Ce que vous devez savoir sur les logiciels malveillants

Devolutions

VOUS DEVEZ SAVOIR CONTRE QUOI VOUS VOUS BATTEZ...

Avant de pouvoir protéger vos appareils et votre organisation contre les attaques par des logiciels malveillants, vous devez savoir contre quoi vous vous battez... Et c'est malheureusement très effrayant. Ça fait comme passer le Roi de la Nuit dans la série Le Trône de fer pour notre mignonne mascotte de hibou en peluche Waykee.

Pour vous préparer au combat, voici donc 6 types de logiciels malveillants, suivis de 6 bonnes pratiques pour rester en sécurité et de 2 mythes à déboulonner.

Types de logiciels malveillants

Virus : ce type de logiciel malveillant s'attache à un document ou à un programme légitime. Il a généralement la capacité de se reproduire de façon répétitive, afin d'infecter et de corrompre d'autres fichiers à l'insu de ses victimes.

Cheval de Troie : ce type de logiciel malveillant est généralement caché ou incorporé dans la pièce jointe d'un courriel ou d'un programme attirant, comme un jeu vidéo, pour encourager les utilisateurs à l'installer. L'un des types les plus insidieux de cheval de Troie est (ironiquement!) un programme qui prétend effacer les virus de votre ordinateur, alors qu'en réalité, il lui en transmet.

Botnet : ce type de logiciel malveillant est un réseau ou un ensemble d'ordinateurs et de routeurs (idO) compromis, reliés à Internet de manière coordonnée à des fins malveillantes. Les machines compromises sont souvent transformées en robots « zombies » et sont utilisées pour envoyer du spam, propager des logiciels malveillants et lancer des cyberattaques. Un botnet est également appelé réseau de machines zombies.

Logiciels espions : ce type de logiciel malveillant est installé sur un ordinateur ou un appareil à l'insu de la victime. Une fois activés, les logiciels espions collectent et transmettent des informations sur une personne ou une organisation, telles que les mots de passe et les numéros de carte de crédit.

Rançongiciel : ce type de logiciel malveillant utilise le cryptage pour bloquer l'accès à un système informatique, puis demande une rançon, généralement en cryptomonnaie (par exemple en Bitcoin), pour que la transaction ne laisse aucune trace. Si la rançon n'est pas payée, les fichiers de la victime sont détruits.

Ver informatique : Ce type de logiciel malveillant est un programme qui se reproduit et se copie d'un ordinateur à l'autre. Plutôt que d'infecter des fichiers, son objectif principal est d'utiliser des ressources comme la mémoire de l'ordinateur et la bande passante réseau pour infliger des dommages.

6 bonnes pratiques pour se protéger contre les logiciels malveillants

Mauvaise nouvelle. Il n'y a aucun moyen efficace à 100 % pour éliminer les logiciels malveillants. La bonne nouvelle, c'est que vous réduisez considérablement les risques d'attaque par des logiciels malveillants si vous adoptez ces bonnes pratiques :

1. Installez un antivirus et un anti-maliciel

Il va sans dire - mais on va le dire quand même - qu'installer un bon logiciel antivirus et anti-maliciel est une première étape cruciale pour la sécurité de votre ordinateur et de votre réseau. Prenez l'habitude d'analyser.

- Pièces jointes des courriels
- Fichiers téléchargés directement à partir d'Internet
- Clés USB, cartes mémoire et autres dispositifs de stockage portables

Ne désactivez ni n'accordez d'exception à votre logiciel antivirus ou anti-maliciel sans savoir vraiment ce que vous faites. C'est un peu comme si vous laissiez la porte de votre maison déverrouillée. Si vous restez à surveiller la porte, c'est correct. Mais si vous êtes endormi, absent ou dans votre « geek cave » en train de jouer à des jeux ou regarder des vidéos, verrouillez la porte!

2. Visitez seulement des sites légitimes

Achetez et téléchargez seulement des applications qui proviennent de sites légitimes. N'ouvrez ou n'exécutez jamais un programme provenant d'une source inconnue ou douteuse. Vous devez également éviter de naviguer sur des sites Web proposant des contenus piratés, parce qu'ils constituent une source importante de logiciels malveillants (en plus, le téléchargement de contenus illégaux peut vous exposer, vous et votre organisation, à de lourdes sanctions juridiques).

3. Pensez avant de cliquer

Soyez toujours prudent si vous recevez un courriel suspect ou non sollicité, même s'il semble provenir d'un collègue, d'un membre de la famille ou d'un ami. Voici quelques conseils à garder à l'esprit:

- Ne cliquez pas sur un lien ou un bouton dans un message. Survolez le lien avec votre curseur pour voir où il vous mène.
- N'ouvrez pas ou ne téléchargez pas de pièces jointes de quelqu'un que vous ne connaissez pas.
- Quand vous naviguez sur le Web, lisez attentivement le contenu d'une fenêtre intruse (pop-up) avant de choisir une option ou d'accepter une offre. Vous serez surpris de voir quelles conditions on vous demande d'accepter!

4. Lisez attentivement

L'une des principales méthodes utilisées pour propager des logiciels malveillants consiste à arnaquer les utilisateurs via l'ingénierie sociale. Portez une attention particulière au contenu d'un courriel. Le formatage est-il étrange et inconnu? Y a-t-il beaucoup de fautes de grammaire et d'orthographe? En cas de doute, contactez directement l'expéditeur et confirmez sa légitimité : appelez-le directement ou envoyez-lui un nouveau courriel. Ne répondez pas au courrier suspect.

5. Faites vos mises à jour

Mettez à jour vos navigateurs, votre système d'exploitation et vos plugiciels. Les mises à jour sont souvent publiées pour corriger les éventuels problèmes de sécurité. Avec les mises à jour, il y a une règle à suivre : le plus tôt sera le mieux.

6. Attention aux signes avant-coureurs

Si, malgré ces recommandations, vous remarquez que votre ordinateur a ralenti ou tombe en panne de manière répétée, que votre disque dur est excessivement sollicité, que vous êtes inondés de fenêtres pop-up ou qu'il y a eu des modifications à la configuration de votre navigateur (exemple : une nouvelle page d'accueil), communiquez immédiatement avec votre équipe d'assistance technique. Les spécialistes vous guideront tout au long du processus de balayage de votre ordinateur ou, s'ils utilisent un outil comme Wayk Now, ils peuvent gérer ce processus de leur côté pendant que vous attendez (et que vous espérez que tout ira pour le mieux!).

Mythes

En terminant, j'aimerais souligner deux mythes persistants sur les logiciels malveillants qui continuent de causer des maux de tête à bien des gens:

Mythe 1 : Si vous installez un antivirus sur votre ordinateur, vous bloquerez tous les virus.

FAUX! Les logiciels antivirus ne sont pas une solution à toute épreuve contre les logiciels malveillants. Leur efficacité dépend en grande partie de leur robustesse et d'à quel point ils sont à jour. De plus, tout antivirus doit être complété par d'autres outils comme un anti-maliciel et un antilogiciel-espion.

Mythe 2 : Si vous utilisez une connexion sécurisée comme le Wi-Fi chiffré, vous êtes toujours protégé contre les logiciels espions.

FAUX! L'utilisation d'une connexion sécurisée ne vous protégera pas contre les logiciels espions. Il se peut même qu'il ne vous protège pas contre les pirates informatiques. C'est pourquoi vous devez toujours utiliser un bon RPV lors d'une connexion par Wi-Fi.

À retenir

L'univers des logiciels malveillants prend de l'ampleur à mesure que les cybercriminels créent de nouvelles menaces et des variantes aux menaces existantes. Heureusement, si vous connaissez bien vos ennemis, vous n'aurez même pas besoin de dragon ou de feu pour les combattre! Vous n'avez qu'à suivre les bonnes pratiques et ne plus croire à ces deux mythes et vous serez en sécurité!