

Aide à la désinfection ! (S'adresse d'abord aux personnes qui sont venues me voir.)  
Important : Toutes les opérations décrites ci-dessous sont réalisées avec Windows XP, il se peut que vous rencontriez des différences avec un Windows plus récent.

Recommandations générales :

En dehors du téléchargement des programmes cités ci-dessous et des mises à jour, il est préférable de désactiver Internet et les autres programmes qui s'ouvrent automatiquement (tel que msn et cie.) pendant les Scans !

Pendant les analyses des différents programmes, restez à proximité de votre ordinateur afin de répondre à des questions sur des problèmes rencontrés lors des scans.

Pendant les analyses veuillez ne pas utiliser l'ordinateur pour autre chose.

1) Tout d'abord avant d'insérer la clef USB, assurez-vous que votre anti-virus est à jour correctement. Dans le cas d'avast 4.x > Cliquez droit sur son icône (la boule bleu avec un petit « a » blanc), choisissez mise à jour > mise à jour de la base virale.

Attendez que la mise à jour se fasse complètement (répétez l'opération jusqu'à ce qu'il vous indique : votre base virale est déjà à jour)

Ensuite il faut mettre à jour le programme. De nouveau un clique droit sur son icône et choisissez maintenant > mise à jour du programme.

Si le programme est mis à jour l'ordinateur doit redémarrer.

2) Lancez un scan de votre ordinateur ; exemple ici avec Avast !:

- Cliquez droit sur l'icône d'avast !
  - Démarrer avast ! antivirus
  - Vous allez voir apparaître deux fenêtres, une blanche que vous pourrez fermer et le programme en lui-même.
  - Sur le programme en haut à gauche cliquez sur le petit bouton (flèche vers le haut)
  - Sélectionnez « Planifiez un scan au démarrage »
- Cochez les cases suivantes :
- Scanner tous les disques locaux
  - Scan des archives
  - Options avancées
- Sélectionnez : Supprimer le fichier infecté dans le premier menu déroulant

Planifié > Redémarrer

3) Votre ordinateur sera déjà moins porteur de problèmes après cette opération mais il n'y a pas que les virus qui endommagent les ordinateurs, les Malwares (Logiciels malveillants) et les Spyware (Logiciels espions) sont aussi source de problèmes.

Pour ceux qui auraient reçu sur leur clef toute une série de programmes, ne les utilisez pas, utilisez plutôt les logiciels mis à votre disposition sur le site de l'école [www.iset.be](http://www.iset.be). Ce serait bête après avoir désinfecté vos clefs de récupérer à nouveau des virus. Les programmes à télécharger en premier sont : la nouvelle version d'Avast, Spybot, Malwarebytes, Anti-autorun.inf et USBFix. Mettez-les sur votre bureau, par exemple, dans un dossier « temp ».

4) Si vous n'êtes pas content de votre antivirus ou, si vous désirez mettre la nouvelle version d'avast (passer de la 4.8 à la 5 par exemple) installez-la maintenant. Si vous ne voulez pas installer avast 5 passez au point 6). Au début de l'installation il va vous demander si vous voulez participer ou non de façon anonyme à la recherche de virus. C'est votre choix. Ensuite il vous propose d'installer Google Chrome, c'est un explorateur Internet (comme Internet

Explorer et Firefox). Si vous n'avez pas Firefox, je vous conseille de l'installer sauf si vous êtes pleinement satisfait de la lenteur d'Internet Explorer.

Sur certaine machine, il va vous demander de redémarrer, faites-le.

Ensuite, double cliquez sur la boule orange avec un « a » dedans près de l'horloge c'est la nouvelle icône d'avast.

Allez en haut à droite dans paramètres.

Mises à jour > Programme > Mise à jour automatique > OK

Dans le menu de gauche > Maintenance > Mise à Jour

Partie de droite :

- Cliquez sur Mettre à jour le moteur et la base de données virale VPS
- Cliquez sur Mettre à jour le programme (redémarrage nécessaire)

5) Ouvrez à nouveau le programme après le démarrage de l'ordinateur.

Cette fois ci sélectionnez > Lancer un Scan > Scanner maintenant > (dans la partie de droite)

Scan minutieux > en dessous de démarrer, cliquez sur « plus de détails... » > Réglages

- Cochez la case « Actions à effectuer automatiquement... »
- Cliquez sur « Ne rien faire » et sélectionnez « Supprimer »
- Faites de même dans l'onglet LPI et Suspect

En dessous, dans « options », vérifiez bien que la case « Si nécessaire, effectuer... » soit bien cochée.

Cliquez sur OK > puis sur le bouton « démarrer » qui est en vis-à-vis de « Scan minutieux »

Attendez la fin du scan, s'il rencontre un virus récalcitrant, il vous proposera de redémarrer votre machine pour faire un scan au démarrage. Acceptez !

Après le scan avec avast :

6) Anti-Autorun.inf est un petit programme super léger qui vous aidera à protéger votre ordinateur contre les applications malveillante qui s'installe au démarrage.

Attention les clefs USB U3 sont considérés malheureusement par se programme comme porteur d'un virus. Si vous voulez être certain qu'il n'y en ait pas, venez me voir avec.

Le programme s'installe très rapidement et vous propose de s'activer au démarrage. Pour les très anciens ordinateurs (+de 5 ans < Win XP SP2) ne le faites pas, ouvrez le programme seulement quand vous allez insérer une clef. Pour les autres vous ne verrez pas de différence point de vue performances.

Si après utilisation de Anti-autorun.inf vous trouvez encore un fichier autorun.inf, allez directement au point 11) et revenez ensuite au point numéro 7)

7) Spybot est un logiciel contre les Spywares, il va construire un mur virtuel dans votre PC qui va fortifiez votre défense dans Firefox et Internet Explorer (jamais testé sur Google Chrome). En l'installant il va vous demander si vous voulez installer Teatimer, ne le faites que sur des ordinateurs qui ont moins de deux ans ou sur un ordinateur qui tourne très bien. Teatimer est un complément de Spybot. Il travail, à la différence de spybot en temps réel et peut donc ralentir fortement votre machine. Spybot et Teatimer travail sur la base de registre de l'ordinateur contrairement aux autres logiciels (antivirus) qui eux travaillent sur les fichiers.

- Une fois spybot installé, il vous propose de faire une sauvegarde de votre base de registre, n'en tenez pas compte et passez au point suivant la mise à jour.

Sélectionnez n'importe quel endroit (en général il surligne le plus rapide) > vous pouvez, à l'étape suivante, cocher toutes les cases, mais seules, les cases pré cochées sont importantes.

Après téléchargement des mises à jour, il va relancer le programme, il va à nouveau proposer de faire une sauvegarde et une mise à jour, passez outre jusqu'à arriver à « Utiliser le programme ».

Cliquez sur le bouclier Bleu et blanc, laissez le travailler un instant pour évaluer « vos défenses » > Cliquez sur le « + (vert) Vacciner » pour lancer la « construction » de votre protection passive.

Une fois terminée, allez sur « Search & Destroy » dans le menu de gauche.

Cliquez sur « Vérifiez tout » et patientez... A la fin du scan il vous propose de « corriger les problèmes ». Faites le ! Si jamais il ne sait pas les corriger il va vous inviter à redémarrer la machine pour les enlever.

8) Malwarebytes est un autre logiciel qui va supprimer les programmes malveillants. Lancez le fichier d'installation et acceptez tout, il n'y a aucune option à changer (sauf peut être pour ceux qui aiment changer les répertoires d'installation par défaut)

A la fin de l'installation, le programme va faire une mise à jour et va ensuite démarrer.

Sélectionnez : Exécuter un examen complet > cliquez sur « Rechercher »

Il coche par défaut tout vos disques locaux et clefs usb et c'est très bien ainsi, vous serez sûr qu'il vérifie tout. S'il trouve quelque chose, cliquez sur « afficher les résultats » >

« Supprimer la sélection ». Le programme vous invitera à redémarrer.

9) Vous avez maintenant analysé votre ordinateur pour les trois plus grands problèmes rencontrés.

Seul l'antivirus, l'Anti-autorun.inf et, pour certains utilisateurs, Teatimer seront actifs. Il est donc recommandé de faire une analyse de Spy et Malware régulièrement (par exemple tous les mois ou tous les 2 mois). Avant chaque analyse, assurez-vous d'être protégé à 100% avec Spybot et Malwarebytes en les mettant à jour avant l'analyse.

10) Afin d'assurer la protection de votre ordinateur, il faut maintenant veiller à ne pas amener une infection avec votre clef USB.

Pour se faire, insérez votre clef dans le port USB, en vérifiant avant que le programme Anti-autorun.inf soit bien actif (icône A vert en bas près de votre horloge). Il va annuler tous les démarrages automatiques qu'il peut y avoir sur votre clef.

Laissez un peu de temps au programme pour réagir (affichage des différentes info-bulles) et il vous affichera, si votre clef est infectée, décontamination effectuée. S'il n'y a pas de risque, aucune info bulle n'apparaîtra.

Ouvrez maintenant votre poste de travail, faites un clic droit sur l'icône de votre clef USB et dans le menu déroulant choisissez les deux options d'analyse. Avast, avec une icône orange, et Malwarebytes, avec une icône rouge et noir.

Une fois les deux analyses terminées, ouvrez votre clef USB. Si vous trouvez un fichier autorun.inf, allez au point 11). Si non vous pouvez commencer à travailler et allez au point 12)

11) Dans votre clef vous observez un fichier « autorun.inf » qui n'a pas été supprimé. Double cliquez sur le programme UsbFix. Choisissez l'option « F » pour français, puis « 2 » pour supprimer les fichiers infectés. Cette opération consiste à redémarrer le PC et effectuer un « déplacement » des virus (cela veut donc dire que vous devrez relancer à la fin des opérations un scan complet de votre ordinateur points 5 / 6 / 7). Lors du redémarrage certaines clefs usb, dites « bootable », vont bloquer le démarrage de l'ordinateur. Débranchez la clef, appuyez sur « enter » et rebranchez-la. A la fin des opérations, il vous invitera à transmettre au concepteur du programme, un fichier rapport au format zip qui se trouve sur votre bureau. Vous le faites

ou non, c'est votre choix. Après avoir fermé la fenêtre de l'explorateur, il vous affichera les statistiques du scan. Vous pourrez voir dans ce fichier les éléments qui étaient infectés et/ou supprimés.

12) Vous venez de « décrasser » votre ordinateur. Faites-le, plus ou moins, une fois tous les mois pour être sûr de ne pas courir de risque.

Les programmes mis à disposition sur le site de l'école, comme tous les programmes d'ailleurs, ne sont pas à 100% fiables. C'est-à-dire qu'aucun programme n'est infaillible. Je vais « imager » un exemple, puis vous le donner de deux façons concrètes :

- Imaginez dans une boîte de nuit un sorteur qui empêche quelqu'un d'entrer, mais le patron de la boîte arrive et l'autorise à entrer.
- Vous êtes sur facebook et une application, proposée par l'un de vos amis, vous invite à découvrir qui vous serez dans le futur. En cliquant sur le lien, vous faites exactement comme le propriétaire de la boîte, et vous l'invitez à entrer sur votre ordinateur. Je ne dis pas non plus que toutes les applications facebook ont un virus, mais soyez vigilant !
- Sur msn, l'un de vos contact vous dit : Regarde j'ai trouvé un super site qui permet d'avoir le mot de passe de n'importe quel compte... Encore une fois vous faites comme le propriétaire et en cliquant sur le lien vous forcez vos antivirus et installez un virus.

J'espère que j'ai pu vous rendre service et que la propagation des virus va diminuer.

Jean-Philippe Debruxelles