LA LIBERTÉ
Depuis 1913

Clinique de
Cyber-Criminologie

GÉNÉRATION CYBER-SMART

TÉLÉCHARGEMENTS ET MALICIELS ****

En explorant le sujet des cybermenaces, nous parlons beaucoup de maliciels. Dans cette section, nous voulons mieux expliquer exactement ce que sont ces types de logiciels, comment ils se manifestent et les types de conséquences qu'ils peuvent entraîner.

generationcybersmart.ca

Un projet rendu possible financièrement grâce à :

Secrétariat aux relations canadiennes Québec

Société de la francophonie manitobaine

QU'EST-CE QU'UN MALICIEL?

Un maliciel, mot-valise pour logiciel malveillant, est un type de logiciel spécifiquement conçu pour perturber, endommager ou obtenir un accès non autorisé à des systèmes, réseaux ou appareils informatiques, souvent à l'insu ou sans le consentement de l'utilisateur. Il y a trois grands "types" de maliciels, qui représentent en fait la manière dont chaque type de programme s'installe dans un système et se propage. Ces maliciels sont les virus informatiques, les vers et les chevaux de Troie.

Virus informatiques

Installation : Les virus infectent généralement un système hôte en s'attachant à des fichiers exécutables, des documents ou d'autres types de fichiers. Ils dépendent souvent des actions de l'utilisateur, telles que l'ouverture d'une pièce jointe infectée ou le téléchargement d'un fichier malveillant sur l'internet, pour s'exécuter et se propager. Ils peuvent aussi changer de forme pour éviter d'être détectés par les logiciels de sécurité.

Propagation : Les virus peuvent se propagent par différents moyens, dont les pièces jointes aux courriels, les fichiers partagés comme sur Google Drive, les appareils de stockage infectés (comme les clés USB) et les sites web compromis. Une fois exécutés, les virus peuvent tenter de se répliquer et d'infecter d'autres fichiers ou systèmes sur le même réseau.

Dommages : Les virus peuvent causer toutes sortes de dommages aux systèmes infectés, comme la perte ou la corruption de données, l'accès non autorisé à des informations sensibles et la perturbation du fonctionnement normal du système. Certains virus peuvent également installer d'autres logiciels malveillants ou créer des portes dérobées que des pirates peuvent exploiter pour accéder à plus d'informations.

Vers informatiques

Installation : Les vers sont des programmes malveillants autonomes qui peuvent se reproduire et se propager sur les réseaux sans intervention de l'utilisateur. Ils exploitent souvent les failles de sécurité ou les faiblesses des systèmes ou des applications pour s'y infiltrer.

Propagation : Les vers se propagent en analysant les réseaux - comme un réseau Wi-Fi public ou une connexion Bluetooth ouverte - à la recherche de vulnérabilités pour obtenir un accès non autorisé. Ils peuvent se propager rapidement en s'autoreproduisant et en infectant d'autres systèmes vulnérables sur le même réseau ou sur internet.

Dommages : Les vers peuvent provoquer des dommages importants en consommant la bande passante du réseau, en surchargeant les serveurs et en compromettant la sécurité et la stabilité des systèmes infectés. Ils peuvent aussi installer des portes dérobées, voler des informations sensibles ou lancer des attaques supplémentaires sur des réseaux ou des sites web ciblés.

Chevaux de Troie

Installation : Les chevaux de Troie sont des programmes malveillants déguisés en logiciels ou fichiers légitimes pour inciter les utilisateurs à les installer sur leur système. Ils se font souvent passer pour des applications, des jeux ou des fichiers multimédias utiles et peuvent être distribués par le biais de pièces jointes à des courriels, des sites et services de téléchargements de logiciels ou de sites web compromis.

Propagation : Contrairement aux virus et aux vers, les chevaux de Troie ne se reproduisent pas. Ils s'appuient sur des tactiques d'ingénierie sociale pour convaincre les utilisateurs de les exécuter volontairement. Une fois installés, les chevaux de Troie peuvent effectuer diverses activités malveillantes, comme le vol d'informations sensibles, l'installation de logiciels malveillants supplémentaires ou la provision d'un accès à distance aux attaquants.

Dommages : Les chevaux de Troie peuvent causer des dommages importants aux systèmes infectés en effectuant des actions non autorisées, incluant le vol de données, la modification du système ou la prise de contrôle à distance par les pirates. Ils peuvent aussi compromettre la sécurité du système, la vie privée de l'utilisateur et perturber le fonctionnement normal du système à l'insu de l'utilisateur.

Une fois installés, les maliciels peuvent effectuer d'autres actions malveillantes. Le rançongiciel, par exemple, est un type de maliciel conçu pour chiffrer des fichiers ou bloquer l'accès à un système informatique ou à ses données jusqu'à ce qu'une rançon soit payée. Les logiciels espions, de leur côté, sont des maliciels conçus pour surveiller et collecter secrètement des informations sur les activités en ligne d'un utilisateur, ses habitudes de navigation, les touches qu'il frappe et ses données personnelles, à son insu et sans son consentement. Enfin, les logiciels publicitaires sont des logiciels qui affichent ou téléchargent automatiquement des publicités sur l'ordinateur ou l'appareil d'un utilisateur. Contrairement aux autres logiciels malveillants, qui sont conçus pour causer des dommages ou exploiter des vulnérabilités, les logiciels publicitaires visent principalement à générer des revenus pour leurs créateurs en diffusant des publicités ciblées aux utilisateurs.

COMMENT SE PROTÉGER DES MALICIELS?

Il est tout d'abord important de se **méfier de tout téléchargement** ne provenant pas d'un distributeur autorisé ou de liens inconnus, même s'ils proviennent de quelqu'un que vous connaissez. Les virus et les chevaux de Troie se propagent de cette manière, et les signes qu'un maliciel a été installé sur votre appareil ne sont pas toujours apparents. Analysez les liens et les fichiers avec des outils comme votre antivirus ou VirusTotal avant de les ouvrir, et si vous n'êtes pas sûr ou si quelque chose vous semble suspect, écoutez votre instinct et ne le téléchargez pas. Si une personne que vous connaissez vous a envoyé un lien par courrier électronique ou par message personnel, mais que vous n'êtes pas confiant qu'il est sécuritaire de cliquer, posez-lui des questions par un autre moyen de communication. Cela vous permettra de vous assurer que vous ne téléchargez pas par erreur un maliciel, au cas où le lien ou fichier aurait été envoyé par un pirate qui aurait compromis le compte de votre ami ou de votre proche.

Méfiez-vous également lorsque vous naviguez sur des réseaux ou appareils qui ne vous appartiennent pas. Comme les vers informatiques peuvent se propager sur des réseaux publics, gardez vos informations sensibles et vos comptes importants en sécurité en évitant d'y accéder. Par exemple, utilisez vos données cellulaires si vous avez besoin de faire une transaction au lieu de l'effectuer sur le réseau d'un restaurant ou d'un parc.

Gardez tous vos outils de sécurité et autres applications à jour afin de maintenir vos défenses aussi actuelles que possible. Vous pouvez vérifier l'état de votre logiciel antivirus en lançant l'application : celle-ci vous indiquera généralement depuis la page d'accueil si une mise à jour doit être effectuée. Pour faciliter cette tâche, vous pouvez activer les mises à jour automatiques de votre antivirus, des systèmes d'exploitation de vos appareils et des applications, et activer également ces fonctions sur les appareils qu'utilise votre enfant.

RESSOURCES

VirusTotal : https://www.virustotal.com/gui/

GLOSSAIRE

- **Logiciel malveillant ou maliciel** : Les maliciels, mot-valise pour logiciels malveillants, désignent tout type de logiciel spécifiquement conçu pour perturber, endommager ou obtenir un accès non autorisé à des systèmes, réseaux ou appareils informatiques, souvent à l'insu ou sans le consentement de l'utilisateur.
- **Téléchargement** : Un téléchargement fait référence au processus de transfert de données, de fichiers ou de contenu d'un serveur distant, d'un site web ou d'une source en ligne vers un ordinateur local ou un appareil.
- **Piratage** : Au sens général, le piratage informatique désigne l'obtention d'un accès non autorisé à des systèmes ou réseaux informatiques, impliquant souvent la manipulation, l'exploration ou l'exploitation de la technologie pour atteindre cet objectif.
- **Fichier infecté** : Un fichier infecté est un fichier qui a été modifié, corrompu ou compromis par un code malveillant, ce qui le rend potentiellement nuisible ou dangereux.
- **Site web compromis** : Un site web compromis est un site web qui a été infiltré, manipulé ou pris en charge par des pirates, souvent à des fins malveillantes.
- **Virus** : Un virus est un type de maliciel qui infecte les systèmes informatiques en insérant son propre code dans des programmes ou des fichiers légitimes. Tout comme les virus biologiques, les virus informatiques se répliquent et se propagent d'un ordinateur à l'autre, souvent dans le but de nuire, de perturber le fonctionnement du système ou de voler des informations sensibles.
- **Cheval de Troie** : Un cheval de Troie est un type de maliciel qui se déguise en logiciel légitime ou inoffensif pour tromper les utilisateurs et les inciter à le télécharger, l'installer et l'exécuter sur leur système informatique.
- **Ver informatique** : Un ver informatique est un type de maliciel capable de s'auto-reproduire et de se propager de manière indépendante dans les réseaux et systèmes informatiques sans requérir d'interaction de la part de l'utilisateur. Contrairement aux virus, qui nécessitent généralement un programme hôte pour être infectés et se propager, les vers sont des programmes autonomes qui peuvent se propager automatiquement en exploitant les vulnérabilités des protocoles de réseau, des systèmes d'exploitation ou des applications logicielles.
- **Logiciel espion** : Un logiciel espion est un type de logiciel malveillant conçu pour surveiller secrètement et recueillir des informations sur les activités informatiques d'un utilisateur à son insu ou sans son consentement.

- **Rançongiciel** : Un rançongiciel est un type de logiciel malveillant conçu pour crypter des fichiers ou verrouiller l'accès au système informatique ou aux données d'une victime, la tenant ainsi en otage jusqu'au paiement d'une rançon.
- **Logiciel publicitaire** : Les logiciels publicitaires sont des logiciels qui affichent ou téléchargent automatiquement des publicités sur l'ordinateur, l'appareil ou le navigateur web d'un utilisateur.
- **Antivirus** : Un antivirus est un type de logiciel de sécurité conçu pour détecter, prévenir et supprimer les logiciels malveillants (maliciels) des systèmes informatiques.
- **Mise à jour** : Une mise à jour fait référence au processus d'application de changements, d'améliorations ou de correctifs à un système afin d'en améliorer la fonctionnalité, les performances, la sécurité ou la stabilité.

Balayez ce QR code à l'aide de votre caméra pour visionner nos vidéos