

Procédure de nettoyage complet et gratuit d'un PC

Cette procédure à usage des particuliers et professionnels détaille comment nettoyer entièrement un ordinateur PC simplement et gratuitement. Son objectif est de nettoyer au maximum votre ordinateur pour le rendre le plus léger, le plus optimisé possible, mais surtout le débarrasser des virus et autres malwares.

Pourquoi suivre cette procédure ?

- Suite à un piratage ou une intrusion sur votre ordinateur,
- L'ouverture automatique de nombreuses fenêtres, d'une page d'accueil anormale ou tout autre fonctionnement anormal,
- Contre les virus, les malwares, les barres de navigateurs, les spywares,
- Pour gagner en performance et optimiser votre système,
- Pour réinitialiser le PC et améliorer sa rapidité.

Cette procédure longue mais complète est simple à appliquer mais vous prendra une bonne demi-journée pour tout exécuter. Il est possible d'opter pour une version allégée si vous préférez aller à l'essentiel, pour cela utilisez seulement les opérations suivies d'une étoile "*". Les délais sont donnés à titre indicatif, certains dépendent de la capacité du disque dur (nous noterons "DD" dans ce cas). D'autre part, si l'exécution d'un programme nécessite un redémarrage de l'ordinateur, nous l'indiquerons par "reboot".

La procédure est basée essentiellement sur l'utilisation successive des divers logiciels sélectionnés et validés pour leurs qualités. Faites bien attention à télécharger ces applications directement sur le site des éditeurs (utilisez de préférence les liens que nous indiquons) afin d'éviter qu'eux-mêmes n'installent de programmes superflus.

Certaines actions sont faites en double, voire en triple, car les logiciels n'optimisent pas de la même manière et ne détectent pas les mêmes éléments. Évidemment, un grand nombre d'actions réalisées sont redondées, mais la complémentarité des solutions permet tout de même de garantir une qualité du résultat global.

Pour désinstaller les différents logiciels proposés dans cette procédure, nous vous conseillons d'utiliser le logiciel Revo Uninstaller Freeware Portable (<http://www.revouninstaller.com/>) afin que toutes les traces soient réellement supprimées (préférer la version 'Portable' présente en bas de la page de téléchargement afin d'éviter l'installation d'un outil supplémentaire).



Ce guide a été écrit par @Sekurigi, un blog d'actualités sur la sécurité informatique : <http://www.sekurigi.com/> . Si vous souhaitez nous soutenir, merci de suivre notre compte twitter : <https://twitter.com/sekurigi> .

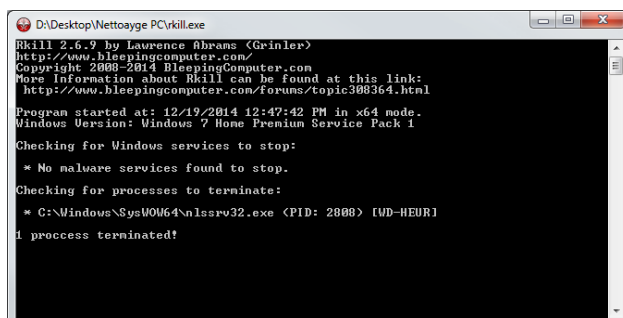
Supprimer les Malwares et barres d'outils et les programmes indésirables

Nous passons volontairement un grand nombre d'applications différentes, car chacune utilise ses propres bases qui assurent une certaine exhaustivité. La première étape consiste à désactiver les programmes malveillants avant l'analyse :

1) RKill (≈ 3')

<http://bleepingcomputer.com/download/rkill/>
[rkill.exe]

RKill est un programme qui arrête les processus et supprime les raccourcis des malwares connus afin que les logiciels de sécurité normale puissent nettoyer votre ordinateur des infections (cela permet d'éviter qu'un malware ne bloque l'antivirus). S'exécute directement sans installation.



```
D:\Desktop\Nettoyage PC\rkill.exe
Rkill 2.6.9 by Lawrence Abrams (Grinler)
http://www.bleepingcomputer.com/
Copyright 2008-2014 BleepingComputer.com
More Information about Rkill can be found at this link:
http://www.bleepingcomputer.com/forums/topic308364.html

Program started at: 12/19/2014 12:47:42 PM in x64 mode.
Windows Version: Windows 7 Home Premium Service Pack 1

Checking for Windows services to stop:
* No malware services found to stop.

Checking for processes to terminate:
* C:\Windows\System0064\nlsrv32.exe (PID: 2808) [WD-HEUR1]
1 process terminated!
```

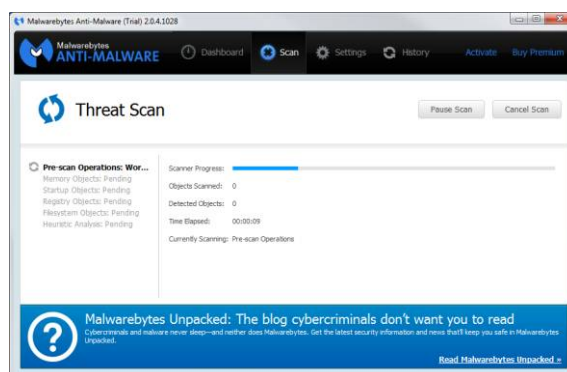
Télécharger et exécuter successivement les logiciels suivants. Désactiver ou supprimer votre antivirus avant d'exécuter les programmes.

2) Malwarebytes Anti-Malware Gratuit * (≈ 20')

<http://fr.malwarebytes.org/antimalware/>
[mbam-setup-2.0.4.1028.exe]

Malwarebytes est un programme de sécurité rapide et excellent pour la suppression des malwares. Le logiciel est mis à jour très régulièrement.

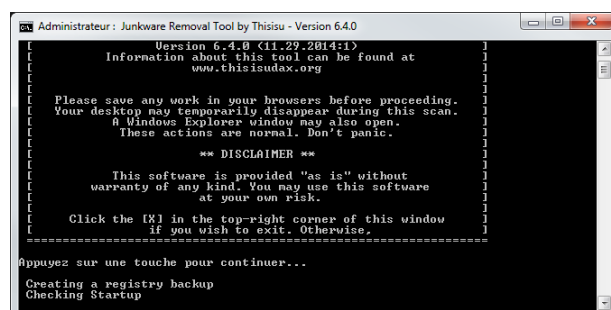
Après installation, une mise à jour automatique est lancée, cliquer ensuite sur "Scan now", puis "Apply Actions". Désinstaller ensuite le programme.



3) Junkware Removal (≈ 30' à 50' selon DD)

<http://www.bleepingcomputer.com/download/junkware-removal-tool/dl/131/>
[JRT.exe]

Junkware Removal Tool est un utilitaire de sécurité qui recherche et supprime les adwares, les barres d'outils et les programmes potentiellement indésirables (PUP) de votre ordinateur . Les



tactiques communes entre éditeurs freeware est d'offrir leurs produits gratuitement, mais les grouper avec PUP afin de gagner des revenus. Cet outil vous aidera à supprimer ces types de programmes.

Il s'exécute directement sans installation en mode console.

4) SUPERAntiSpyware Portable Scanner Personal Edition (≈ 20' à 40' selon DD)

<http://superantispyware.com/portablescannerhome.html>
[SAS_987B92.EXE]

Il détecte et supprime les logiciels espions, logiciels publicitaires et supprime les logiciels malveillants, chevaux de Troie, vers, keyloggers, pirates de l'air, parasites, rootkits, Rogue Security Products et de nombreux autres types de menaces. Effectue également quelques réparations sur le système.

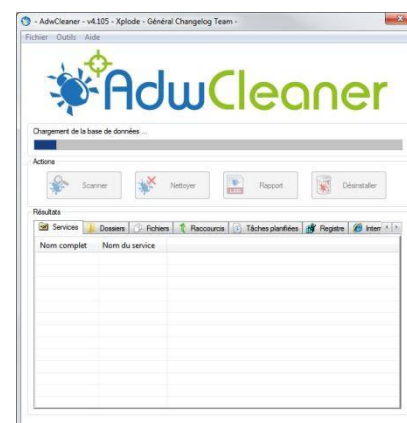


Nécessite une installation (malgré le titre "portable") en conservant tout par défaut, puis décliner la version pro, cliquer sur "Scan this Computer", puis "Complete Scan", puis "Continue" à la fin de l'analyse pour supprimer les éléments suspects. Désinstaller le programme après utilisation.

5) AdwCleaner * (≈ 10' + Reboot)

<http://general-changelog-team.fr/fr/downloads/viewdownload/20-outils-de-xplode/2-awcleaner>
[adwcleaner_4.105.exe]

AdwCleaner est un nouveau nettoyeur développé par Xplode qui vise à supprimer tous les adwares, les PUPs/LPIs (Logiciels potentiellement indésirables).



S'exécute sans installation préalable, mais bien s'assurer d'utiliser la dernière version du programme. Cliquer sur "Scanner", puis "Nettoyer". Un reboot sera nécessaire.

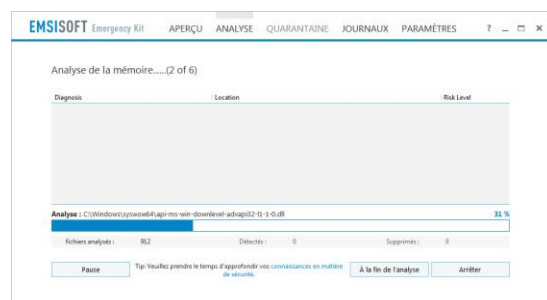
Supprimer les virus et autres logiciels malveillants

L'objectif de cette phase consiste à passer des kits de nettoyages antivirus puissants qui soient capables de détecter tous types de malwares différents. Ces outils sont complémentaires et permettent à eux tous un très haut niveau de détection. De manière générale, bien que beaucoup plus longue, nous conseillons l'option de scan complet sur chacun d'eux.

6) Emsisoft Emergency Kit * (≈ 1h30 selon DD)

<http://www.emsisoft.fr/fr/software/eeek/>
[EmsisoftEmergencyKit.exe]

Emsisoft Emergency Kit est un ensemble de logiciels qui vous permettent, sans les installer, d'analyser un ordinateur infecté de manière simple et rapide, pour voir s'il y a des malwares.



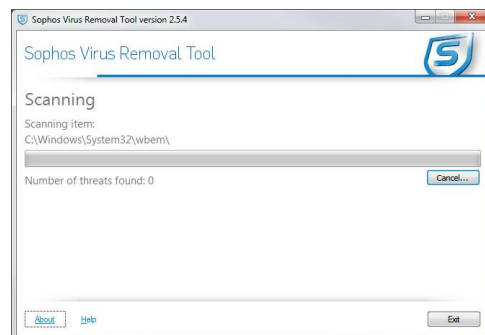
Lancer l'installation, exécuter "Start Emsisoft Emergency Kit" sur le bureau en effectuant une recherche de mise à jour (≈ 15'), puis lancer l'analyse en cliquant sur "Balayer" en mode "Analyse complète", avec les "Logiciels PUPs". Supprimer l'ensemble des éléments trouvés "Supprimer choisis", pour terminer, supprimer le dossier "C:\EEK" et l'icône sur le bureau.

7) Sophos VirusTool (≈ 1h30 selon DD)

<http://www.sophos.com/fr-fr/products/free-tools/virus-removal-tool.aspx>

[Sophos Virus Removal Tool.exe]

Avec sa technologie de pointe, ce puissant outil détecte tous les types de logiciels malveillants sur votre ordinateur, y compris les virus, les spywares, les rootkits et Conficker et le remet en parfait état de fonctionnement.



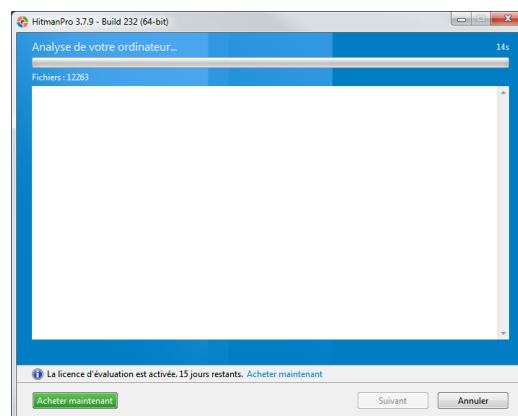
Installer, puis lancer "Sophos Virus Removal Tool", "Start scanning" puis après suppression des éléments trouvés, désinstaller le programme.

8) Surfright Hitman Pro 3 * (≈ 15mns)

<http://www.surfright.nl/en/hitmanpro/>

[HitmanPro_x64.exe]

HitmanPro 3 est un outil rapide tout- en-un pour localiser, identifier et supprimer les virus, logiciels espions, chevaux de Troie, rootkits et autres malwares. HitmanPro 3 va rapidement montrer si votre PC est infecté par des logiciels malveillants. HitmanPro 3 utilise des techniques innovantes de cloud computing pour détecter et supprimer les menaces de logiciels malveillants potentiels avec un impact minimal sur les performances du système.



Lancer l'installation, accepter tous les paramètres par défaut en cliquant plusieurs fois sur "Suivant", l'activation gratuite (saisir une adresse email) est nécessaire pour pouvoir supprimer les problèmes. Puis désinstaller le programme.

9) Comodo Cleaning Essentials (≈ 2h15 selon DD avec Reboot)

https://www.comodo.com/business-security/network-protection/cleaning_essentials.php

[cce_2.5.242177.201_x64.zip]

CCE est un ensemble d'outils de sécurité puissants conçus pour aider les utilisateurs à identifier et supprimer les logiciels malveillants et les processus dangereux à partir d'ordinateurs Windows. Conçu comme une application portable, le logiciel ne nécessite aucune installation et peut être lancé directement depuis un support amovible comme une clé USB.



C'est un des programmes les plus longs en temps d'exécution car il va au fond des choses. Dézipper tout d'abord le fichier zip, puis exécuter le programme "CCE.exe", accepter les conditions et lancer "Full Scan", puis supprimer le répertoire "CCE".

Optimiser et nettoyer votre ordinateur

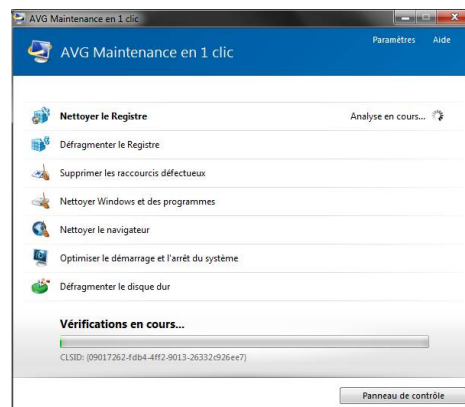
Ces outils ont pour objectifs de nettoyer l'ordinateur des traces laissées par l'installation de logiciels et autres outils, de faire de la place et de remettre d'équerre certains paramètres. Ils permettent également l'optimisation du système par la désactivation de fonctions inutiles ou la modification de certaines configurations.

10) AVG PC TuneUp (≈ 20')

<http://www.tuneup.fr/>

[avg_tuht_stf_fr_2015_238_15cmp15.exe]

AVG PC TuneUp est un ensemble d'outils avancés d'optimisation des performances qui aident les utilisateurs à bénéficier de temps de chargement rapides de leurs applications. Ceci leur permet de travailler plus rapidement et de bénéficier d'un fonctionnement des jeux beaucoup plus fluide.



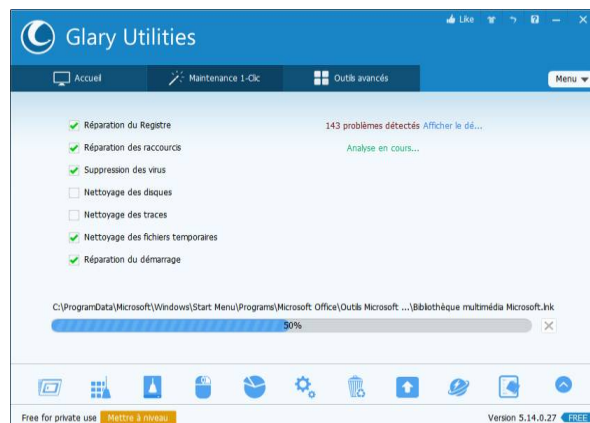
Installer le produit et "Démarrer l'analyse maintenant", puis "Exécuter la maintenance". Une fois que c'est terminé vous pouvez lancer : "Analyse" la "Performance de l'ordinateur" en plus et "Réparer maintenant" de l' "État de l'ordinateur". Désinstaller le programme.

11) Glary Utilities 5 * (≈ 15')

<http://www.glarysoft.com/>

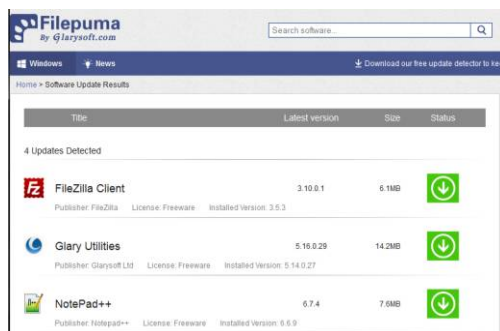
[gu5setup.exe]

Utilitaire puissant et tout-en-un pour nettoyer votre PC, augmente la vitesse du PC et corrige les erreurs de paramétrage système et de blocage.



Après l'installation, vérifier les mises à jour, puis dans l'onglet " Maintenance 1-Clic", cliquer sur "Analyser". Si vous avez un peu de temps, cocher l'ensemble des cases, sinon laisser celles par défaut.

Pour terminer cliquer sur "Réparer", puis désinstaller le programme.



Cet outil intègre également un module de vérification des versions des applications installées sur votre ordinateur nommé Filepuma. L'idéal serait d'avoir tous les logiciels à jour. Nous vous conseillons donc de faire le nécessaire pour les mettre à jour en téléchargeant et installant successivement les dernières versions de chaque logiciel.

12) Slowin' Killer (≈ 5' à 30' selon le nombre de logiciels à supprimer)

<http://www.security-helpzone.com/download/slowin%20killer/>

[Slowin Killer.exe]

Slowin' Killer est un outil d'optimisation tout-en-un pour optimiser votre ordinateur sur : optimisation du registre, désactivation des services inutiles, suppression des fichiers inutiles, détection des logiciels installés inutiles, détection des logiciels lancés au démarrage inutiles et détection des raccourcis corrompus.



Installer le logiciel, puis cliquer successivement sur "Analyse" puis "Optimiser", nous vous conseillons de le faire onglet par onglet, l'un après l'autre. Désinstaller le programme.

Supprimer les applications inutiles

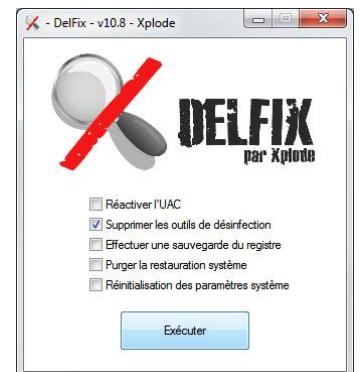
L'objectif de cette phase est de supprimer de l'ordinateur toutes les applications inutiles qui consomment de l'espace et des ressources inutilement.

13) Delfix (≈ 5')

<https://toolslib.net/downloads/viewdownload/2-delfix/>

[delfix_10.8.exe]

DelFix est un programme permettant la suppression d'un grand nombre d'outils de désinfection. Par défaut, seule la case "Supprimer les outils de désinfection" est cochée, et si celle-ci est cochée Delfix se supprimera lui-même à la fin des opérations.



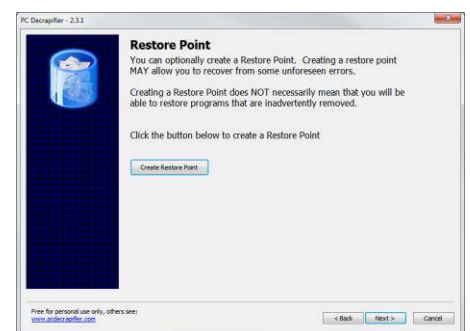
Après lancement, tout cocher, puis "Exécuter".

14) PCDecrapfier (≈ 5' à 30' selon les applications)

<http://www.pcdecrapfier.com/download>

[pc-decrapfier-2.3.1.exe]

Cet outil a pour objectif de vous aider à supprimer les logiciels inutiles livrés par défaut sur certaines versions de PC vendues en version OEM. Surtout utile lorsque l'on vient de faire l'acquisition d'un nouveau PC, il peut tout de même être utile de supprimer a posteriori ces softs inutiles.



Après exécution, cliquez sur "Check for updates", puis "Next". Préciser que votre ordinateur n'est pas "out of the box". Laisser le programme désinstaller seulement pour les applications sélectionnées par défaut.

15) AppRemover (≈ 5')

<http://www.appremover.com/download>

[AppRemover.exe]

L'utilitaire gratuit AppRemover désinstalle facilement des logiciels antivirus, des suites de sécurité publiques et les applications de partage de fichiers de votre ordinateur.

Simplement lancer, puis "Démarrer".



Nettoyer le registre

Après la suppression des programmes, nous devons relancer des optimisations sur les bases de registre afin de faire un dernier nettoyage du PC.

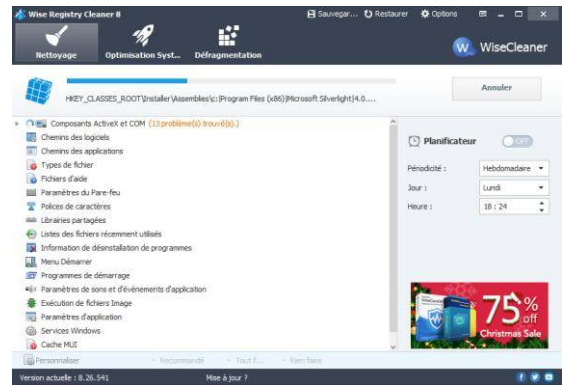
16) WiseCleaner (≈ 5')

<http://wisecleaner.com/wiseregistrycleanerfree.html>

[WRCFree.exe]

Nettoyer les entrées du registre, réparer les erreurs de Windows, et garder votre PC à des performances de pointe.

Installer, lancer le "Nettoyage" en cliquant sur "Analyser" puis "Nettoyer", puis "Optimisation Système" et enfin "Défragmentation". Supprimer le programme après utilisation.

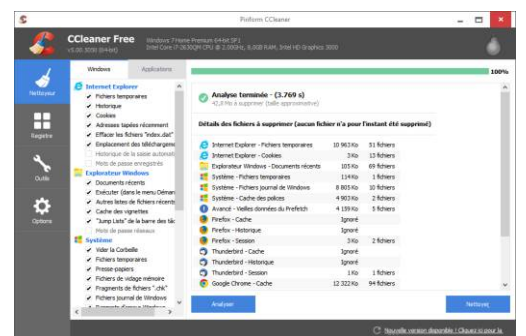


17) CCleaner * (≈ 5')

<https://www.piriform.com/CCLEANER>

[ccsetup500.exe]

Ce dernier outil très pratique est le seul pouvant être conservé sur l'ordinateur afin d'être exécuté de temps en temps. Lancer le nettoyage des logiciels et de la base de registre.



Vérifier et réparer le disque

Pour terminer le tout, une vérification du disque dur permettra de repartir sans crainte avec un PC comme neuf.

18) Vérification du disque (≈ 1h00 selon DD)

Démarrer un "Invité de commande" (menu Démarrer / Accessoires) en tant qu'Administrateur. Taper ensuite « CHKDSK /F /R ». Redémarrer votre PC, une vérification du disque sera effectuée, cela peut prendre un peu de temps.

Conclusions

En guise de conclusions, nous proposons quelques conseils sous forme de questions-réponses pour conserver un ordinateur propre et sain et améliorer son fonctionnement :

Que faire pour conserver un ordinateur sain ?

- Conserver Windows et l'ensemble de vos applications à jour,
- Toujours télécharger le logiciel que vous souhaitez sur le site de son éditeur (et pas par l'intermédiaire du premier lien 'adwords' trouvé sur Google),
- Installer un antivirus de qualité et s'assurer qu'il se mette régulièrement à jour,
- Etre prudent lors de la navigation sur Internet et au moment de la récupération vos emails,
- En entreprise, sensibiliser les utilisateurs et sauvegarder vos données.

Quel antivirus choisir ?

BitDefender et Kaspersky arrivent généralement en tête des tests effectués par les laboratoires indépendants, mais par expérience nous recommandons plutôt l'usage d'antivirus à doubles moteurs comme : Emsisoft Internet Security (<http://download.emsisoft.com/>) et GData Internet Security (<https://www.gdata.fr/>) un peu plus gourmands mais plus performants dans l'analyse et la réactivité.

Concernant les antivirus gratuits, ceux offrant actuellement les meilleurs performances d'analyse sont : Panda Free Antivirus (<http://telecharger.cloudantivirus.com/>) et Avira Free Antivirus 2015 (<http://www.avira.com/fr/avira-free-antivirus>).

Dans le cadre professionnel, en plus d'un antivirus sur les postes, s'équiper de la forteresse contre les malwares Altospam (<http://www.altospam.com/>), elle intègre 5 anti-virus complémentaires ainsi qu'un système de détection de fichiers suspects pour bloquer les attaques 0-days (<http://www.altospam.com/actualite/2014/02/la-forteresse-daltospam-les-malwares/>).

Comment optimiser l'analyse du poste ?

Idéalement, mais cela nécessite un peu plus d'expérience technique, il serait intéressant de compléter cette procédure d'analyse à l'aide de LiveCD. Vous trouverez une liste relativement complète de LiveCD d'analyse antivirus à l'adresse : <http://www.tech2tech.fr/liste-de-20-antivirus-bootable-cd-de-secours-antivirus/> . Nous recommandons les logiciels suivants : "Kaspersky Rescue Disc 10", "BitDefender Rescue CD" et "DrWeb LiveCD".

Comment conserver un PC entièrement à jour ?

Pour assurer une parfaite sécurité de l'ordinateur, il convient d'avoir un poste à jour aussi bien au niveau système d'exploitation et antivirus, mais également sur les applications et les drivers qui peuvent comporter des failles de sécurité.

Concernant le système et l'antivirus, cela est désormais intégré en standard, vérifier simplement que la mise à jour automatique est bien activée. Par contre, pour les logiciels et les drivers, nous vous conseillons l'usage de produits tiers afin d'être exhaustifs. Pour les applications, le module Filepuma de Glary Utilities 5 fait très bien son travail. Concernant les drivers, l'outil gratuit SlimDrivers de SlimWare Utilities (<https://www.slimwareutilities.com/slimdrivers.php>) est particulièrement pertinent.

Attention cependant à la mise à jour des drivers, nous avons quelquefois remarqué des effets indésirables (incompatibilité avec certains logiciels notamment), leur mise à jour doit être faite progressivement et en toute connaissance de cause. Nous vous recommandons fortement de créer un point de restauration système avant de mettre à jour les drivers afin de pouvoir revenir facilement en arrière.

Quels outils peuvent être conservés ?

Parmi les outils utilisés dans cette procédure, nous préconisons de conserver ou d'installer les versions 'Premium' des logiciels ci-dessous, nous les considérons comme particulièrement efficaces et intéressants :

- Emsisoft Internet Security (<http://download.emsisoft.com/>)
- Malwarebytes Anti-Malware Premium (<http://fr.malwarebytes.org>)
- CCleaner (<https://www.piriform.com/CCLEANER>)
- Glary Utilities 5 (<http://www.glarysoft.com/>)

Nous espérons que cette procédure vous aura été utile, qu'elle vous permettra d'utiliser votre ordinateur en toute sécurité. Nous espérons aussi vous avoir sensibilisé au domaine de la sécurité informatique et de la cybersécurité...

Ce guide a été écrit par @Sekurigi, un blog d'actualités sur la sécurité informatique : <http://www.sekurigi.com/> . Si vous souhaitez nous soutenir, merci de suivre notre compte twitter : <https://twitter.com/sekurigi> .

