OUCH! Février 2021

OUCH!

SANS SECURITY AWARENESS

Votre publication mensuelle de conscientisation à propos de la Sécurité

Je suis piraté. Quoi faire maintenant?

Ai-je été piraté?

Peu importe votre niveau de sécurité, tôt ou tard vous pourriez avoir un accident et être piraté. Voici quelques indices qui pourrait révéler que vous avez été piraté et si tel est le cas ce que vous pouvez faire.

Vos comptes en ligne

- Votre famille ou vos amis disent qu'ils reçoivent des messages inhabituels ou des invitations de votre part que vous n'avez pas envoyé.
- Votre mot de passe pour un compte ne fonctionne plus, même si vous êtes certain que c'est le bon.
- Vous recevez des alertes de sites web indiquant que quelqu'un s'est connecté dans votre compte alors que vous savez que vous ne vous êtes pas connecté. Ne cliquez pas sur aucun liens provenant de telles alertes pour vérifier votre compte; tapez plutôt l'adresse du site web vous même dans votre navigateur, utiliser vos favoris existant ou accéder votre compte depuis une application mobile.

Votre ordinateur ou appareil cellulaire

- Votre logiciel d'antivirus affiche une alerte que votre système est infecté. Assurez vous que c'est votre logiciel antivirus qui génère l'alerte et non une fenêtre de notification d'un site web qui essaie de vous berner en vous demandant d'appeler un numéro ou d'installer quelque chose d'autre. Pas certain? Ouvrez et vérifier votre logiciel d'antivirus afin de confirmer que votre ordinateur est vraiment infecté.
- Vous avez une fenêtre indiquant que votre ordinateur à été encrypté et que vous devez payer une rançon afin de récupérer vos fichiers.
- Les applications semble s'arrêter aléatoirement ou démarrent très lentement.
- Lorsque vous naviguez sur le web, vous êtes souvent redirigé vers des pages que vous ne vouliez pas visiter ou de nouvelles pages non sollicitées s'affichent.

Financier

- Il y a des transactions suspectes ou inconnues sur votre carte de crédit ou compte bancaire que vous savez n'avoir faite.

Quoi faire maintenant? - Comment reprendre le contrôle

Si vous croyez avoir été piraté, rester calme; vous allez passer au travers. Si le piratage est relié à votre travail, n'essayez pas de régler le problème vous-même; rapporter l'incident immédiatement. Si c'est un système ou un compte qui vous appartient, voici quelques étapes vous pouvez suivre:

- **Récupérer vos comptes en ligne:** Si vous avez encore accès à votre compte, connectez-vous depuis un ordinateur que vous êtes confiant qu'il ne soit pas infecté et réinitialisez votre mot de

passe. Une fois connecté, assurez-vous de définir un nouveau mot de passe, qui n'est pas utilisé ailleurs et complexe, le plus long possible. Rappelez-vous, chacun de vos comptes doit avoir un mot de passe différent. Si vous n'arrivez pas à vous souvenir de tous ceux-ci, nous vous recommandons d'utiliser un gestionnaire de mot de passe. Aussi, si c'est possible, activer l'authentification à double facteurs (DFA) pour vos comptes, aide à s'assurer que les cyber attaquants ne peuvent se reconnecter. Si vous n'avez plus accès à votre compte, communiquer avec le site web et dites-leur que votre compte vous a été volé.

- **Récupérer votre ordinateur ou appareil personnel:** Si le logiciel d'antivirus n'est pas capable de récupérer l'ordinateur infecté ou vous voulez être plus sûre qu'il est sécuritaire, considérer la réinstallation du système d'exploitation et réinitialiser votre ordinateur. Il est souvent nécessaire d'effacer ou de remplacer votre disque dur et de réinstaller puis mettre à jour votre système d'exploitation. Ne réinstallez pas votre système d'exploitation à l'aide de vos copies de sauvegarde. Les copies de sauvegarde ne doivent être utilisées que pour récupérer vos fichier de données personnel. Si vous n'êtes pas sûr de pouvoir réaliser la réinstallation vous-même, penser faire appel à un service professionel afin de vous aider. Ou si votre ordinateur ou appareil est vieux, il serait peut-être temps d'en acheter un plus récent.
- **Récupérer vos comptes bancaires:** Pour des incidents avec votre carte de crédit ou tout autre comptes bancaire, appelez votre banque ou compagnie de crédit immédiatement. Appelez-les via un numéro de téléphone de confiance, tel que celui indiqué à l'endos de votre carte bancaire, celui inscrit sur votre relevé bancaire, ou visiter leur site web. Surveiller vos relevés ainsi que vos rapports de crédit périodiquement. De plus, pensez mettre un ordre de gel sur votre dossier de crédit.

Si vous avez subi des dommages financier ou vous vous sentez menacé, rapporter l'incident aux autorités policières.

Rédacteur invité

Maxim Deweerdt (Twitter @alfasec) est un instructeur certifié de the SANS Institute, il enseigne principalement les cours de Cyber Defense. Il est aussi un consultant principal chez NVISO, ou ils se spécialise sur la découverte de vulnérabilités, la résolution d'attaques et l'amélioration des projets de SOC.

Ressources

La puissance des mises à jour: https://www.sans.org/security-awareness-training/resources/power-updating
Avez-vous des copies de sauvegarde: https://www.sans.org/security-awareness-training/resources/got-backups
Gestionnaire de mots de passe: https://www.sans.org/security-awareness-training/resources/making-passwords-simple
Logiciels de rançon: https://www.sans.org/security-awareness-training/resources/ransomware
Rapporter les vols d'identité: https://www.identitytheft.gov
Blocage du dossier de crédit: https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

Traduit pour la communauté par: Jérôme Boutin et Sebastien Kierszka