OUCH! | Décembre 2014

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

OUCH!

Dans ce numéro...

Qu'est-ce qu'un Anti-Virus?

Vue d'ensemble

Un Anti-Virus est un programme de sécurité que vous installez sur votre ordinateur ou sur votre appareil mobile pour le protéger contre l'infection de logiciels malveillants. Le terme "malware" est une expression « fourre-tout » désignant tout type de logiciels malveillants tels que les virus, les vers, les chevaux de Troie et les logiciels espions. En fait, le terme malware vient de la combinaison des mots malveillant (malicious) et logiciel (software). Si votre ordinateur est infecté par des logiciels malveillants, un cyberattaquant peut capturer tous vos frappes clavier, voler vos documents ou encore utiliser votre ordinateur pour en attaquer d'autres. Contrairement à ce que certains croient, tout système d'exploitation, y compris Mac OS X et Linux, est susceptible d'être infecté.

Editeur invité

Jake Williams est le fondateur de Rendition Infosec (**www.renditioninfosec.com**) et est instructeur et auteur de cours certifié SANS. Il est actif sur Twitter **@MalwareJake** et tient également un blog **malwarejake.blogspot.com**.

Vous pouvez acheter un logiciel Anti-Virus en tant que solution autonome, il est aussi souvent inclus dans le cadre d'une suite de sécurité. Le problème est que l'Anti-Virus ne peut dès lors plus faire face aux cyberattaquants, qui sont en constante évolution et libèrent de nouveaux types de logiciels malveillants. Il y'a tellement de nouvelles versions de logiciels malveillants publiés chaque jour, qu'aucun programme Anti-Virus ne peut détecter et vous protéger contre tous. Voilà pourquoi il est important pour vous de comprendre que tout Anti-Virus que vous possédez pour protéger votre ordinateur, ne peut pas détecter ou arrêter tous les types de logiciels malveillants. Pour mieux comprendre pourquoi, regardons comment la plupart de ces programmes fonctionnent.

Comment les Anti-Virus fonctionnent-ils?

En général, il y'a deux manières pour les logiciels Anti-Virus d'identifier des logiciels malveillants; la détection par signature et la détection comportementale. La détection par signature fonctionne comme le système immunitaire humain. Il scanne votre ordinateur à la recherche de caractéristiques ou de signatures de programmes malveillants connus. Il le fait en se référant à un dictionnaire de logiciels malveillants connus, si quelque chose sur votre ordinateur correspond à un modèle dans le dictionnaire, le programme tente de le neutraliser. Comme le système immunitaire humain, l'approche dictionnaire nécessite des mises à jour, tout comme le vaccin contre la grippe, pour se protéger contre de nouvelles souches de logiciels malveillants. L'Anti-Virus peut seulement protéger contre ce qu'il reconnaît comme dangereux. Le problème majeur est que les cyberattaquants développent de nouveaux logiciels malveillants si vite que les éditeurs d'Anti-

Qu'est-ce qu'un Anti-Virus?

Virus ne peuvent pas suivre. Par conséquent, peu importe la façon dont votre Anti-Virus a été mis à jour, il y'a toujours de nouvelles variantes de logiciels malveillants qui peuvent potentiellement contourner votre logiciel Anti-Virus.

Bien que l'Anti-Virus soit une partie importante de votre sécurité, il ne peut pas détecter ou arrêter toutes les attaques. En fin de compte, vous êtes la meilleure défense, en complément de la technologie.

Avec la détection comportementale, l'Anti-Virus ne cherche pas à identifier les programmes malveillants connus, mais surveille le comportement des logiciels installés sur votre ordinateur. Quand un programme agit étrangement, comme par exemple en tentant d'accéder à un fichier protégé ou à modifier un autre programme, un logiciel Anti-Virus basé sur la détection comportementale repère l'activité suspecte et vous avertit. Cette approche offre une protection contre des types de logiciels malveillants qui n'existent encore dans aucun dictionnaire. Le problème avec cette approche est qu'elle peut générer de fausses alertes. En tant qu'utilisateur de l'ordinateur, vous ne pouvez pas être sûr de ce qu'il faut autoriser ou non et au fil du temps, vous êtes susceptible de devenir insensible à tous ces avertissements. Vous pourriez être tenté de cliquer sur «Accepter» sur chaque avertissement, laissant ainsi votre ordinateur ouvert aux attaques et infections. En outre, au moment où le comportement est détecté, le malware est déjà probablement exécuté sur votre machine et vous ne savez pas quelles actions le malware a pris avant que le logiciel Anti-Virus l'identifie.

L'Anti-Virus est une partie importante de la sécurisation de votre ordinateur et de vos périphériques mobiles. Chaque fois que possible, nous vous recommandons de l'installer et de l'utiliser activement. Cependant, le point essentiel à retenir est que, indépendamment de la façon dont votre Anti-Virus fonctionne, il ne peut jamais vous protéger contre tous les types de logiciels malveillants. En fin de compte, vous êtes, en complément de la technologie, la meilleure défense contre les cyberagresseurs d'aujourd'hui.

Conseils à propos des Anti-Virus

1. Obtenez un logiciel Anti-Virus à partir de sources, et d'éditeurs de confiance connus. Il est courant pour les cyberattaquants de distribuer de faux programmes Anti-Virus qui sont en fait des logiciels malveillants.
2. Assurez-vous que vous avez la dernière version de votre logiciel Anti-Virus installée et active, que votre cotisation annuelle est payée et que, votre Anti-Virus est configuré pour se mettre à jour automatiquement. Si votre ordinateur a été déconnecté ou mis hors tension pendant un certain temps, votre logiciel Anti-Virus doit se mettre à jour lorsque vous le rallumez ou le reconnectez à Internet. Ne différez pas ces mises à jour.
3. Assurez-vous que votre Anti-Virus scanne automatiquement vos médias portables, tels que les clés USB, et assurez-vous que la protection en temps réel est activée.

Qu'est-ce qu'un Anti-Virus?

4. Faites attention aux avertissements et aux alertes à l'écran générés par votre logiciel Anti-Virus. La plupart des alertes comprennent la possibilité d'obtenir plus d'informations ou une recommandation sur ce qu'il faut faire ensuite. Si vous obtenez une alerte sur un ordinateur de travail fourni, assurez-vous de contacter immédiatement le service d'assistance ou votre superviseur.
5. Ne désactivez pas et ne désinstallez pas votre logiciel Anti-Virus parce que vous sentez qu'il ralentit votre ordinateur, bloque un site web, ou vous empêche d'installer une application ou un programme. La désactivation de votre Anti-Virus vous expose à des risques inutiles et pourrait entraîner un grave incident de sécurité. Si les problèmes persistent sur un ordinateur de travail, contactez votre service d'assistance. Si les problèmes persistent sur votre ordinateur personnel, essayez de contacter votre vendeur d'Anti-Virus, en visitant son site web pour plus d'informations ou le remplacement de votre Anti-Virus avec un autre produit.
6. N'installez pas plus d'un programme Anti-Virus sur votre ordinateur. Cela serait susceptible de causer des conflits entre eux et pourrait même réduire la sécurité de votre ordinateur.
7. Apprenez à reconnaître les alertes de votre logiciel Anti-Virus. Les cyberattaquants peuvent mettre en place des sites Web malveillants qui affichent de fausses alertes très réalistes et proposent de vous aider à «réparer» votre ordinateur. Cliquer sur les liens ou les boutons de ces sites peut réellement nuire à 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

Les comparaisons de produits Anti-Virus:	http://www.av-test.org/fr/
Ingénierie sociale:	http://www.securingthehuman.org/resources/newsletters/ouch/2014#november2014
Attaques par phishing:	http://www.securingthehuman.org/resources/newsletters/ouch/2013
J'ai été hacké, que dois-je faire maintenant?:	http://www.securingthehuman.org/resources/newsletters/ouch/2014

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