

# Malwarebytes Anti-malware

# **Présentation**

- Logiciel conçu par une société californienne : Malwarebytes Corporation Origine du nom : byte : 1 Byte = 1 octet = 8 bits Malware : logiciel malveillant : on dit aussi « maliciel » (contraction de « malicious » et « software »)
- Un malware est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur de celui-ci.

#### Table des matières

Pı	résenta	tion
1	Inst	allation de MBAM
-	11	Installation
	1.1	Les nouvelles mises à jour
	1.2	La nouvelle édition de MBAM
$\mathbf{r}$	1.5 Dom	La nouvene cutton de MBAN
2	Para	uneurage de MIDAM
	2.1	Paramétrage général
	<ul> <li>ésentation</li> <li>Installation de MBAM</li> <li>1.1 Installation</li> <li>1.2 Les nouvelles mises à jour</li> <li>1.3 La nouvelle édition de MBAM</li> <li>Paramétrage de MBAM</li> <li>2.1 Paramétrage général</li> <li>2.2 Paramétrage de la sécurité</li> <li>Détection</li> <li>3.1 L'analyse</li> <li>3.2 Eradication</li> </ul>	
3	Dét	ection
-	3.1	L'analyse
	2.1	
	3.2	Eradication



# 1 Installation de MBAM

### 1.1 Installation

Commencer l'installation de MBAM avec le setup de Malwarebytes anti malware qu'on va chercher sur le site d'AIVM (téléchargements)

Antimalware		
MBAM, Spybot -Trusteer Malware Hunter MSRT (Microsoft)	MBAM var leur site allez dans le bas de la page et prenez la version gratuite	https://www.malwarebytes.com/adwcleaner/jump/?ref=adw http://www.cimbic.com/telecharger-fiche215092-malwarebytes-anti-malware.html http://www.cimbic.com/telecharger-fiche215092-malwarebytes-anti-malware.html http://www.pcashces.com/logithegue/malwarebytes-anti-malware.htm
Adweleaner, McAfee Web, dvisor Rogue Killer Trusteer Rapport	Mahsare bytes' Anti-Mahsare (32b et 64b) Anti mahsare puissant	Instile de supprimer la version précédente, soué en cas de champement de version prime de Pas de problème à l'austiliation. A prendre de préférence sur Praktuces.

On accepte toutes les étapes de l'installation (on ne peut pas éviter l'installation de la version premium à l'essai)

Dans la fenêtre de l'assistant, choisir Options avancées et avec le dérouleur dans la fenêtre qui s'ouvre, aller chercher Français puis cliquer sur Enregistrer.

Sinon, l'installation se fait en anglais, ce qui n'est quand même pas grave car, dans les paramètres, on peut toujours changer la langue.

Victor Accurl Partage	Affichage Dutits d'application	- a ×	Howerships Setue	140 H (K
Malwarebytes Setup	e dans Assistant de configuration	n Malwarebytes	Cyprions avandes	E Order un recourd sur le l
En installant ou en utilisant o	te produit, vous acceptez de vous contormer à son <u>Contrat de licence utilis</u>	steur final et à ca Ebilitique de confidentialité		

Qu'on ait choisi ou non la langue, on revient à la fenêtre de l'assistant, on clique sur Installer et il faut refuser l'installation du navigateur spécifique de Malwarebytes. Bien sûr, on peut l'accepter si on veut mais cela ajoute un navigateur de plus au risque d'alourdir le PC.

Meinantigtet Setur	Malvaretades Setap -
Bienvenue dans Assistant de configuration Malwarebytes	Ajouter la protection du Installier navigateur Inclut la protection du navigateur Inclut la protection du navigateur
Options avancées	Retour C'est d'ecord
The excession of the end of the second state second states in the Carter & Second &	If you agree, the extension you destend on the process and the cest time you bunch your browser. To subject non-other or public our angeler driver our ordered have build and a subject to the subject to a subject to
The monotone of a difference provided in the second of the content of the Content of Links and Advances of the Content of the	If you agree, the extension will install the next time you bunch your brow Tainingbet even observe probations assessed in our conference is an <u>control of installed states</u> that it is a <u>control of the set</u>

L'installation se fait sans intervention nécessaire, sauf, à la fin, Malwarebytes peut redemander le redémarrage de l'ordinateur.





Aller dans j	paramètres de N	Malwarebytes		I	Le compte	e est désc	ormais	gratuit.				
et cliquer s	sur Compte Et e	ensuite sur Désact	iver.		Malwarebytes	s Gratuit 4.5.2					- 1	
Malwarebytes Gra	ituit 45.2		- 0	×	M Free					Activer la licenci	. Δ	\$ (
M Free		Ac	tiver la licence	<b>\$</b> 0	Paramètres							×
Paramètres				×	Général	Notifications	Sécurité	Affichage	Liste Autorisés	Compte	À propos	
Général N	lotifications Sécurité	Affichage Liste Autorisés	Compte À propos		Information	s sur le compt	e		40			
Informations su	ur le compte				Nom de l'appar	rek Édition		Clè de licence	Etut			
Nom de l'appareil	Edition	Clé de licence	Etat		HPAIVM	Malwareby	tes Free	Sector Content	Always free (Up)	grade to Premiun	n for real-time	protection
HPAIVM	14-day Premium Trial	54 (Sec. 1)	Essai expiré - Obtenez la	mise à				Activer la licence	Acheter mainten	ant		
		/	Acheter maintenant									
			1		Gérer les	appareils						
Gérer les app	pareils				Pour ajouter	ou supprimer des	appareits d	ans le cadre de vob	e abonnement, rend	dez-vous sur	Accèder a	o comote
Pour ajouter ou s votre compte	supprimer des appareils dans le	cadre de votre abonnement, rendez	-vous sur Accéder au	compte	votre compte	e		_			Constant Con	
votre compte			Accourta					7				

#### 1.2 Les nouvelles mises à jour

La présentation des mises à jour a changé, elle peut faire passer obligatoirement par l'essai de la fonction premium et semble-t-il, passe de temps en temps à l'emploi de l'anglais.

Malwarebytes peut proposer une mise à jour directement quand la version de l'application est un peu ancienne. Sinon, la recherche des mises à jour passe par l'onglet paramètres

$\ensuremath{\diamondsuit}$ Analyseur			Malwarebytes Gratuit 43.0	and the second second	- E
Analyseur	Planificateur d'analyse Comptes-rendus.	-	M   Free	Activer la licence	Acheter maintenant
	Une nouvelle version de Matwarebytes est prête à être installée. La mise à jour peut nécessiter le redémarrage de votre ordinateur. Installer maintenant ?	ésumé 20 m	Paramètres Général Notifications Sécurité	Affichage Liste Auto	risés Compte À propos
	PUP détectés PUM détectés Détections ignorées	375	Mises à jour d'application Télécharger et installer automatiquement les mise	es à jour	0

Puis l'installation se fait comme précédemment, en faisant attention au choix de la langue et le refus du navigateur spécifique.

Général         Notifications         Sécurité         Affichage         Liste Autorisés         Compte         À propos           Mises à jour d'application	Téléchargement de la mise à jour en cours
Telécharger et installer automatiquement les mises à jour Me prévenir lorsqu'une nouvelle version est disponible Rechercher les mises à jour	Installation de la mise à jour en cours
Paramètres Windows Explorer Ajouter options Malwarebytes à Windows Explorer	We need a moment to
Impact d'une analyse manuelle sur les performances   Les analyses manuelles sont proritaires sur les autres applications	apply some updates Malwarebytes restarting in: 15s
Les analyses manuelles n'ont pas la priorité (moins d'impact sur les performances)  Données du journal d'événements Recueilir des données détailées du journal d'événements à des fins d'assistance (déconseillé)	Restart Malwarebytes
Accès utilisateur Verson Premium seulement Restreignez l'accès aux paramètres de sécurité de votre compte Malwarebytes	

# 1.3 La nouvelle édition de MBAM

Suivant le cas, on peut avoir la version gratuite ou la version avec essai de la formule Premium

			Malwaretates Premium Essai 452		- 0 ×
			M i Phemiam Trial	Activer la licence	
	EarthA, you're wit hals protection bere smorth none roate out after Very earth		Q	Your device is protected Great job staying safe and see	CLUTH
J	φ	0	a data and		
Hardeniga on advertion: Device on a quantizer on or Indevice engine	ingen perior Parage	Growth Road Brow Probability for their exheritory before They fragme	U Historique des détections	ф. Алабитеци	Protection on termos rikel
Garactions (17)	Anidyne	Sty save for fine	Calmenti mis en quanantaria di tera del la daminina analigari di Tattat des elatrocetta places esti gi	Analyses plantities Augustation 10.27	Protective Week
			quarertane	Analyse	Partaction courtes les espin.

# 2 Paramétrage de MBAM

Dans le coin supérieur à droite, cliquer sur la roue dentelée des paramètres



#### 2.1 Paramétrage général

Onglet Paramètres, sous-onglet Général, rechercher la mise à jour matique (2)	(1) et choisir ou non la mise à jour auto-
C'est là que se fait le choix de la langue (3)	
Et choisir ou non de mettre Malwarebytes dans les menus contextu	uels (4)
H Mainandytes Gratuit 453	
♥   Free	Activer la licence Achieter maintement
Paramètres	
Général Notifications Sécurité Affichage Liste-Autorisés Compte A propos	
Télécharger et instater automatiquement les mises à jour	<b>)</b> 🔊
Me prévenir lorsqu'une nouvelle version est disponible 🛈	<b>_</b>
Rechercher les mises à jour	
Paramètres Windows Explorer	
Ajouter options Malwarebytes & Windows Explorer	1 >0
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	4
Langue	
Hangas	

#### 2.2 Paramétrage de la sécurité

Onglet Paramètres, sous-onglet Sécurité :

Vérifier les options d'analyse qui doivent être cochées

Activer les 4 options d'analyse.

Vérifier les éléments potentiellement indésirables

Les détections <u>PUP</u> (Programmes potentiellement indésirables) et <u>PUM</u> (Modifications potentiellement indésirables) doivent être configurées sur <u>Toujours</u>

Dptions d'analyse Recherchenies motivits	
Analyser les aechives	
Détecter les menaces avec intelligence artificiele	
dentifiez les fichiers maiveillants à l'aide d'algorithmes système puissants	
Eléments potentiellement indésirables Les fonctionnalités font partie à la fois de la protection en temps néel et des analyses	
Défecter les programmes potentiellement indésirables (PUP) Toujours (recommandé)	Ψ
Détecter les modifications potentielement indésirables (PUM) Toujours (recommandé)	v

# 3 Détection

# 3.1 L'analyse

Dans la fenêtre générale, cliquer sur Analyse

	M   Free	Activer la licence	cheter maintenant 🛛 🗘 🕸 (
	For stronger security, get the new upda	te. It's free. Update now	
		Careful, you're not fully prot Some security issues require your View details	ected attention
	U Historique des détections	Analyseur	Protection en temps réel
	Élément mis en quarantaine 0 lors de la demière analyse 0	Analyses planifiées Permium	Unlock Real-Time Protection to stop infections before they happen
	Total des éléments placés en 12 quarantaine	Analyse	Try now for free
Iwarebytes (	Gratuit 4.3.0		
Free Free Analyse	Gratuit 4.3.0	Activer la licence Achete	ー 口 r maintenant )
Free ↓ Free ↓ Analyse Analyse	Gratuit 4.3.0 with and the new wordste life free l eur ur Planificateur d'analyse	Activer la licence Achete	r maintenant )
iwarebytes (   Free → Analyse Analyse	Gratuit 4.3.0 with act the new undate We free I eur ur Planificateur d'analyse An	Activer la licence Achete	ー 口 r maintenant   ① 袋
alwarebytes (   Free	Gratuit 4.3.0	Activer la licence Achete Indata accur Comptes-rendus alyse des menaces en cours Recherche de mises à jour Recherche de rootkits Analyse de la mémoire Analyse de séléments de démarrage Analyse du registre Analyse du système de fichiers	r maintenant Durée de l'analyse 10 m 4 s Éléments analysés 158 252 Détections 0
Analyse	Gratuit 4.3.0	Activer la licence       Achete         Undata accur       Comptes-rendus         alyse des menaces en cours       Recherche de mises à jour         Recherche de mises à jour       Recherche de rootkits         Analyse de la mémoire       Analyse des éléments de démarrage         Analyse du registre       Analyse du système de fichiers         Interrompre       Annuler	r maintenant Durée de l'analyse 10 m 4 s Éléments analysés 158 252 Détections 0

Au cours de l'analyse, peuvent apparaitre ou non des menaces détectées

Malwarebytes Promium Essai 4.5.2		- 0 ×	Compte-rendu d'analyse		×
Premium Trial	Activer la Scence Activeter maintenam	0 4 0	Résumé Avance		
O Analyseur		2	Résumé de l'analyse No Rems detected	Date 11/03/2022 17:48	
Analyseur Planticateur d'analyse	Completemendus		And 25-PERSONNELS	Scan result Terminé	
	Analyse des menaces -	résumé			
1	Desig (Tanalyse	3833m121			
F CI	Eximents analysis	416099			
	Menaces détectées	0			
	PUP detectes PUH detectes	0			
4	Diffectors ignosies	D			
	Diffections mean en quarantaine	0	Exporter *		Farme
	Afficher le compte-rendu	Termine			
			ľ Š		

# 3.2 Eradication

Si à la fin de l'examen : des éléments ont été détectés, le programme incriminé est nommé et Malwarebytes propose la quarantaine : on clique

La mise en quarantaine s'effectue silencieusement mais on peut aller vérifier en affichant le compte-rendu.

alwarebytes Premium Essai 4.5.2		- 0	Malwarebytes Premium Essat 45.2		- D		
Premium Trial Activer la	licence Acheter maintenant	8 A 8	M Premium Trial	Activer is licence Activette materie	• • •		
🗘 Analyseur		Ľ	O Analyseur				
Analyse des menaces – résultats	Durée d'analyse 1 35 m 41 s	e Éléments analysés 415774	Analyseur Parification d'analyse	Comptes-relidue			
Nom         Type         Type d'           Makwar. box 23         Programme malveillant         Fichier	bjet Emplacement C:\USERS\AIVM37\APPDATUT	TIL\RENFIC\RENFIC.EXE	Partages l'amour des appareils sécurisés	Analyse des menaces – résumé 16/02/2022 16/23			
1			Partager Halvoretytes Premium c'est amer. Otrainer 40% de réduction pour 1 apparaits à partager avec roct proches.	Corde d'analyse Démonte analysés	35 m 41 41577		
		1		C Planaces definition.			
				* Délections generées	3		
		1		Scheffens men an average			

Mahanetytes Parnium Total	Active to the	Max Annual State	arrest.	-	0 0	× O	
Comple rends d'analyse					×		
Hésamé Avancé							
Historie de Cardiges 1 Alimento difectór 1 Alimento nis en gueranteire	Denv Metal 2022 (28-47 Nam-Heat Termini						
Cléments détectés Insure 1 Programme potentiale	nen initiation (S. Madder	tion president the	invities if				
Size A Spin	Employment		Atter				
Halinans Sandhoo 21 Pediar	CILIEBEANACTAND 1		Engineertaine				
Equite *		_		[	Permer	5	