OUCH! | Avril 2016

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

OUCH!

Dans ce numéro...

J'ai été hacké, que dois-je faire maintenant?

Vue d'ensemble

Nous savons que vous vous souciez de la protection de votre ordinateur et de vos périphériques mobiles et que vous prenez des mesures pour les sécuriser. Cependant, peu importe la façon dont vous utilisez la technologie en toute sécurité, tôt ou tard, vous pouvez être piraté ou "compromis". Dans ce numéro, vous apprendrez à déterminer si votre ordinateur ou appareil mobile a été piraté et si tel est le cas, ce que vous pouvez faire à ce sujet. En fin de compte, plus vite vous détecterez que quelque chose ne va pas, plus vite vous pourrez y répondre, et plus il est probable que vous puissiez réduire les dommages qu'un cyber attaquant peut causer.

Editeur invité

Samantha Davison (**@sam_e_davison**) est responsable de la sensibilisation à la sécurité et gestionnaire de programme d'éducation à Uber, où elle dirige le développement de la sensibilisation à la sécurité pour les employés dans plus de 350 villes à travers le monde.

Indices de compromission

Il peut être difficile de déterminer si vous avez été piraté car il n'existe pas de démarche unique à suivre pour déterminer si votre ordinateur a été compromis. Au lieu de cela, les pirates laissent généralement plusieurs indices, souvent appelés indicateurs. Si vous identifiez une combinaison de plusieurs indicateurs, cela peut signifier que votre ordinateur a été compromis.

- Votre programme anti-virus a déclenché une alerte indiquant que votre système est infecté, en particulier s'il vous signale qu'il n'a pas été en mesure de supprimer ou de mettre en quarantaine les fichiers concernés.
- La page d'accueil de votre navigateur a changé inopinément ou bien votre navigateur vous redirige vers des sites Web que vous ne souhaitez pas consulter.
- De nouveaux comptes que vous n'avez pas créés sont présents sur votre ordinateur ou vos appareils mobiles, ou encore, de nouveaux programmes que vous n'avez pas créés non plus sont en cours d'exécution.
- Votre ordinateur ou applications plantent en permanence, il y'a des icônes d'applications inconnues ou des fenêtres étranges qui surgissent.
- Un programme sur votre ordinateur sollicite votre autorisation en vue d'appliquer des modifications à votre système et ce même si actuellement vous n'installez ni ne mettez à jour l'une de vos applications.
- Votre mot de passe ne fonctionne plus lorsque vous essayez de vous connecter à votre système ou à un compte en ligne, même si vous savez que votre mot de passe est correct.
- Vos amis vous demandent pourquoi vous leur envoyez des spams alors que vous ne leur avez pas envoyé d'emails.

© SANS Institute 2016

J'ai été hacké, que dois-je faire maintenant?

- Votre appareil mobile est à l'origine de frais non autorisés à des numéros de SMS surtaxés.
- Votre appareil mobile a soudainement des données inexpliquées ou l'utilisation de la batterie est très élevée.

Tôt ou tard, votre ordinateur ou appareil peut être compromis, plus vite vous détecterez un incident et plus tôt vous y répondrez, meilleure sera votre réponse.

Comment réagir

Si vous pensez que votre ordinateur ou appareil a été piraté, plus tôt vous réagirez, mieux cela sera. Si l'ordinateur ou l'appareil vous a été fourni par votre employeur ou est utilisé dans le cadre professionnel, n'essayez pas de résoudre le problème vous-même. Non seulement vous pourriez causer plus de mal que de bien, mais vous pourriez aussi détruire des preuves précieuses qui pourraient être utilisées pour une enquête. Au lieu de cela, signalez l'incident à votre employeur immédiatement, par le biais de votre helpdesk, de l'équipe de sécurité ou de votre superviseur. Si pour une raison quelconque vous ne pouvez pas communiquer avec votre organisation, ou si vous êtes préoccupé par un retard, débranchez votre ordinateur ou périphérique du réseau, puis mettez-le en veille, ou en mode avion. Même si vous n'êtes pas sûr que vous avez été piraté, il est préférable de le signaler maintenant juste au cas où. Si l'ordinateur ou le périphérique est pour votre propre usage personnel, voici quelques étapes que vous pouvez prendre en considération.

- **Changez vos mots de passe** : Soyez certain de changer tous vos mots de passe. Cela inclut non seulement les mots de passe de vos ordinateurs et appareils mobiles, mais également l'ensemble de vos mots de passe en ligne. Assurez-vous de modifier tous ces mots de passe depuis un autre ordinateur, sécurisé et de confiance.
- **Anti-virus** : Si votre logiciel anti-virus vous informe de la présence d'un fichier infecté, vous pouvez suivre les actions qu'il préconise. Ceci peut inclure la mise en quarantaine du fichier, son nettoyage ou encore sa suppression. La plupart des logiciels anti-virus mettent à disposition des liens que vous pouvez suivre lors d'une infection afin d'en savoir plus sur cette infection spécifiquement. En cas de doute, mettez en quarantaine le fichier. Si cela n'est pas possible, alors supprimez-le.
- **Reconstruction** : Si vous êtes incapable d'arranger l'infection ou si vous voulez être absolument sûr que votre système est fixe, une option plus sûre consiste à reconstruire. Pour les ordinateurs, suivez les instructions du fabricant de votre système. Dans la plupart des cas, cela se traduira par l'utilisation des utilitaires intégrés pour réinstaller le système d'exploitation. Si ces utilitaires sont manquants, corrompus ou infectés, contactez votre fabricant pour obtenir des conseils ou visitez leur site web. Ne réinstallez pas le système d'exploitation à partir de sauvegardes, ces dernières

© SANS Institute 2016

J'ai été hacké, que dois-je faire maintenant?

peuvent en effet avoir les mêmes vulnérabilités qui ont permis au pirate de prendre initialement l'accès. Les sauvegardes ne doivent pas être utilisées pour récupérer vos données. Pour les appareils mobiles, suivez les instructions du fabricant de votre appareil ou service fournisseur, ceux-ci devraient être sur leur site web. Dans de nombreux cas, cela peut être aussi simple que la restauration de votre appareil mobile par défaut. Si vous vous sentez mal à l'aise avec le processus de reconstruction, envisagez d'utiliser un service professionnel pour vous aider. Ou, si votre ordinateur ou appareil est vieux, il peut être plus simple et encore moins cher d'en acheter un nouveau. Enfin, une fois que vous avez reconstruit votre ordinateur ou appareil, ou acheté un nouveau, assurez-vous qu'il soit complètement mis à jour et activez la mise à jour automatique à chaque fois que possible.

- **Sauvegardes** : L'étape la plus importante que vous pouvez prendre en considération pour vous protéger est de mettre en place des sauvegardes régulières à l'avance. Le plus souvent vous sauvegardez, mieux ce sera. Certaines solutions sauvegarderont automatiquement des fichiers nouveaux ou modifiés toutes les heures. Quelle que soit la solution de sauvegarde que vous utilisez, vérifiez régulièrement que vous êtes en mesure de restaurer ces fichiers. Très souvent, la récupération de vos données de sauvegarde est la seule solution qui s'offre à vous.
- **Application de la loi** : Si vous vous sentez menacé, signalez l'incident à la police locale.

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

Sauvegarde et récupération : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201508_fr.pdf

Phrases de passe : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201504_fr.pdf

Qu'est-ce qu'un Malware : https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201603_fr.pdf

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

OUCH! est publiée par le programme SANS « sécuriser l'humain » (Securing The Human) et est distribuée sous la licence « Creative Commons BY-NC-ND 4.0 ». La distribution de cette lettre d'information est autorisée tant que vous faites référence à la source, qu'elle n'a subie aucune modification et qu'elle n'est pas utilisée à des fins commerciales. Afin d'obtenir des traductions ou plus d'informations, merci de contacter ouch@securingthehuman.org.

Comité de rédaction : Bill Wyman, Walt Scrivens, Phil Hoffman, Lance Spitzner

Traduit par : Marilyn Combet