Zeitschrift: Générations
Herausgeber: Générations, société coopérative, sans but lucratif
Band: - (2019)
Heft: 116

Artikel: Les "malwares", comment lutter
Autor: Lamon, Karin
DOI: https://doi.org/10.5169/seals-906203

Nutzungsbedingungen
Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation
L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use
The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 13.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

Les « malwares », comment lutter

Votre ordinateur peut être contaminé par des virus : nous les appelons plus globalement « malwares » ou logiciels malveillants. Il en existe une pléthore. Petit tour d'horizon des plus répandus.

Nous voici tout émoustillé par l'achat de notre nouvel ordinateur. Une grande histoire d'amour commence entre lui et nous jusqu'à ce que la prunelle de nos yeux se grippe et attrape un virus dont nous ne savons pas faire façon. C'est la panique. Votre écran est rempli de fenêtres qui s'ouvrent sans que vous l'ayez demandé ou votre ordinateur est beaucoup plus lent que d'habitude, tels sont des signes qui peuvent vous faire craindre la contamination. Et, effectivement, les « malwares » sont hostiles, intrusifs et conçus pour envahir, endommager ou désactiver vos ordinateurs. Alors, comment lutter contre ces pirates qui, comme le dit Alexandre Bisenz, responsable de la communication à la Police cantonale vaudoise, « font preuve d'imagination quand il s'agit de nuire ».

KARINE LAMON

TROIS GRANDES FAMILLES

Il existe beaucoup de variantes de « malwares », qu'on peut regrouper en trois grandes familles, comme l'explique la Police cantonale vaudoise.

LES LOGICIELS E-BANKING

Les logiciels e-banking sont sournois. Vous recevrez dans votre boîte mail un courriel semblant provenir de votre banque. L'environnement graphique étant recopié à l'identique, il est facile de tomber dans le panneau. Dans la plupart des cas, on vous demandera d'entrer toutes les données nécessaires pour accéder à votre compte en banque et, par la suite, on effectuera des transactions à votre insu.

COMMENT S'EN SORTIR

Il faut savoir que les institutions bancaires n'envoient jamais de demande par mail. Si vous deviez passer par la voie électronique, c'est uniquement par la messagerie très sécurisée et sur la plateforme officielle de votre banque.
Si vous recevez un tel courriel, ne l'ouvrez en aucun cas. Et placez-le dans la corbeille de votre messagerie. Si, dans le doute, vous n'osez pas le supprimer, la police vous recommande de contacter directement votre banque par téléphone pour en avoir le cœur net.

LES FAUX SUPPORTS MICROSOFT

Des escrocs vous envoient des courriers électroniques indésirables ou prennent contact avec vous directement par téléphone, afin de vous inciter à payer des services de support technique inutiles, supposés résoudre des problèmes imaginaires d'appareils, de plateformes ou de logiciels. Les pirates vous feront installer une application pour prendre le contrôle de votre ordinateur à distance et vous « aider ».

COMMENT S'EN SORTIR

Demandez à vos petits-enfants ou à un proche de désinstaller les applications que les fraudeurs vous ont demandé de télécharger.
Si vous leur avez déjà accordé l'accès, il conviendra de réinitialiser votre appareil. Un spécialiste ou les vendeurs du magasin où vous avez acheté votre machine pourront vous aider.

CRYPTOLOCKER OU « RANSOMWARE »

Un « ransomware » est un logiciel malveillant qui infecte votre ordinateur et donne aux pirates informatiques la capacité de verrouiller votre PC à distance et de crypter vos fichiers, leur permettant ainsi de prendre le contrôle de toutes vos informations et de vos données stockées. En général, vous recevez un mail contenant un lien. C'est au moment où vous cliquez sur le lien que le virus s'active. Dans la deuxième phase, une fenêtre s'ouvre et vous demande une rançon sous la forme d'un paiement pour vous débarrasser du virus.

COMMENT S'EN SORTIR

Faites appel à un spécialiste qui vous aidera à reprendre le contrôle de votre machine. Gardez vos données hors de portée des pirates en leur retirant le pouvoir de les détruire : sauvegardez-les dans un disque dur séparé.

QUELQUES BONNES ASTUCES

Pour prévenir plutôt que guérir, quelques pratiques sont applicables afin d'éviter la contamination de votre appareil.

Quel que soit la nature du logiciel malveillant, les règles de prévention pour s'éviter des mésaventures sont les mêmes!

1 Téléchargez des programmes «anti-malwares» comme Malwarebytes for Windows, Malwarebytes for Mac, Malwarebytes for Android. Installez le logiciel, puis lancez une analyse. Il détectera d'éventuels virus s'ils sont déjà présents (39 fr. 90 pour 12 mois).

2 Quand vous recevez un mail provenant d'un destinataire inconnu, évitez d'ouvrir les pièces jointes en annexe. Elles contiennent souvent un virus.

3 Aucune institution ni organe financier ne demandent vos accès par mail. Ne les transmettez jamais!

4 Choisissez des mots de passe sûrs et faciles à retenir, mais difficiles à deviner pour autrui.

5 Equipez votre ordinateur d'un antivirus et d'un pare-feu.

6 Faites régulièrement les mises à jour de vos systèmes d'exploitation, de vos navigateurs et plug-in.

kaptnali