Eviter de se Faire Pirater : Le Guide Ultime

INTRODUCTION

Avec le développement des connexions Internet à large bande, les services en ligne / en nuage sont devenus de plus en plus nombreux. **Vos données ne se trouvent plus seulement sur votre ordinateur**, mais sur une multitude de serveurs en ligne. Vous devez non seulement envisager maintenant ce qui pourrait **arriver si votre ordinateur est infecté**, mais également ce qui pourrait se produire **si l'un de vos comptes en ligne était compromis**.

PROBLÈMES POSSIBLES

- **Vol de données** : Votre ordinateur est infecté par un logiciel malveillant ou un service en ligne est compromis, **et l'attaquant a volé des fichiers privés** que vous ne souhaitez VRAIMENT pas voir en ligne.
- **Vol d'identité** : Une fois que l'attaquant a obtenu des données spécifiques, il peut **se faire passer pour vous** et utiliser cet avantage à des fin malicieuses.
- **Perte de données:** Certains auteurs de malwares se spécialisent dans la création de malwares conçus pour chiffrer les fichiers sur votre ordinateur et demandant une rançon pour les récupérer. La perte de données peut être liée à des activités malveillantes mais aussi à la perte de votre ordinateur portable ou une **panne de disque dur**.

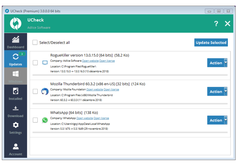
Toutes les menaces décrites ci-dessus peuvent être, dans la plupart des cas, évitées en suivant certaines **bonnes pratiques**. Vous pouvez **prévenir l'infection de votre ordinateur** et éliminer les dommages au cas où **l'un de vos comptes en ligne serait compromis**. Regardons comment.

EVITER L'INFECTION

GARDEZ VOS LOGICIELS À JOUR

Des vulnérabilités logicielles peuvent être utilisées pour installer des logiciels malveillants sur votre ordinateur. Utilisez **uniquement des logiciels mis à jour** où ces vulnérabilités sont corrigées lorsqu'elles sont détectées. Appliquer les **mises à jour système et mettre à jours vos logiciels** est également un conseil avisé pour éviter d'éventuelles exploitations.

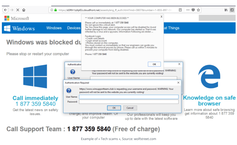
Nous recommandons le téléchargement et l'installation de UCheck et de **réaliser des scans et mises à jours régulièrement**. Si vous êtes un utilisateur Premium, c'est encore plus simple si vous activez l'option « Mises à jour automatiques ».



BLOQUEZ LES PUBLICITÉS (DANGEREUSES)

De nombreux sites Web affichent des publicités. Il y a les publicités classiques (non intrusives), les publicités problématiques (affichage de pop-ups, boutons indiquant en erreur, etc.) et les **publicités malveillantes**. Ces dernière sont évidemment plus dangereuses, elles peuvent effrayer l'utilisateur avec de faux messages d'erreur ou même télécharger et installer des malware sans nécessiter d'interaction avec l'utilisateur (téléchargement furtif). En bloquant les publicités, vous réduisez le risque d'infection.

L'installation d'un bloqueur de publicités permettra d'éviter ce type d'attaque. Nous recommandons uBlock Origin pour son efficacité, sa faible empreinte mémoire et son support étendu. Toutefois, soyez responsable et désactivez votre bloqueur de publicité sur les sites que vous souhaitez soutenir.



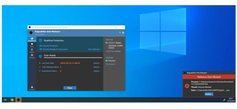
Call Support Team : **1 877 359 5840** (Free of charge)

Exemple of « Tech scams », Source: wolfconsec.com

INSTALLEZ UN ANTIVIRUS + UN ANTIMALWARE

L'antivirus est la première barrière de protection contre les logiciels malveillants lorsqu'ils ont atteint votre ordinateur. Il est donc important d'installer un antivirus efficace. Si vous utilisez Windows 10, Windows Defender Antivirus est la solution. Si vous utilisez une ancienne version de Windows, nous recommandons, Avira Free Antivirus ou Kaspersky Security Cloud Free. Sur Windows XP, Panda Dome Free Antivirus est le produit recommandé (considérés toutefois une mise à jour vers un système plus récent).

La seconde couche de protection est basée sur des méthodes heuristiques (anti-malware nouvelle génération) et est principalement utilisée pour détecter les menaces inconnues. Notre produit phare, BouncyKiller Premium (à partir de la version 14) remplit cette fonction et comprend une protection en temps réel contre les logiciels malveillants ainsi qu'une fonction spéciale « **Dossiers protégés** » qui protège vos fichiers contre les ransomware.



NOUVREZ JAMAIS LES PIÈCES JOINTES OU E-MAILS PROVENANT D'EXPÉDITEURS INCONNUS

Les campagnes de spam sont toujours très utilisées pour infecter les machines, souvent sous la forme de documents Office contenant des macros malveillantes. Même si votre antivirus ne détecte pas de code malveillant dans la pièce jointe, cela ne signifie pas qu'elle est inoffensive. En règle générale, **si vous ne connaissez pas l'expéditeur**, ne cliquez sur aucun lien contenu dans le corps de l'e-mail et n'ouvrez pas les fichiers joints.

Une autre règle importante est de ne **jamais aveuglément croire le contenu des messages reçus**. La plupart des campagnes de spam utilisent l'ingénierie sociale sous la forme d'un chantage, d'un appât ou n'importe quelle autre technique qui **incitera l'utilisateur à cliquer sur un lien ou à ouvrir un fichier**. Le contenu peut être effrayant, incitatif ou questionnable. Ils ont été rédigés dans ce optique, déplacez les directement dans le dossier « SPAM ».

EVITEZ L'UTILISATION D'ACTIVATEURS / CRACKS / KEYGENS

Les activateurs de logiciels, connus également sous le nom de cracks/keygens sont de petits logiciels créés **pour utiliser des logiciels commerciaux sans payer**. Généralement, 10% d'entre eux fonctionnent comme promis, 40% sont buggés (mais sans danger) et **50% d'entre eux sont des logiciels malveillants**, attendant d'être exécutés.

La plupart vous demanderont de **désactiver votre antivirus**. Choisir d'activer un logiciel de cette manière est comme jouer à la « Roulette Russe ». Nous vous recommandons plutôt **d'acheter le logiciel** (renseignez-vous sur d'éventuels réductions auprès de l'éditeur de celui-ci ou d'utiliser des licences alternatifs gratuits (Linux, Open Office, etc.).

BONNES PRATIQUES

N'UTILISEZ JAMAIS DEUX FOIS LE MÊME MOT DE PASSE

Lorsque vous vous abonnez à un compte en ligne, vous devez fournir un nom d'utilisateur et un mot de passe. Le mot de passe est, la plupart du temps, chiffré, mais pas toujours (mauvaises pratiques).

Si, pour une raison quelconque, **le service est compromis**, votre email et mot de passe tomberont entre les mains de l'attaquant et celui-ci **essaiera de se connecter à d'autres services en ligne** pour accéder à tous vos comptes en ligne. C'est pourquoi nous vous recommandons de ne jamais utiliser deux fois le même mot de passe. Ce n'est pas un conseil facile à suivre, mais nous vous proposons des solutions ci-après.

Vous pouvez utiliser le service « Have i been pwned? » pour vérifier si votre adresse électronique se trouve dans une base de données piratée.

UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Se souvenir de tous les mots de passe est compliqué, voir impossible si vous utilisez de nombreux services. Heureusement, il existe maintenant des services disponibles sur toutes les plateformes (ordinateurs, smartphones, tablettes, etc.) qui s'occupent de **la création et du stockage des mots de passe pour vous**. Ils sont mêmes capables de remplir automatiquement les champs obligatoires lorsque vous devez vous connecter à un compte en ligne.

Nous déconseillons l'utilisation du gestionnaire inclus à votre navigateur, car il est très facile à d'éventuels attaquants de voler le fichier contenant tous vos mot de passes. Nous recommandons plutôt l'utilisation d'un service en ligne, tel que LastPass. Vous ne devrez retenir qu'un unique mot de passe (mot de passe maître) pour accéder à votre compte, votre « coffre » est ensuite accessible sur tous vos périphériques.

UTILISEZ 2FA AUTANT QUE POSSIBLE

2FA (authentification à deux facteurs), est un moyen d'authentifier un utilisateur avec un élément supplémentaire à son mot de passe. Cette vérification supplémentaire est effectuée en utilisant «quelque chose que seul l'utilisateur possède». La plupart du temps il s'agit d'un **code SMS** ou un **jetson d'accès** (matériel ou logiciel).

Certains services en ligne vous permettent d'utiliser l'authentification 2FA, qui **renforce la sécurité de votre compte**. Si c'est le cas, nous vous conseillons vivement de l'activer. Les solutions les plus populaires pour les jetons d'accès logiciels sont disponibles à la fois sur Android et iOS, Authy and Google Authenticator.

Important : N'oubliez pas de conserver vos codes de récupérations, une fois le service activé.

UN CADENAS VERT NE SIGNIFIE PAS QUE VOUS ETES SUR UN SITE SÛR

L'un des mythes plus courant de la sécurité Internet concerne le **cadenas affiché par le navigateur lors de la visite d'un site** : si le cadenas est fermé et surligné en vert, le site est sûr. En réalité le site POURRAIT être sûr, mais ce n'est pas toujours le cas.

Les auteurs de malware **utilisent énormément ce mythe pour inciter les utilisateurs** à leur faire confiance. Un cadenas vert signifie que **les données transmises entre l'ordinateur et le site sont sont chiffrées**, et c'est tout. Les exemples ci-dessous illustrent un site malveillant tentant de se faire passer pour sophos.com :

FAITES DES SAUVEGARDES RAPIDEMENT, FAITES DES SAUVEGARDES SOUVENT

Les sauvegardes sont votre roue de secours en cas de problème. Elles ne vous empêcheront pas d'avoir un accident, mais **vous aideront à réparer**. Il y a trois règles à suivre concernant les sauvegardes :

- **Sauvegardez rapidement** (dès que vous avez des données précieuses à sauvegarder)
- **Sauvegardez souvent** (chaque jour / semaine, en fonction de la quantité de changements)
- **Testez régulièrement vos sauvegardes** (vérifiez qu'elles soient correctement sauvegardées et exploitables)

De nos jours, il existe de nombreuses façons de sauvegarder vos données : **localement** (à l'aide d'un disque dur externe ou un NAS) ou en utilisant un **service de stockage en nuage** (Google Drive, Dropbox, etc.). Malheureusement, **n'utiliser qu'un seul de ces moyens est insuffisant**.

Quelle que soit la méthode choisie, vous serez toujours vulnérable face à **une panne matérielle ou un chiffrement de vos données** (ransomware). Si votre NAS est disponible sur le réseau, un ransomware le détectera, même chose pour un service en ligne. Un disque dur externe peut être volé, détruit ou autre.

Les recommandations sont **d'avoir au minimum trois sauvegardes similaires**, à des emplacement différents :

- **La première copie** est stockée sur votre disque dur local ou un NAS (copie de travail)
- **La deuxième copie** est stockée sur un service de stockage en nuage (copie en ligne)
- **La troisième copie** est stockée sur un disque dur externe, non connectée au réseau (copie hors ligne).

Nous recommandons les NAS Synology et les service de stockage en nuage Google Drive or Dropbox.

Auteur Curson

Curson develop tools and algorithms for malware analysis and research as well as new scanning and removal technologies. Involved in all the Adlice projects as support developper, Curson is also Adlice Community and Support representative.