



MAJ le 17/10/2017

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.

Sommaire

Présentation

- 1 Installation de MBAM
 - 1.1 Installation
 - 1.2 La nouvelle édition de MBAM
- 2 Paramétrage de MBAM
 - 2.1 Paramétrage des applications
 - 2.2 Paramétrage de la détection et de la protection
- 3 Détection et éradication des malwares
 - 3.1 Mise à jour à faire selon les indications du logiciel
 - 3.2 Détection
 - 3.3 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



MBAM sur leur site allez dans le bas de la page et prenez la version gratuite

<https://www.malwarebytes.com/adwcleaner/jump/?ref=adw>

<http://www.commentcamarche.net/download/telecharger-34055379-malwarebytes-anti-malware>

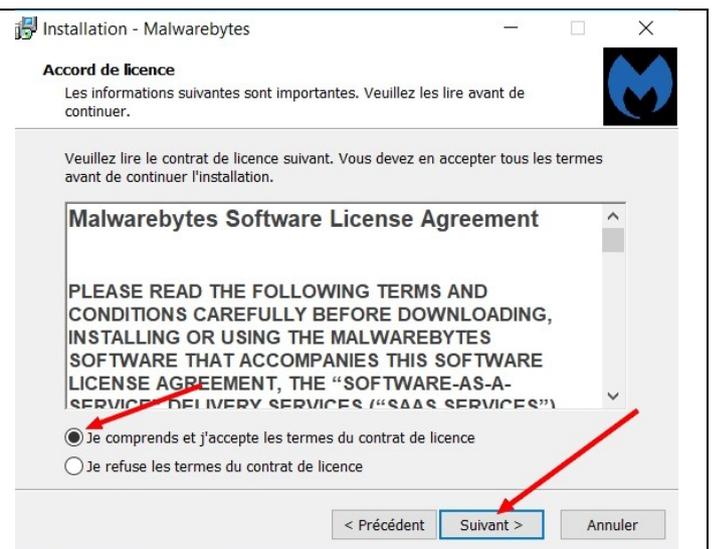
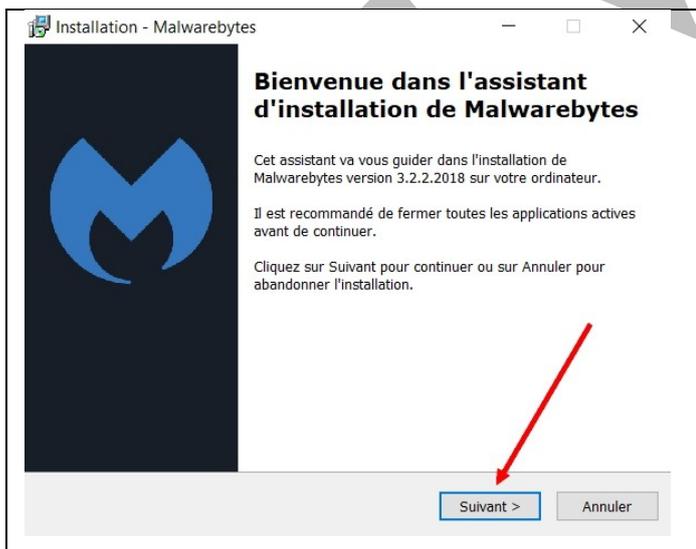
<http://www.clubic.com/telecharger-fiche215092-malwarebytes-anti-malware.html>

http://www.pcastuces.com/logitheque/malwarebytes_anti-malware.htm

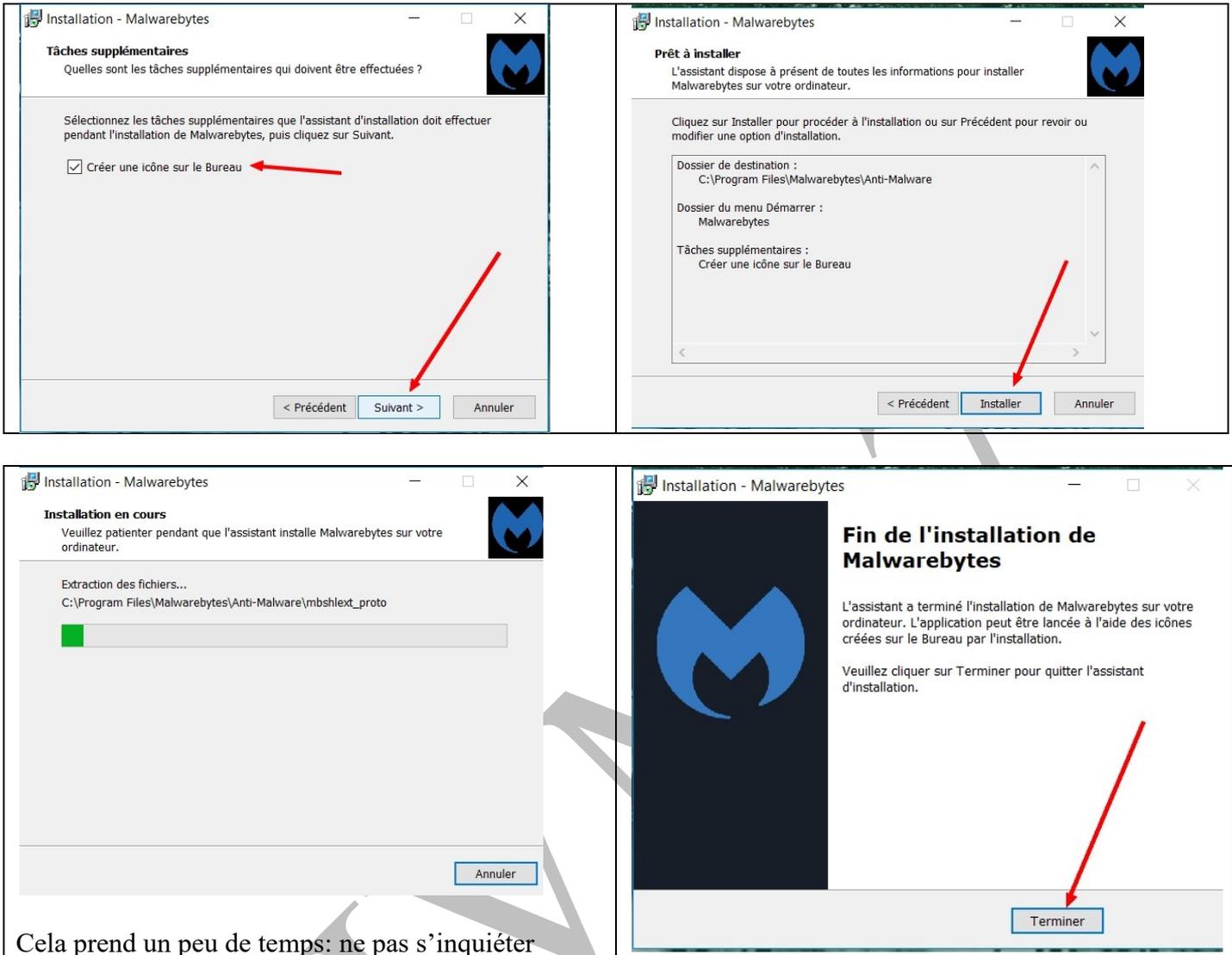
Malware bytes' Anti-Malware (32b et 64b) Anti malware puissant

Inutile de supprimer la version précédente, sauf en cas de changement de version principale. Pas de problème à l'installation. A prendre de préférence sur PCastuces.

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



Fiche Pratique

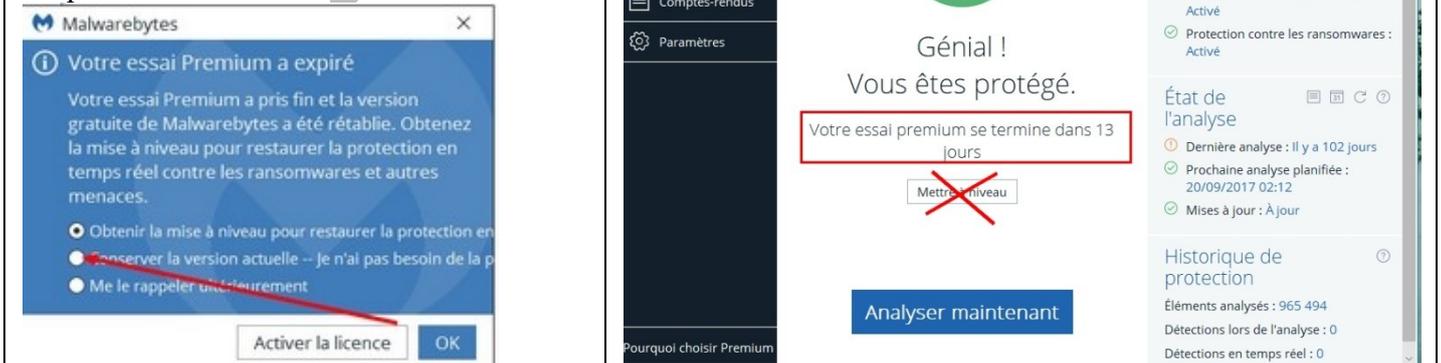


Cela prend un peu de temps: ne pas s'inquiéter

1.2 La nouvelle édition de MBAM

L'essai premium assure la protection en temps réel, ce que fait aussi votre anti-virus. Au bout des 13 jours, à condition de ne pas cliquer sur **Mettre à niveau**, MBAM passe en mode gratuit

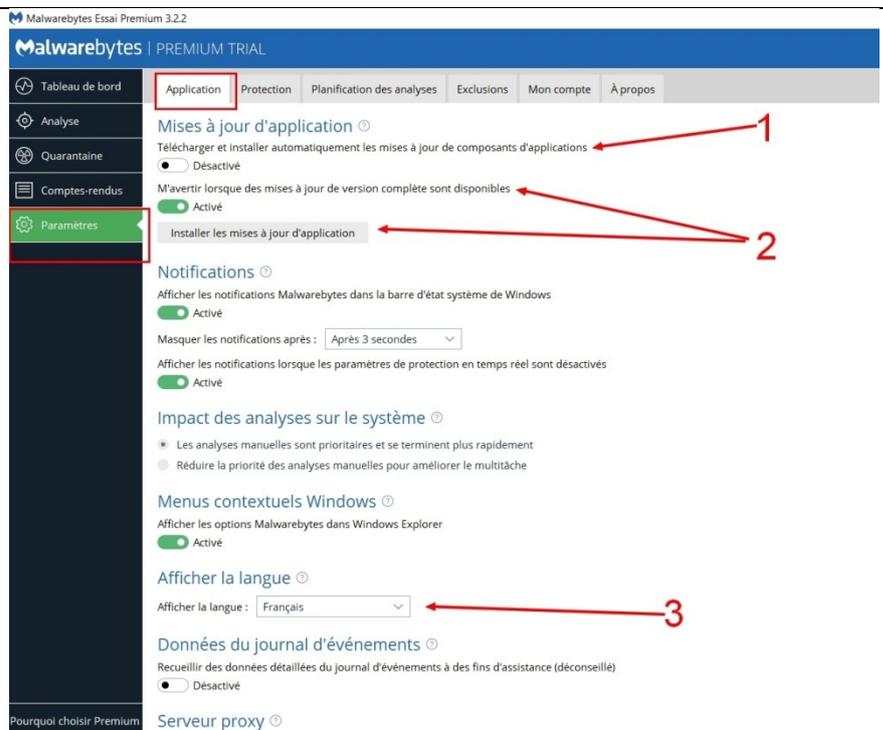
Cliquer sur **Conserver la version actuelle**



2 Paramétrage de MBAM

2.1 Paramétrage des applications

Onglet **Paramètres**, sous-onglet **Application**, choisir ou non la mise à jour automatique (1 et 2)
C'est là que se fait le choix de la langue (3)



2.2 Paramétrage de la détection et de la protection

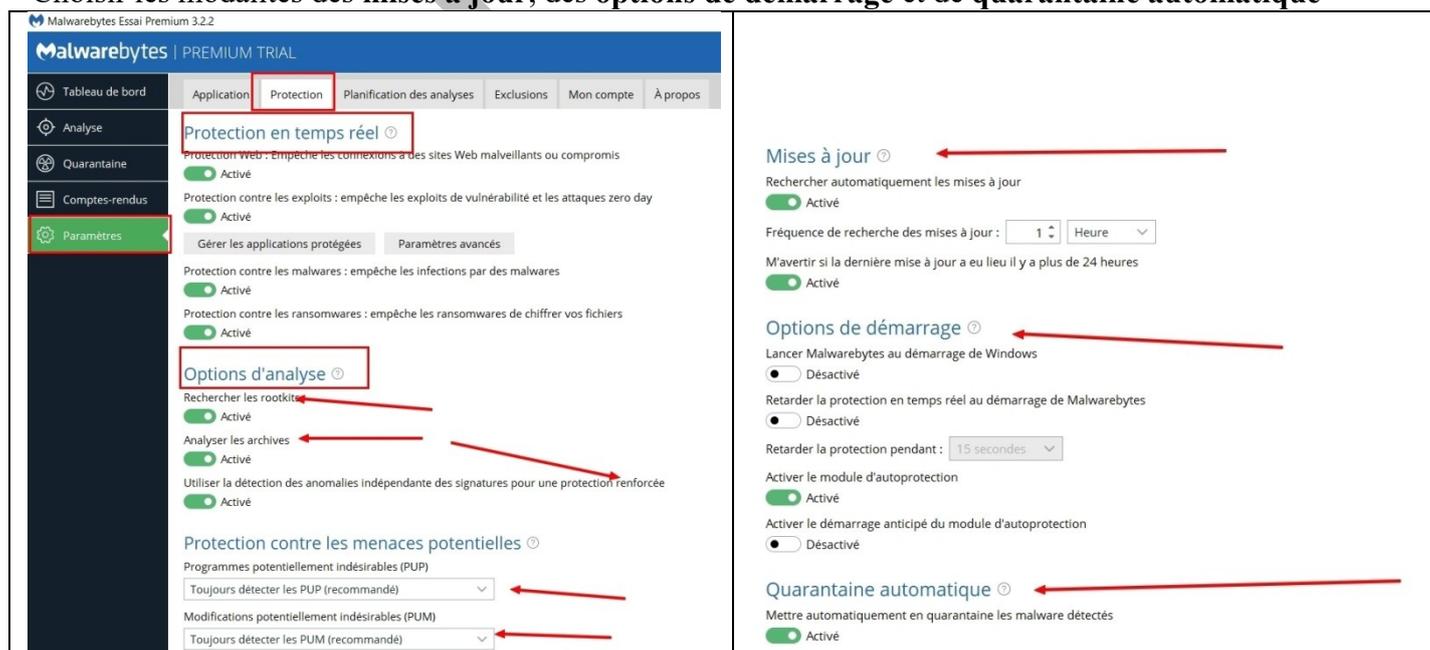
Onglet **Paramètres**, sous-onglet **Protection**:

La protection en temps réel disparaît avec la version gratuite (free).

Activer les **3 options d'analyse**.

Les détections **PUP** (Programmes potentiellement indésirables) et **PUM** (Modifications potentiellement indésirables) doivent être configurées sur **Toujours détecter les PUP** et **Toujours détecter les PUM**

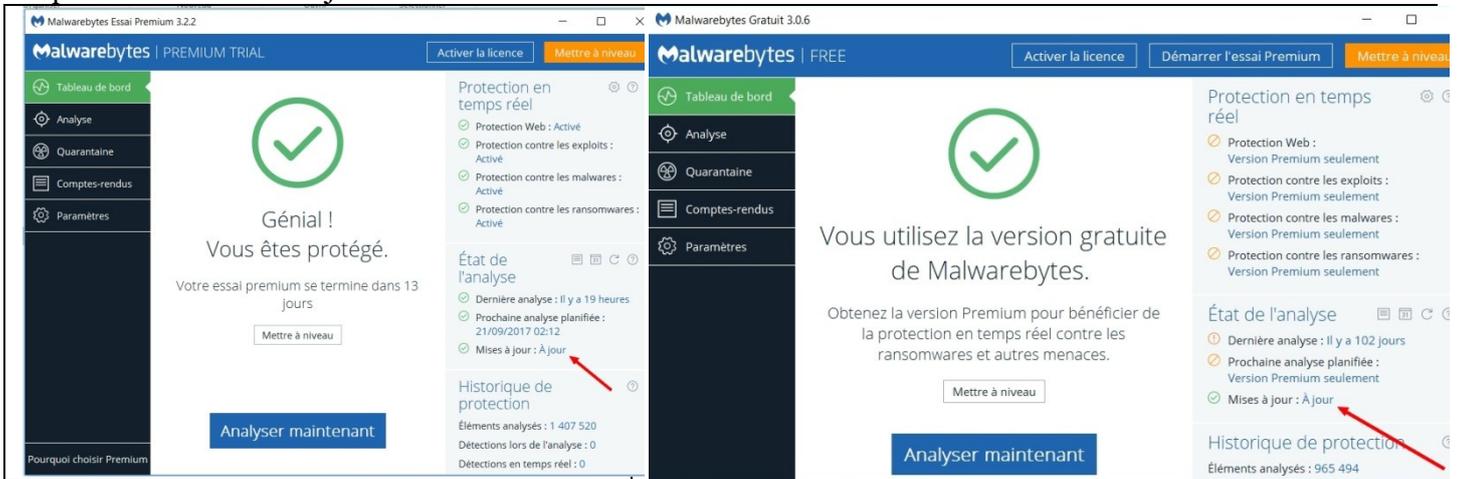
Choisir les modalités des **mises à jour**, des **options de démarrage** et de **quarantaine automatique**



3 Détection et éradication des malwares

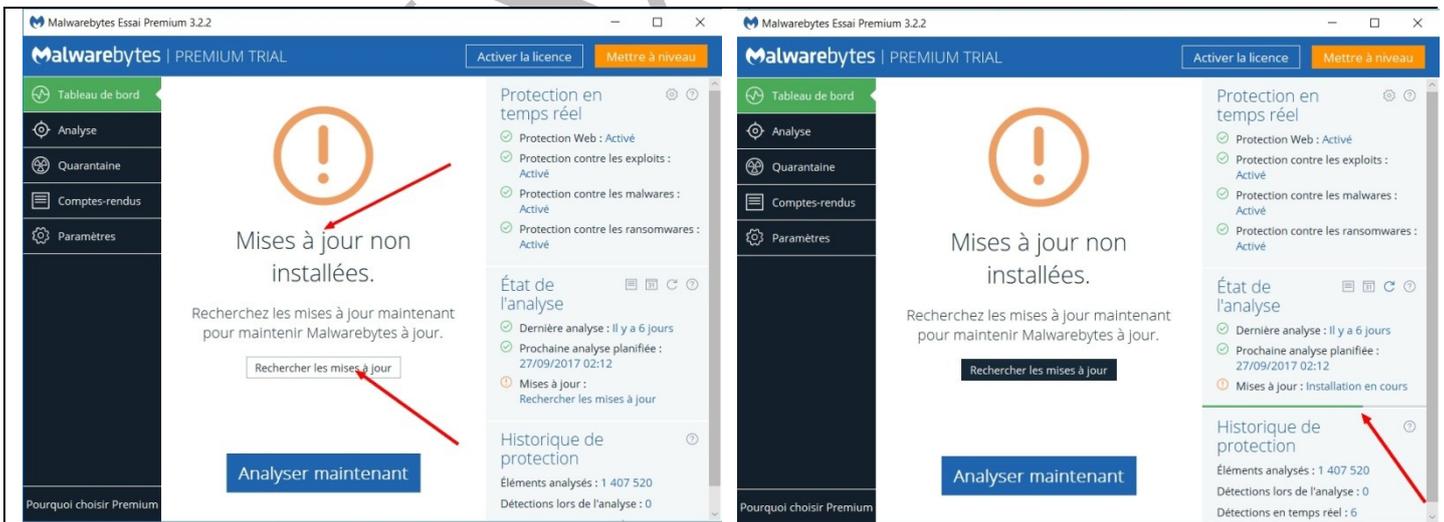
3.1 Mise à jour à faire selon les indications du logiciel

Selon la version, le texte d'introduction change mais le bouton de mise à jour est à la même place : il indique l'état des mises à jour.



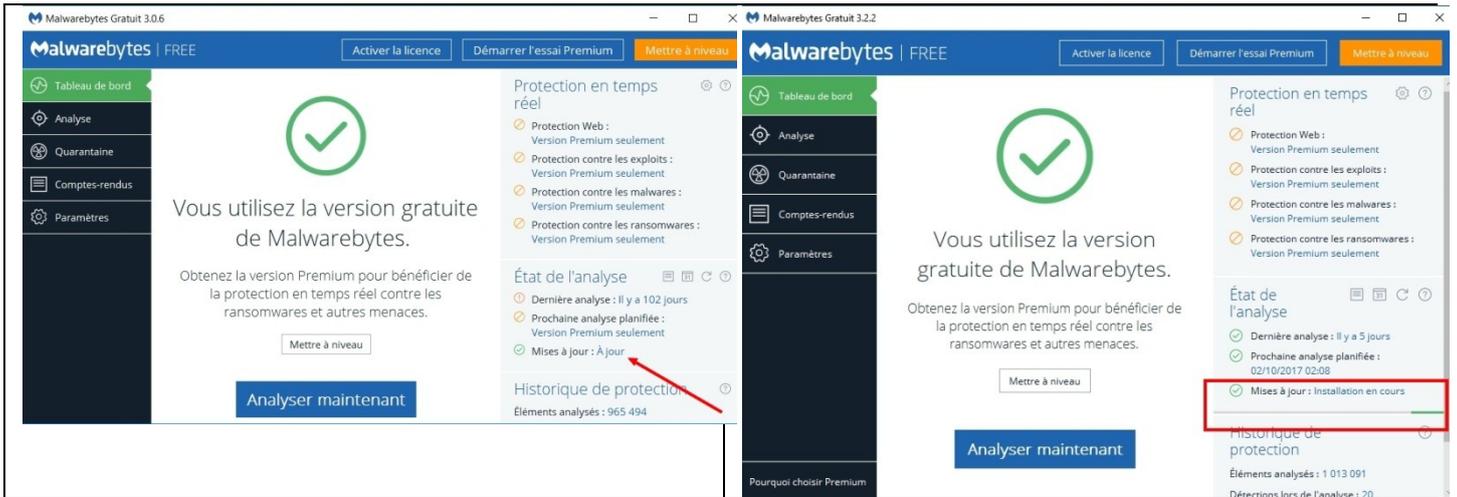
Désormais, MBAM dans la version premium indique les mises à jour à installer. Cliquer sur le bouton Rechercher les mises à jour.

On peut suivre la progression de l'installation des mises à jour



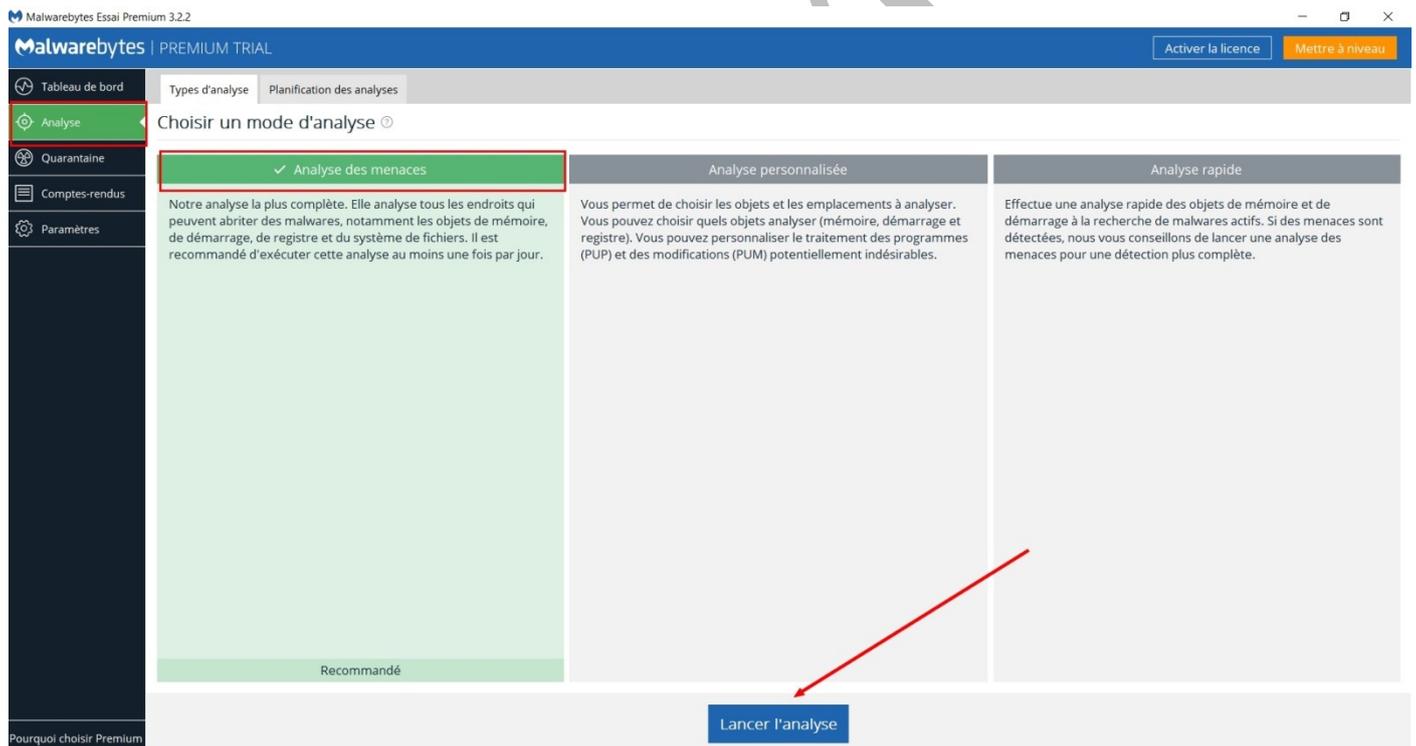
Dans la version gratuite, aller systématiquement chercher la mise à jour du logiciel (même si la mention À jour est là)

Fiche Pratique



3.2 Détection

Onglet **Analyse**: trois types d'analyse sont proposés
Choisir **Analyse des menaces** et cliquer sur **Lancer l'analyse**



Déroulement de l'examen : analyse des menaces

Fiche Pratique

The screenshot shows the Malwarebytes Premium 3.2.2 interface. The title bar indicates 'Malwarebytes | PREMIUM TRIAL'. The main window is titled 'Analyse des menaces'. A progress bar at the top shows the following steps: 'Rechercher les mises à jour' (checked), 'Préparation avant analyse' (checked), 'Rechercher les rootkits' (checked), 'Analyser la mémoire' (hourglass icon), 'Analyser les fichiers de démarrage' (hourglass icon), 'Analyser le registre' (hourglass icon), 'Analyser le système de fichiers' (hourglass icon), and 'Analyse heuristique' (hourglass icon). Below the progress bar, the status is: 'Analyse en cours : Recherche de rootkits', 'Éléments analysés : 87', 'Temps écoulé : 00:00:06', and 'Menaces identifiées : 0'. At the bottom, there is a button 'Afficher les menaces identifiées' and buttons 'Interrompre' and 'Annuler'.

Au cours de l'analyse, peuvent apparaître les menaces détectées

The screenshot shows the Malwarebytes Gratuit 3.2.2 interface. The title bar indicates 'Malwarebytes | FREE'. The main window is titled 'Analyse des menaces'. A progress bar at the top shows the following steps: 'Rechercher les mises à jour' (checked), 'Préparation avant analyse' (checked), 'Rechercher les rootkits' (checked), 'Analyser la mémoire' (checked), 'Analyser les fichiers de démarrage' (checked), 'Analyser le registre' (checked), 'Analyser le système de fichiers' (checked), and 'Analyse heuristique' (hourglass icon). Below the progress bar, the status is: 'Analyse en cours : C:\USERS\AIVM37\APPDATA\ROAMING\SPOTIFY\APPS\PEOPLE.SPA', 'Éléments analysés : 392 949', 'Temps écoulé : 00:11:30', and 'Menaces identifiées : 344'. At the bottom, there is a button 'Afficher les menaces identifiées' and buttons 'Interrompre' and 'Annuler'.

Si au cours de l'analyse, aucune menace n'a été détectée, on ferme le logiciel

Fiche Pratique

The screenshot shows the Malwarebytes Premium 3.2.2 interface. The top bar includes the logo, 'PREMIUM TRIAL', and buttons for 'Activer la licence' and 'Mettre à niveau'. The left sidebar contains navigation options: 'Tableau de bord', 'Analyse', 'Quarantaine', 'Comptes-rendus', and 'Paramètres'. The main content area displays a green checkmark and the message 'L'analyse et la mise en quarantaine sont terminées.' Below this is a table with the following data:

Heure de l'analyse :	8 m : 19 s
Éléments analysés :	442 026
Menaces détectées :	0
Menaces mises en quarantaine :	0

A red box highlights the '0' values in the 'Menaces détectées' and 'Menaces mises en quarantaine' rows. A red arrow points to a 'Fermer X' button in the top right corner. On the right side, there is a promotional message: 'Ne risquez plus les infections. Passez à Malwarebytes Premium dès maintenant pour un blocage proactif des menaces avant qu'elles puissent endommager votre ordinateur.' with a 'Mettre à niveau' button. At the bottom, there are buttons for 'Exporter le résumé' and 'Afficher le compte-rendu'.

3.3 Eradication

A la fin de l'examen: si des éléments ont été détectés, MBAM les a mises en quarantaine. On peut alors fermer le logiciel ou aller voir le contenu de la quarantaine.

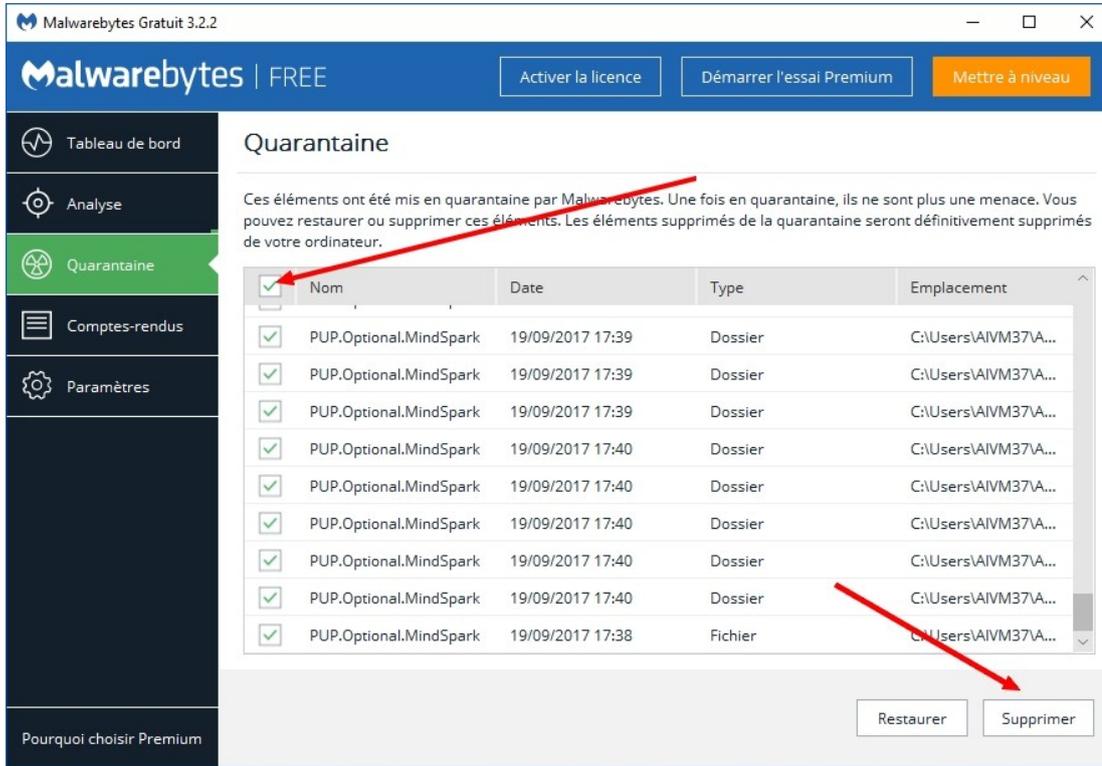
The screenshot shows the Malwarebytes Gratuit 3.2.2 interface. The top bar includes the logo, 'FREE', and buttons for 'Activer la licence', 'Démarrer l'essai Premium', and 'Mettre à niveau'. The left sidebar contains navigation options: 'Tableau de bord', 'Analyse', 'Quarantaine', 'Comptes-rendus', and 'Paramètres'. The main content area displays a green checkmark and the message 'L'analyse et la mise en quarantaine sont terminées.' Below this is a table with the following data:

Heure de l'analyse :	24 m : 50 s
Éléments analysés :	505 375
Menaces détectées :	18
Menaces mises en quarantaine :	18

A red box highlights the message 'L'analyse et la mise en quarantaine sont terminées.' A red arrow points to a 'Fermer X' button in the top right corner. On the right side, there is a promotional message: 'Ne risquez plus les infections. Passez à Malwarebytes Premium dès maintenant pour un blocage proactif des menaces avant qu'elles puissent endommager votre ordinateur.' with a 'Mettre à niveau' button. At the bottom, there are buttons for 'Exporter le résumé' and 'Afficher le compte-rendu'.

Fiche Pratique

Onglet **Quarantaine**: Supprimer ou non les éléments détectés après les avoir sélectionnés



Onglet: **Comptes-rendus**, sélectionner le compte rendu de l'analyse pour plus de précisions

