## **Fiche Pratique**



# 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

MAJ le 04/04/2022

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.

n loi 1901

ocia

### Sommaire

- 1 Télécharger le logiciel. Mise à jour du logiciel
- 2 Paramétrage
- 3 Rechercher les fichiers toxiques
  - 3.1 Si l'ordinateur est propre
  - 3.2 -Si des fichiers douteux ou dangereux ont été trouvés :
  - 3.3 Il peut aussi y avoir des logiciels préinstallés

# 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 »



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



### 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.

Actions de Réparation 🕘	
Actions à effectuer durant lors des réparations e	de base
Supprimer les clefs IFEO	Réinitialiser le pare-feu
• off	• or
Supprimer les clefs tracing	Réinitialiser IPSec
0n	• off
Supprimer les fichiers Prefetch	Réinicialiser la file BITS
Off.	• Off
Réinitialiser les Proxy	Réinitialiser les politiques IE
Off	Off.
Réinitialiser les politiques de Chrome	Réinitiakser Winsock
Off	0n
Réinitialiser TCP/IP	Réinitialiser le fichier hosts
• Off	• Off

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

Malwaretrytre Advectment #3.1		EI.	C Malwarebytes	AdwGeaner II.3.1		-
Malwarebytes   AdvClumer		ra Malaaratiya	Malwarebytes	AdwCleaner		Ouwrin Malwaretype
Statune in ter	dwCleaner		Tattanu de land	Analyse en cours		
Trouver les adwares, Indésirables	les programmes poten et les logiciels préinstall	tiellemei lés	Fichier_aumaus	Analyse		
O'rearran ar an	nalyser maintenant		@Paramètres	Temps écoulé : Objets analysés :	00:00:15 30:382	
() () () ()	omière analyse i Fy a NAT, pure ontere d'analyses i 9 mé des stélectores : 13		@Ade	Éléments détectés i Éléments de logiciel préinstal	0 Né détectés i 🕐 2	
				and a		
	-		f I			Annuler

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

## Fiche Pratique

🕄 Malwarebytes	AdwCleaner 7.2.3		() <del></del> ()		×					
Malwarebytes	AdwCleaner		Ouvr	ir Malwarebyte	s					
🐼 Tableau de bor	Votre analyse	Votre analyse est terminée								
🛞 Quarantaine	Aucune menace n'a été	Aucune menace n'a été détectée sur votre système.								
Rapports	Temps d'analyse :	00:00:28								
O Paramètres	Éléments analysés:	41 927								
? Aide	Vous pouvez exécuter paramètres à leurs val	une réparation de base eurs par défaut.	equi réinitialisera V	Vinsock et autro	ł					
	Voir le rapport	fectuer les réparat	tions de bas	Retour à l'accu	eil					

## 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.

Malwarebytes	AdwCleaner 7.2.0	- 🗆 X	Malwarebytes AdwCleaner	×
Malwarebytes	AdwCleaner	Ouvrez Malwarebytes Premium		
Tabienu de bor	Résultat de l'analyse		Tous les processus seront fermés - veuillez en travail en cours.	registrencout
🛞 Quarantaine	"Nettoyer && Réparer" va supprimer les me les réparations de base. Seules ces dernière menace de sélectionnée.	naces sélectionnées ainsi qu'appliquer is selon appliquées s'il n'y a aucune		
Rapports	🗸 Туре	Détails	ttoyer et redémarrer plus ta :oyer et redémarre	er mainter
(ô) Paramètres	PUP.Optional.Legacy	14 menaces détectées		
-	PUP.Optional.Reimage	3 menaces détectées		
(?) Adde				
	Voir le rapport	nnuler Nettoyer & Réporer		

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

AthiClease	n(COII) tot - Bioc-wates		-	×
Fichier Edition	n Format Affichage 1			
# Malwareb	ytes AdwCleaner 7.2.0.0			111
\$				
# Build:	06-05-2018			
# Database	: 2818-06-12-1			
# Support:	https://www.malwarebytes.com/support			
1				
ŧ				
# Mode: Cl	ean			100
# Start:	06-13-2018			
# Duration	1 00:00103			
# 05:	Nindows 10 Pro			1.0
# Cleaned:	17			
<pre># Falled;</pre>				
***** ( se	rvices ] *****			
No malicio	us services cleaned.			
***** [ Fo	lders 1 *****			
Deleted	C:\rei			
Deleted	C:\ProgramData\Microsoft\Windows\Start Menu\Programs\reimage repair			
Deleted	C:\ProgramData\Reimage Protector			
***** [ Fi	les ] *****			
Deleted	C:\Windows\Reimage.ini			
***** { DL	r 1			
No malicio	us DLLs cleaned.			
				. *
S		10000000		

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...).

Malwarebytes   /	AdwClea	inër				Ouvrir Malwarebyte
Tableau de bort	Ces élér	nents ont été mis en quara	nteine par Ma	iwarebytes	AduxCleaner. Its ne construent pas une mierace forsque mis en quarantaine. Vous pouvez restaurer ou supprimer définitivément ces éléments de votre ordinateur.	
Distantana -		Nom	Date 😐	Type	Emplacement	
		PUP.OptionalLegecy	13/06/2018	Dossier	Col/regramData/Reimage Protector	
I rapports	T LI	PUP.OptionalLegacy	13/06/2018	Dessier	CI/ProgramData/Microsoft/Windows/Start Menu/Programs/inimage repair	
O Parametres		PUP.OptionalLegacy	13/06/2018	Dessier	Cise	
Om		PUP.OptionalLegacy	13/06/2018	Clief de registre	H9CU/Software(Microsoft)Windows).CurrentVersion/Est/Setting1/(10ECCE17-2983-480/-ABF3-EAD/200611484)	
(C)~~~		PUP.OptionalLegacy	13/06/2018	Clef de registre	HKLM/Software/Classes)interface((98831AD8:5D82-4596-A301-0EA5)66238A4)	
		PUP.OptionalLegacy	13/06/2018	Clef-de registre	HRLM:Software/Wow6432Node/Classes/Interface/(98831ADI-5082-459E-A901-0EA336F238A4)	
		PUP.OptionalLegacy	13/06/2018	Clef-de registre	HKUM/Settware)ClassesInterFace(EDS):A4EE-(ESF-4454-0774-EF962DF44546)	
		PUP.OptionalLegacy	13/06/2018	Cief de registre	HRUM/Sethume/Wow6432Node/ClassesUnterface(BD31A48E-EBSF-4454-8774-EF962DF64546)	
		PUP.OptionalLegacy	13/06/2018	Clef de registre	HRLM:Software/Classes(TypeLil/)(FA646802-FA24-4951-A338-2A5CF9CCDA36)	
		PUP.OptionalLegacy	13/06/2018	Clef de registre	HKI.M.Sertwarei.Classeri.AppiDV;28FF4285-a00A-48E5-9881-62600598350A)	
		PUP.OptionalLegacy	13/06/2018	Cief de registre	HRIAN SOFTWARE: Classes Appl DIREL AuControl DLL	
		PUP.Optional Reimage	12/06/2018	Fichier	C//Windows/Reimage.inv	
		PUP.Optional.Reimage	13/06/2018	Clef.de registre	HKIM Software Reimage	
		PUP.Optional.Reimage	13/06/2018	Clief de registre	HICUSoftwartReimage	

### 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.

X

Malwarebytes AdwCleaner 7.4.1

Malwarebytes	AdwCleaner	Ouvrir Malwa	arebytes
Tableau de boi	Résultat de l'analyse Logiciel préinstallé ⑦		
	Sélectionnez les logiciels préinstallés que v cliquez sur "Mettre en quarantaine" pour d pouvez les supprimer	rous souhaitez mettre en quarantaine et désactiver. léplacer les logiciels préinstallés en quarantaine, où	Puis vous
Rapports	Preinstalled software elements found: 1		
O Paramètres	Nom	A Distributeur ASUSTAK Computer las	
(?) Aide		Asosiek computer nic.	
		Annuler Mettre en qua	arantaine