MalwareBytes' Anti-Malware - Tutoriel

Août 2015

Description

Cet anti-malware vraiment excellent, enlève les infections sur vos ordinateurs avec une simplicité déconcertante !
(Tous les mots possédant une "*" seront expliqués dans le lexique) MalwareBytes' Anti-Malware s'est révélé être un must pour désinfecter les ordinateurs ! Il intègre les signatures des derniers **Malwares*** avec une rapidité démontrant le travail des laboratoires, et de plus, celui-ci intègre une détection heuristique très efficace contre les nouveaux **Malwares*** qui ne sont pas répertoriés dans les signatures. Il intègre également le détecteur de **rootkit*** de Gmer, une des meilleures technologies **Anti-Rootkit***, et un module de suppression des fichiers bloqués par le système afin de supprimer les fichiers récalcitrants (FileAssassin). Il permet aussi de supprimer les **PUPs/LPIs***. De plus, ce logiciel est gratuit mais sans le

bouclier de protection en temps réel (Votre antivirus est censé protéger activement le système à l'aide de son **scan*** en temps réel).

Avantages et défauts

Avantages

- Travail des laboratoires (mises à jour des définitions rapides),
- Détection heuristique efficace,
- Enlève infections avec simplicité,
- L'interface s'améliore de plus en plus,
- Gratuit sans le bouclier de protection,
- **Scan*** relativement rapide alors qu'il utilise des méthodes complémentaires et heuristiques.
- Compatible avec Windows XP/Vista/7/8/8.1/10

Défauts

- Le bouclier en temps réel n'est pas disponible dans la version gratuite (et dans la version "Premium", le bouclier, est bien présent, mais s'avère totalement inutile !)
- Ce logiciel fait régulièrement des **faux-positif***, il est donc préférable de lire attentivement le résultat de la recherche, et de conserver quelques temps en quarantaine les éléments supprimés.

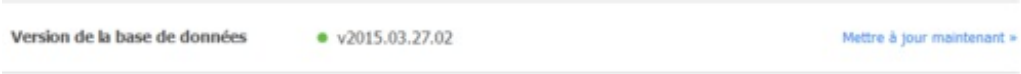
Télécharger et installer

- Téléchargez MalwareBytes' Anti-Malware à partir de cette page.
- Installez puis lancez le programme (pensez à décocher la case "Activer l'essai gratuit de Malwarebytes Anti-Malware Premium" à la fin de l'installation).

Mettre à jour

MalwareBytes Anti-Malware va automatiquement vérifier que la dernière version est installée et se mettre à jour si besoin. Pour le faire manuellement :

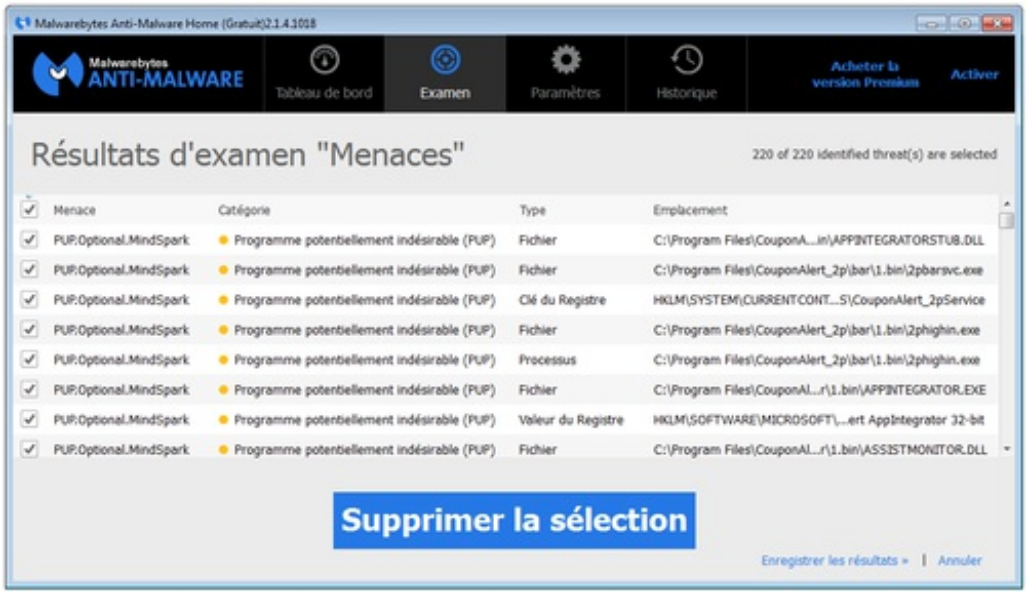
- Tableau de bord, version de la base de données et cliquez sur "Mettre à jour maintenant >>".



- Une fois mis à jour, vous pouvez lancer un scan*.

Comment faire un scan* ?

- Cliquez sur "Analyser maintenant" présent dans le "Tableau de bord" ou dans l'onglet "Analyse", sélectionnez "Analyse des menaces" puis cliquez sur "Lancer l'analyse".
- (Acceptez la mise à jour en cliquant sur "Mettre à jour maintenant" si proposé).
- Une fois le **scan*** terminé, cliquez sur "Supprimer la sélection".



- Quand MalwareBytes Anti-Malware a fini de mettre les éléments détectés en quarantaine, cliquez sur "Terminer". Si un message demande de redémarrer le PC pour terminer la suppression, acceptez.
- Le rapport est disponible dans Historique > Journaux d'application en tant que "Journal d'analyse" (Scan Log). Vous pouvez l'exporter afin de faire une analyse personnelle ou de le poster sur le forum Virus / Sécurité (où vous expliquerez pourquoi vous avez fait ce scan).

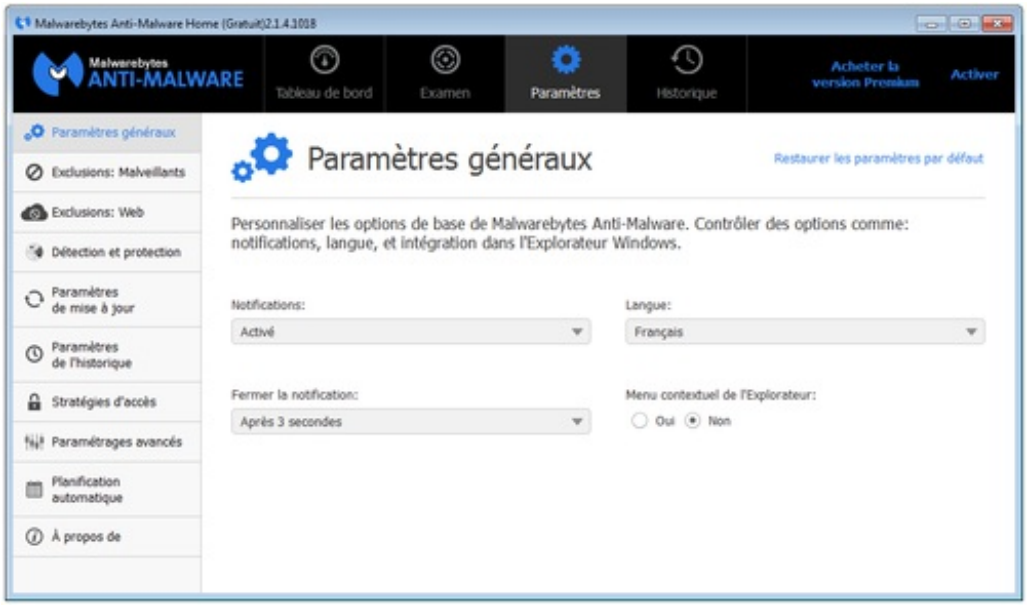
Conseil : Le scan* sera bien plus efficace contre les infections actives si vous n'utilisez pas votre navigateur Internet durant ce scan* et surtout si vous n'êtes **pas** en Mode sans échec*.

Onglet Paramètres

- A partir de cet onglet vous allez pouvoir configurer correctement le logiciel.

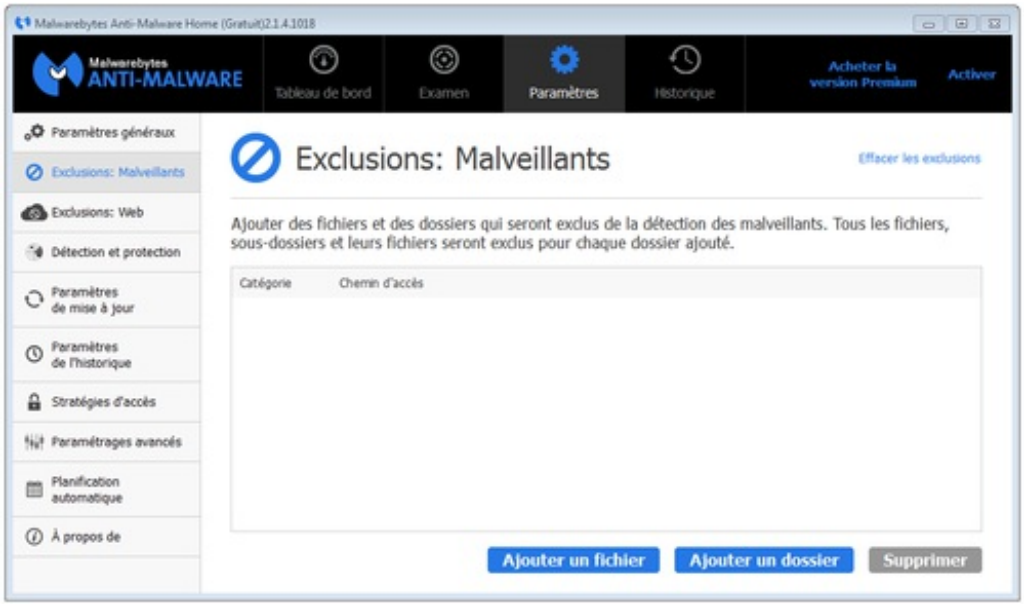
Paramètres généraux

- Mettre en Français si cela n'est pas déjà fait. Pour le reste, vous n'avez pas à toucher.



Exclusions: Malveillants

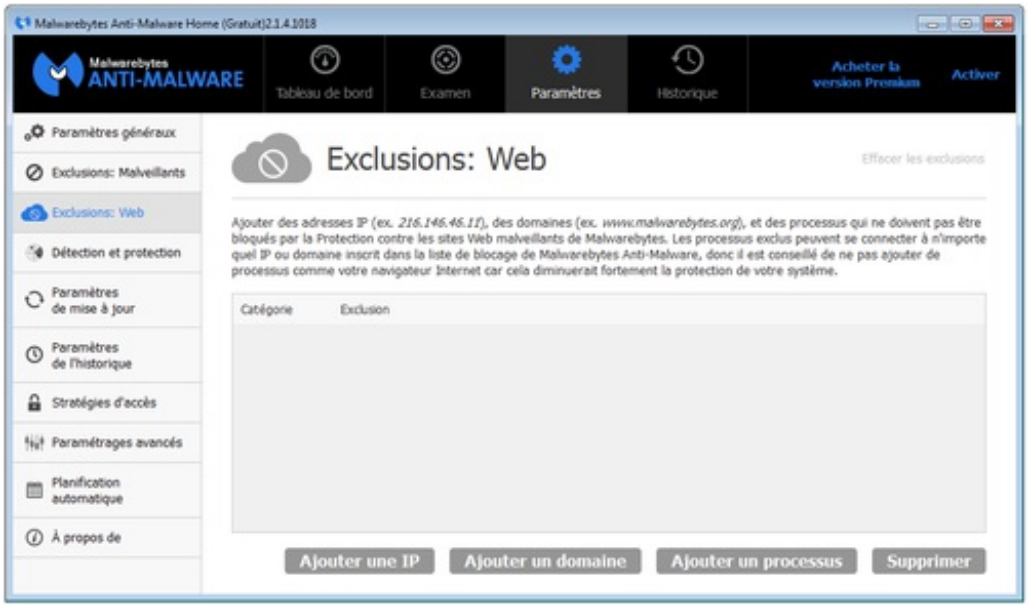
- Cela permet de configurer les faux positifs, c'est-à-dire les fichiers qui ne sont pas dangereux mais détectés comme, surtout que le logiciel est très sensible.



- Pour ajouter une exclusion, rien de plus simple que de sélectionner le fichier ou le dossier correspondant.
- On peut le faire à la suite d'un scan en sélectionnant exclusion sur l'objet suspect.

Exclusions: Web (version Premium)

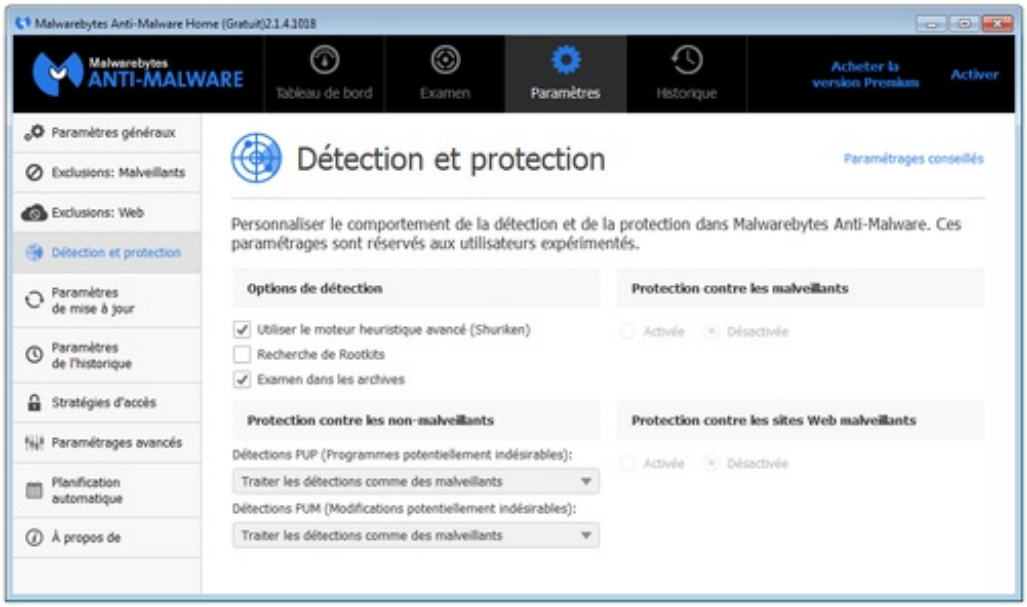
- Vous allez avoir des fenêtres d'avertissements qui peuvent signaler qu'une IP / qu'un processus est bloqué(e). Vous pouvez estimer que ce n'est pas malveillant et l'autoriser, ce qui peut être fait à partir de la fenêtre d'avertissement mais en réalité se gère grâce à ce sous-menu.



- Ce qui est bien depuis la mise à jour de la version 2, c'est que lorsque vous naviguer et que vous avez la version Premium et le blocage de site web malveillants, au lieu de finir sur une page erreur site introuvable, un logo de Malwarebytes va vous permettre d'identifier que c'est bien lui qui bloque le site. A partir de là c'est à vous de décider si vous acceptez ou pas.

Détection et protection

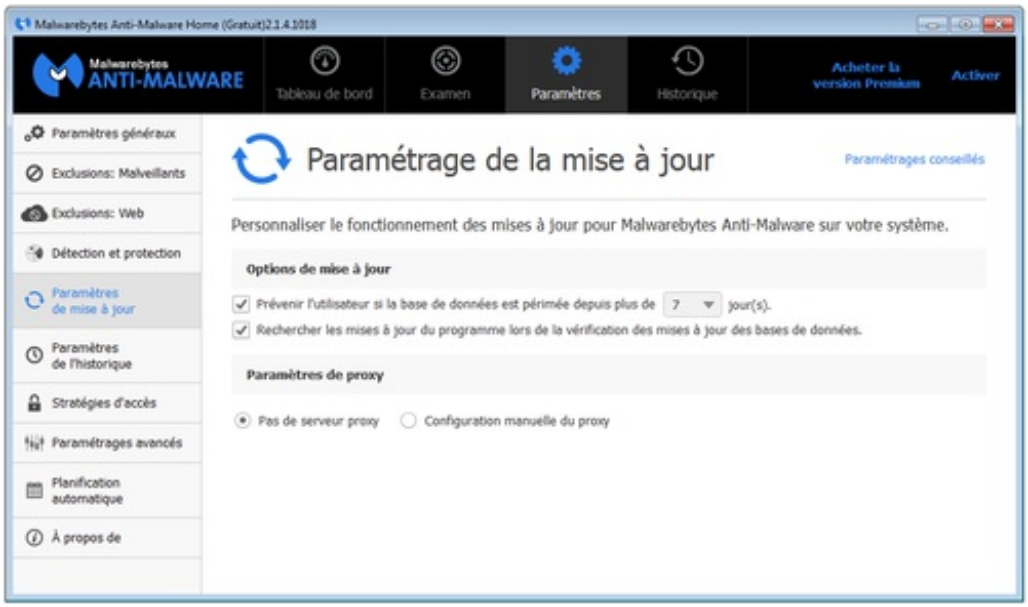
- Si vous avez la version Premium, vous pouvez profiter des deux protections, l'une contre les malveillants, l'autre protection contre les sites web malveillants.



- Vous pouvez aussi cocher détection de Rootkits.

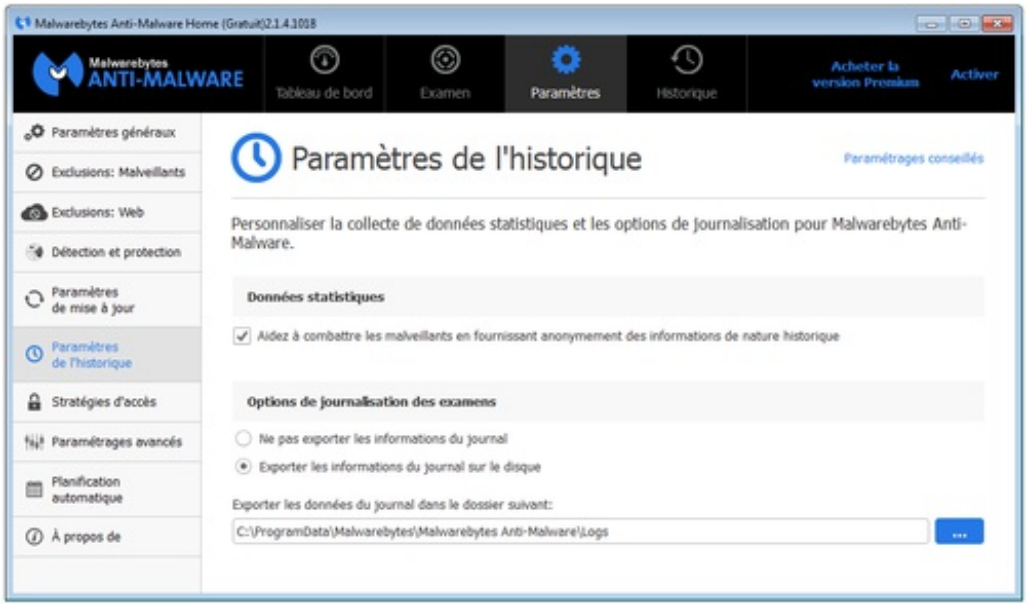
Paramétrage de la mise à jour

- Attention : il se peut que vous soyez agacer par les alertes trop récurrentes, lorsque vous êtes en train d'utiliser le PC, comme pour voir un film par exemple. Régler la fréquence courte si vous êtes plutôt paranoïaque, et longue si vous voulez la paix et que vous le faites manuellement.



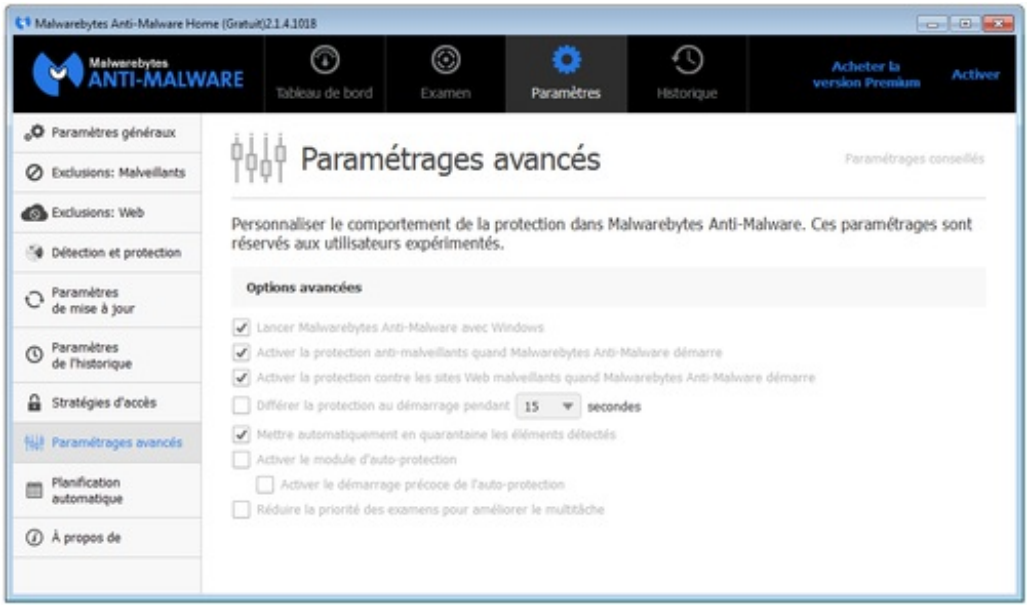
Paramètres de l'historique

- Remarquez l'adresse du fichier log des scans précédents.



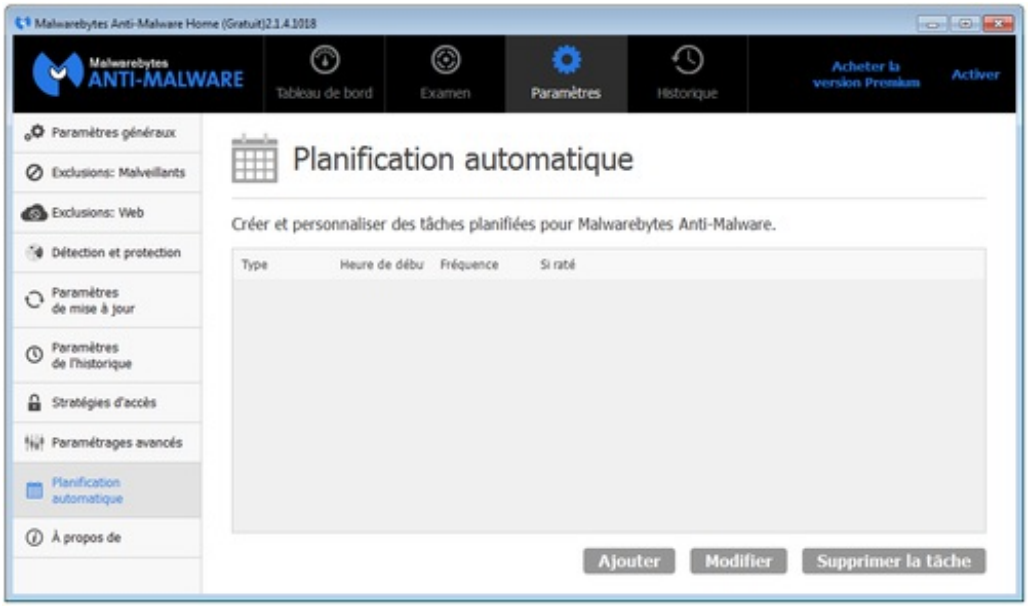
Paramétrages avancés (version Premium)

- Options classiques comme activer au démarrage de Windows, et affiner d'autres réglages.



Planification automatique (version Premium)

- Par défaut il planifie deux tâches, dont un scan et des recherches de mises à jours. Si vous voulez le faire manuellement et ne pas être averti constamment par des pop-up supplémentaires, supprimez-les.



- Vous pouvez planifier toutes les tâches.

Lexique

- **Scan** : Mode d'identification des suites de bits des fichiers, ce dernier, intégré bien souvent dans des antivirus, des logiciels de nettoyage ou de correction du registre, permet d'identifier les virus (Par le biais des définitions virales apportées par les laboratoires, ou la détection heuristique permettant d'identifier le comportement des programmes afin de déterminer s'ils sont normaux ou malveillants), de nettoyer votre ordinateur des fragments de fichiers inutiles créés par l'activité des programmes et du système d'exploitation, et la correction du registre afin d'optimiser la sûreté d'utilisation de l'ordinateur...
- **Windows** : Système d'exploitation au même titre que Leopard (Mac), Ubuntu Hardy Heron (Linux), Bart

PE...

- **Rootkit :** appelé également "kit racine", ce programme permet de masquer la présence de virus sur l'ordinateur, notamment, vous ne pourrez pas voir les infections actives sur le système dans la liste des processus avec la combinaison "Ctrl + Alt + Suppr" par exemple.
- **Malware**: Programme malveillant ne pouvant que être nuisible pour votre ordinateur: pour exemple, il peut voler vos données, les détruire ou bien encore manipuler votre ordinateur.
- **Anti-Rootkit** : Programme intégré généralement dans le scan, qui enlève les rootkits.
- **Faux-positif** : Un faux positif est une erreur de jugement d'un logiciel de sécurité, qui va détecter un fichier alors que celui-ci est sain.
- **PUPs/LPIs** : Logiciels potentiellement indésirables, ce sont des programmes souvent proposés lors de l'installation d'autres programmes qui sont en général gratuits. Ils peuvent changer la page d'accueil, le moteur de recherche, afficher de la pub de manière intempestive.

Réalisé sous la direction de Jean-François PILLOU, fondateur de CommentCaMarche.net.