- Le **rançongiciel** est une charge utile qui verrouille des systèmes ou des données jusqu'à ce que la victime ait versé une rançon.
  Supposons qu'il existe une vulnérabilité non identifiée dans un réseau d'appareils connectés.
  Un cybercriminel peut exploiter cela pour accéder à tous les fichiers sur ce réseau et les chiffrer.
  L'attaquant exige ensuite une rançon pour déchiffrer les fichiers.
  Il peut menacer de supprimer tous les fichiers si la rançon n'a pas été payée avant un délai défini.
- Les **logiciels espions** sont un type de charge utile qui espionne un appareil ou un système.
  Par exemple, le programme malveillant peut installer un logiciel d'analyse du clavier sur l'appareil d'un utilisateur, collecter des informations de mot de passe et les transmettre à l'attaquant, le tout sans la connaissance de l'utilisateur.
- **Portes dérobées** : Une porte dérobée est une charge utile qui permet à un cybercriminel d'exploiter une vulnérabilité dans un système ou un appareil pour contourner les mesures de sécurité existantes et causer des dommages.
  Imaginez un cybercriminel infiltrant une société de développement de logiciels et laissant du code lui permettant d'effectuer des attaques.
  Cela devient une porte dérobée que le cybercriminel peut utiliser pour pirater l'application, l'appareil sur lequel elle s'exécute et même les réseaux et systèmes de l'organisation et des clients.
- Le **botnet** est un type de charge utile qui joint un ordinateur, un serveur ou un autre appareil à un réseau d'appareils infectés de la même façon, et qui peut être contrôlé à distance pour effectuer une action mal intentionnée.
  Une application courante des botnets est l'exploration crypto (on parle aussi de programme malveillant de crypto-mining).
  Dans ce cas, le malware connecte un appareil à un botnet qui utilise la puissance de calcul de l'appareil pour miner ou générer des cryptomonnaies.
  L'utilisateur peut remarquer que son ordinateur marche plus lentement qu'avant et que ça devient pire chaque jour.

Unité suivante: Décrire les stratégies d’atténuation de base

Continuer

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231023
"C'est ensemble qu'on avance"