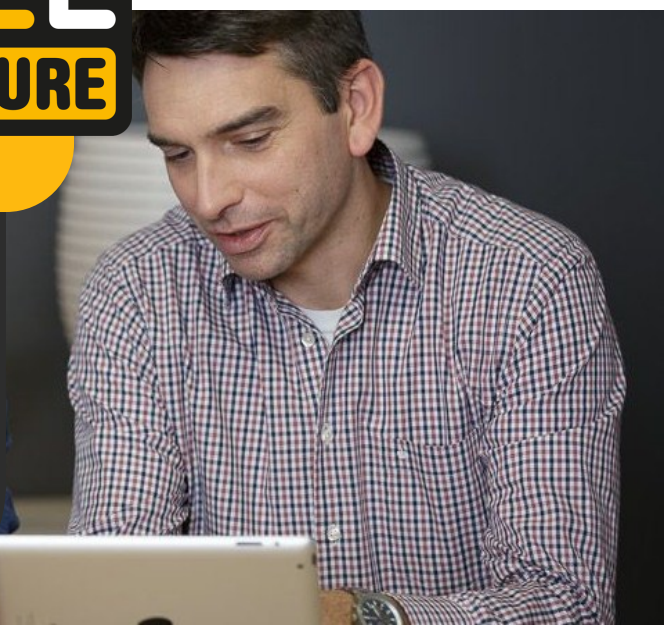
Protéger son ordinateur...
Mais pourquoi ?



CONTENU

Un virus paralyse votre ordinateur – il ne fonctionne plus correctement et devra être réparé. C'est très fâcheux !

Si, comme la plupart des internautes, vous pensez que cette perte temporaire de disponibilité soit la pire des choses qui puisse vous arriver, vous vous trompez. Ce n'est que la partie émergée de l'iceberg. L'ampleur réelle d'une attaque informatique ne se manifeste que rarement. Car dans presque tous les ordinateurs, les cybercriminels trouvent des « butins » de grande valeur. En effet, l'usurpation de ces butins, que vous, en tant que propriétaire légitime, ne considérez pas comme tels, peut entraîner d'énormes dégâts.

Sont notamment convoités :

1. IDENTIFIANTS ET MOTS DE PASSE

Les cybercriminels accèdent aux identifiants et aux mots de passe à l'aide d'e-mails de hameçonnage (Phishing) ou de chevaux de Troie qui enregistrent toutes les touches saisies sur le clavier.

Bien souvent, c'est encore plus facile : si vous utilisez un mot de passe trop simple, il peut être « deviné » en quelques secondes à l'aide d'un logiciel spécifique ou par un expert en ingénierie sociale.

Les données de connexion sont très convoitées par les personnes malintentionnées car elles leur permettent de se connecter à des services en ligne sous votre nom. Par exemple :

- sur les serveurs de votre société pour accéder aux données confidentielles de l'entreprise
- sur les sites de banque en ligne pour voler de l'argent sur votre compte
- sur votre serveur en ligne pour accéder aux données qui y sont sauvegardées
- sur votre boutique en ligne pour acheter des articles en votre nom qui vous seront facturés
- sur votre réseau social, votre compte de messagerie ou dans votre tchat pour usurper votre identité en ligne et l'utiliser à des fins abusives

2. CONTACTS PRIVÉS

Les cybercriminels recueillent les noms, les adresses e-mail et les numéros de téléphone des personnes de votre liste de contacts afin de les vendre à des tiers. Ces derniers les utiliseront pour envoyer des spams ou des e-mails de hameçonnage, permettant ainsi d'élargir le champ d'action des criminels.

Si votre liste de contacts comprend des personnes de la vie publique ou occupant des postes de responsabilité dans certaines industries, les criminels pourraient aussi rechercher ces contacts de manière ciblée.

3. COMMUNICATIONS SENSIBLES

Vous menez des discussions privées ou professionnelles importantes par e-mail ou par tchat ? Les criminels pourraient eux aussi s'intéresser à ces contenus ! Il faut savoir que les e-mails ne conviennent pas comme moyen de communication pour l'envoi de données confidentielles et encore moins pour l'envoi de données secrètes.

4. BIENS VIRTUELS

Les cybercriminels jettent un œil sur tout ce qu'il puisse leur apporter de l'argent. Les biens non matériels, tels que licences de logiciels, clés de licence de systèmes d'exploitation ou licences de jeux, faciles à copier et à revendre, en font également partie. Les personnages, objets et moyens de paiement de jeux vidéo ainsi que des scores élevés sont également lucratifs.

5. VOTRE SITUATION FINANCIÈRE

Dès lors que les cybercriminels ont accès à votre ordinateur, ils peuvent le fouiller à la recherche d'informations précieuses. Par exemple des informations sur vos cartes de crédit, vos données fiscales ou vos plans d'investissement.

Selon les renseignements sur votre situation financière obtenus, les cybercriminels décident de vous garder ou non dans leur ligne de mire.

6. VOTRE ORDINATEUR, MAILLON D'UN GRAND RÉSEAU

Les botnets sont de grands réseaux d'ordinateurs compromis (également appelés « zombies ») qui sont contrôlés de l'extérieur et commandés à distance. Sans que vous ne vous en rendiez compte, votre ordinateur peut être intégré à un tel réseau, puis être utilisé à des fins criminelles, comme l'envoi de spams ou d'e-mail de hameçonnage à des millions d'utilisateurs dans le monde entier, ou la réalisation d'attaques par déni de service qui paralysent des sites et des services Web entiers. Votre ordinateur est la source du mal, même si vous n'y participez pas personnellement.

7. VOTRE ORDINATEUR COMME SERVEUR WEB

C'est tout aussi dangereux : les criminels peuvent transformer votre ordinateur en serveur Web qu'ils utiliseront ensuite pour mettre à disposition des contenus illégaux.
Font partie de ces contenus :

- les sites Web de hameçonnage (Phishing) qui servent à voler les données de connexion ou d'accès aux services de banque en ligne des utilisateurs innocents
- les outils d'attaque avec lesquels les ordinateurs de tiers innocents peuvent être compromis
- matériel pédophile et/ou pornographique, copies pirates de vidéos et de musique

8. VOTRE ORDINATEUR COMME MOYEN DE CHANTAGE

L'une des méthodes courantes des cybercriminels est d'infecter l'ordinateur de leur victime par des logiciels malicieux et de leur proposer ensuite un « nettoyage » contre paiement. Le criminel peut chiffrer toutes les données de l'ordinateur selon un schéma que lui seul est en mesure de déchiffrer. Dans ce cas, le criminel demandera une somme d'argent importante pour le déchiffrement des données. Si vous ne payez pas, vous ne pourrez plus récupérer vos données.

Si vous avez visité des contenus problématiques, tels que sites pornographiques ou mené une conversation intime par webcam il se peut que les criminels aient fait un compte-rendu de vos activités et vous demandent alors une certaine somme d'argent pour la non-publication de ces informations. Si vous êtes une personne publique, vous devriez redoubler de vigilance quant à ce type d'interventions.

9. COMMENT SAVOIR, SI VOTRE ORDINATEUR A ÉTÉ PIRATÉ ?

Si le logiciel malicieux est bien écrit, il est difficile voire impossible pour non initiés de constater l'infection de l'ordinateur. Prêtez tout de même attention à quelques anomalies :

- votre ordinateur, fonctionne-t-il plus lentement que d'habitude ?
- Votre logiciel antivirus sonne-t-il l'alerte ?
- Lors de votre recherche sur Google, êtes-vous redirigé vers des résultats d'autres moteurs de recherche ?
- Vos amis vous parlent-ils d'e-mails ou de messages bizarres qu'ils ont reçus de votre part ?
- Votre compte de messagerie ou votre profil sur les réseaux sociaux ont-ils été bloqués parce qu'ils ont diffusé des spams ?
- Votre webcam s'allume-t-elle automatiquement ?
- Indépendamment des sites Web visités, des messages publicitaires apparaissent-ils dans votre système d'exploitation ?
- Votre ordinateur se bloque-t-il soudainement pendant une mise à jour d'un logiciel ?

Ce ne sont que quelques exemples d'anomalie qui devraient vous alerter sur une éventuelle infection de votre ordinateur.

Si vous avez la possibilité, utilisez un Live CD* pour scanner l'appareil. Ce processus permet d'analyser l'ordinateur sans démarrer le système principal et convient donc idéalement pour les opérations antivirus.

Il est également conseillé de réaliser une sauvegarde (backup) de vos données, puis de réinstaller l'ordinateur. Si vous avez besoin d'aide, n'hésitez pas à vous adresser à un expert en informatique (p.ex. un « PC Doctor »*).

Comme toujours, l'adage suivant est de mise : mieux vaut prévenir que guérir !

Afin de minimiser au mieux la vulnérabilité de votre ordinateur, appliquez de manière préventive les mesures de protection techniques et adoptez une conduite sûre sur Internet.

**Plus d'informations : www.bee-secure.lu*