Le bulletin mensuel de sensibilisation à la sécurité pour vous

Suis-je piraté?

Vue d'ensemble

Quel que soit votre niveau de sécurité, vous pouvez avoir un incident tôt ou tard, comme si vous conduisiez une voiture. Vous trouverez ci-dessous des indices pour vous aider à déterminer si vous avez été piraté et, le cas échéant, quoi faire. Plus tôt vous identifiez quelque chose de grave, plus vous aurez des facilités à résoudre le problème.

Indices vous indiquant que vous avez été piraté

- **Votre programme antivirus génère une alerte indiquant que votre système est infecté. Assurez-vous que votre logiciel antivirus génère l'alerte et qu'il ne s'agit pas d'une fenêtre contextuelle d'un site Web essayant de vous tromper en composant un numéro ou en installant autre chose. Pas sûr de cela? Ouvrez votre programme anti-virus.**
- **Vous obtenez une fenêtre contextuelle indiquant que votre ordinateur a été chiffré et que vous devez payer une rançon pour récupérer vos fichiers.**
- **Votre navigateur vous emmène vers toutes sortes de sites Web sur lesquels vous ne voulez pas aller.**
- **Votre ordinateur ou vos applications se bloquent constamment. Des icônes pour des applications inconnues ou des fenêtres étranges apparaissent.**
- **Votre mot de passe ne fonctionne plus même si vous êtes certain que votre mot de passe est correct.**
- **Des amis vous demandent pourquoi vous les spammer avec des emails, vous êtes pourtant sûr que vous ne leur avez jamais rien envoyé.**
- **Il y a des frais sur votre carte de crédit ou des retraits de votre compte bancaire que vous n'avez jamais effectués.**

Comment réagir

Si vous pensez avoir été piraté, plus tôt vous agirez, mieux cela sera. Si le piratage est lié à votre travail, n'essayez pas de résoudre le problème vous-même, mais signalez-le immédiatement. Si c'est un système personnel ou un compte qui a été piraté, voici quelques étapes à suivre:

- **Modifier vos mots de passe:** Ceci inclut non seulement la modification des mots de passe sur vos ordinateurs et appareils mobiles, mais également pour vos comptes en ligne. N'utilisez pas l'ordinateur piraté pour changer vos mots de passe, utilisez un autre système que vous savez sécurisé. Si vous avez beaucoup de comptes, commencez par les plus importants. Si vous ne pouvez pas vous souvenir de tous vos mots de passe, utilisez un gestionnaire de mots de passe.

Financier: En cas de problème avec votre carte de crédit ou un compte bancaire, appelez immédiatement votre banque ou votre compagnie de carte de crédit. Utilisez un numéro de téléphone de confiance pour les appeler, par exemple à l'arrière de votre carte bancaire, sur vos relevés de comptes bancaires ou visitez leur site Web à partir d'un ordinateur de confiance. En outre, envisagez de geler votre dossier de crédit.

Anti-virus: Si votre logiciel antivirus vous informe qu'un fichier est infecté, suivez les mesures recommandées. La plupart des logiciels anti-virus comportent des liens que vous pouvez suivre pour en savoir plus sur l'infection en question.

Réinstallation: Si vous ne parvenez pas à réparer un ordinateur infecté ou si vous souhaitez être plus sûr que votre système est sécurisé, réinstallez le système d'exploitation. Ne réinstallez pas à partir de sauvegardes, les sauvegardes ne doivent être utilisées que pour récupérer vos fichiers personnels. Si vous ne vous sentez pas à l'aise pour faire cela, envisagez de faire appel à un service professionnel pour vous aider. Ou, si votre ordinateur ou votre périphérique est ancien, il peut être plus facile d'en acheter un nouveau. Enfin, une fois que vous avez reconstruit votre système ou acheté un nouveau, assurez-vous qu'il soit mis à jour et activez la mise à jour automatique chaque fois que cela est possible.

Les sauvegardes: Pour vous protéger, il est essentiel de vous préparer à l'avance avec des sauvegardes régulières. De nombreuses solutions sauvegardent automatiquement vos fichiers tous les jours, voire toutes les heures. Quelle que soit la solution que vous utilisez régulièrement, vérifiez que vous êtes en mesure de restaurer ces fichiers. Souvent, la récupération de vos sauvegardes de données est le seul moyen de récupérer vos fichiers suite à un piratage.

Forces de l'ordre: Si vous vous sentez menacé, signalez l'incident aux forces de l'ordre locales. Si vous êtes victime d'un vol d'identité et que vous résidez aux États-Unis, rendez-vous sur https://www.identitytheft.gov.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Le Dr. Johannes Ullrich *(@johullrich) est le doyen de la recherche du SANS Technology Institute, le directeur du SANS Internet Storm Center et un associé SANS. Il a créé le réseau de capteurs collaboratifs DShield et héberge le podcast quotidien de nouvelles sur la sécurité du réseau Internet Storm Center.*

Sources

Sauvegardes :	https://www.sans.org/u/JGP
Phrases de passe :	https://www.sans.org/u/JGU
Gestionnaires de mots de passe :	https://www.sans.org/u/JGZ
Qu'est-ce qu'un malware :	https://www.sans.org/u/JH4
Gel de crédit :	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet