PROTECTION DE VOTRE ORDINATEUR : antivirus et logiciels malveillants

Contenu

1) L'antivirus gratuit de Microsoft

Pour protéger l'ordinateur des virus et autres logiciels malveillants ou espions, le revendeur ou le fabriquant installe très souvent un programme dit « antivirus » (Avast, McAfee, Norton...)

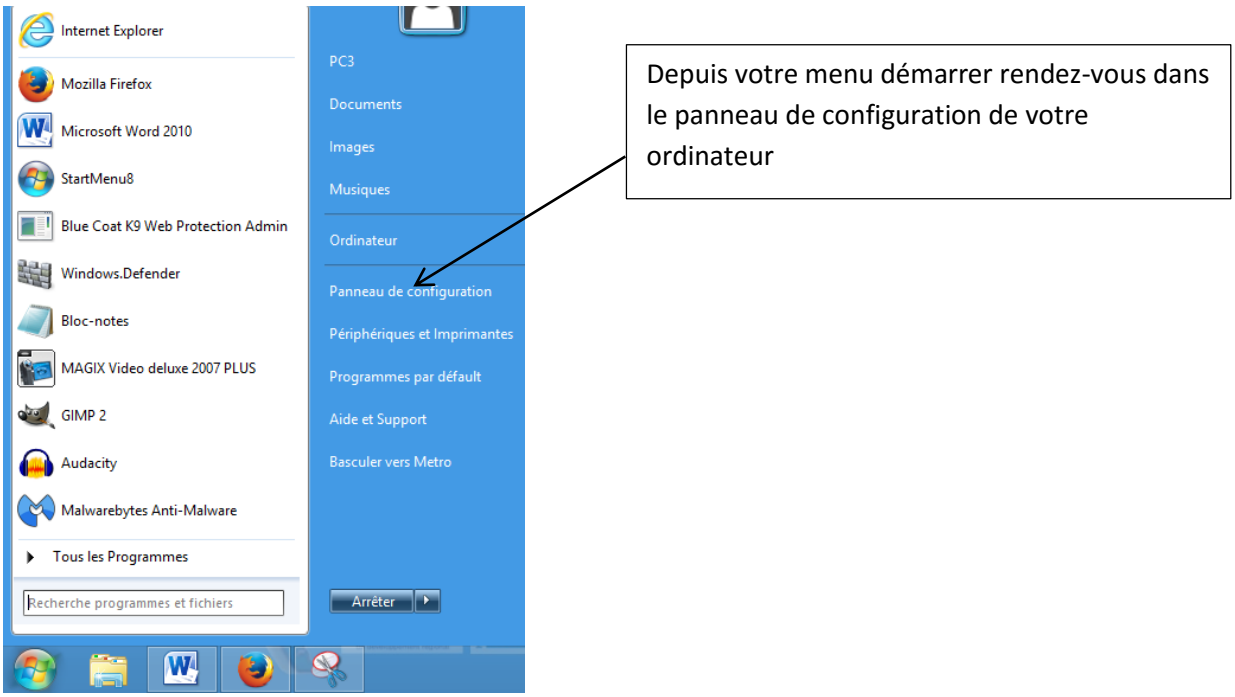
Bien que ces programmes fonctionnent correctement et soient gratuits, vous serez rapidement sollicité pour en acheter la version complète, via des messages apparaissant dans votre barre de tâches. Rien de plus agaçant ! Et bon nombre d'utilisateurs finissent par acheter ces produits par peur d'être mal protégé…

Certains vous diront également que ces antivirus sont beaucoup plus efficaces…si vous téléchargez sur des sites à risques et de façon régulière, effectivement certains antivirus seront plus fiables (et souvent payants), mais pour une utilisation classique d'Internet, ils ne sont pas indispensables.

En effet le système d'exploitation Windows inclue systématiquement un logiciel de protection dans votre ordinateur : depuis Windows 8 ce programme se nomme Windows defender. Sur les versions antérieures de Windows, le même programme s'appelle Microsoft Security Essential.

Ce programme est très souvent désactivé par le revendeur ou le fabriquant, qui vous propose un autre antivirus en fonction des partenariats commerciaux conclus avec des sociétés de développement d'antivirus, dans le but de vous encourager à les acheter en vous les imposant.

a) Commencez par désinstaller l'antivirus de votre ordinateur :

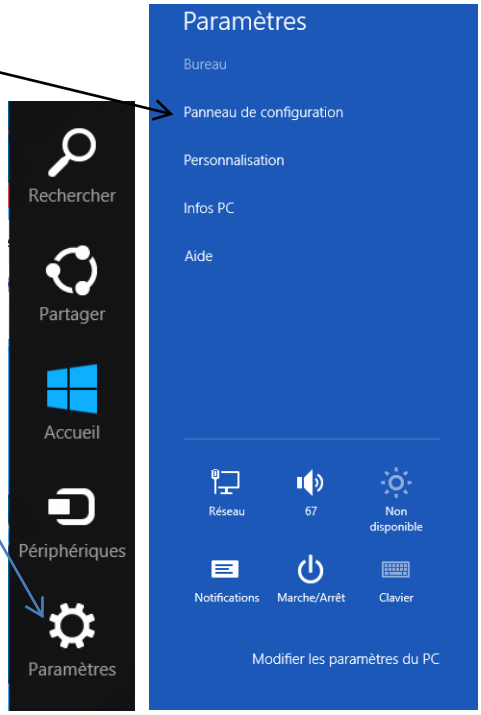


Avec Windows 8, vous pouvez accéder au panneau de configuration depuis la barre des Charms, menu « paramètres » puis « panneau de configuration »

Le panneau de configuration est également accessible depuis votre menu Démarrer, en bas à gauche de bureau !

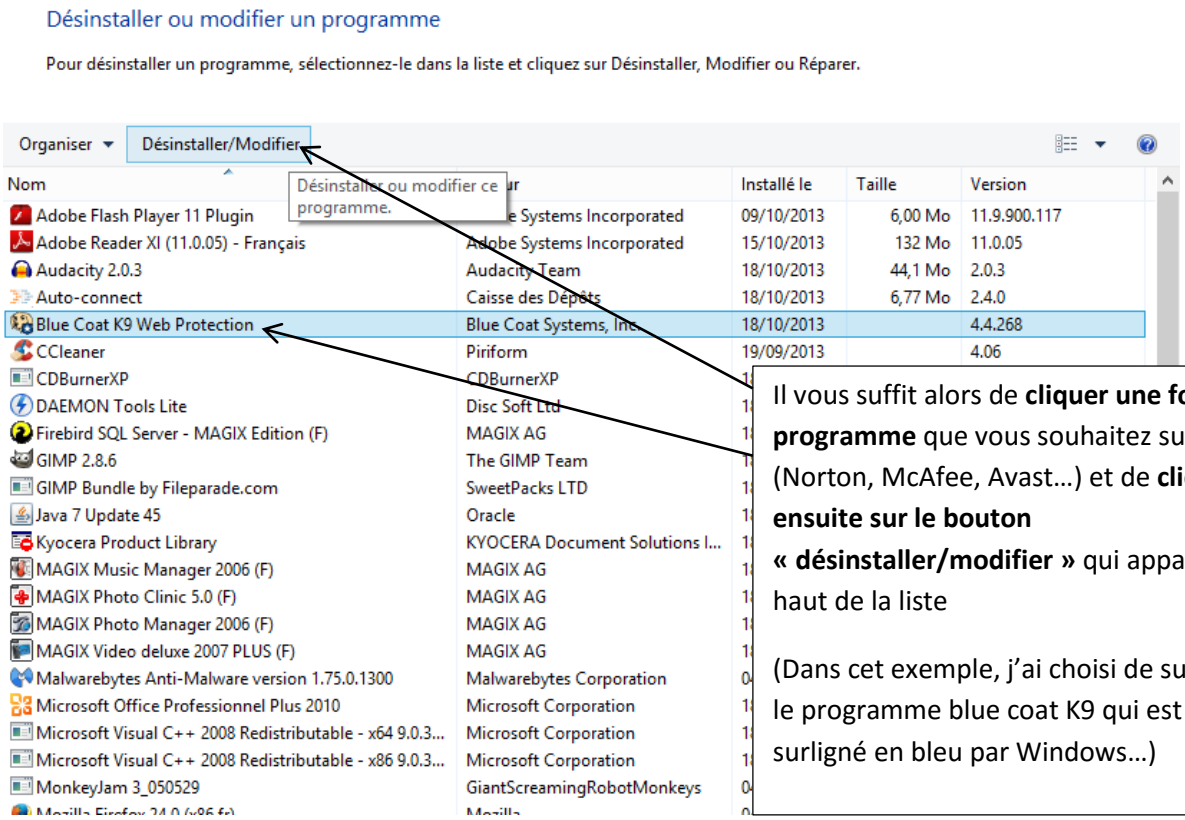
Cliquez avec le bouton droit de la souris (Windows 8.1)

Cliquez avec le bouton gauche de la souris (Windows 10)



Dans le panneau de configuration, cliquez sur le lien « désinstaller un programme »

La liste des programmes présents dans votre ordinateur s'ouvre alors :

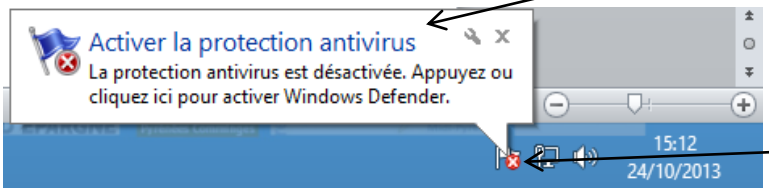


Une fenêtre s'ouvrira alors pour vous guider dans la désinstallation. Suivez les étapes une à une en prenant le temps de lire les indications (vérifiez entre autre que vous supprimez bien tous les composant de ce programme).

Un message « désinstallation réussie » vous confirmera la fin du processus de désinstallation de votre antivirus.

b) Activez ou installez l'antivirus de Microsoft

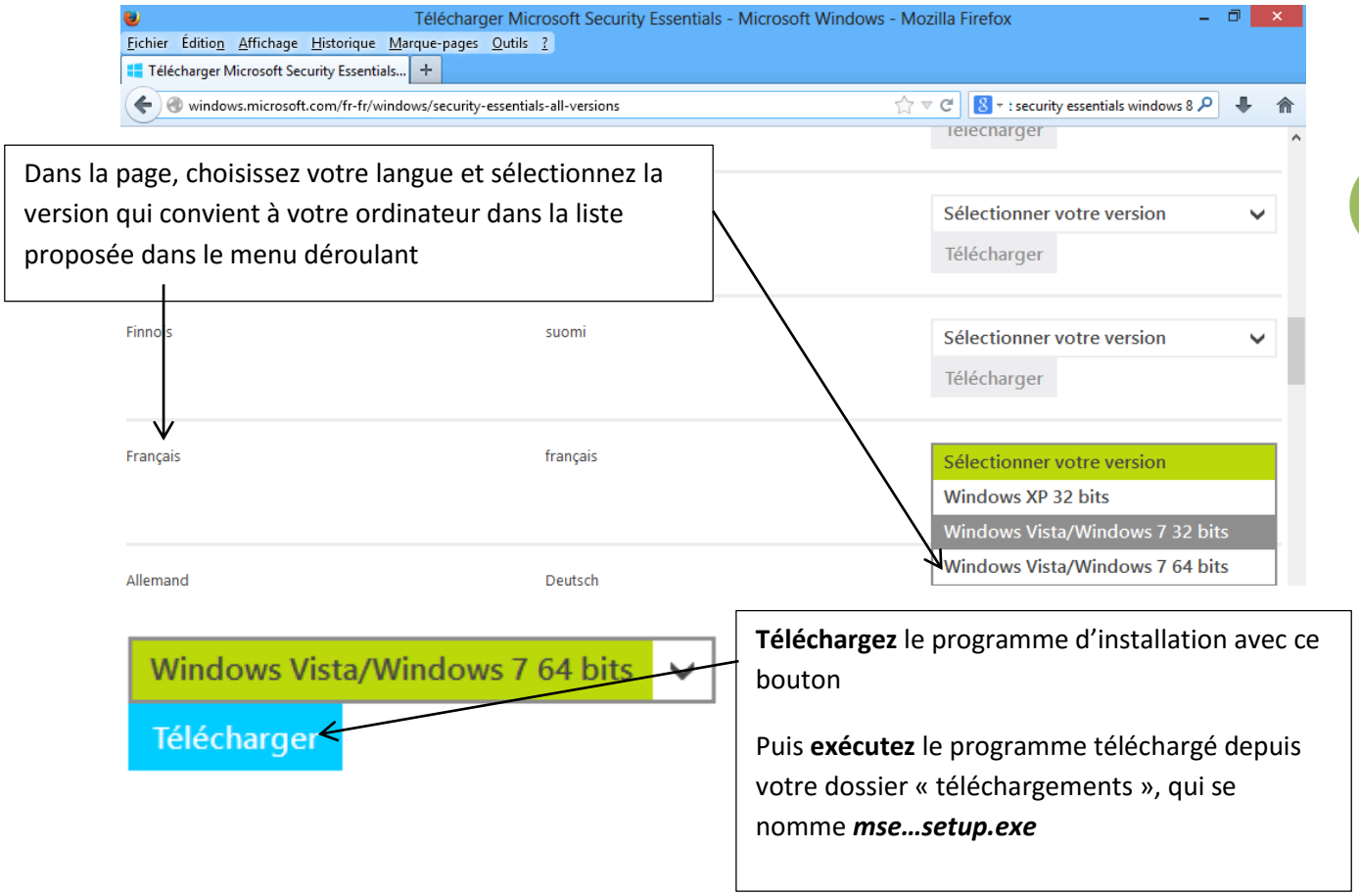
Comme vous venez de désinstaller votre antivirus, ce message apparait en barre de tâches :



<u>Il vous suffit de cliquer sur le message : l'antivirus de Windows s'active automatiquement</u> !

Si cet antivirus n'est plus présent dans votre ordinateur, vous pouvez le télécharger gratuitement et le réinstaller à cette adresse :

Pour Windows vista, 7 : http://windows.microsoft.com/fr-fr/windows/security-essentials-all-versions



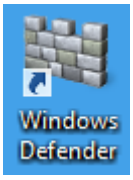
Pour Windows 8 : Windows Defender est installé dans l'ordinateur (le fabriquant l'a juste désactivé)

Pour le trouver

- faites une recherche « DEFENDER » dans la barre de recherche de la barre de charms ou de l'écran « Accueil »

Ici dans la barre de charmes

Windows vous propose alors le programme dans les résultats :



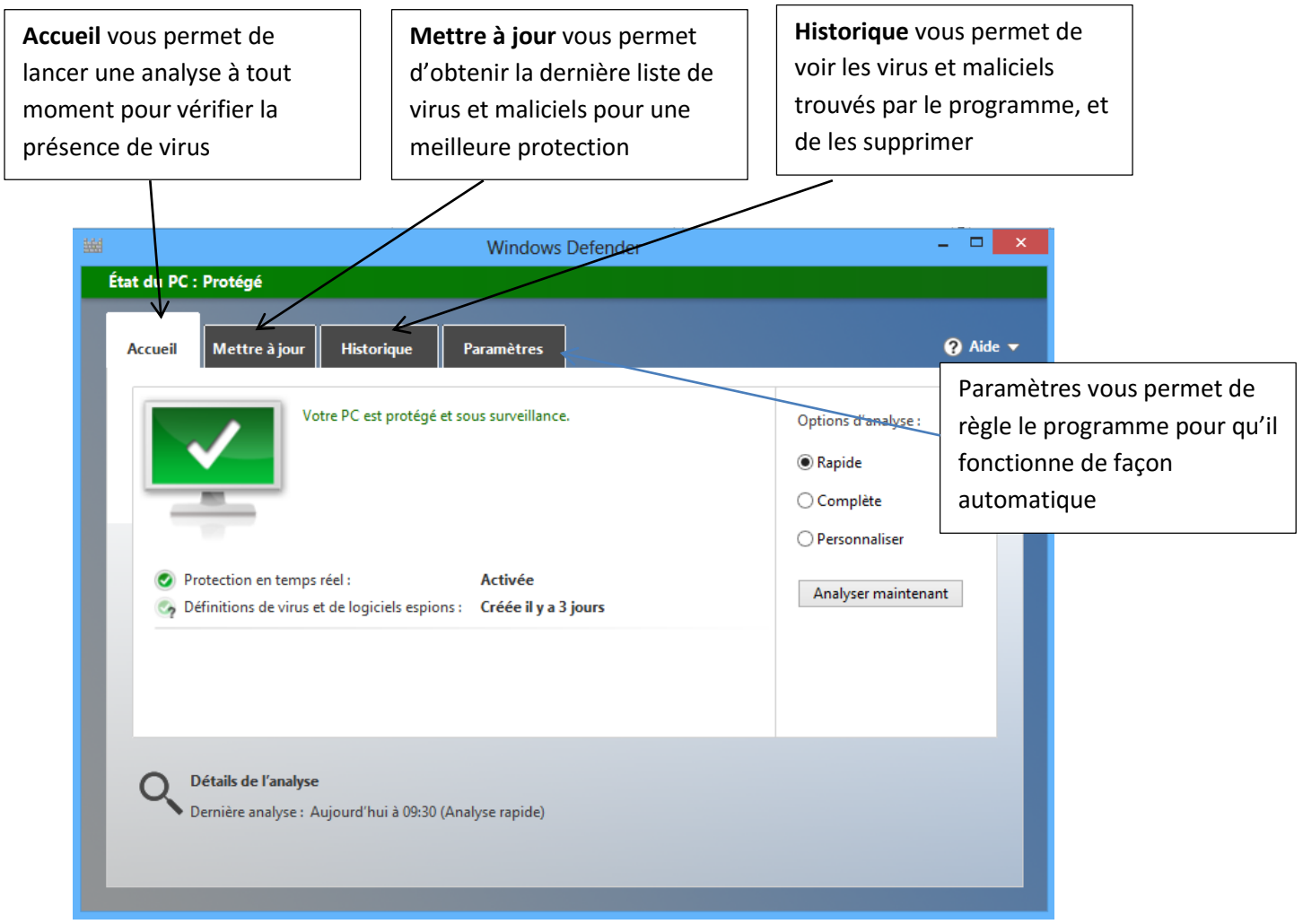
Voici l'icône de Windows Defender

Une fois que vous avez accédé à Windows Defender, vous pouvez lancer le logiciel pour le paramétrer.
Ce paramétrage permettra ensuite à Defender de fonctionner de façon automatique ! Pas besoin donc d'y revenir régulièrement…

c) Utiliser Windows Defender

L'utilisation du programme est très simple. Un bon paramétrage permettra à Defender de fonctionner de façon automatique au quotidien.

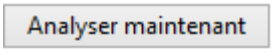
Le programme présente 4 onglets thématiques clairs et simples.



- **<u>Lancer une analyse</u> :**

Choisissez le type d'analyse en cochant selon votre choix :

- **Rapide** scannera le répertoire système de Windows sans se soucier des fichiers, bibliothèques…
- **Complète** scannera l'ensemble de vos disques durs en totalité.
- **Personnaliser** permet de choisir les répertoires que vous souhaitez analyser (dossiers, clé USB, disques durs…

Une fois votre choix fait, cliquez sur le bouton 

et attendez la fin de l'analyse (cela peut aller de quelques minutes à plus d'une heure selon le type d'analyse choisi)

- **<u>Mettre à jour</u> :**

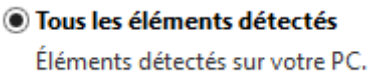
Les mises à jour se font automatiquement si votre ordinateur est réglé pour faire les mises à jour automatiquement (réglages constructeur).

Dans le cas contraire, cliquez sur le bouton 

dans l'onglet mettre à jour.

- **<u>Supprimer les éléments infectés</u> :**

Dans l'onglet « historique », vous pouvez voir les éléments détectés comme infectés en cochant



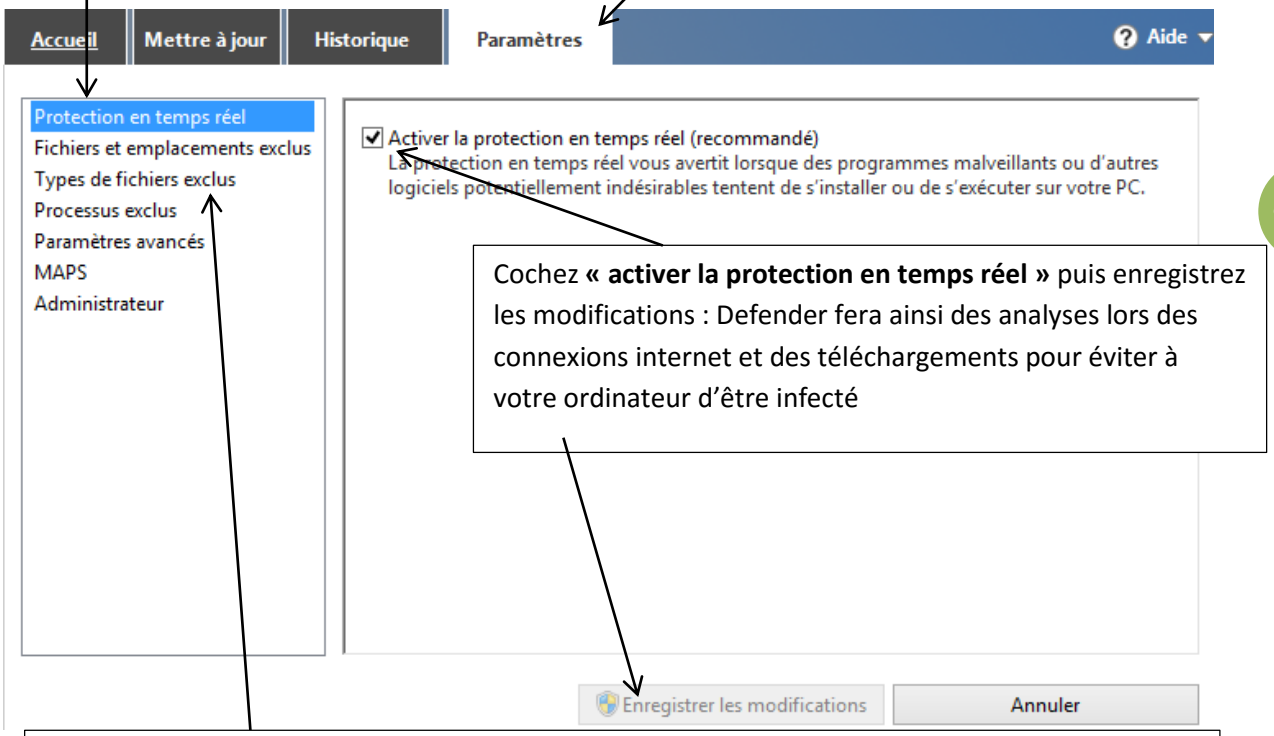
Dans la liste qui apparait, choisissez les éléments que vous voulez supprimer et cliquer sur « supprimer »

Les éléments en quarantaine *sont des emplacements jugés douteux par le programme et placés dans une zone de quarantaine où ils sont rendus inoffensifs pour votre ordinateur. Cette zone de quarantaine se vide automatiquement selon les réglages que vous paramétrez.*

- **<u>Paramétrer votre programme</u> :**

Régler correctement les paramètres va vous permettre d'automatiser le programme : ainsi ; il effectuera des analyses de vos disques durs à heure fixe, et vous protègera en temps réel lors de vos connexions internet. Pour cela, cliquez sur l'onglet « paramètres »

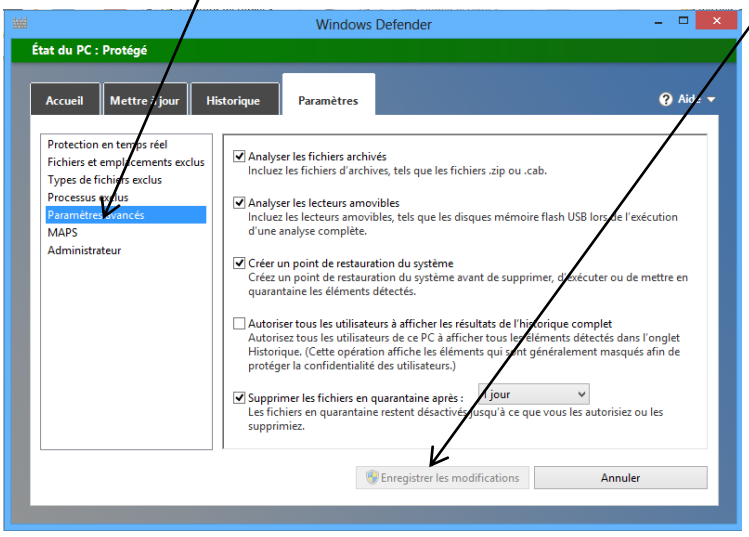
Les menus sur le côté gauche vous proposent différents réglages :



Cochez **« activer la protection en temps réel »** puis enregistrez les modifications : Defender fera ainsi des analyses lors des connexions internet et des téléchargements pour éviter à votre ordinateur d'être infecté

Les fichiers, types de fichiers et processus exclus vous permet d'empêcher l'analyse de certains éléments de votre ordinateur. Ces paramètres sont obsolètes pour un usage normal…

Définir les paramètres avancés permet de définir les actions automatiques du programme : cochez toutes les options pour une protection optimale et pensez à enregistrer les modifications.



Avec ces options, le programme effectuera une analyse sur tous les fichiers, dès que vous bancherez un support amovible (clé USB, cd-rom, disque dur externe…), supprimera seul les fichiers placés en

quarantaine et créera un point de restauration avant chaque suppression pour vous permettre de revenir en arrière en cas de suppression non désirée.

Une fois ces réglages terminés, vous pouvez fermer le programme. Votre ordinateur sera maintenant protégé contre les virus et maliciels courants, et des messages vous seront adressés en barre des tâches en cas de détection d'élément suspect ou de problème de mise à jour.


Surveillez donc ce petit drapeau et cliquez-le lorsqu'il est rouge !

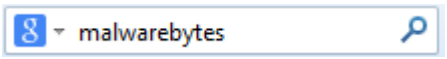
2) Malwarebytes, le complément sécurité de votre antivirus

Bien que Defender protège votre ordinateur au quotidien, certains maliciels ou problèmes peuvent passer au travers des mailles du filet.

En effet, un retard de mise à jour ou un maliciel perfectionné peuvent déjouer la protection et tenter d'endommager votre ordinateur.

Malwarebytes Antimalware est un logiciel puissant pour détecter et supprimer les éléments que Defender n'a pas supprimé.

a) Télécharger et Installer Malwarebytes

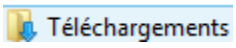
Cherchez ce terme dans votre moteur de recherche : 

Le site **malwarebytes.org** vous propose son produit en version gratuite :

Rendez-vous sur ce site et cliquer sur le bouton vous proposant le téléchargement

(Attention ce bouton est susceptible de changer d'apparence ou de place dans la page, mais il sera toujours bien visible)

Cliquez sur ce bouton pour accéder au téléchargement, puis sur le bouton

Enfin choisissez d'exécuter le fichier ou lancez son exécution dans votre dossier 

en cliquant sur ce fichier :

Ce fichier doit toujours s'appeler « mbam-setup….exe »

Les numéros eux varient à chaque nouvelle mise à jour du site !

Contrairement à de nombreux logiciels gratuits sur Internet, Malwarebytes ne propose aucun autre programme ou piège à l'installation, validez donc sans méfiance les différentes étapes jusqu'au lancement du programme

b) Utiliser Malwarebytes

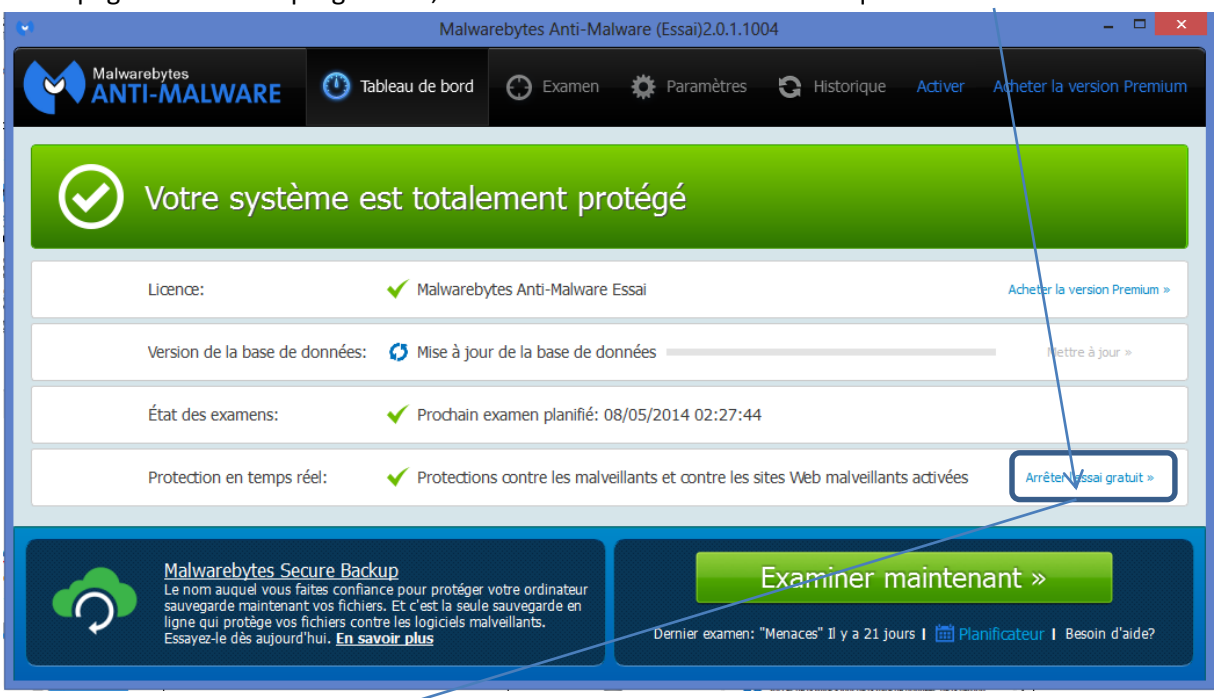
A la différence de Defender, Malwarebytes n'est pas automatisé. Il vous faudra le lancer manuellement de temps en temps pour effectuer une analyse de votre ordinateur.

Vous trouverez le programme sur votre bureau grâce à son raccourci :

Ou bien en utilisant l'outil « rechercher » et en tapant « malwarebytes »

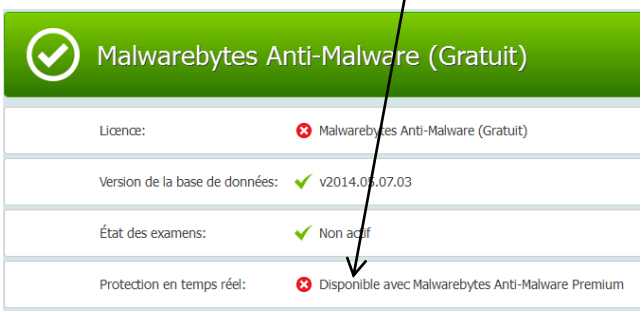
Version gratuite

La version de Malwarebytes que vous lancez est une version d'essai de la version professionnelle.
Il se peut donc que vous voyiez en page d'accueil un message de type « il vous reste 3 jours »…
Pas d'inquiétude, vous pouvez passer en version gratuite sans aucune autre installation !
Sur la page d'accueil du programme, il vous suffit d'arrêter l'essai en cliquant sur ce lien



Vous passez en mode totalement gratuit. Et le logiciel fonctionnera normalement sans vous proposer aucun achat.

En revanche, les outils d'analyse automatique en temps réel ne seront pas disponibles en version gratuite :

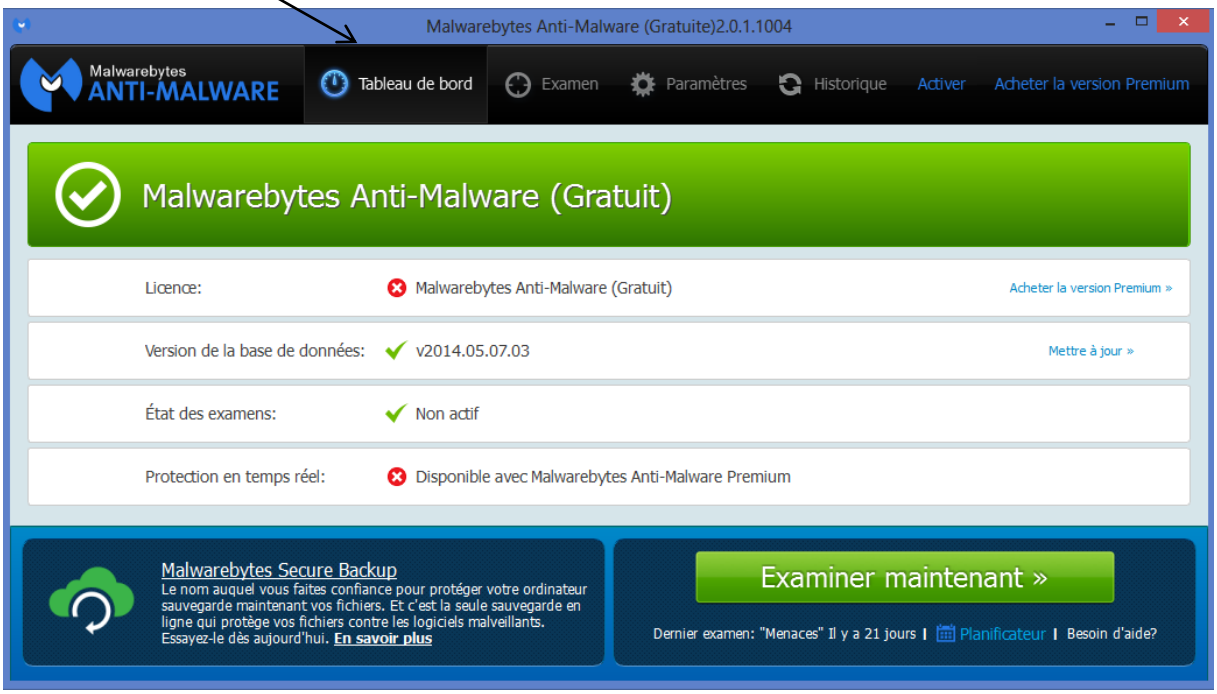


Interface et outils du programme

Le programme vous propose comme defender différents menus.

Sachez que les réglages du constructeur sont les meilleurs et si nous les présentons rapidement ici, vous n'aurez besoin que du tableau de bord, qui vous guidera pour toutes les étapes de la protection

- **Tableau de bord** (1er menu) pour assurer la protection de votre ordinateur.

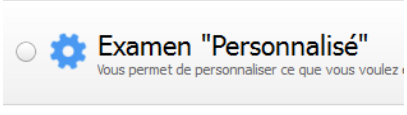


- **Le menu « examen »**

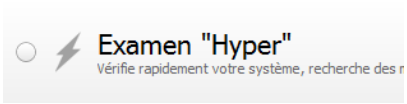
Il vous permet de choisir (comme avec Defender) le type d'examen que vous souhaitez effectuer.

3 examens vous sont proposés :

Le plus performant et complet (examen par défaut du constructeur)



Choisir vous-même les endroits du disque à examiner

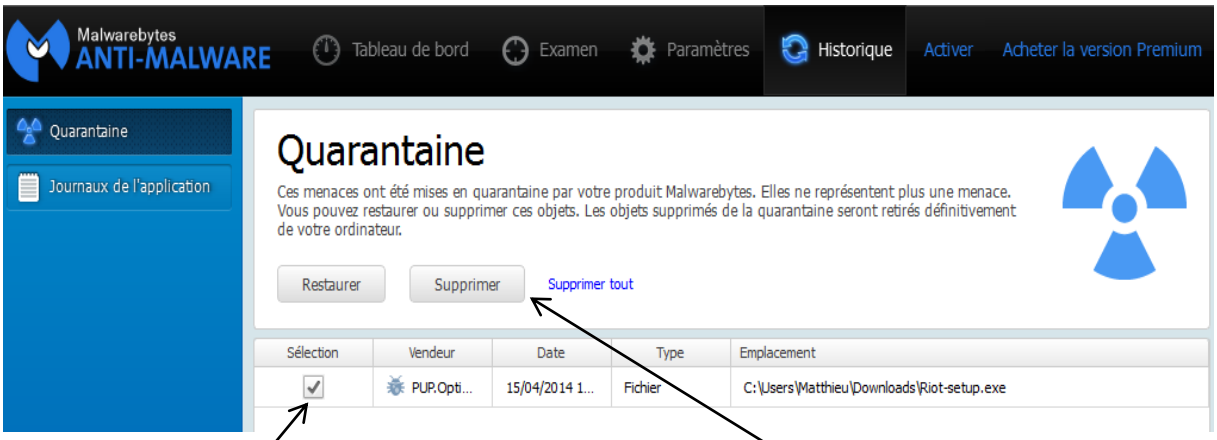


Analyser rapidement en quelques secondes (peut efficace)

- **Le menu paramètres** vous donne accès à un ensemble de réglages, dont beaucoup sont indisponibles en mode gratuit.

Ce menu peut vous être utile pour changer de langue, mais les autres réglages, prévus par le constructeur, sont optimaux pour une protection efficace.

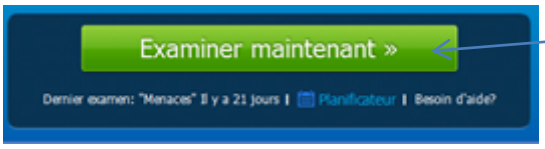
- **Le menu historique**, comme avec Defender, vous donne la liste des objets menaçants trouvés dans votre ordinateur.



Cochez les objets trouvés puis utilisez le bouton « supprimer » pour les effacer de votre ordinateur.

Analyser et nettoyer les menaces

Pour lancer une analyse de votre ordinateur, utilisez le menu « tableau de bord »



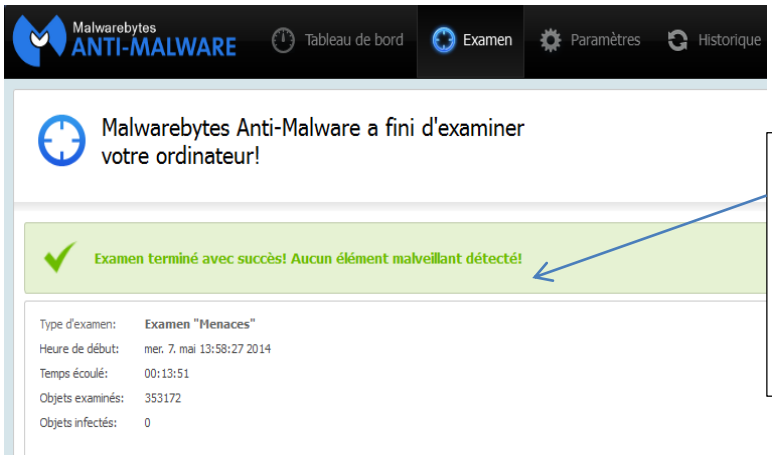
Lancez l'examen avec ce bouton.

Si vous n'avez pas modifié les réglages, il s'agira d'un examen de tous les emplacements de votre ordinateur, donc le plus efficace

La barre d'avancement vous indique où en est l'examen en temps réel

Comprendre les résultats de l'analyse

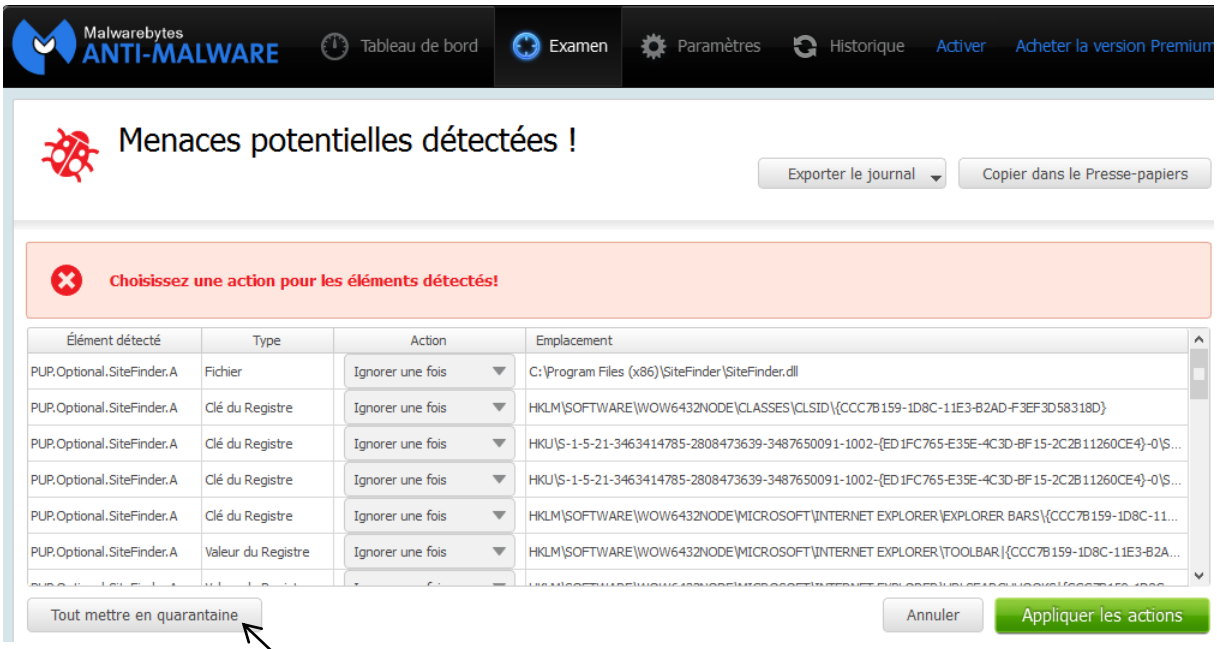
En fin d'analyse, le programme vous propose ses résultats et vous propose automatiquement des actions à exécuter avec les éléments détectés.



Si aucun élément n'est détecté, c'est que votre ordinateur ne présente aucune menace de sécurité.

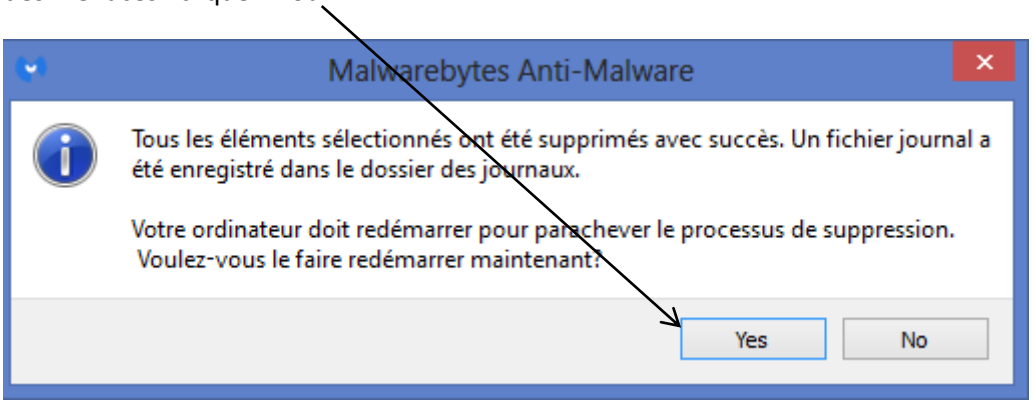
Fermez le programme

Quand des menaces sont détectées, une liste vous est proposée :



Cliquez sur le bouton « tout mettre en quarantaine » pour neutraliser les

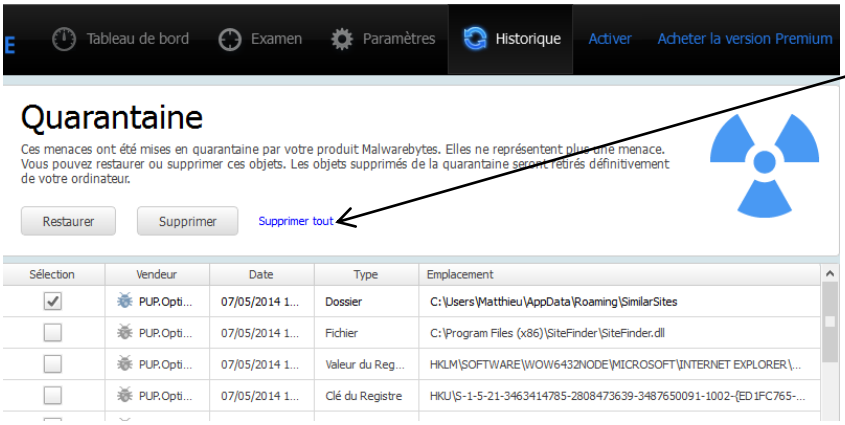
Malwarebytes vous demande alors de redémarrer votre ordinateur pour terminer la neutralisation des menaces : cliquez « oui »



Votre ordinateur s'éteint et redémarre automatiquement. Les menaces ont été écartées et votre ordinateur est nettoyé !

Rien d'autre à faire !

Toutefois, si vous souhaitez supprimer manuellement les menaces trouvées, vous pouvez le faire à tout moment en lançant à nouveau le programme et en vous rendant dans le menu « historique » vu précédemment.



Le bouton « supprimer tout » vous permet de vider manuellement la zone de quarantaine

3) Nettoyer vos navigateurs Internet et supprimer les modules complémentaires intrusifs

Il peut arriver que certains logiciels malveillants persistent, essentiellement ceux liés à vos navigateurs Internet : certains d'entre eux modifient votre page d'accueil Internet, d'autres vos moteurs de recherches, enfin certains appellent et ouvrent des fenêtres de façon automatique…

L'antivirus et Malwarebytes peuvent se trouver impuissant face à ces menaces.

Deux outils vont vous permettre dans un premier temps de nettoyer, et dans un second temps d'éviter les pubs et autres boutons contenant des liens malveillants.

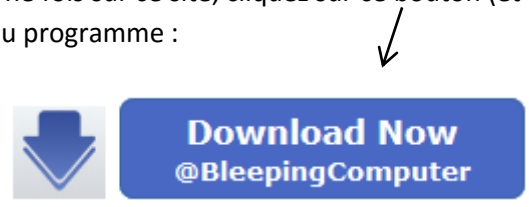
a) ADWCLEANER, nettoyeur de dernier recours.

Adware cleaner est un logiciel simple à usage unique, à utiliser quand vos navigateurs Internet ont des comportements inhabituels (fenêtres surgissantes, moteurs de recherche et page d'accueil modifiés…)

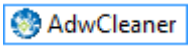
Pour le télécharger, utilisez le site google.fr et tapez « adwcleaner bleeping » pour trouver l'adresse (ou bien rendez-vous manuellement à cette adresse) :

www.**bleeping**computer.com/download/**adwcleaner**/

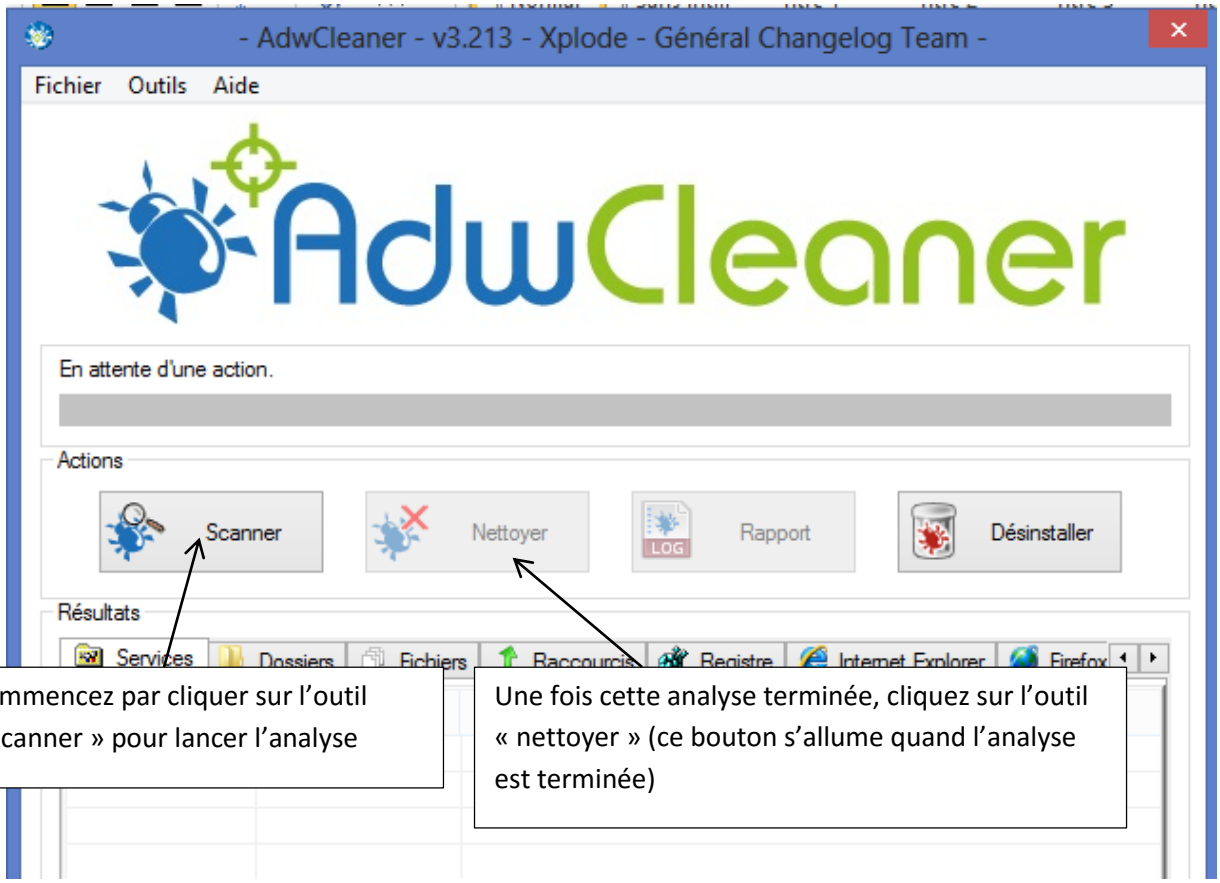
Une fois sur ce site, cliquez sur ce bouton (et uniquement ce bouton !) pour lancer le téléchargement du programme :



Enregistrez le fichier (Il se range dans votre dossier « téléchargement »)

Dans ce dossier ; lancer le programme en double cliquant : 

Ce programme est très simple et vous propose une seule tache :



Le programme vous demandera de redémarrer en cliquant sur « ok » en fin de nettoyage.

Les modules complémentaires malveillants (adwares) seront ainsi supprimés.

Il vous faudra *dans certains cas* régler à nouveau votre page d'accueil Internet en vous rendant dans le menu « options » de votre navigateur.

Conclusion : les règles pour éviter une infection par des virus

- Ne remplissez pas n'importe quel formulaire en ligne, ou alors interrogez-vous sur la pertinence des réponses à donner.
- N'acceptez jamais systématiquement un message émis par un site web : on vous propose de télécharger un programme afin de vous faire bénéficier d'offres promotionnelles extraordinaires ? Il est certain qu'un spyware est installé dans ce programme, et que vous ne recevrez jamais d'offres... Ne cochez donc pas de manière compulsive les cases "oui" ou "ok" dès qu'une fenêtre de dialogue s'affiche sur un site web.
- N'acceptez pas sans réfléchir les programmes supplémentaires éventuellement proposés lors de l'installation d'un logiciel : il suffit de décocher les cases correspondantes pour qu'ils ne soient pas installés.
- Avant d'ouvrir une pièce jointe, même si l'expéditeur est un proche, vérifiez qu'elle provient bien de lui.
- N'hésitez pas à supprimer un message suspect.

- Méfiez-vous des exécutables envoyés en pièce jointe, souvent de la part d'une société informatique (comme Microsoft). Ces sociétés n'envoient JAMAIS de mise à jour par e-mail. Il vaut mieux supprimer cet e-mail et télécharger la mise à jour sur le site de la société.
- Si un e-mail comporte une pièce jointe avec une double extension (fichier.mp3.pif, document.doc.bat, x.jpg.vbs, ...), supprimez-le. Il s'agit d'un virus.
- Sur votre boite mail faites aussi très attention au phishing. Vous recevrez un message en provenance de votre fournisseur d'accès, de votre banque, du site Paypal… Dans celui-ci, on vous invite à fournir des informations très personnelles (mot de passe, n° de compte, de carte bancaire…). Même si ce mail reprend les couleurs ou le logo de votre organisme, il s'agit d'un mail réalisé par des pirates informatiques. Un organisme ne vous demandera jamais par mail de fournir des informations aussi sensibles. Supprimez sans le lire ce message.
- **Les attaques sur le web sont de plus en plus fréquentes : toutes les fenêtres que vous voyez sur Internet du type « vérifier gratuitement, l'état de votre ordinateur » ou bien « 528 erreurs ont été trouvées sur votre PC, cliquez ici pour les supprimer » sont des appâts pour vous inciter à cocher le lien.** Malheureusement, l'effet produit est souvent opposé à celui recherché : en cliquant sur ces fenêtres, vous ouvrez la porte à des infections variées parfois peu graves mais très gênantes au quotidien (votre page d'accueil internet change, des barres d'outils s'installent et ne veulent plus se supprimer…voire un virus est téléchargé dans votre disque dur)

- Ne donner pas votre adresse mail sur des sites qui vous la réclame sans raison.

- Eviter les sites à risque (site de téléchargement généraliste (softonic…), site de charme, site de rencontres peut connus, site de téléchargements illégaux (vidéos, musiques…)

- Vérifiez les fichiers que peuvent vous donner des amis (films téléchargés, musiques illégale, programmes « crackés »)

Faites régulièrement une analyse de votre ordinateur avec Malwarebytes pour assurer une protection supplémentaire en plus de votre antivirus « Defender ».