OUCH! | Juin, 2018

La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

Arrêtez les logiciels malveillants

Vue d'ensemble

Vous avez probablement entendu parler de termes tels que virus, cheval de Troie, ransomware ou rootkit lorsque les gens parlent de cybersécurité. Ce sont différents types de programmes malveillants, appelés des logiciels malveillants, que les cybercriminels utilisent pour infecter les ordinateurs et les périphériques. Une fois installés, ils peuvent faire ce qu'ils veulent. Apprenez ce qu'est un logiciel malveillant, quel danger il représente et, surtout, ce que vous pouvez faire pour vous en protéger.

Qu'est-ce qu'un Malware?

Autrement dit, les logiciels malveillants sont des logiciels - des programmes informatiques - utilisés pour effectuer des actions malveillantes. Le terme Malware est une combinaison du mot malveillant et logiciel. Les cybercriminels installent des logiciels malveillants sur vos ordinateurs ou périphériques pour en prendre le contrôle. Une fois installé, un logiciel malveillant peut permettre aux criminels d'espionner vos activités en ligne, de voler vos mots de passe ou vos fichiers ou d'utiliser votre système pour attaquer d'autres personnes. Les logiciels malveillants peuvent même prendre le contrôle de vos propres fichiers, exigeant que vous payiez une rançon pour les récupérer. Beaucoup de gens croient que les logiciels malveillants sont un problème uniquement pour les ordinateurs Windows. Malheureusement, un logiciel malveillant peut infecter n'importe quel appareil, des ordinateurs Mac, des smartphones jusqu'aux DVR et aux caméras de sécurité. Plus d'ordinateurs et d'appareils sont infectés par les cybercriminels, plus ces derniers peuvent gagner d'argent. Par conséquent, tout le monde est une cible, vous y compris.

Protégez-vous - Arrêtez les logiciels malveillants

Vous pouvez penser que tout ce que vous avez à faire est d'installer un programme de sécurité comme un logiciel anti-virus et de ce fait êtes sûr de ne pas être infecté. Malheureusement, l'antivirus ne peut pas arrêter tous les logiciels malveillants. Les cybercriminels développent constamment de nouveaux logiciels malveillants plus sophistiqués qui peuvent échapper à la détection. À leur tour, les fournisseurs d'antivirus mettent constamment à jour leurs produits avec de nouvelles capacités pour détecter les logiciels malveillants. À bien des égards, c'est devenu une course aux armements, et les criminels ont généralement une longueur d'avance. Puisque vous ne pouvez pas compter uniquement sur un antivirus, voici d'autres mesures à prendre pour vous protéger:

Les cybercriminels infectent souvent les ordinateurs ou les appareils en exploitant les vulnérabilités de votre logiciel. Plus votre logiciel est récent, moins les vulnérabilités de votre système sont nombreuses et plus il est difficile pour les cybercriminels de les infecter. Assurez-vous que vos systèmes d'exploitation, applications, navigateurs, ainsi que les appareils sont toujours à jour. Le moyen le plus simple de vous en assurer est d'activer la mise à jour automatique dans la mesure du possible.

Les cybercriminels infectent souvent les ordinateurs ou les appareils mobiles en créant de faux programmes informatiques ou applications mobiles, en les publiant sur Internet, puis en les téléchargeant et en les installant. Ne téléchargez et n'installez que des programmes ou des applications provenant de boutiques en ligne de confiance. De même, évitez les applications mobiles qui sont toutes nouvelles, qui ont peu de critiques positives, qui sont rarement mises à jour ou qui ont été téléchargées par un petit nombre de personnes. Vous n'utilisez plus un programme informatique ou une application mobile? Supprimez-le.

Les cybercriminels incitent souvent les gens à installer des logiciels malveillants pour eux. Par exemple, ils peuvent vous envoyer un e-mail qui semble légitime et qui contient une pièce jointe ou un lien. Peut-être que l'email semble provenir de votre banque ou d'un ami. Cependant, si vous ouvrez le fichier joint ou cliquez sur le lien, vous activez un code malveillant qui installe un logiciel malveillant sur votre système. Si un message crée un fort sentiment d'urgence ou semble trop beau pour être vrai, il peut s'agir d'une attaque. Soyez méfiant, le bon sens est souvent votre meilleure défense.

Sauvegardez régulièrement votre système et vos fichiers sur des services Cloud ou stockez vos sauvegardes hors ligne, par exemple sur des disques externes déconnectés. Cela protège vos sauvegardes au cas où les logiciels malveillants tentent de les chiffrer ou de les effacer. Les sauvegardes sont essentielles, elles sont souvent le seul moyen de récupérer une infection par un logiciel malveillant.

En fin de compte, la meilleure façon de se défendre contre les logiciels malveillants est de garder tous vos logiciels et appareils à jour, d'installer un logiciel antivirus de confiance lorsque cela est possible et d'être à l'affût de toute tentative d'infection de votre propre système. Lorsque tout le reste échoue, les sauvegardes régulières sont souvent le seul moyen de tout récupérer.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Lenny Zeltser *combat les logiciels malveillants en créant des produits de sécurité pour les terminaux à Minerva Labs et est également enseignant à l'Institut SANS. Lenny est actif sur Twitter en tant que @lennyzeltser et écrit un blog de sécurité sur zeltser.com.*

Sources

Ransomware :	https://www.sans.org/u/EdI
Sauvegardes :	https://www.sans.org/u/EdN
Arrêtez les phishing :	https://www.sans.org/u/EdS

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet