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

OUCH!

Dans ce numéro...

Oui, vous êtes réellement une cible

Vue d'ensemble

Une fausse idée commune dans l'esprit de beaucoup de personnes est qu'ils ne sont en rien une cible pour la cybercriminalité : eux ou leurs ordinateurs n'ont pas de valeur. Rien ne pourrait être plus éloigné de la vérité. Si vous avez un ordinateur, un appareil mobile, un compte en ligne, une adresse e-mail, une carte de crédit, ou que vous vous engagiez dans un autre type d'activité en ligne, vous valez de l'argent pour les cybercriminels. Dans ce numéro, nous expliquons pourquoi vous êtes une cible, comment vous êtes attaqué, et ce que vous pouvez faire pour vous protéger.

Editeur invité

Eric Conrad est le Président et le CTO de Backshore Communications et est le principal auteur de la Seconde Édition des Guides d'Étude CISSP et de la Seconde Édition de Eleventh Hour CISSP. Il est également le co-auteur pour le SANS Institute du cours Surveillance Continue et Opérations de Sécurité (SEC511).

Pourquoi vous êtes une cible

Des crimes tels que la fraude, le vol d'identité ou l'extorsion existent depuis aussi longtemps qu'il y a des civilisations, et font partie de notre vie quotidienne. Le but d'un criminel a toujours été le même : engranger autant d'argent que possible, aussi facilement que possible, et avec le moins de risques possibles. Traditionnellement, cela s'avérait plus difficile parce que les criminels étaient souvent limités par leur emplacement et devaient interagir physiquement avec leurs victimes potentielles. Cela ne limitait pas seulement qui ciblaient les criminels, mais les criminels étaient également exposés à beaucoup de risques. Toutefois, la criminalité a radicalement changé avec l'avènement d'Internet et de la technologie en ligne. Maintenant, les cybercriminels peuvent facilement cibler presque tout le monde partout sur la planète, à moindre coût, et avec très peu de risques. En outre, les cybercriminels sont devenus très organisés et performants, ce qui leur permet d'être plus efficaces que jamais.

En fin de compte, les cybercriminels savent que plus ils volent de cartes de crédit, plus ils peuvent pirater des comptes bancaires, ou encore plus de mots de passe ils compromettent, plus ils peuvent gagner d'argent. Ils vont littéralement tenter de pirater toute personne connectée à Internet, vous y compris. Le fait de pirater des millions de personnes à travers le monde semble représenter beaucoup de travail, mais cela s'avère étonnamment facile car les cybercriminels utilisent des outils automatisés pour faire tout le travail. Par exemple, ils peuvent constituer une base de données comportant des millions d'adresses e-mail et utiliser un outil automatisé pour envoyer un message de phishing à chacune de ces adresses. L'envoi d'emails ne coûte presque rien aux criminels : ils utilisent tout simplement les autres ordinateurs piratés, peut-être même le vôtre, pour faire leur sale boulot. C'est également un autre exemple qui démontre bien que vos appareils ont de la valeur, à défaut d'autre chose, ils peuvent être utilisés pour pirater ou nuire à autrui. En fin de compte, ces criminels ne savent

Oui, vous êtes réellement une cible

pas qui va être victime de leurs attaques par e-mail, en revanche, ils savent que plus d'e-mails ils envoient, plus de victimes il y'aura. Ou encore les criminels vont peut-être littéralement analyser chaque ordinateur sur Internet (en utilisant une fois de plus des ordinateurs piratés pour effectuer l'analyse), à la recherche de tous les ordinateurs ou appareils qu'ils peuvent pirater. Rappelez-vous que vous n'êtes pas choisi parce que vous êtes spécial. Au contraire, ces criminels ciblent tous ceux qu'ils peuvent, ce qui peut vous arriver à vous aussi.

Vous ne le réalisez peut-être pas, mais vos appareils et vos informations ont une valeur inestimable pour les cybercriminels à travers le monde.

Se protéger

Lorsque les cybercriminels tentent de pirater des personnes dans le monde, ils le font généralement en utilisant des méthodes relativement simples. Heureusement, en suivant quelques étapes basiques, vous pouvez aussi vous prémunir de ces méthodes et vous protéger. Certaines mesures que nous préconisons sont les suivantes:

- **Vous-même**: Finalement, vous êtes la première ligne de défense contre les cybercriminels. De nombreuses attaques commencent par un cybercriminel essayant de vous tromper, comme en vous incitant à ouvrir une pièce jointe infectée ou en vous dupant pour que vous donniez votre mot de passe par téléphone. Le bon sens est votre meilleure défense: si quelque chose vous semble étrange, suspect ou trop beau pour être vrai, il s'agit probablement d'une attaque.

- **Mise à jour**: Assurez-vous que n'importe quel ordinateur ou appareil mobile que vous utilisez est entièrement mis à jour et dispose de tous les derniers correctifs. Ce n'est pas seulement important pour votre système d'exploitation, mais pour toutes les applications ou plugins que vous utilisez. Le fait de toujours garder vos systèmes et applications à jour vous aide à vous protéger contre les attaques les plus courantes.

- **Les mots de passe**: Utilisez un mot de passe fort unique pour chacun de vos comptes. De cette façon, quand un site Web que vous utilisez est piraté et que tous les mots de passe de ce site sont par conséquent compromis (y compris le vôtre), vos autres comptes restent protégés. Assurez-vous également que tous vos différents appareils sont protégés par un mot de passe fort unique, un code PIN ou un autre type de mécanisme de verrouillage. Pour garder une trace de tous vos mots de passe différents en toute sécurité, nous vous recommandons d'utiliser un gestionnaire de mot de passe.

Oui, vous êtes réellement une cible

- **Cartes de crédit**: Vérifiez souvent vos états financiers, nous vous recommandons de le faire au moins chaque semaine (chaque mois ne suffit pas). Dès que vous voyez des transactions non autorisées sur votre carte de crédit, signalez-le immédiatement à l'émetteur de votre carte. Si votre banque vous permet de configurer des alertes par e-mail ou par messages sur votre téléphone pour les transactions anormalement élevées ou impaires, utilisez-les pour avoir une notification encore plus rapide de toute activité suspecte.

- **Votre réseau**: Sécurisez votre point d'accès réseau Wi-Fi à la maison avec un mot de passe administrateur fort et assurez-vous que votre réseau Wi-Fi nécessite un mot de passe pour que quiconque puisse le rejoindre. Assurez-vous également que vous savez quels sont les appareils que vous avez connectés à votre réseau domestique et qu'ils sont tous mis à jour.

- **Médias sociaux**: Plus vous publiez d'informations en ligne, plus vous pouvez vous exposez à des risques. Non seulement les informations que vous publiez peuvent aider les cybercriminels à vous cibler et vous duper plus facilement, mais les informations que vous postez peuvent réellement faire de vous une cible de valeur.

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

OUCH! Gestionnaires de mots de passe:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Sécuriser votre réseau domestique:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH ! Attaques par phishing:	http://www.securingthehuman.org/ouch/2013#february2013
Poster : Vous êtes une cible:	http://www.securingthehuman.org/resources/posters

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