MORDEHAI
BTSSIO
Ethan

LES TYPES DE PROGRAMMES MALVEILLANTS

Qu'est ce qu'un programme malveillant?

SOMMAIRE

Les virus informatiques

Un virus informatique est un programme malveillant conçu pour infecter les ordinateurs et se propager en modifiant ou en endommageant les fichiers, les données ou le fonctionnement du système.

Propagation

Ils se propagent en infectant des fichiers ou en s'attachant à des programmes légitimes.

Effets

Peuvent causer des dommages, voler des données ou perturber le fonctionnement des ordinateurs.

Origine

Peuvent être créés par des cybercriminels ou se propager par accident via des logiciels ou des fichiers infectés.

Les vers informatiques

Un ver informatique est un type de logiciel malveillant autonome qui se propage de manière autonome à travers les réseaux informatiques. Contrairement aux virus, les vers n'ont pas besoin de fichiers hôtes pour se propager, mais exploitent plutôt des vulnérabilités dans les systèmes d'exploitation ou les logiciels reseau.

1

Auto-Réplication

Se propagent en se copiant d'un ordinateur à un autre, sans avoir besoin d'un programme hôte pour se propager.

2

Infiltration Silencieuse

Peuvent se propager sans être détectés et altérer les performances des systèmes infectés.

3

Propagation Rapide

Peuvent se répandre rapidement à travers les réseaux et causer des dégâts importants.

Les chevaux de Troie

Un cheval de Troie est un type de logiciel malveillant qui se présente comme un programme légitime, mais qui dissimule des fonctionnalités malveillantes. Contrairement aux virus et aux vers, les chevaux de Troie ne se reproduisent pas par eux-mêmes. Ils nécessitent souvent une action de l'utilisateur pour être installés, par exemple en téléchargeant un fichier apparemment inoffensif ou en cliquant sur un lien malveillant.

Ingéniosité

Se cachent dans des programmes légitimes pour tromper les utilisateurs et s'infiltrer dans les systèmes.

Infiltration Discrète

Souvent déguisés en logiciels utiles ou inoffensifs pour encourager les utilisateurs à les télécharger.

Les logiciels espions

85K

Nombreuses Infections

Environ 85 000 types de logiciels espions identifiés à ce jour.

Les ransomwares

Un ransomware est un type de logiciel malveillant qui chiffre les fichiers sur un système informatique, rendant ainsi les données inaccessibles à l'utilisateur.

1

Propagation

Peuvent se propager via des pièces jointes malveillantes ou des sites web compromis.

2

Chiffrement

Chiffrent les fichiers des utilisateurs, les rendant inaccessibles jusqu'à ce qu'une rançon soit payée.

3

Demande de rançon

Exigent des paiements en cryptomonnaie pour restaurer l'accès aux données.

Les adwares

Les adwares (Advertising Supported Software) sont des logiciels légitimes qui vont, par exemple, afficher des publicités indésirables sur un système, souvent de manière intrusive. Cependant, certains adwares peuvent avoir des comportements plus malveillants.

1

Annonces Intrusives

Génèrent des publicités non sollicitées qui peuvent être perturbatrices pour les utilisateurs.

2

Infiltration Discrète

S'installent souvent avec des logiciels gratuits ou des applications légitimes.

3

Collecte de Données

Peuvent collecter des informations personnelles et de navigation pour le ciblage publicitaire.

Les botnets

Un botnet est un réseau de dispositifs informatiques infectés par des logiciels malveillants, appelés bots, qui sont contrôlés à distance par un attaquant, souvent appelé « botmaster ». Ces bots peuvent être des ordinateurs, des serveurs, des appareils IoT (Internet des objets) ou d'autres dispositifs connectés à Internet.

Les botnets sont utilisés de 2 façon différentes:

Contrôle Centralisé	Un serveur contrôle et coordonne les actions des ordinateurs infectés.
Attaques DDoS	Peuvent être utilisés pour lancer des attaques par déni de service en combinant la puissance de nombreux ordinateurs.

Conclusion

La prévention et la sensibilisation sont cruciales pour la protection contre ces formes de programmation malveillante.

Cela permettra d'éviter par exemple de se faire voler ses données personelles , afin déviter de payer des sommes astronomiques a des hackers.

Ou encore eviter de devoir racheter un ordinateur car on a clique sur le mauvais lien (notamment les chevaux de Troie).

Afin d'éviter cela, vous devez TOUJOURS avoir un Antivirus sur son ordinateur (Windows defender fait assez bien le taff), et faire attention sur quel site on va (en regardant si le site est sécurisé).

SOURCE:
CHAT GPT
https://www.cohesity.com/fr/glossary/ransomware/