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

OUCH!

Dans ce numéro...

Qu'est-ce qu'un Malware

Vue d'ensemble

Vous avez sans doute déjà entendu des termes tels que Virus, Cheval de Troie, ransomware ou rootkit lorsque des personnes discutent de cybersécurité. Tous ces mots décrivent en fait la même chose : des types de programmes utilisés par des criminels pour infecter vos ordinateurs et appareils. Le terme commun employé pour décrire tous ces différents programmes est le mot Malware. Dans ce numéro, nous allons vous expliquer ce qu'est un Malware, qui le développe et pourquoi, et bien sûr le plus important, qu'est-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 **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). Les Cybercriminels installent des Malwares sur vos ordinateurs et appareils pour en prendre le contrôle total et ainsi avoir accès à ce qu'ils contiennent. Ces attaquants peuvent utiliser les Malwares installés pour espionner vos activités en ligne, voler vos mots de passe et fichiers ou encore utiliser votre système pour attaquer d'autres cibles. Les Malwares peuvent également vous refuser l'accès à vos propres fichiers, en vous demandant de payer une rançon afin que vous puissiez en reprendre le contrôle.

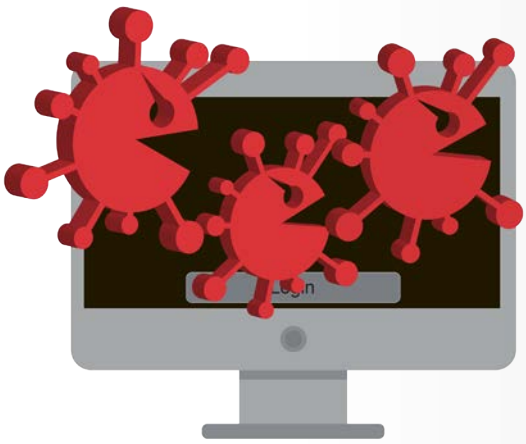
Beaucoup de gens ont la fausse idée que les Malwares sont un problème impliquant uniquement les ordinateurs Windows. Alors que Windows est largement utilisé, et donc une cible importante, les Malwares peuvent infecter n'importe quel périphérique informatique, y compris les ordinateurs Macintosh, les smartphones et tablettes. Plus il y'aura d'ordinateurs et d'appareils mobiles infectés par les cybercriminels, plus ces derniers pourront gagner de l'argent. C'est pourquoi, tout le monde peut être une cible potentielle, vous y compris.

Qui développe les Malwares?

Le Malware n'est plus seulement créé par quelques curieux ou des pirates amateurs, mais par des cybercriminels sophistiqués. Leur but est de gagner de l'argent en infectant votre ordinateur ou autre dispositif, peut être en vendant des données qu'ils vous ont volées, en envoyant des spams par mail, en lançant des attaques par déni de service ou encore en vous extorquant des fonds. Le type

Qu'est-ce qu'un Malware

de personnes qui créent, déploient et bénéficient de logiciels malveillants peut varier : on effet, il peut s'agir de particuliers agissant seuls ou des groupes criminels organisés ou encore 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 plein temps. De plus, une fois leur Malware développé, ils le vendent souvent à d'autres individus ou organisations, et fournissent des mises à jour et du support régulier à leurs « clients ».



Protégez-vous contre les logiciels malveillants en étant sceptique sur les messages suspects, en gardant vos appareils mis à jour et en ayant des anti-virus actuels installés lorsque cela est possible.

Savoir se protéger

L'étape usuelle pour vous protéger est d'installer un logiciel anti-virus à partir de fournisseurs de confiance. Ces outils, parfois appelés logiciels anti-virus, sont conçus pour détecter et arrêter les logiciels malveillants. Cependant, les anti-virus ne sont pas en mesure de bloquer ou de supprimer tous les programmes malveillants. Les cybercriminels ne cessent d'innover, de développer de nouveaux et logiciels sophistiqués malveillants qui peuvent échapper à la détection. À leur tour, les éditeurs d'anti-virus mettent constamment à jour leurs produits avec de nouvelles capacités pour détecter les logiciels malveillants. À bien des égards, ceci est devenu une course aux armements, les deux parties tentant de déjouer l'autre. Malheureusement, les cybercriminels ont généralement une longueur d'avance. Puisque vous ne pouvez pas compter sur l'anti-virus seul, voici des étapes supplémentaires que vous devez prendre en considération pour vous protéger:

- Les cybercriminels infectent souvent des ordinateurs ou des appareils en exploitant les failles dans leur logiciel. Plus récent est votre logiciel, moins de vulnérabilités vos systèmes auront et plus il sera difficile pour les cybercriminels de les infecter. Par conséquent, assurez-vous que vos systèmes d'exploitation, applications et appareils sont activés pour installer automatiquement les mises à jour.
- Une façon courante pour les cybercriminels d'infecter les appareils mobiles est de créer une fausse application mobile, la publier sur Internet, et ensuite amener les gens à la télécharger et à l'installer. En tant que tel, ne téléchargez et installez seulement des applications à partir de magasins en ligne de confiance. En outre, installez uniquement des applications mobiles qui ont été mises en ligne pendant une longue période, téléchargées par un grand nombre de personnes, et qui a de nombreuses critiques positives.
- Sur les ordinateurs, utilisez un compte standard dont les droits sont limités plutôt que des comptes privilégiés tels que «Administrateur» ou «root». Ceci fournit une protection supplémentaire en empêchant de nombreux types de logiciels malveillants d'être en mesure de s'installer.

Qu'est-ce qu'un Malware

- Les cybercriminels incitent souvent les gens à installer des logiciels malveillants à leur place. Par exemple, ils pourraient vous envoyer un courriel qui semble légitime contenant une pièce jointe ou un lien. Ce courriel peut sembler provenir de votre banque ou d'un ami. Toutefois, si vous deviez ouvrir le fichier joint ou cliquer sur le lien, vous activeriez alors le code malveillant qui installe des logiciels malveillants sur votre système. Si un message crée un fort sentiment d'urgence, est source de confusion, ou semble trop beau pour être vrai, il pourrait s'agir d'une attaque. Soyez suspicieux, le bon sens est souvent votre meilleur moyen de défense.
- Faites régulièrement une sauvegarde de votre système et des fichiers vers des services basés sur le Cloud, ou stockez vos sauvegardes hors ligne tels que sur des disques externes déconnectés. Cela protège vos sauvegardes au cas où des logiciels malveillants tenteraient de crypter ou de les effacer. Les sauvegardes sont essentielles, elles sont souvent la seule façon de récupérer vos données à partir d'un logiciel malveillant.

En fin de compte, la meilleure façon de vous défendre contre les logiciels malveillants est de garder votre logiciel à jour, d'installer un logiciel anti-virus de confiance auprès de fournisseurs bien connus et d'être vigilant sur quiconque tenterait de vous tromper ou vous inciterait à infecter votre propre système.

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.answer.ch et http://answersecurity.com/

Sources

Phishing / l'hameçonnage : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201512_fr.pdf

Ingénierie sociale : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201411_fr.pdf

Utiliser les applications mobiles en toute sécurité : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201501_fr.pdf

Sécuriser votre nouvelle tablette : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201601_fr.pdf

Sauvegardes : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_fr.pdf

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