Parcours : DISCOVERY

Module : Naviguer en toute sécurité

Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

1 - Introduction à la sécurité sur Internet
2 - Créer des mots de passe forts
3 - Fonctionnalité de sécurité de votre navigateur
4 - Éviter le spam et le phishing
5 - Comment éviter les logiciels malveillants
6 - Achats en ligne sécurisés
7 - Comprendre le suivi du navigateur
8 - Principes de base de la confidentialité des médias sociaux

Tous Ces exercices ont été faits par pratique et je pense que cela ne nécessite pas une réponse détaillé ici. Merci.

9 - Que faire si votre ordinateur est infecté par un virus

Malheureusement, il peut parfois arriver que le logiciel antivirus installé sur votre ordinateur soit incapable de détecter de nouveau virus, vers ou chevaux de Troie, même s'il est à jour. La triste vérité est qu'aucun logiciel antivirus ne peut vous garantir une sécurité fiable à 100%. Si votre ordinateur est infecté, vous devrez déterminer l'origine de l'infection, identifier le fichier infecté et l'envoyer au fournisseur dont le produit n'a pas détecté le logiciel malveillant et n'a pas réussi à protéger votre ordinateur.

Néanmoins, les utilisateurs sont souvent incapables de détecter une infection sur leur ordinateur par eux-mêmes sauf s'ils sont aidés par une solution antivirus. De nombreux vers et chevaux de Troie ne révèlent jamais leur présence. Exceptionnellement, certains chevaux de Troie informent directement l'utilisateur que leur ordinateur a été infecté : il se peut qu'ils chiffrent les fichiers personnels de l'utilisateur afin de demander une rançon en échange d'un utilitaire de déchiffrement. Cependant, un cheval de Troie s'installe normalement sur un système de manière secrète et emploie des méthodes spéciales afin de rester caché. L'infection peut donc uniquement être détectée de manière indirecte.

Les symptômes d'une infection

Une augmentation du trafic sortant est généralement indicatrice d'une infection : cela s'applique aussi bien aux ordinateurs individuels qu'aux réseaux d'entreprise. Si aucun utilisateur ne travaille sur Internet pendant une période de temps spécifique (par exemple, la nuit), mais que le trafic Web continue, cela pourrait signifier que quelqu'un d'autre est actif sur le système, et il s'agit probablement d'activités malveillantes. Si un firewall est configuré sur le système, des tentatives de connexions à Internet établies par des applications inconnues peuvent également indiquer une infection. L'ouverture de nombreuses fenêtres pop-up alors que vous visitez des sites Web peut également indiquer que votre système est infecté par un

adware. Si un ordinateur se bloque ou crashe fréquemment, cela peut également être lié à l'activité d'un malware. De tels problèmes de fonctionnement proviennent plus souvent de problèmes liés au matériel ou à des logiciels qu'à des activités malveillantes. Néanmoins, si de tels symptômes se produisent simultanément sur plusieurs ordinateurs d'un même réseau, accompagnés d'une augmentation considérable du trafic interne, il y a de grandes chances qu'un vers ou qu'un cheval de Troie exploitant une backdoor se soit répandu sur le réseau.

Une infection peut également être détectée indirectement grâce à des symptômes qui ne sont pas liés à l'ordinateur, tels qu'une facture de téléphone indiquant des appels que personne n'a effectués ou des SMS que personne n'a envoyés. Ces éléments pourraient indiquer qu'un cheval de Troie a infecté votre ordinateur ou votre téléphone mobile. Si on a accéder à votre compte bancaire ou que votre carte de crédit a été utilisée sans autorisation, un spyware pourrait se trouver dans votre système.

Que faire ?

La première chose à faire est de vous assurer que les bases de données de votre antivirus sont à jour pour ensuite réaliser une analyse de votre ordinateur. Si cela n'aide pas, les solutions antivirus d'autres fournisseurs pourraient faire l'affaire. De nombreux fabricants d'antivirus offrent des versions d'essai gratuites de leurs produits : nous vous recommandons d'utiliser un de ces produits sur votre ordinateur. Si un virus ou un cheval de Troie est détecté, assurez-vous d'envoyer une copie du fichier infecté à l'éditeur de la solution antivirus qui n'a pas réussi à le détecter avant. Cela aidera ce dernier à développer une protection contre cette menace plus rapidement et à empêcher les autres utilisateurs qui utilisent également cet antivirus d'être infectés.

Si un autre antivirus ne détecte pas de malware, nous vous recommandons de déconnecter l'ordinateur d'Internet ou du réseau local, de désactiver la connexion Wi-Fi et le modem, avant de rechercher des fichiers infectés. N'utilisez le réseau que si c'est absolument nécessaire. N'utilisez surtout pas les systèmes de paiement en ligne ou les services bancaires en ligne. Évitez d'utiliser des données personnelles ou confidentielles, n'utilisez pas de site Web qui requiert un nom d'utilisateur et un mot de passe.

Comment trouver un fichier infecté

Dans certains cas, détecter un virus ou un cheval de Troie peut être complexe et peut requérir des qualifications techniques : néanmoins, dans d'autres cas cela peut être très facile et tout dépend du degré de complexité du malware et des méthodes utilisées pour cacher le code du malware intégré dans le système. Dans les cas les plus difficiles quand des méthodes spéciales (comme par exemple des technologies rootkits) sont employées pour dissimuler un code malveillant dans un système, une méthode non-professionnelle ne sera peut-être pas capable de localiser le fichier infecté. Ce problème peut nécessiter des utilitaires et des actions spéciales, comme connecter le disque dur à un autre ordinateur ou démarrer le système depuis un CD. Néanmoins, s'il s'agit d'un ver normal ou un simple cheval de Troie, vous pourrez peut-être le localiser en utilisant des méthodes relativement simples.

La grande majorité des vers et des chevaux de Troie ont besoin de prendre le contrôle de l'appareil à son démarrage. Il existe donc deux méthodes relativement simples pour cela :

- Un lien vers le fichier infecté est écrit dans les clés autorun du registre de Windows.
- Le fichier infecté est copié dans un fichier autorun de Windows.

Les dossiers autorun les plus communs sur Windows 2000 et XP sont les suivants :

%Documents and Settings%\%user name%\Start Menu\Programs\Startup\
%Documents and Settings%\All Users\Start Menu\Programs\Startup\

Il existe un certain nombre de clés autorun dans le registre du système, les clés les plus populaires incluent Run, RunService, RunOnce et RunServiceOne et elles se situent dans les dossiers suivants :

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\]
[HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\]

Il y a de grandes chances pour qu'une recherche dans ces dossiers fasse apparaitre plusieurs clés avec des noms qui ne fourniront pas beaucoup d'informations et d'accès vers les fichiers exécutables. Une attention particulière doit être portée aux fichiers situés dans le catalogue du système Windows ou dans le répertoire racine. Souvenez-vous du nom de ces fichiers, vous en aurez besoin dans l'analyse suivante.

Écrire sur la clé suivante est également une pratique commune :

[HKEY_CLASSES_ROOT\exefile\shell\open\command\]

La valeur par défaut de cette clé est » %1 » » %* « .

Le catalogue du système de Windows (et système 32) et le répertoire racine sont les endroits les plus communs pour installer des vers et des chevaux de Troie. Cela est dû à deux choses : les contenus de ces catalogues ne sont pas montrés dans l'exploreur par défaut et ces catalogues hébergent un nombre important de fichiers du système et de fonctions qui sont complètement inconnus pour un utilisateur moyen. Même un utilisateur expérimenté trouvera certainement difficile de définir si un fichier appelé winkrnl386.exe fait partie du système d'exploitation ou s'il s'agit d'un fichier étranger.

Il est recommandé d'utiliser un gestionnaire de fichiers qui pourra organiser les fichiers par date de création/modification et organiser les fichiers situés dans les catalogues mentionnés précédemment. Tous les fichiers créés et modifiés apparaitront en haut du catalogue : ces fichiers seront essentiels pour vos recherches. Si certains de ces fichiers sont identiques à ceux trouvés dans les clés autorun, il s'agit déjà d'un premier signe.

Les utilisateurs avancés peuvent également vérifier les ports de réseau ouverts en utilisant Netstat, un utilitaire standard. Nous vous recommandons également d'utiliser

un firewall et d’analyser les processus en cours dans les activités du réseau. Vérifiez également la liste des processus en cours en utilisant des utilitaires adaptés disposant de fonctionnalités avancées au lieu des utilitaires Windows standard : de nombreux chevaux de Troie réussissent à ne pas être détectés par les utilitaires Windows standard.

Il est néanmoins impossible de vous donner des conseils universels qui pourraient s’appliquer à toutes les situations. Les vers et les chevaux de Troie avancés sont souvent difficiles à localiser. Dans ce cas, il est mieux de consulter le support technique de votre fournisseur de sécurité informatique, de contacter une société offrant des services d’assistances en sécurité, ou de demander de l’aide sur des forums spécialisés. Ces ressources Web incluent www.virusinfo.info, www.rootkit.com et www.gmer.net (en anglais). De nombreuses sociétés antivirus disposent également de forums similaires conçus pour aider les utilisateurs.

Source : https://encyclopedia.kaspersky.fr/knowledge/what-if-my-computer-is-infected/