Protéger votre organisation contre les maliciels

JUILLET 2022

ITSAP.00.057

Les auteurs de menace peuvent avoir recours aux **maliciels**, ou logiciels malveillants, pour s'infiltrer dans votre réseau, vos systèmes et vos appareils, ou les endommager. Dès lors qu'un maliciel a été installé sur les systèmes et les appareils de votre organisation, les auteurs de menace peuvent se donner accès à vos informations sensibles. Ce document présente les types de maliciels courants, propose des conseils permettant de voir si vos appareils ont été infectés et énonce la marche à suivre pour protéger les ressources de votre organisation contre les compromissions issues de maliciels.

Types de maliciels courants

Voici certains types de maliciels couramment employés par les auteurs de menace :

- **Rançongiciel**: Type de maliciel qui vous empêche d'accéder à vos données ou à vos systèmes tant que vous n'avez pas versé une rançon à l'auteur de menace. Pour en savoir plus sur les rançongiciels et la façon de protéger votre organisation, consultez le *Guide sur les rançongiciels (ITSM.00.099)* sur le site Web du Centre pour la cybersécurité.
- **Espiogiciel**: Logiciel infecté que les auteurs de menace utilisent pour accéder à vos appareils et voler de l'information sensible.
  - **Cheval de Troie**: Type d'**espiogiciel** auquel on a donné l'apparence d'un logiciel inoffensif pour vous convaincre de le télécharger.
  - **Publiciel**: Type **d'espiogiciel** qui surveille votre historique de navigation Internet et vos téléchargements dans le but d'afficher des fenêtres publicitaires qui font la promotion de produits ou de services qui pourraient vous intéresser.
- **Maliciel effaceur :** Le disque dur, les données et les programmes de l'ordinateur infecté sont effacés, écrasés ou supprimés. Les maliciels effaceurs peuvent se faire passer pour des rançongiciels, mais ils continueront de détruire l'ensemble des données et des fichiers en arrière-plan. Toutefois, si des processus de sauvegarde rigoureux ont été mis en place, il pourrait être possible de restaurer une partie ou l'ensemble des données.
- **Virus**: Programme informatique qui se propage, souvent discrètement, en se reproduisant à plusieurs reprises.
- **Enregistreur de frappe (Keylogger):** Logiciel ou dispositif matériel conçu pour enregistrer les informations que vous saisissez au clavier (frappes). Les frappes sont stockées ou transmises de manière à ce que l'auteur de menace puisse collecter de l'information de valeur.
- **Dissimulateur d'activité (Rootkit):** Programme employé par un auteur de menace pour se donner accès à vos réseaux, systèmes et appareils. Un dissimulateur d'activité se fait passer pour une composante du système d'exploitation de votre appareil.
- **Maliciel VPNFilter:** Maliciel conçu pour infecter les routeurs et ainsi permettre à un auteur de menace de collecter de l'information, d'exploiter des appareils et de bloquer le trafic réseau.
- **Ver:** Programme malveillant qui s'exécute de lui-même et se réplique, généralement par les connexions réseau, dans le but de causer des dommages (p. ex. suppression de fichiers, envoi de documents par courriel, ou saturation de la bande passante).

Modes par lesquels un maliciel peut infecter des ressources

Voici quelques exemples de moyens par lesquels un maliciel pourrait infecter vos réseaux, systèmes et appareils:

- Acceptation des fenêtres publicitaires
- Téléchargement de logiciels non fiables (p. ex. logiciel se faisant passer pour une mise à jour de Flash Player)
- Ouverture de fichiers malveillants joints à un courriel
- Téléchargement de contenu ou de logiciels de sources ou de fournisseurs non fiables
- Échange de fichiers (comme les services de partage de fichiers poste à poste)
- Utilisation de supports amovibles (par exemple, clé USB, disque dur, CD, DVD) sans les avoir préalablement analysés ou vérifiés

Signes indiquant qu'un appareil a été infecté

Il n'est pas toujours facile de savoir si vos appareils ont été infectés par un maliciel. Voici quelques exemples de symptômes à surveiller:

- Fenêtres contextuelles s'affichant sur votre appareil
- Modification de la page d'accueil
- Pourriels envoyés depuis votre compte
- Plantage du système ou d'une page
- Ralentissement de la performance de l'ordinateur
- Exécution de programmes inconnus sur votre appareil
- Modification non autorisée de mots de passe

SÉRIE SENSIBILISATION

Cat. No. D97-1/00-057-2022F-PDF
ISBN 978-0-660-43196-3

Conseils pour se protéger contre les maliciels

Voici quelques mesures à adopter pour protéger votre appareil contre les maliciels :

- Sauvegarder vos appareils et vos données.
- Installer les mises à jour et les correctifs de logiciels dès qu'ils sont disponibles.
- Installer des logiciels antivirus et antimaliciel et les tenir à jour.
- Installer des logiciels antihameçonnage
  - Veiller à ce que les logiciels soient conformes au protocole DMARC (Domain-Based Message Authentication, Reporting and Conformance) – par exemple, protocole d'authentification des courriels et de signalement (visibilité des noms de domaine, signalement des intrusions).
- Utiliser un système de détection des intrusions sur l'hôte (SDIH)
- Utiliser un pare-feu
- Mettre en œuvre une liste d'applications autorisées pour veiller à ce que seules les applications autorisées puissent être installées et s'exécuter
- S'assurer que les fichiers et les pièces jointes proviennent de sources légitimes avant de les télécharger
- Utiliser un bloqueur de publicité
- Utiliser une application de suivi de l'utilisation des données (par exemple, pour surveiller l'utilisation des données d'applications lorsqu'un appareil n'est pas utilisé pour détecter toute activité suspecte)
- Éviter de vous connecter aux réseaux sans fil (Wi-Fi) publics
- Désactiver les fonctions Wi-Fi, GPS et Bluetooth lorsqu'elles ne sont pas utilisées
- Éviter de partager des renseignements personnels sur les réseaux sociaux, puisque ces renseignements pourraient permettre à des auteurs de menace de pirater vos autres comptes (par exemple, l'utilisation de l'adresse domiciliaire pour une question de sécurité en vue d'accéder à des informations bancaires)
- Éviter de débrider (jailbreak) vos appareils (par exemple, désactiver les mesures de sécurité imposées par le fabricant de l'appareil)

Étapes à suivre en cas d'infection

Si votre appareil a été infecté par un maliciel, prenez les mesures suivantes :

1. Communiquer immédiatement avec votre bureau des services de sécurité des TI
2. Déconnecter l'appareil infecté du réseau
3. Éteindre la fonction Wi-Fi et débrancher les câbles qui relient l'appareil au réseau (comme les câbles Ethernet)
4. Connecter l'appareil à un réseau non infecté, puis réinstaller le système d'exploitation
5. Lancer le logiciel antivirus et analyser toutes les copies de sauvegarde avant de restaurer l'appareil
6. Reconnecter l'appareil à votre réseau
7. Surveiller le trafic et lancer des analyses antivirus pour vous assurer que tous les maliciels ont été supprimés de l'appareil

Ordinateurs:

- Assurez-vous que votre appareil et les programmes sont mis à jour
- Si vous effectuez des analyses antivirus et que votre ordinateur montre toujours des signes d'infection, vous devrez peut-être le réinitialiser et réinstaller tous les programmes
- Il sera possible de récupérer les données si l'ordinateur avait été sauvegardé avant que les signes d'infection par maliciel apparaissent

Autres appareils

- Il faudra peut-être réinitialiser les téléphones et les tablettes sur lesquels il est impossible d'exécuter des analyses antivirus. Si la réinitialisation ne règle pas le problème, il faudra peut-être faire appel à un spécialiste

Logiciel antivirus

Les logiciels antivirus protègent les appareils contre les virus, les chevaux de Troie, les vers et les espiogiciels. Ils peuvent détecter les maliciels connus en analysant les fichiers de démarrage, les secteurs de démarrage ainsi que tous les fichiers qui passent par le système. Les logiciels antivirus peuvent également surveiller les applications courantes.

SDIH

Les systèmes de détection des intrusions sur l'hôte (SDIH) surveillent le système dans le but de déceler les intrusions et les accès non autorisés. Les SDIH permettent de voir qui ouvre et modifie les fichiers sur votre système et de déterminer ce que la personne tente de faire.

Pare-feu

Un pare-feu est une barrière de sécurité qui protège les ressources système locales contre les accès provenant de l'extérieur. Le pare-feu d'un réseau restreint le trafic qui passe d'un réseau à un autre. Le pare-feu basé sur l'hôte restreint le trafic réseau entrant ou sortant pour un seul hôte ou un seul point terminal.

Antimaliciel

Les logiciels antimaliciel analysent les fichiers pour déterminer s'ils sont conformes aux caractéristiques prédéterminées appropriées, qu'on appelle leur signature. S'ils ne sont pas conformes, les fichiers sont désignés comme maliciel puis supprimés. Les antimaliciels peuvent également isoler les fichiers suspects ou surveiller le comportement des fichiers pour détecter toute anomalie.

DNS De Protection (PDNS)

Les services de protection liés au système d'adressage par domaines (DNS pour Domain Name System) sont des solutions de sécurité qui offrent une protection en ligne en analysant les adresses IP et les noms de domaine pour ensuite bloquer le contenu indésirable avant que l'appareil soit exposé à un maliciel.

Pour en savoir plus sur les outils de sécurité préventive, consultez Les outils de sécurité préventive (ITSAP.00.058) sur le site Web du Centre pour la cybersécurité. Vous trouverez également de l'information supplémentaire sur les services DNS de protection dans la publication intitulée Système d'adressage par domaine de protection (ITSAP.40.019).

Vous avez des questions ou vous avez besoin d'aide? Vous voulez tout savoir sur la cybersécurité? Consultez le site Web du Centre canadien pour la cybersécurité (Centre pour la cybersécurité) à **cyber.gc.ca**.