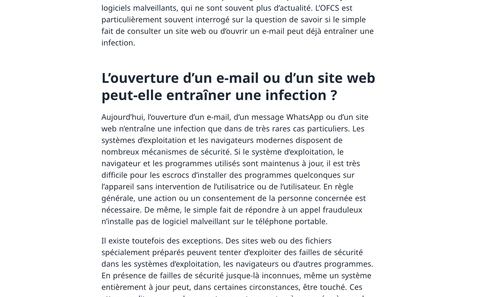
Publié le 6 octobre 2026

Semaine 40 : Mythes sur les logiciels malveillants et mesures à prendre en cas de suspicion d'infection

L'OFCS reçoit actuellement un nombre croissant de signalements concernant des attaques ciblées de logiciels malveillants. Après avoir abordé la semaine dernière les voies d'infection, le deuxième volet explique ce qu'il convient de faire en cas de suspicion d'infection. Il déconstruit également des mythes répandus au sujet desquels l'OFCS reçoit régulièrement des demandes.



Il existe de nombreuses idées reçues largement répandues au sujet des logiciels malveillants, qui ne sont souvent plus d'actualité. L'OFCS est particulièrement souvent interrogé sur la question de savoir si le simple fait de consulter un site web ou d'ouvrir un e-mail peut déjà entraîner une infection.

L'ouverture d'un e-mail ou d'un site web peut-elle entraîner une infection ?

Aujourd'hui, l'ouverture d'un e-mail, d'un message WhatsApp ou d'un site web n'entraîne une infection que dans de très rares cas particuliers. Les systèmes d'exploitation et les navigateurs modernes disposent de nombreux mécanismes de sécurité. Si le système d'exploitation, le navigateur et les programmes utilisés sont maintenus à jour, il est très difficile pour les escrocs d'installer des programmes quelconques sur l'appareil sans intervention de l'utilisatrice ou de l'utilisateur. En règle générale, une action ou un consentement de la personne concernée est nécessaire. De même, le simple fait de répondre à un appel frauduleux n'installe pas de logiciel malveillant sur le téléphone portable.

Il existe toutefois des exceptions. Des sites web ou des fichiers spécialement préparés peuvent tenter d'exploiter des failles de sécurité dans les systèmes d'exploitation, les navigateurs ou d'autres programmes. En présence de failles de sécurité jusque-là inconnues, même un système entièrement à jour peut, dans certaines circonstances, être touché. Ces attaques dites « zero day » sont rares et ne sont guère menées à grande échelle, mais de manière très ciblée contre des victimes sélectionnées (p. ex. des personnes politiquement exposées, des membres du personnel d'organisations internationales, des diplomates, etc.).

Aujourd'hui, les cybercriminels tentent bien plus souvent d'inciter directement l'utilisatrice ou l'utilisateur à effectuer une action. Ils cherchent par exemple à leur faire installer un programme sous un prétexte ou exécuter une commande qui entraînera ensuite une infection.

Les systèmes macOS sont-ils mieux protégés contre les cyberattaques ?

Les utilisatrices et utilisateurs de macOS peuvent eux aussi être touchés par des logiciels malveillants, car il existe également de nombreux programmes malveillants pour macOS. Il s'agit notamment de programmes destinés à voler des identifiants de connexion, de logiciels espions et de logiciels malveillants qui chiffrent des fichiers ou utilisent l'ordinateur pour mener d'autres attaques. En bref : tout ce qui existe sur les appareils Windows existe en principe aussi pour macOS.

Apple a intégré différentes fonctions de sécurité à macOS. Celles-ci offrent une protection importante, mais ne rendent pas un Mac invulnérable. Il convient donc également d'installer les mises à jour de sécurité sur un Mac et de ne télécharger des programmes qu'à partir de sources fiables.

Un antivirus protège-t-il contre toutes les infections ?

Un antivirus constitue une mesure de protection importante, mais ne peut garantir une protection complète. Un nouveau logiciel malveillant peut dans un premier temps être inconnu. Il faut un certain temps avant qu'un logiciel malveillant puisse être détecté par l'antivirus. La détection par un logiciel antivirus peut notamment être retardée dans le cas d'infections répandues à l'échelle régionale. En outre, une attaque peut viser à inciter l'utilisatrice ou l'utilisateur à effectuer elle-même ou lui-même une action malveillante. Un antivirus ne doit donc être considéré que comme une couche de protection supplémentaire et non comme l'unique protection. Il ne remplace ni les mises à jour de sécurité ni un comportement prudent de la part des utilisateurs et des utilisatrices.

Comment reconnaître une infection ?

Une infection n'est pas toujours immédiatement identifiable : les logiciels malveillants sont généralement programmés pour fonctionner discrètement. Les cybercriminels cherchent en effet à rester le plus longtemps possible indétectés. Les avertissements du programme antivirus ou du système d'exploitation constituent un indice important. Ils ne doivent en aucun cas être ignorés. En particulier lorsqu'un programme de sécurité a détecté et bloqué un logiciel malveillant, il convient d'examiner le message plus attentivement. La prudence est de mise lorsque des messages s'affichent soudainement en indiquant que l'appareil est infecté et qu'il faut appeler un numéro donné : il s'agit de tentatives d'escroquerie (fake-support).

Parmi les autres signes possibles figurent notamment :

- Extensions de navigateur inexplicables;
- Modifications inhabituelles des paramètres du navigateur ou du système;
- Publicités ou redirections inattendues dans le navigateur;
- Utilisation inhabituellement élevée du processeur, de la mémoire ou du réseau;
- L'appareil devient nettement plus lent sans raison apparente.
- Des programmes démarrent ou se ferment de manière inattendue.
- Multiplication des erreurs système;
- Des fichiers locaux ont été modifiés, supprimés ou chiffrés.
- Connexions inconnues à des comptes en ligne;
- Des messages ou des e-mails suspects ont été envoyés.
- Des mots de passe ou d'autres identifiants de connexion cessent soudainement de fonctionner.

Aucun de ces signes ne constitue à lui seul la preuve d'une infection. Un ordinateur lent peut également avoir d'autres causes. Toutefois, plusieurs observations inhabituelles simultanées devraient inciter à procéder à un examen plus approfondi.

Recommandations

- En cas de suspicion de logiciel malveillant, faites examiner votre appareil par un spécialiste.
- Les modifications apportées au système par des programmes malveillants ne peuvent souvent pas être simplement annulées. En cas d'infection, il convient donc de réinstaller entièrement le système. Des sauvegardes régulières permettent d'éviter la perte de vos données.
- Après la réinstallation, modifiez vos mots de passe pour tous vos accès en ligne (e-mail, e-banking, réseaux sociaux, etc.). Le logiciel malveillant pourrait les avoir transmis aux cybercriminels.
- Si vous utilisez également l'appareil à des fins professionnelles ou s'il s'agit d'un appareil professionnel, informez votre employeur ou le service informatique de l'entreprise
- Pour un smartphone, il est recommandé de rétablir les paramètres d'usine de l'appareil (« factory reset »), puis de le configurer à nouveau.
- Les appareils IoT peuvent eux aussi être réinitialisés aux paramètres d'usine puis configurés à nouveau. Installez la dernière version du micrologiciel, protégez l'appareil à l'aide d'un mot de passe robuste et n'autorisez aucune connexion à l'appareil depuis Internet. Si l'appareil est si ancien qu'aucun micrologiciel à jour n'est plus disponible, il convient d'envisager si possible de le remplacer.

Informations complémentaires

Appareil infecté – Que faire ?

Statistiques et chiffres actuels

Les annonces de la dernière semaine selon les catégories sont publiées sous:

Chiffres actuels