Savoir détecter une éventuelle infection

Comment détecter la présence d'un virus sur son ordinateur ? Plus vous vous en rendez compte tôt, plus vous serez aptes à le traiter et à le supprimer. Comment procéder ? Apprenez à repérer certains signes qui ne trompent pas.

1. Votre ordinateur fonctionne au ralenti

Votre ordinateur se montre particulièrement lent, et ce sans raison particulière. Les logiciels malveillants peuvent exécuter des tâches en arrière-plan qui consomment beaucoup de ressources et ralentissent ainsi votre machine. Toutefois, d'autres raisons peuvent l'expliquer : mémoire insuffisante, disque dur rempli, batterie défectueuse…

2. Votre PC est incontrôlable

Des pop-ups intempestives, des fenêtres de dialogue imprévisibles, des publicités multiples apparaissent soudainement sur votre bureau ? Des programmes démarrent ou se ferment automatiquement ? Impossible d'ouvrir certaines applications ? Autant de signes qui témoignent de la présence possible d'un logiciel malveillant sur votre PC. Certains virus endommagent en effet Windows ou certains de vos programmes. Résultat : Windows peut s'arrêter inopinément et les applications se montrent hors de contrôle.

3. Internet ne fonctionne plus ou mal

Un malware peut se connecter à des sites malveillants à votre insu et réduise ainsi la bande passante disponible. Le débit est alors fortement ralenti ou le réseau inaccessible. De même, de nombreuses fenêtres non désirées s'ouvrent, votre page d'accueil a été modifiée sans restauration possible, votre adresse IP a été blacklistée... Attention, de nombreux virus sont en effet conçus pour vous amener sur des sites malveillants et tenter de soutirer vos informations personnelles telles que vos données bancaires ou vos mots de passe.

4. Votre environnement de travail a changé

Des dossiers ont disparu, de nouveaux fichiers sont apparus, certains vous demandent désormais un code d'accès pour s'ouvrir, des barres d'outils inconnues apparaissent ? Vérifiez que vos fichiers n'ont pas été déplacés lors d'une mise à jour de votre système d'exploitation. En revanche, si vous recevez une demande de « rançon » pour ouvrir ces fichiers attention, il s'agit bel et bien d'un virus.

5. Plus de trace de votre antivirus ou de votre firewall

Votre antivirus a soudainement disparu et votre firewall a été désactivé sans votre intervention ? La première action des virus est de s'en prendre à vos systèmes de sécurité pour tenter de les neutraliser. Si seul l'un de vos systèmes est désactivé, pas de panique. Il peut s'agir d'un problème de licence ou de mise à jour. Essayez alors de télécharger ou de réinstaller votre antivirus. Mais si tous les systèmes se révèlent indisponibles ou que vous ne parvenez pas à exécuter l'antivirus, alors votre PC est sûrement infecté.

6. Impossible d'accéder à votre disque dur et/ou à vos périphériques

Votre disque dur est inaccessible ? De même, vous ne parvenez plus à ouvrir votre lecteur CD/DVD ou à imprimer correctement ? Autre signe : les bibliothèques de jeux et de logiciels ont disparu de votre ordinateur. Vous pouvez essayer de réinstaller ces matériels car une désinstallation incomplète ou mal effectuée peut en être à l'origine. Mais il se peut aussi qu'il s'agisse d'un logiciel malveillant.

7. Les boîtes de dialogue et les menus apparaissent déformés

Les icônes de votre bureau présentent un aspect inhabituel, vos boîtes de dialogue ou les menus n'ont plus la même apparence. Ou pire, vous avez perdu toutes les icônes de votre bureau soudainement. Il peut s'agir d'un problème d'affichage – donc pensez à vérifier vos paramètres – ou d'un virus.

8. Votre ordinateur vous parle en langue étrangère

Do you speak English? Sprechen sie deutsch? La langue des menus, des programmes… a été changée ? Votre écran bascule également dans une langue étrangère… Vérifiez d'abord les mises à jour récentes de votre système. Si aucune n'a été effectuée, alors votre PC est infecté.

9. Votre ordinateur fonctionne seul

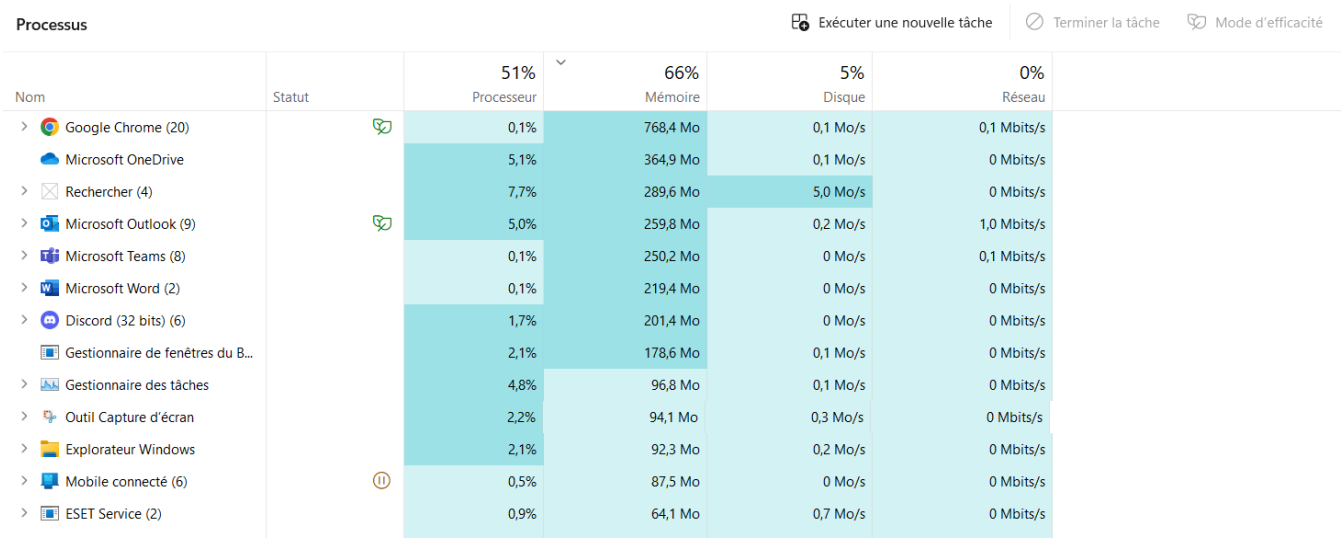
Votre PC agit sans même votre intervention ou se bloque ? Votre modem ou votre disque dur fonctionne sans raison apparente ? Vous constatez que des emails ont été envoyés sans jamais les avoir rédigés, que des fenêtres web s'ouvrent ou se ferment d'elles-mêmes ? Votre ordinateur s'éteint brusquement, redémarre sans arrêt ou ne démarre plus normalement ? Il est probable qu'un logiciel malveillant en a pris possession.

Apporter une solution appropriée

1 - Le gestionnaire de tâches Windows

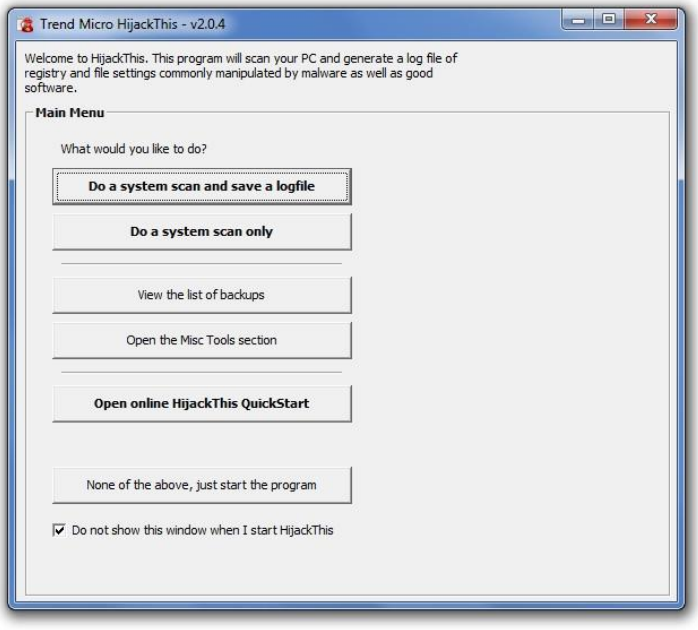
Sur un ordinateur sous Windows, le gestionnaire de tâches peut fournir des informations permettant d'identifier des processus suspects. Pour détecter ces derniers plus facilement, il est donc préférable de connaître précisément les processus légitimes.

Attention toutefois puisqu'un programme malveillant peut parfois se dissimuler derrière un processus normal. Pour détecter des anomalies, il suffit d'observer la consommation de mémoire et de ressources processeur. Les programmes malveillants se montrent dans certains cas gourmands, même si les cybercriminels s'efforcent désormais de faire preuve de discrétion.



Nom	Statut	51% Processeur	66% Mémoire	5% Disque	0% Réseau
Google Chrome (20)		0,1%	768,4 Mo	0,1 Mo/s	0,1 Mbits/s
Microsoft OneDrive		5,1%	364,9 Mo	0,1 Mo/s	0 Mbits/s
Rechercher (4)		7,7%	289,6 Mo	5,0 Mo/s	0 Mbits/s
Microsoft Outlook (9)		5,0%	259,8 Mo	0,2 Mo/s	1,0 Mbits/s
Microsoft Teams (8)		0,1%	250,2 Mo	0 Mo/s	0,1 Mbits/s
Microsoft Word (2)		0,1%	219,4 Mo	0 Mo/s	0 Mbits/s
Discord (32 bits) (6)		1,7%	201,4 Mo	0 Mo/s	0 Mbits/s
Gestionnaire de fenêtres du B...		2,1%	178,6 Mo	0,1 Mo/s	0 Mbits/s
Gestionnaire des tâches		4,8%	96,8 Mo	0,1 Mo/s	0 Mbits/s
Outil Capture d'écran		2,2%	94,1 Mo	0,3 Mo/s	0 Mbits/s
Explorateur Windows		2,1%	92,3 Mo	0,2 Mo/s	0 Mbits/s
Mobile connecté (6)		0,5%	87,5 Mo	0 Mo/s	0 Mbits/s
ESET Service (2)		0,9%	64,1 Mo	0,7 Mo/s	0 Mbits/s

2- HiJackThis (trend micro)



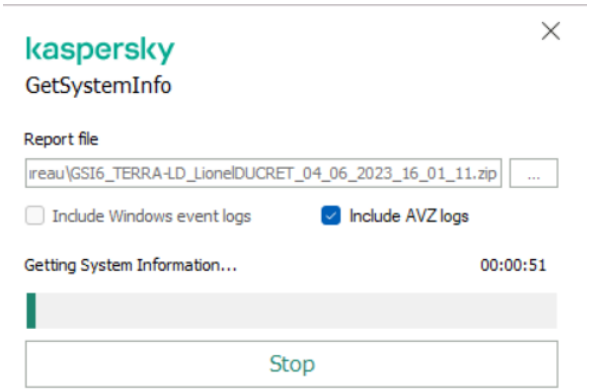
HijackThis est un utilitaire gratuit très performant, mais pas forcément facile d'accès. Sa fonction est de scanner un système afin de lister les paramètres susceptibles d'avoir été altérés par des programmes malveillants, tels que des spywares ou des adware.

Le scan effectué, HijackThis génère un rapport très utile pour établir un diagnostic (conservez le log une fois sain afin de

disposer à l'avenir d'une image de votre système). Sur de nombreux forums, les internautes apportent leur connaissance technique pour aider les utilisateurs moins expérimentés à décrypter le rapport.

Des sites comme HiJackThis.de Security et NetworkTechs.com proposent de copier le log fourni par l'application et d'obtenir une analyse automatique.

3 - GetSystemInfo



Kaspersky propose un outil comparable à HiJackThis : GetSystemInfo. L'utilitaire effectue une analyse du système et génère un rapport (sysinfo.txt). Grâce au parser en ligne de l'éditeur, il est alors possible d'obtenir une analyse automatique et donc des informations utiles pour identifier les causes d'un dysfonctionnement.

Précaution : comme pour HijackThis, il est préférable d'être un utilisateur expérimenté pour comprendre les rapports et agir en conséquence, notamment en ignorant certaines recommandations faites par l'application.

4 - Microsoft Baseline Security Analyzer

Prévenir, c'est guérir. Pour bloquer les virus avant même une infection, il suffit parfois simplement de détecter et corriger les vulnérabilités de son système. Pour cela, il existe divers scanneurs de vulnérabilités sur Internet, notamment gratuits, comme Microsoft Baseline Security Analyzer.

MBSA permet de faire de l'audit de vulnérabilité en local ou en réseau via un nom de domaine ou une plage d'adresses IP. Dans un rapport, l'outil liste les paramétrages à risque (par exemple un compte invité actif) et les correctifs logiciels manquants.

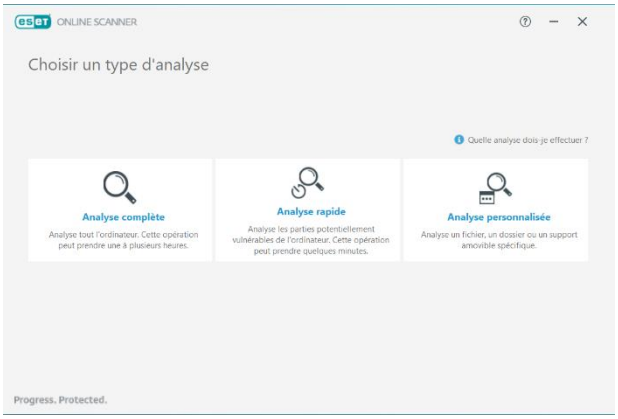
5 – Utiliser un Antivirus

Pas de vulnérabilités, pas de malware ? Malheureusement, ce n'est pas toujours aussi simple, surtout lorsqu'un virus, pour s'exécuter sur un ordinateur, exploite une vulnérabilité encore inconnue (exploit zero-day).

Lien vers un site google qui recense les Zero-day

https://googleprojectzero.blogspot.com/

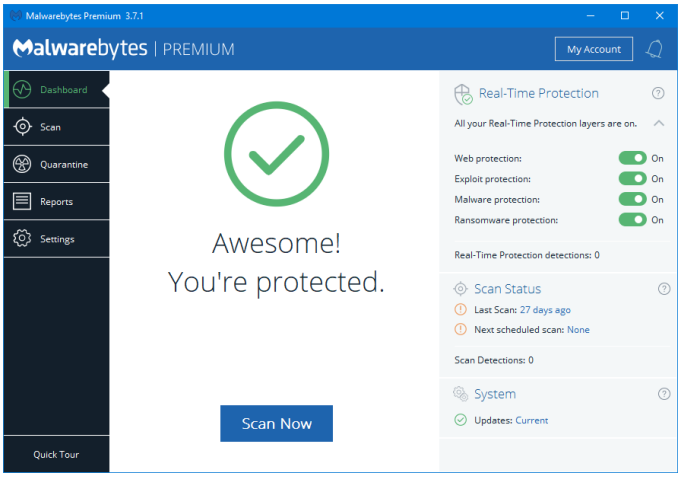
Dans ces situations, il est préférable de disposer d'un antivirus, même si aucune de ces technologies n'est infaillible. Un antivirus payant sera préférable à un antivirus gratuit (de base Windows 10 et plus) intègre un antivirus gratuit « Defender »



Vous pouvez aussi utiliser un Antivirus online (par exemple : Eset oneline Scanner) pour faire un scan et détecter le/les malwares

https://www.eset.com/lu-fr/particuliers/online-scanner/

6 - Malwarebytes Anti-Malware



Méconnu mais efficace, sans pour autant être infaillible, notamment en matière de détection des rootkits. MBAM est disponible en version gratuite ou payante, avec dans cette dernière un mode de protection temps réel.

Léger, MBAM est accessible en français, exécute des scans rapidement et, dans la grande majorité des cas, parvient à détecter et supprimer les programmes malveillants.

Produits que je vous recommande pour faire une analyse en cas de doute

7 – Cybermalveillance.gouv.fr

En cas de doute vous pouvez aussi aller sur le site de Cyber-malveillance du gouvernement ou vous pourrez réaliser un diagnostic, suivi des préconisations associées.

https://www.cybermalveillance.gouv.fr/diagnostic/profil

8 – Restauration Usine

En dernier recours et si, après toutes ces recommandations, les symptômes persistent, il serait utile de penser à réinstaller votre appareil ou de le remettre en configuration d'usine. Comme pour la restauration du système, référez-vous à la documentation de votre appareil pour en savoir plus ou bien effectuez une recherche sur un moteur de recherche.

Si les symptômes persistent, cela peut signifier aussi que votre appareil n'est peut-être pas infecté par un virus. En effet, avec le temps, les ordinateurs ou les téléphones mobiles peuvent ralentir en raison de l'installation de nombreux logiciels ou applications sur l'appareil qui sont très consommateurs en ressources.

De même, avec les usages d'Internet et autres nouveaux logiciels qui sont en constante augmentation, les ressources requises pour les faire fonctionner sont de plus en plus importantes, ce qui peut ralentir un appareil "ancien" qui aura besoin de plus de temps pour remplir la tâche qui lui sera demandée.

SÉCURITÉ LOGICIEL ET MATÉRIEL