Les infections par malware

Pour surfer sur Internet en toute sécurité, il est indispensable de disposer d'un programme antivirus et d'un système d'exploitation avec fonction de mise à jour automatique. Mais il peut arriver malgré tout qu'un ordinateur soit infecté par un malware. Apprenez à reconnaître les logiciels malveillants et adoptez les bons réflexes !

À quoi puis-je reconnaître une infection par malware ?
Les indices possibles :

- alerte d'infection de la part de l'antivirus.
- messages d'erreur lors du démarrage ou de l'arrêt de l'ordinateur.
- ordinateur instable, plantages répétés.
- système lent, mémoire de travail et/ou processeur constamment saturé(e), disque dur constamment surchargé.
- antivirus désactivé (même après que vous l'ayez expressément activé).
- impossibilité d'accéder au site Internet d'un ou plusieurs fabricants d'antivirus.

Consultez la « Règle n°2 – Surveiller » (https://www.ebas.ch/fr/2-surveiller-avec-lantivirus-et-le-pare-feu/) de nos « 5 règles pour votre sécurité numérique » (https://www.ebas.ch/fr/5-regles-pour-votre-securite-numerique/) pour en savoir plus sur les mesures à suivre pour vous protéger contre les infections par malware. Vous y trouverez également une liste de programmes antivirus dont un certain nombre gratuits. Si vous pensez que votre dispositif est infecté, vous devez savoir quoi faire.

Les principales étapes à suivre en cas d'infection par malware :

1. garder son calme, couper la connexion Internet et vérifier le dernier backup. (#step1)
2. évaluer l'opportunité de faire appel à un spécialiste. (#step2)
3. identifier le malware et l'éliminer. (#step3)
4. dernier recours : la réinstallation du système d'exploitation. (#step4)

Le terme malware est un mot-valise anglais, contraction de « malicious » (malveillant) et « software », rendu en français par le terme « maliciel ». Malware est le terme générique pour désigner les logiciels qui exécutent des fonctions nuisibles sur un dispositif (ex. virus, vers, chevaux de Troie, rançongiciels...).

Pour aller plus loin
Que faire en cas d'infection par un logiciel malveillant ?

Étape n°1 : gardez votre calme, coupez votre connexion Internet et vérifiez votre dernier backup.

La première chose à faire est de couper la connexion Internet (débrancher le câble LAN ou interrompre la connexion wifi). Il faut ensuite contrôler la date du dernier backup de vos données. Il est recommandé de créer une nouvelle sauvegarde sur un support de stockage externe différent de celui utilisé pour le backup normal.

NB : il se peut que cette nouvelle sauvegarde contienne également une copie du maliciel, mais cela est sans importance pour le moment.

Étape n°2 : évaluez l'opportunité de faire appel à un spécialiste

Il convient maintenant de réfléchir à l'éventualité de recourir à un expert pour éliminer le programme malveillant. Les éditeurs d'antivirus offrent souvent des services de suppression des malwares. Il s'agit la plupart du temps d'une assistance téléphonique ou d'un « service de suppression des virus à distance ». Sachez toutefois que ce service a un coût. Beaucoup de magasins d'informatique proposent également des services de réparation spécifiques pour les infections par malware.

Étape n°3 : identifiez le malware et éliminez-le

Certains maliciels peuvent être éliminés par l'antivirus installé, mais pas tous. Si vous ne parvenez pas à supprimer le malware avec votre programme antivirus, il est recommandé d'utiliser un antivirus « deuxième avis », tel que par exemple :

- Malwarebytes (https://fr.malwarebytes.com)
- HitMan Pro (https://www.hitmanpro.com)

Si cela ne marche pas, il importe d'identifier précisément le logiciel malveillant. Le mieux est de reprendre la dénomination du malware (telle qu'elle est donnée par l'antivirus) et de rechercher sur Internet (à partir d'un dispositif non infecté bien sûr !) la procédure à suivre pour s'en débarrasser. La plupart des fabricants d'antivirus mettent à la disposition des internautes des bases de données regroupant de nombreuses informations sur les malwares et les méthodes permettant de les éradiquer. Si vous disposez d'un CD auto-bootable de dépannage (fourni par l'éditeur de l'antivirus), vous pouvez démarrer votre ordinateur avec ce CD et essayer d'éliminer le malware.

Bases de données pour les malwares

- Avira (https://www.avira.com/fr/support-virus-lab)
- Microsoft (https://www.microsoft.com/security/portal/)
- Broadcom-Symantec (https://www.broadcom.com/support/security-center/a-z)
- Trend Micro (https://www.trendmicro.com/vinfo/fr/threat-encyclopedia/)

Utilitaires de désinfection (Removal Tools)

- Microsoft (https://support.microsoft.com/en-us/topic/remove-specific-prevalent-malware-with-windows-malicious-software-removal-tool-kb890830-ba51b71f-39cd-cdec-73eb-61979b0661e0)
- Norton-Symantec (https://support.norton.com/sp/en/us/home/current/solutions/kb20100824120155EN)

Pour les maliciels très répandus, les éditeurs d'antivirus proposent gratuitement des utilitaires de désinfection permettant de rechercher et d'éliminer automatiquement les malwares en question. Avant de télécharger un utilitaire de désinfection, mieux vaut cependant vous assurer que vous vous trouvez sur un site sérieux (celui d'un éditeur d'antivirus p. ex.). Il existe en effet de faux programmes antivirus et de faux utilitaires de désinfection spécialement mis au point par des cyberpirates en vue de diffuser de nouveaux programmes malveillants.

Étape n°4 : dernier recours, la réinstallation du système d'exploitation

Si toutes ces mesures échouent, vous devrez procéder au reformatage complet de votre ordinateur. Vous pouvez également retourner à l'étape n°2 et décider de faire appel maintenant à un spécialiste.

Pour en savoir plus sur comment restaurer votre système et réduire le risque d'une nouvelle infection, consultez notre fiche d'instructions (pour Windows 10) (https://www.ebas.ch/fr/reinstallation-de-windows-10/) .