OUCH! | Mai 2014

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 êtes préoccupé par la protection de votre ordinateur ainsi que des informations qu'il contient et que vous prenez les mesures nécessaires pour les protéger. Cependant, tout comme c'est le cas lors de la conduite d'une voiture, peu importe à quel point vous conduisez prudemment, tôt ou tard, vous pouvez avoir un incident. Dans ce numéro, nous allons vous apprendre ce à quoi vous devez être attentif afin de déterminer si votre ordinateur est piraté, et si oui, ce que vous pouvez faire pour y remédier. Au final, plus vite vous constaterez que votre ordinateur a été piraté et plus vite vous agirez, alors bien meilleure sera votre gestion de tout dommages éventuels envers vous-même ou bien envers votre entreprise.

Editeur invité

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) est scientifique en chef au sein de la société CSRgroup Computer Security Consultants. Il est également le co-auteur des cours Memory Forensics (FOR526) et Malware Reverse Engineering (FOR610) au SANS Institute.

Indicateurs de compromission

Tout d'abord, vous devez comprendre que dans de nombreux cas, il n'existe pas de démarche unique à suivre pour déterminer si votre ordinateur est compromis. Au lieu de cela, il y'a généralement plusieurs indicateurs. Si vous identifiez une combinaison de ceux-ci, alors cela implique que votre ordinateur est compromis. Voici quelques exemples de ces différents indicateurs :

- Votre programme anti-virus a déclenché une alerte indiquant que votre ordinateur 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 souhaitiez pas consulter.
- Présence de nouveaux comptes sur votre ordinateur que vous n'avez pas créés.
- Présence de nouveaux programmes en cours d'exécution que vous n'avez pas installés.
- Votre ordinateur plante en permanence ou est très lent.
- 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 pare-feu vous alerte qu'un programme que vous ne connaissez pas demande l'autorisation d'accéder à Internet.

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

Comment réagir

Si vous pensez que votre ordinateur a été compromis, plus tôt vous réagirez, mieux ce sera. Si l'ordinateur que vous utilisez vous a été donné par votre employeur ou bien que vous vous en servez pour votre travail, alors n'essayez surtout pas de le réparer par vous-même et ne l'éteigniez pas. Non seulement vous pourriez causer plus de mal que de bien, mais vous pourriez également détruire de précieuses preuves qui pourraient être utilisées dans le cadre d'une enquête. Au lieu de cela, signalez immédiatement l'incident à votre employeur, généralement en prenant contact avec le help desk, l'équipe de sécurité ou bien votre responsable. Si pour une quelconque raison vous ne pouvez contacter votre entreprise, ou bien si vous êtes préoccupé par un éventuel délai, alors déconnectez votre ordinateur du réseau, puis mettez-le en veille ou bien en hibernation. Même si vous n'êtes pas sûr que vous avez été compromis, il est de loin préférable de le signaler quand même juste au cas où. Votre entreprise a probablement des processus et une équipe en place pour gérer ce genre de situations, laissez-les donc s'en occuper.

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

Si l'ordinateur est détenu pour votre usage exclusif, voici quelques mesures que vous pouvez entreprendre :

- **Sauvegardes** : L'étape la plus importante est de mettre en place des sauvegardes à l'avance. Plus précisément, sauvegardez vos données de manière régulière et vérifiez périodiquement que vous êtes en mesure de restaurer vos fichiers à partir desdites sauvegardes. Très souvent, lorsqu'un ordinateur est compromis, la seule option que vous avez est de formater le disque dur et de réinstaller un système d'exploitation ou bien d'acheter un nouvel ordinateur. Quoi qu'il en soit, vous aurez besoin de vos sauvegardes pour restaurer vos données personnelles.
- **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 équipements 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.
- **Réinstallation** : Si finalement vous ne parvenez pas à nettoyer l'ordinateur avec un anti-virus, alors l'une des façons les plus sûres pour repartir est de reconstruire l'ordinateur à partir de zéro. Commencez par déconnecter

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

votre ordinateur du réseau. Ensuite, suivez les instructions du fabricant de votre ordinateur ce qui, dans la plupart des cas, signifie d'utiliser la partition de récupération intégrée ("built-in recovery partition") afin de réinstaller le système d'exploitation. Si la partition de récupération est manquante, endommagée ou infectée, alors contactez le fabricant et demandez-lui qu'il vous envoie un DVD de restauration. Ne réinstallez pas le système d'exploitation à partir de vos sauvegardes. Vos sauvegardes peuvent en effet comporter les mêmes vulnérabilités que celles qui ont permis au pirate d'obtenir son accès initial. La seule chose pour laquelle vous devez utiliser vos sauvegardes est la récupération de vos données personnelles. De plus, si votre ordinateur est vieux ou obsolète alors il peut être plus simple (et peut-être même moins cher) d'acheter un nouvel ordinateur plutôt que de passer des heures à le réinstaller.

- **Recours à un professionnel** : Si vous suspectez une compromission de votre ordinateur mais que vous ne pensez pas avoir les compétences ou les connaissances pour y remédier, vous serez peut-être intéressé par l'apporter auprès d'un professionnel. Par exemple, après avoir été compromis, vous pouvez réaliser que vos sauvegardes sont incomplètes ou bien non-à-jour. Dès lors, vous pourriez être tenté de transférer des fichiers critiques tels que des photos, des documents ou encore des vidéos entre votre machine infectée et une nouvelle machine. Cependant, en faisant cela, vous pourriez par inadvertance transférer le logiciel malveillant et ainsi infecter votre nouvel ordinateur par la même occasion. L'alternative la plus sûre dans ce cas de figure est d'apporter l'ordinateur infecté auprès d'un technicien qualifié qui pourra, quant à lui, récupérer ces fichiers en toute sécurité et sans risquer de transférer l'infection.

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! Sauvegarde et restauration personnelles:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201309_fr.pdf
OUCH! Mots de passe:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201305_fr.pdf
OUCH! Qu'est-ce qu'un Malware:
http://www.securingthehuman.org/newsletters/ouch/issues/OUCH-201402_fr.pdf
Poster "Detecting Evil":
https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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