Virus et autres menaces sur Internet

La sécurité d'un système passe également par le contrôle de ce que font les applications sur ce système, et la détection de tout comportement anormal.

Voici une liste des principaux types d'applications qui peuvent être néfastes pour votre ordinateur :

- Virus : c'est un programme qui est capable d'infecter des fichiers et de se propager en utilisant des supports amovibles ou les réseaux.
- Ver : programme qui se répand d'un ordinateur à l'autre via les réseaux.
- Ransomware : crypte et bloque l'utilisation de vos données en échange d'un paiement.
- Spyware ou logiciel espion : désigne un programme qui espionne puis transmet des informations confidentielles vous concernant à une tierce personne.
- Adware : traque vos habitudes sur Internet et peut, par exemple, afficher des fenêtres publicitaires en fonction du profil qui a été défini. De nombreux sites web peuvent installer, à votre insu, ce type de logiciel.
- Enregistreur de frappe (keylogger) : programme qui enregistre toutes les données saisies au clavier et les transmet (mots de passe, numéro de carte bancaire...).
- Drive-by download : désigne un programme qui se télécharge sans votre consentement. Cela peut arriver quand vous essayez de fermer une boîte de dialogue.
- Redirecteur de page : désigne un programme qui va rediriger une partie ou l'ensemble des pages prédéfinies (page d'accueil, de recherche, etc.) vers un site malveillant.
- Spam : désigne un e-mail commercial qui n'est pas sollicité.
- BHO ou *Browser Helper Objects* ou Hijacker : désigne un programme qui permet de personnaliser et de contrôler certains paramètres d'un navigateur comme Internet Explorer. Il peut donc être proposé soit à des fins "pacifiques" (la barre d'outils proposée par Google) ou malveillantes.
- Dialer : désigne un programme qui va établir, en plus de votre connexion par défaut, une connexion d'accès à distance à un tarif surfacturé.
- Trojan ou Cheval de Troie : désigne un programme qui contient des fonctions cachées pouvant s'exécuter en arrière-plan à l'insu de l'utilisateur. Ils donnent un accès à la machine sur laquelle il est exécuté en ouvrant une porte dérobée (Backdoor).

Signalons que la frontière entre ces types de menaces reste floue et que beaucoup de programmes malicieux peuvent utiliser différentes techniques pour se développer.

1. Le centre de Sécurité Windows

Windows 10 propose par défaut et de manière centralisée un système de protection, **Sécurité Windows**, une sorte de panneau de configuration vérifiant différents paramètres de votre ordinateur :

- **Protection contre les virus et menaces** : il détecte la présence d'un antivirus tiers ou propose l'antivirus Windows Defender et s'assure de sa mise à jour.
- **Protection du compte** : gestion des informations du compte de l'utilisateur et sa synchronisation.
- **Pare-feu et protection du réseau** : il redirige vers l'interface de gestion du pare-feu, vue précédemment.
- **Contrôle des applications et du navigateur** : cette partie, également appelée SmartScreen, permet de filtrer les applications téléchargées via le navigateur ou Windows Store et les sites web consultés, en s'assurant qu'ils sont sans danger. Il compare les fichiers téléchargés ou les sites visités à une liste de fichiers dangereux ou de sites de hameçonnage et, le cas échéant, bloque le téléchargement ou le chargement du site tout en vous prévenant. Ce filtre est désactivable si vous constatez qu'il vous empêche de télécharger un fichier fiable ou de visiter un site de

confiance.

- **Sécurité des appareils** : cette section gère la sécurité du matériel via les fonctionnalités offertes matériellement par la machine.
- **Performances et intégrité de l'appareil** : cette catégorie vérifie certains paramètres comme l'espace de stockage, les pilotes de périphériques...
- **Options de contrôle parental** : il vous redirige vers votre compte Microsoft en ligne où vous pourrez paramétrer les comptes Microsoft des membres de votre famille qui se connectent à Internet, ainsi que les différents appareils que vous souhaitez surveiller.

2. Supprimer un virus

Rappelons tout d'abord quelques règles essentielles :

- Votre antivirus doit être constamment tenu à jour.
- Vous ne devez pas installer plusieurs antivirus à la fois sous peine de provoquer des conflits système.
- Ce n'est pas parce qu'un antivirus est gratuit qu'il est moins efficace que les autres produits qui sont payants.
- En dépit des affirmations des spécialistes et des tests dans les revues spécialisées, la majorité des antivirus se valent !
- Il y a des comportements à risque et d'autres non !

Une manière de dire que c'est souvent une affaire de bon sens et que les gens qui se plaignent du manque d'efficacité de leur antivirus sont souvent les plus grands consommateurs de sites "adultes" et de réseaux de Peer-To-Peer.

Voici maintenant un scénario classique d'éradication d'un virus.

→ Procédez à une mise à jour des définitions de virus.

Si vous n'avez plus accès à Internet, téléchargez à partir d'une autre machine le dernier fichier de définition de virus afin de pouvoir procéder manuellement à la mise à jour. La plupart des antivirus proposent en effet un fichier de définitions qu'il est possible de télécharger si votre antivirus ne peut plus procéder à une mise à jour automatique de la base de définitions virales.

→ Désactivez le processus de restauration système sur tous les lecteurs.

Sous les systèmes NT, ce répertoire fait partie des emplacements protégés. Un antivirus n'y a pas accès, mais souvent un virus est capable de se loger dans les fichiers qui sont stockés dans ce répertoire. Autrement dit, vous ne pourrez pas éradiquer un virus tant que cette fonctionnalité est active (cf. chapitre Maintenance du système).

→ Débranchez physiquement votre connexion Internet en enlevant le câble USB ou Ethernet, ou en déconnectant le Wi-Fi.

C'est une manière de s'assurer que le virus ne puisse plus communiquer avec l'extérieur et utiliser d'autres informations pour cacher sa présence à votre antivirus.

→ Redémarrez en mode sans échec.

→ Procédez à une vérification complète de tous les lecteurs.

Il n'est pas toujours possible de lancer un antivirus à partir du mode sans échec puisqu'il se peut que, dans ce mode, certains services qui sont nécessaires à son exécution ne soient pas démarrés.

- Redémarrez en mode normal.
- Dans un moteur de recherche comme Google, lancez une requête en saisissant simplement le nom du virus. En cherchant bien, vous allez trouver des pages, des sites d'éditeurs d'antivirus qui expliquent la façon de supprimer manuellement un virus ou un cheval de Troie. La plupart du temps, cela consiste à supprimer des entrées présentes dans le Registre et des fichiers dans l'Explorateur Windows.
- Une fois que vous êtes sûr que votre ordinateur est "sain", vous pouvez réactiver la fonctionnalité de restauration système.

Mon expérience me fait dire que beaucoup d'antivirus ne détectent pas correctement toutes les menaces et notamment celles créées par les spywares ou certains chevaux de Troie. N'hésitez pas dans ce cas à utiliser plusieurs programmes de désinfection. Oui ! C'est parfois un vrai parcours du combattant.

3. Les antivirus gratuits

Les adresses suivantes permettent de télécharger ou d'utiliser en ligne des solutions antivirus gratuites proposées par les plus grands éditeurs spécialisés en sécurité. Ces outils ne remplaceront pas les produits payants plus complets, mais offrent une sécurité de base pour protéger efficacement votre ordinateur contre les principales menaces.

- https://security.symantec.com/getnss.aspx
- https://www.trendmicro.com/en_us/forHome/products/housecall.html
- https://www.bitdefender.com/solutions/free.html
- https://www.kaspersky.fr/free-cloud-antivirus
- https://www.avast.com
- https://www.avira.com
- https://www.avg.com/fr-fr/homepage#pc
- https://www.pandasecurity.com/fr/homeusers/solutions/free-antivirus/

Un site offrant des liens vers plusieurs outils, mais apparemment souffrant de mises à jour :

- http://www.secuser.com/telechargement/index.htm

4. Les outils spécialisés

Ce sont de simples fichiers exécutables qui permettent de supprimer un virus bien précis. L'avantage est que cela peut remédier à une situation compromise si votre antivirus n'était pas à jour.

- http://www.symantec.com/business/security_response/removaltools.jsp
- https://www.bitdefender.com/toolbox/
- https://www.kaspersky.fr/downloads/thank-you/free-virus-removal-tool
- https://www.sophos.com/fr-fr/products/free-tools/virus-removal-tool.aspx
- https://docs.microsoft.com/fr-fr/windows/security/threat-protection/intelligence/safety-scanner-download
- http://www.secuser.com/telechargement/desinfection.htm

5. Outil de suppression des logiciels malveillants

L'outil de suppression des logiciels malveillants (MRT, *Microsoft Removal Tool*) est régulièrement installé et amélioré à chacune de vos mises à jour mensuelles avec Windows Update.

Pour l'exécuter, dans la barre de recherche, saisissez `mrt.exe`.

Il est également possible de vérifier votre disque à partir des fonctionnalités WinRE. Cela peut être éventuellement utile si vous n'avez plus d'accès en mode normal et que votre antivirus ne peut se lancer à partir du mode sans échec.

Voyons comment procéder :

- Une fois que vous avez démarré à partir du DVD-ROM d'installation de Windows 10, cliquez sur le lien **Réparer l'ordinateur**, puis accédez en mode d'invite de commandes.

Vous allez retrouver le prompt **x:\sources>**.

- En utilisant la commande `cd`, allez sur le répertoire : C:\Windows\System32. Saisissez ensuite la commande : `mrt.exe`.
- Cochez enfin le bouton radio correspondant au type d'analyse que vous souhaitez effectuer, puis laissez-vous guider par l'assistant.

Les commutateurs autorisés sont les suivants :

- `/Q` ou `/quiet` : mode silencieux, aucune interface n'est affichée.
- `/?` ou `/help` : affiche la syntaxe et la version du moteur de détection.
- `/N` : mode détection seule.
- `/F` : effectue une analyse complète.
- `/F:Y` : effectue une analyse complète et nettoie les fichiers infectés.

6. Désinstaller complètement un antivirus

Si la suppression de votre antivirus ne fonctionne pas via la fonctionnalité d'ajout/suppression de programme de Windows disponible dans le Panneau de configuration, il faudra supprimer manuellement votre antivirus.

Dans la majorité des cas, il faut vous procurer un programme spécialisé que vous pourrez télécharger sur le site de l'éditeur. Prenons l'exemple des produits Symantec : Norton Removal Tool est un outil vous permettant de désinstaller tous les produits Norton présents dans le système. Avant de continuer, vérifiez que vous disposez des CD d'installation ou des fichiers d'installation téléchargés pour les produits Norton à réinstaller. Il est compatible avec toutes les versions NT de Windows. Vous pouvez le télécharger directement sur le site de la société Symantec à partir de cette adresse : https://support.norton.com/sp/fr/fr/home/current/solutions/v60392881

McAfee fournit le même genre d'aide dans sa section support.