FC07

INFO-AIVM37

Adwcleaner

Adwcleaner

MAJ le 04/04/2022

Présentation du problème

Logiciel qui cherche et retire de l'ordinateur tous les installations publicitaires potentiellement dangereuses introduites subrepticement lors de recherches sur internet ou à l'occasion d'un chargement de logiciel

Très utilisé dans le cadre d'AIVM37, ce logiciel est déjà expliqué dans les fiches suivantes
http://aivm37.free.fr/BI/JT/JT204_adwcleaner.pdf

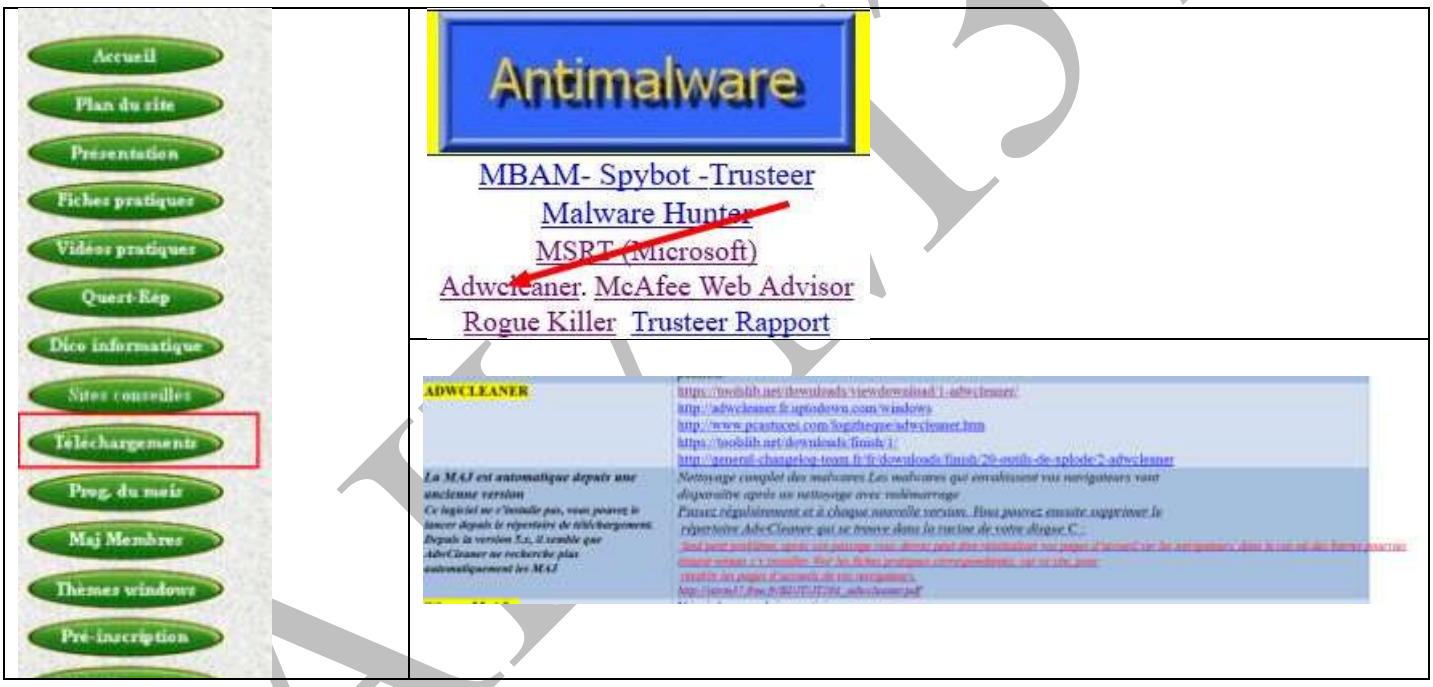
http://aivm37.free.fr/BI/JT/JT028_NettoyerSonSysteme.pdf
Page 3.
http://aivm37.free.fr/BI/JT/JT078N_Maintenance-Freeware.pdf
page 54
Comme la présentation du logiciel a une fois de plus été remaniée, cette fiche montre les nouvelles interfaces et rappelle les modalités d'utilisation.

AIVM37

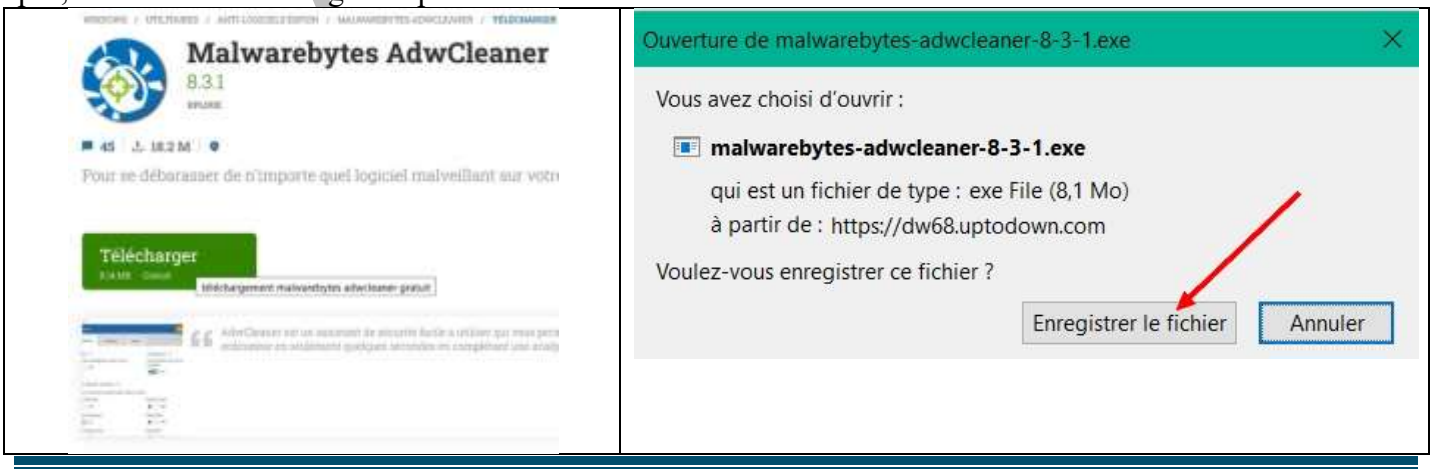
Sommaire

1 Télécharger le logiciel. Mise à jour du logiciel

Aller chercher dans le site AIVM « Téléchargements » la page Internet d'où télécharger le fichier exécutable d'Adwcleaner

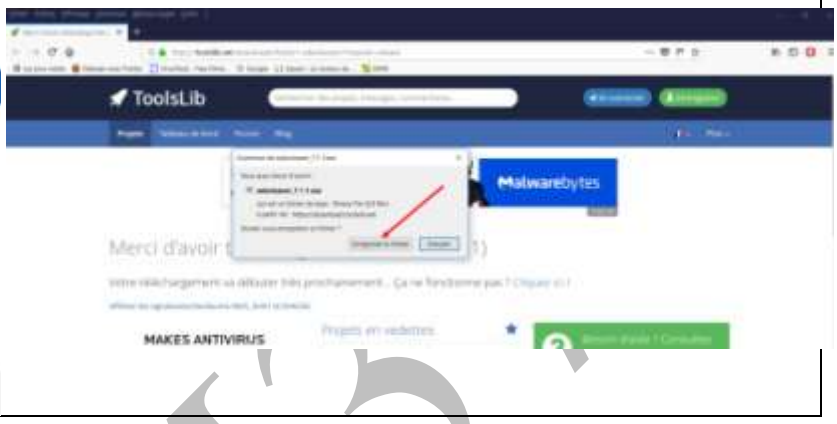


A partir du fichier : Adwcleaner .xxx Exe, ouvrir directement le logiciel. Comme ce logiciel ne s'installe pas, il vaut mieux l'enregistrer pour le mettre dans un dossier comme « maintenance »



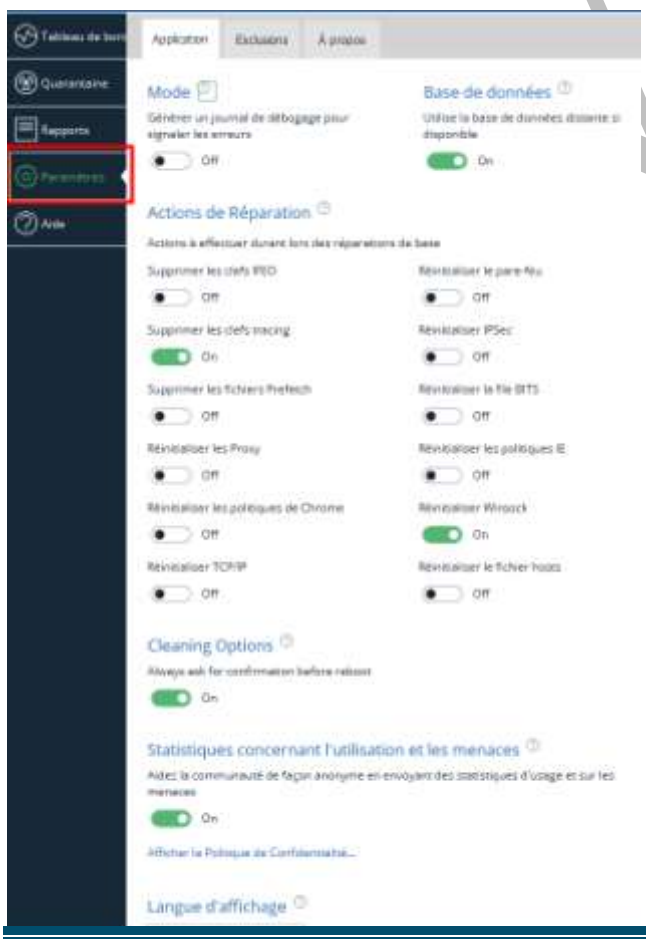
AIVM37

Si l'enregistrement est un peu ancien, une mise à jour peut être nécessaire

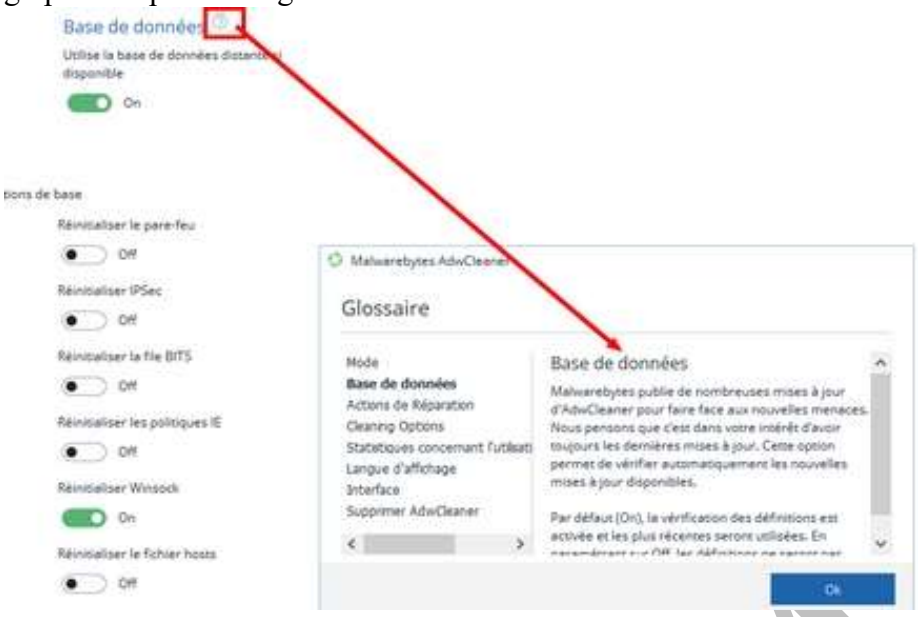
Si l'exécutable Adwcleaner .xxx Exe enregistré dans le PC n'est pas à jour, quand on le lance, apparait une fenêtre de mise à jour On clique sur Oui	S'ouvre alors directement une page internet qui propose d'enregistrement du nouveau fichier de mise à jour. On enregistre et on lance l'exécutable
	

2 Paramétrage

L'onglet paramètres propose un paramétrage minimum par défaut. Le plus simple est de le respecter sauf gros problèmes.



Pour connaitre ce qui est proposé, on peut cliquer sur les points d'interrogation à coté de chacun des paragraphes de paramétrage



Mais les Actions de Réparation peuvent demander quelques éclaircissements.

Supprimer les clés IFEO : supprime toutes les sous clés IFEO,
L'abréviation "IFEO" désigne les options d'exécution du fichier image. C'est un mécanisme Windows très complexe qui permet de vérifier dans les applications des erreurs potentielles. IFEO apparaît sous la forme d'une clé de registre,

Supprimer les clés tracing : supprime l'ensemble des clés Tracing pouvant être utilisées par certains logiciels malveillants.

Supprimer les fichiers Prefetch : la fonction Prefetch consiste à répertorier les logiciels lancés le plus souvent de façon à optimiser leur positionnement sur le disque et donc à accélérer leur lancement.

Réinitialiser les proxys : Supprime l'ensemble des proxies utilisés par le système c.-à-d. des programmes servant d'intermédiaire pour accéder à un autre réseau,

Réinitialiser les politiques de Chrome et de IE : remet à défaut les politiques de confidentialité

Réinitialiser le TCP/IP : réinitialise les paramètres TCP/IP, qui est l'exécutable définissant la façon dont le PC communique avec d'autres PC.

Réinitialiser le pare-feu : réinitialise les règles du pare-feu par défaut.

Réinitialiser IPSec : réinitialise les paramètres IPSec par défaut. C'est un protocole utilisé pour mettre en place des connexions chiffrées.

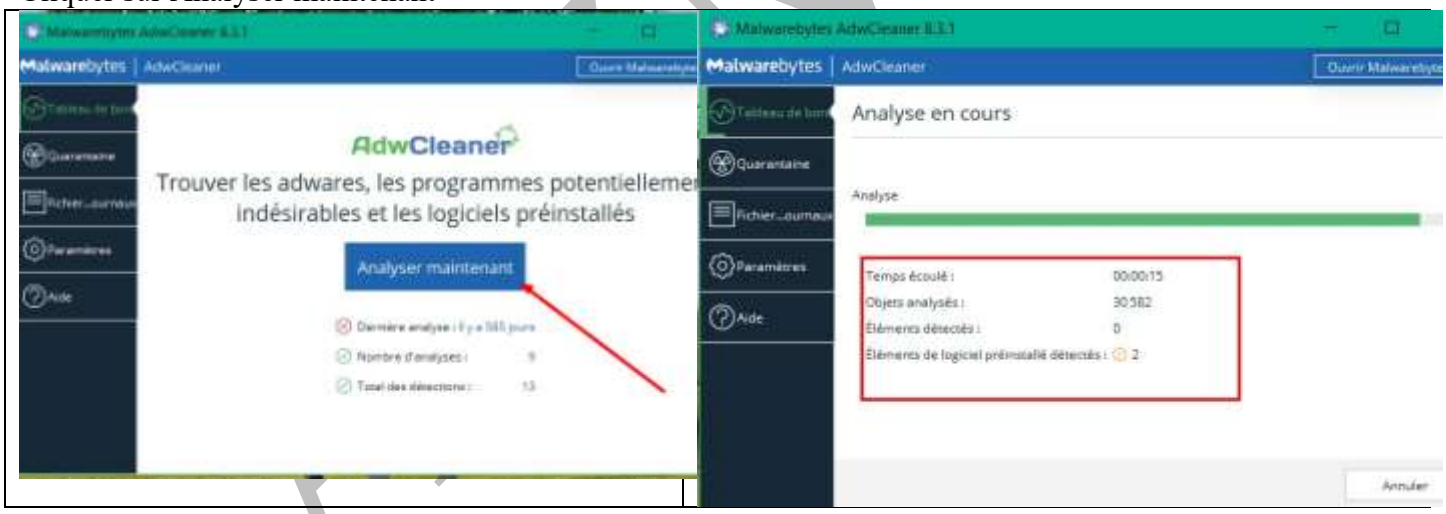
Réinitialiser la file BITS : vide la file du "Background Intelligent Transfer Service", composant de Windows utilisé pour le transfert de fichiers (certaines mises à jour de logiciels par exemple)

Réinitialiser Winsock : réinitialise l'ensemble des paramètres Winsock afin de résoudre les problèmes de connectivité. (Winsock une bibliothèque dynamique de fonctions DLL sous Windows dont le but est d'installer un logiciel en réalisant les adaptations nécessaires à son fonctionnement.)

Réinitialiser les fichiers hosts : remet à défaut le fichier Hosts (fichier présent sur la plupart des systèmes d'exploitation, permettant de transposer un nom de machine (nom de domaine) en adresse IP

3 Rechercher les fichiers toxiques

Cliquer sur Analyser maintenant

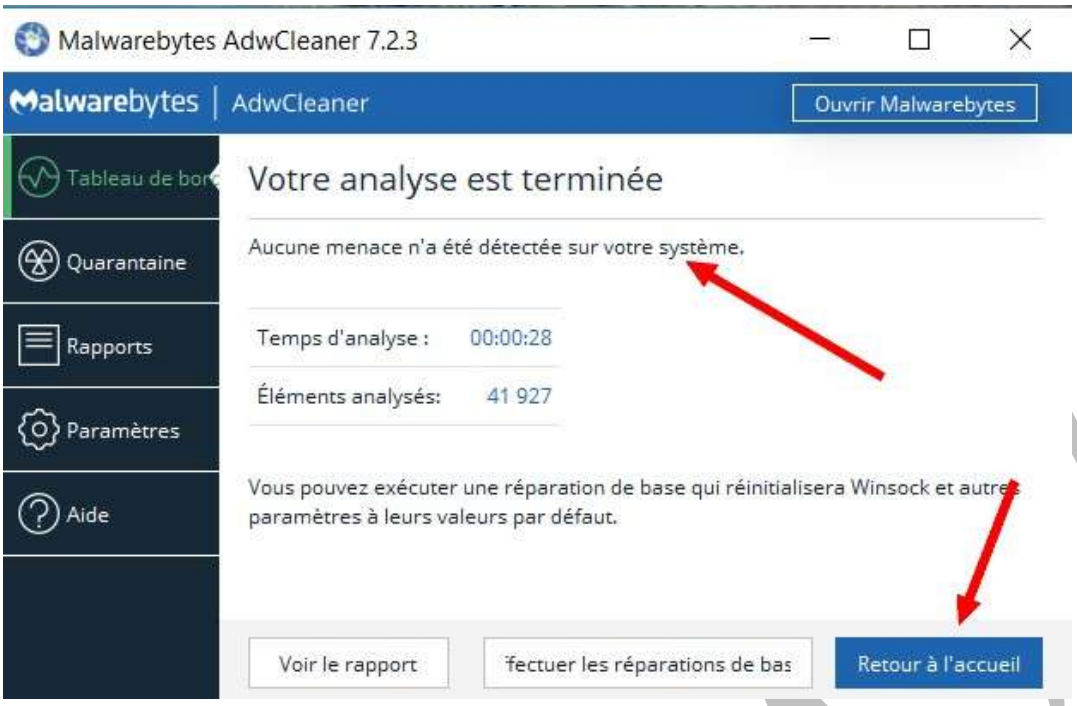


Laisser la recherche se faire (cela peut prendre un peu de temps), les résultats apparaissent peu à peu.

Trois possibilités :

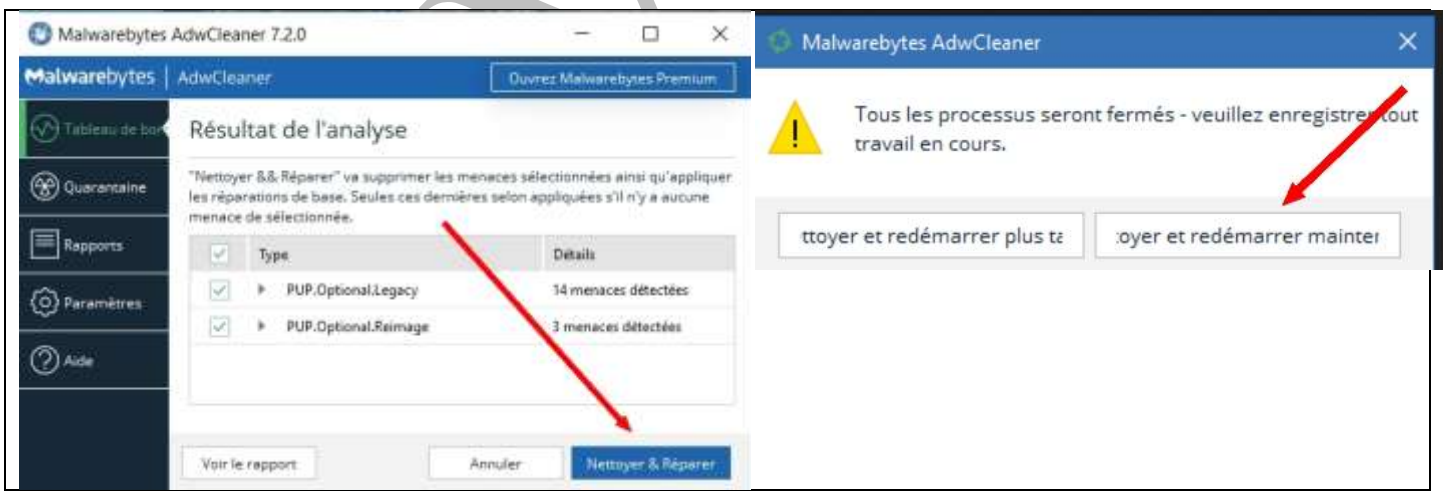
3.1 Si l'ordinateur est propre

On clique sur OK, on peut retourner à l'accueil et on ferme le logiciel

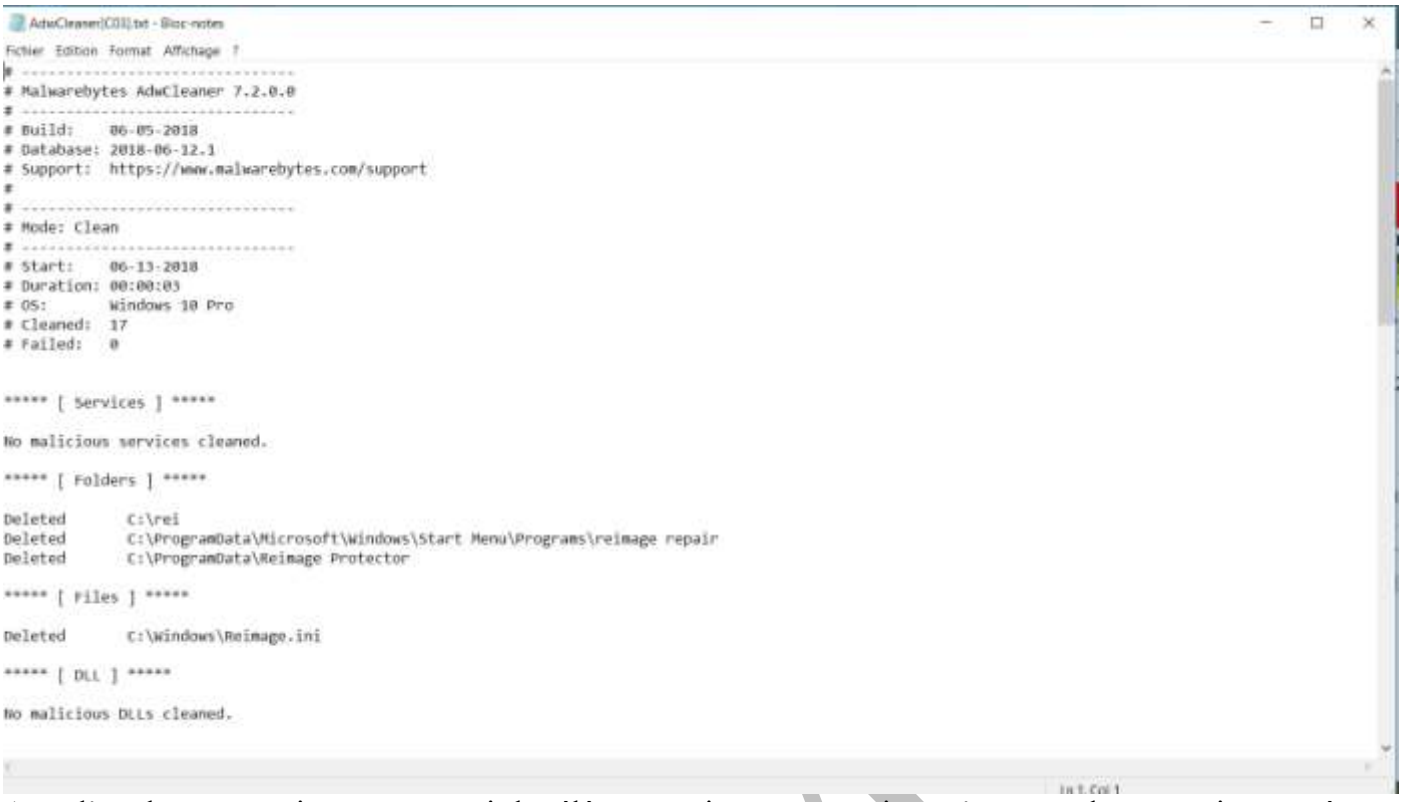


3.2 -Si des fichiers douteux ou dangereux ont été trouvés :

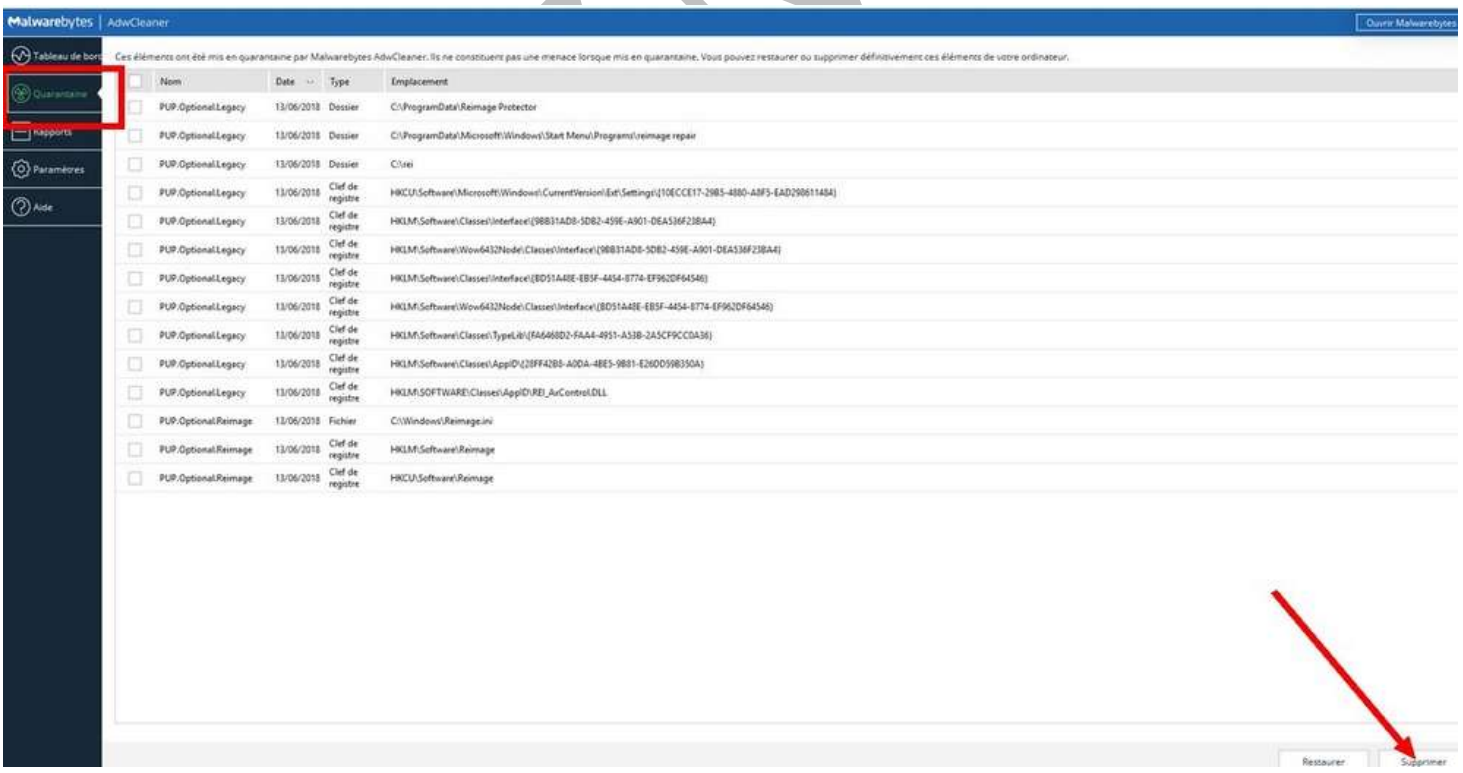
On clique sur Nettoyer et Réparer et dans la fenêtre qui s'ouvre, on choisit de préférence Nettoyer et redémarrer maintenant.



Une fois l'ordinateur redémarré, s'ouvre un fichier texte avec le compte rendu de ce qui a été supprimé



Avec l'onglet quarantaine, on peut voir les éléments mis en quarantaine qu'on peut alors supprimer après avoir sélectionné ceux qui apparaissent comme gênants (en principe, tous…).



3.3 Il peut aussi y avoir des logiciels préinstallés

Adwcleaner propose de les mettre en quarantaine.
Il va, dans ce cas, falloir vérifier si le logiciel préinstallé est à supprimer ou non en fonction de son utilité ou sa nuisance.
En général, ils ne sont pas dangereux, si ce sont des applications ajoutées par le fabriquant, la plupart sont inutiles et dépassés par les logiciels nouveaux installés et ils encombrent le disque dur
Mais leur suppression peut poser des problèmes
Il s'agit dans cet exemple d'un logiciel de la marque du PC et dont la suppression aurait pu allonger le temps de démarrage de l'ordinateur. Donc, ici, on annule la mise en quarantaine.