OUCH! | Février 2014

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

OUCH!

Dans ce numéro...

- Qu'est-ce qu'un Malware
- Qui et Pourquoi
- Savoir se protéger

Qu'est-ce qu'un Malware

Vue d'ensemble

Vous avez peut-être déjà entendu parler de certains termes tels que virus, ver, cheval de Troie ou rootkit quand les gens parlent de cybersécurité. Ces termes décrivent les types de programmes utilisés par les cybercriminels pour infecter et prendre le contrôle d'ordinateurs et d'appareils mobiles. Aujourd'hui, ces différents termes sont maintenant simplement appelés malware. Dans ce numéro, nous allons vous expliquer qu'est-ce qu'un malware, qui le développe et pourquoi, et ce que vous pouvez faire pour vous en protéger.

Editeur invité

Lenny Zeltser se concentre sur la sauvegarde des opérations informatiques des clients de NCR Corp et enseigne la lutte contre les malwares à l'Institut SANS. Lenny est actif sur Twitter à **@lennyzeltser** et écrit un blog sur la sécurité à **blog.zeltser.com**.

Qu'est-ce qu'un Malware

En termes simples, un malware est un logiciel, un programme d'ordinateur utilisé pour effectuer des actions malveillantes. En fait, le terme malware est une combinaison du mot malveillant (malicious) et logiciel (software). L'objectif final de la plupart des cybercriminels consiste à installer des malwares sur vos ordinateurs ou périphériques mobiles. Une fois installés, ces attaquants peuvent potentiellement en prendre le contrôle total. Beaucoup de gens ont la fausse idée que les malwares sont un problème impliquant uniquement les ordinateurs Windows. Alors que Windows est largement utilisé, et donc une cible importante, les malwares peuvent infecter n'importe quel périphérique informatique, y compris les smartphones et les tablettes. En effet, la prévalence de logiciels malveillants destinés à infecter les appareils mobiles est en constante augmentation. En outre, n'oubliez pas que tout le monde est une cible, y compris vous. Plus il y aura d'ordinateurs et d'appareils mobiles infectés par les cybercriminels, plus ils pourront gagner de l'argent. Ces criminels ne se soucient généralement pas de qui ils infectent, tant qu'il s'agit du plus grand nombre de personnes possible.

Qui et Pourquoi

Le Malware n'est plus seulement créé par quelques curieux ou des pirates amateurs, mais par des cybercriminels sophistiqués que les malwares aident à atteindre des objectifs spécifiques. Ces objectifs peuvent inclure le vol de données confidentielles, la récolte d'identifiants et de mots de passe, l'envoi de courriels de spam, des attaques par déni de service, de l'extorsion ou du vol d'identité. Par exemple, les logiciels malveillants connus comme Cryptolocker sont utilisés par les cybercriminels pour infecter et chiffrer tous les fichiers sur votre ordinateur. Une fois que ces derniers sont infectés et chiffrés, les cybercriminels exigent alors une rançon en échange du déchiffrement de vos fichiers.

Qu'est-ce qu'un Malware

Les gens qui créent, déploient et bénéficient de logiciels malveillants peuvent varier de particuliers agissant seuls à des groupes criminels organisés ou encore à des organismes gouvernementaux. En outre, les personnes qui créent aujourd'hui des logiciels malveillants sophistiqués sont souvent dédiées à cet effet, le développement de logiciels malveillants constitue un emploi à temps plein. En fait, une fois qu'ils développent leurs logiciels malveillants, ils les vendent souvent à d'autres individus ou organisations et fournissent des mises à jour et du support régulier à leurs «clients». Une fois acheté, d'autres criminels gagnent de l'argent en installant le logiciel malveillant sur des millions de systèmes de victimes confiantes, en créant un botnet de systèmes infectés. Ce botnet devient alors une armée commandée à distance, que le cybercriminel peut alors utiliser à ses propres fins, ou encore vendre les ordinateurs infectés à d'autres cybercriminels.

La meilleure façon de vous protéger contre les logiciels malveillants est de vous assurer que vos appareils sont mis à jour, si possible qu'ils aient un antivirus actuel, et, enfin, d'être à l'affût des attaques.

Savoir se protéger

L'étape usuelle pour protéger vos ordinateurs et appareils mobiles contre les logiciels malveillants est d'installer un logiciel antivirus fourni par un éditeur de confiance. L'antivirus, parfois appelé anti-malware, est un logiciel de sécurité conçu pour détecter et arrêter les logiciels malveillants. Cependant, un antivirus ne peut pas bloquer ou supprimer tous les logiciels malveillants. Les Cyber-agresseurs ne cessent d'innover, de développer de nouvelles attaques de plus en plus sophistiquées qui peuvent contourner les programmes antivirus. À leur tour, les éditeurs d'antivirus mettent constamment à jour leurs produits avec de nouvelles capacités pour détecter de nouveaux logiciels malveillants. À bien des égards, ceci est devenu une course aux armements, les deux parties tentant de déjouer l'autre. Malheureusement, les cybercriminels prennent presque toujours le dessus. En tant que tel, n'oubliez pas que si tout antivirus peut détecter et bloquer un grand nombre de logiciels malveillants, les pirates créent toujours de nouvelles versions qui ne seront pas détectées. En conséquence, vous ne pouvez pas compter uniquement sur l'antivirus pour vous protéger, vous devez prendre des mesures supplémentaires pour vous protéger.

Tout d'abord, assurez-vous que vos systèmes d'exploitation et les applications sont configurés pour installer automatiquement les mises à jour de sécurité. Plus récent est le logiciel, plus il est difficile pour les cybercriminels d'infecter vos ordinateurs ou périphériques mobiles.

Deuxièmement, n'oubliez pas que vous êtes l'un des meilleurs moyens de défense contre les logiciels malveillants. Les infections de logiciels malveillants impliquent bien souvent l'ingénierie sociale, qui n'est rien de plus qu'un attaquant vous dupant ou vous trompant pour que vous installiez le malware pour lui. Un exemple courant est les attaques par phishing : ce sont des courriels qui semblent légitimes, mais qui sont en fait des faux conçus pour vous

Qu'est-ce qu'un Malware

inciter à infecter votre ordinateur. Par exemple, un cybercriminel peut vous envoyer un e-mail prétendant provenir de votre banque vous demandant de cliquer sur un lien. Si vous cliquez sur le lien, vous êtes redirigé vers un site qui tente automatiquement de pirater et infecter votre ordinateur. Il se peut qu'il vous envoie aussi un avis stipulant que votre colis ne peut être livré et vous demande d'ouvrir le document de suivi joint, qui, lorsqu'il est ouvert va infecter votre ordinateur.

Les attaques par ingénierie sociale peuvent aussi avoir lieu sur d'autres technologies, telles que votre téléphone. Par exemple, les pirates peuvent vous appeler en se faisant passer pour le support technique Microsoft en vous informant que votre ordinateur est infecté. Ceci est un mensonge, il y'a de bonnes chances que votre ordinateur se porte bien. Leur but est de vous tromper en vous faisant croire que vous êtes infecté pour vous inciter à leur donner accès à distance à votre système ou vous faire acheter leur logiciel de sécurité qui n'est rien de plus qu'un logiciel malveillant. Utilisez votre bon sens. Si un appel téléphonique ou un message semble bizarre, suspect ou trop beau pour être vrai, le plus probable est qu'il le soit.

En fin de compte, la meilleure façon de se défendre contre les logiciels malveillants est de garder votre logiciel à jour, d'installer des logiciels antivirus dignes de confiance auprès de fournisseurs bien connus et d'être vigilant pour quiconque tente de vous tromper pour infecter votre ordinateur.

Version Française

La division sécurité de ANSWER S.A. offre des services de Conseil, d'Audit et d'Architecture en sécurité des systèmes d'information. Ces activités sont accompagnées d'une veille active sur les solutions de sécurité du marché permettant ainsi à ses consultants de répondre efficacement aux problématiques de ses clients.
Pour en savoir plus, veuillez vous référer aux liens suivants :
http://www.answersolutions.ch et http://answersecurity.com/

Ressources

Attaques par Phishing OUCH :

http://www.securingthehuman.org/resources/newsletters/ouch/2013#february2013

Sept points pour sécuriser son ordinateur OUCH :

http://www.securingthehuman.org/resources/newsletters/ouch/2012#december2012

Poster « Vous êtes une cible » :

http://www.securingthehuman.org/resources/posters

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner
Traduit par : Julien Bouillot, Marilyn Combet