FC04

INFO-AIVM37

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.

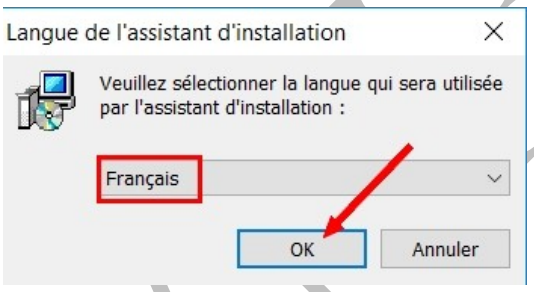
Sommaire

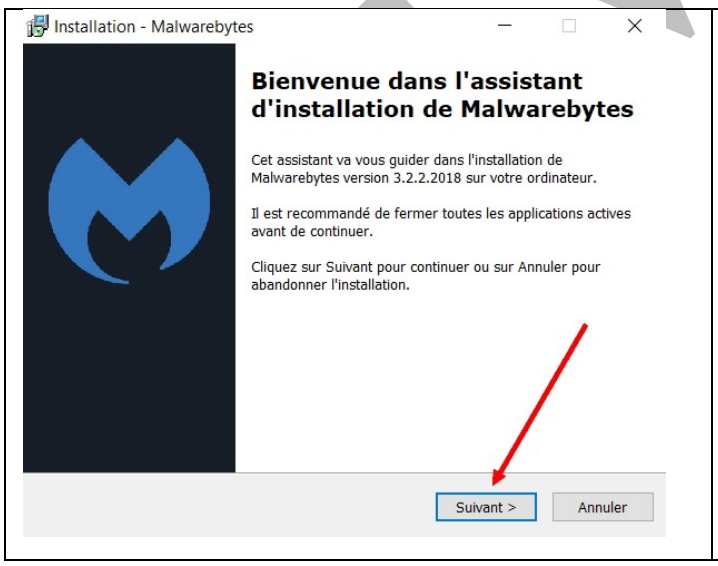
1 Installation de MBAM

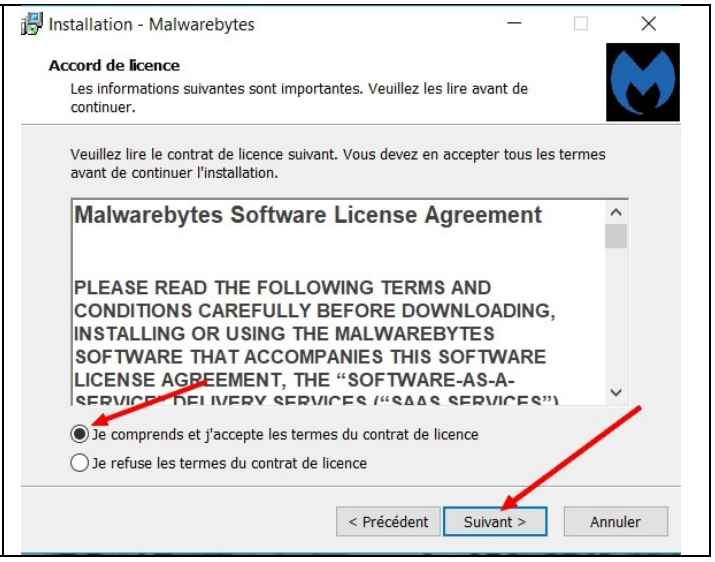
1.1 Installation

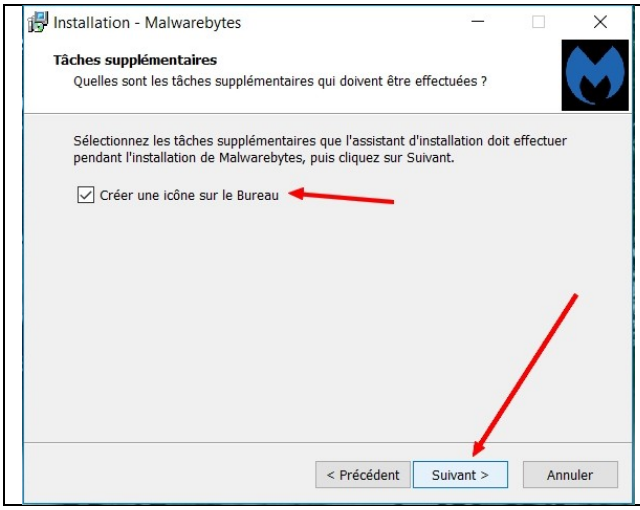
Commencer l'installation de MBAM avec le **setup** de Malwarebytes anti malware qu'on va chercher sur le site d'AIVM

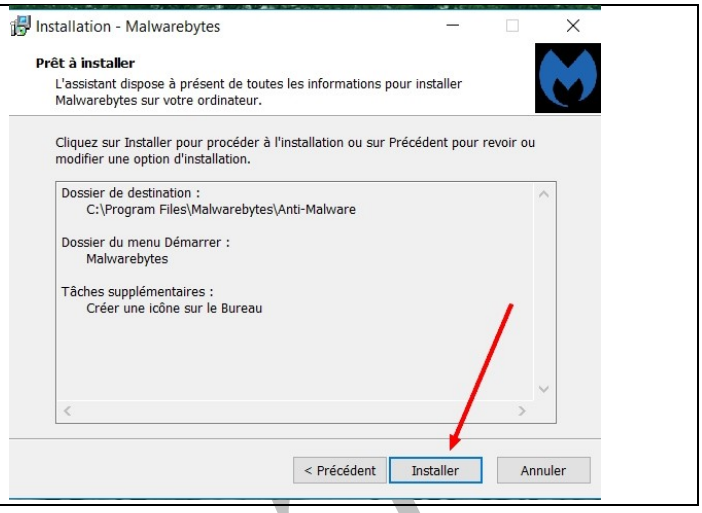
On accepte toutes les étapes de l'installation (on ne peut pas éviter l'installation de la version premium à l'essai)

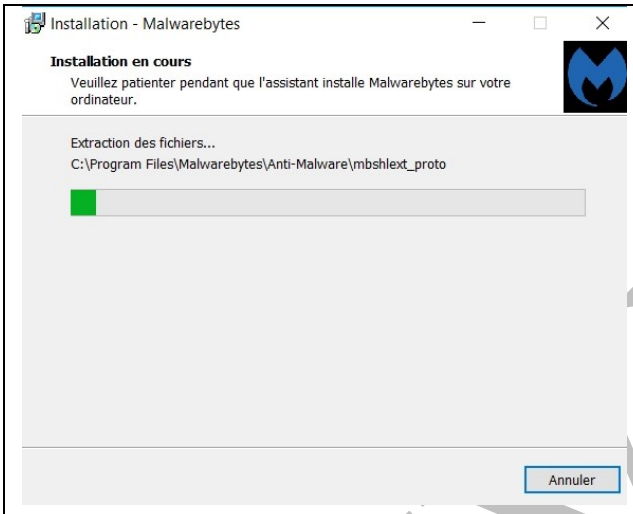




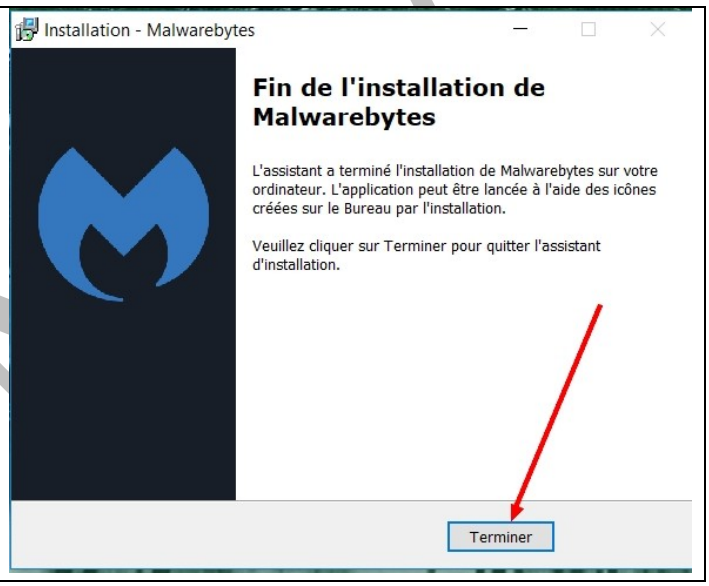








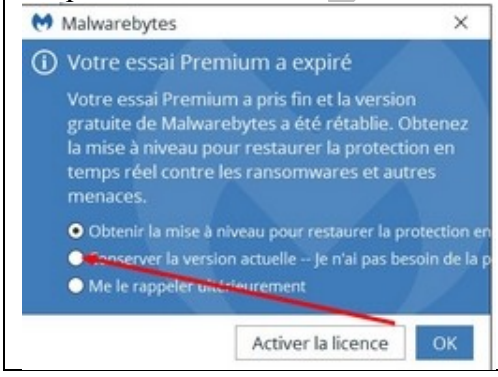
Cela prend un peu de temps: ne pas s'inquiéter

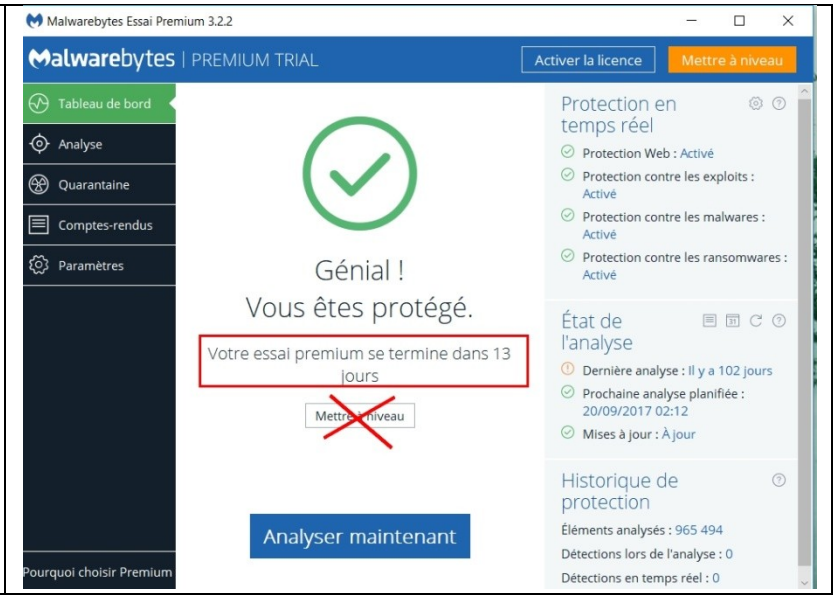


1.2 La nouvelle édition de MBAM

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**

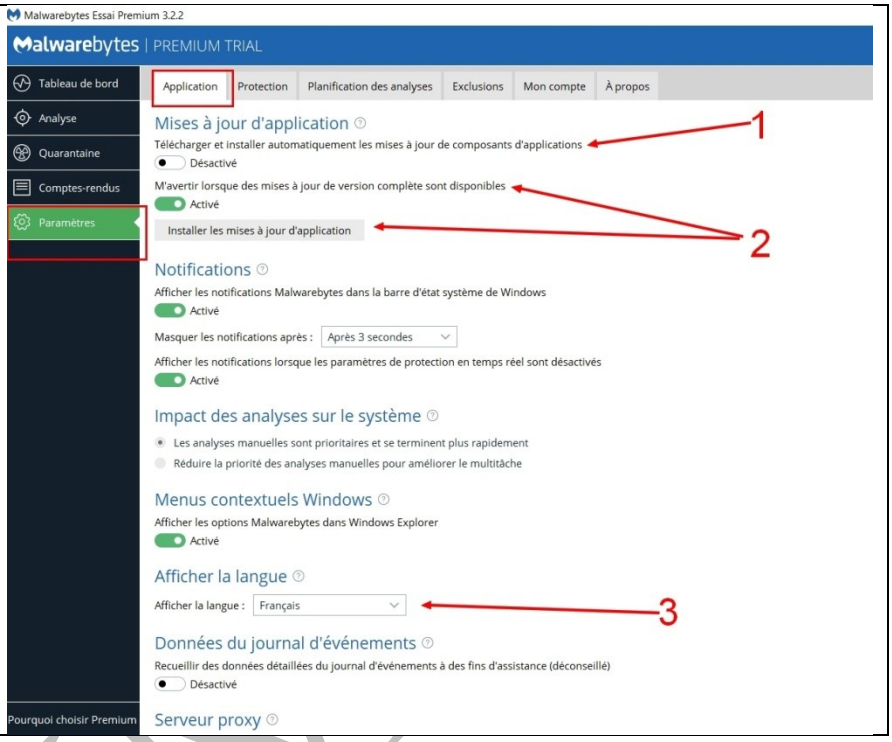




2 Paramétrage de MBAM

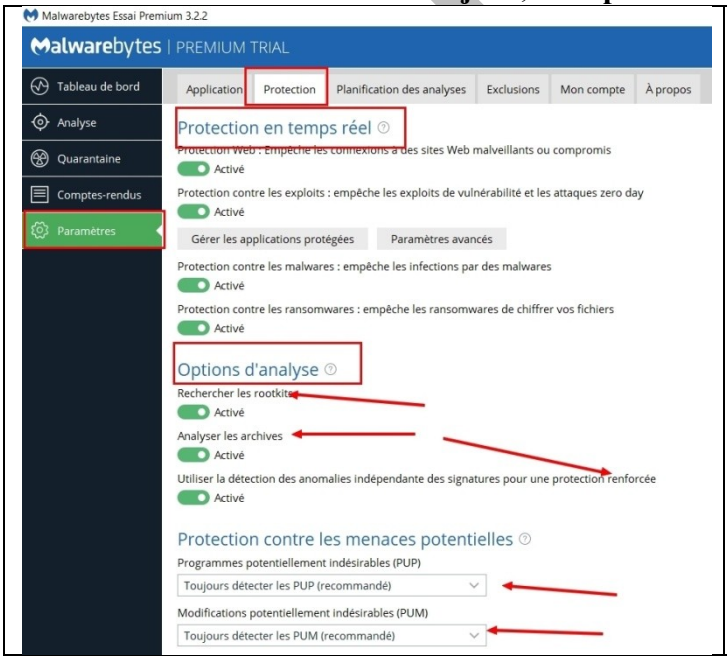
2.1 Paramétrage des applications

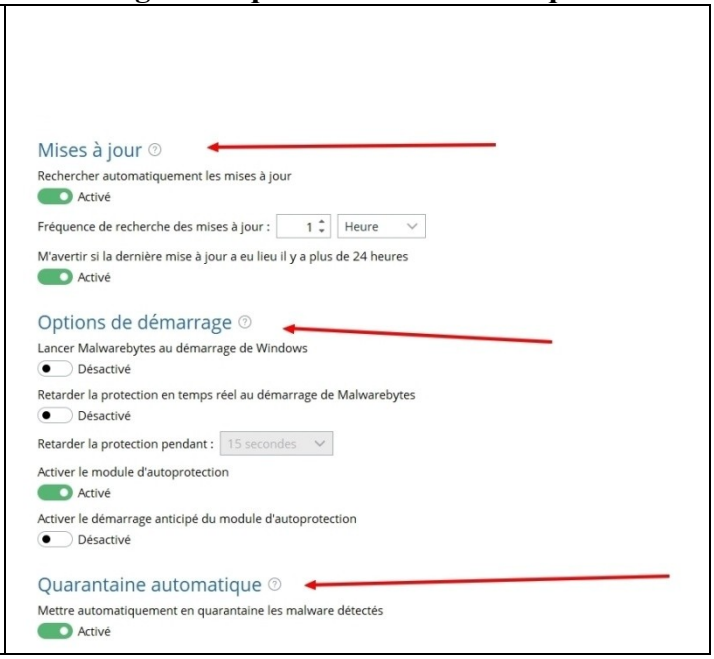
Onglet **Paramètres**, sous-onglet **Application**, choisir ou non la mise à jour automatique (1 et 2)
C'est là que se fait le choix de la langue (3)



2.2 Paramétrage de la détection et de la protection

Onglet **Paramètres**, sous-onglet **Protection**:
La protection en temps réel disparait 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**

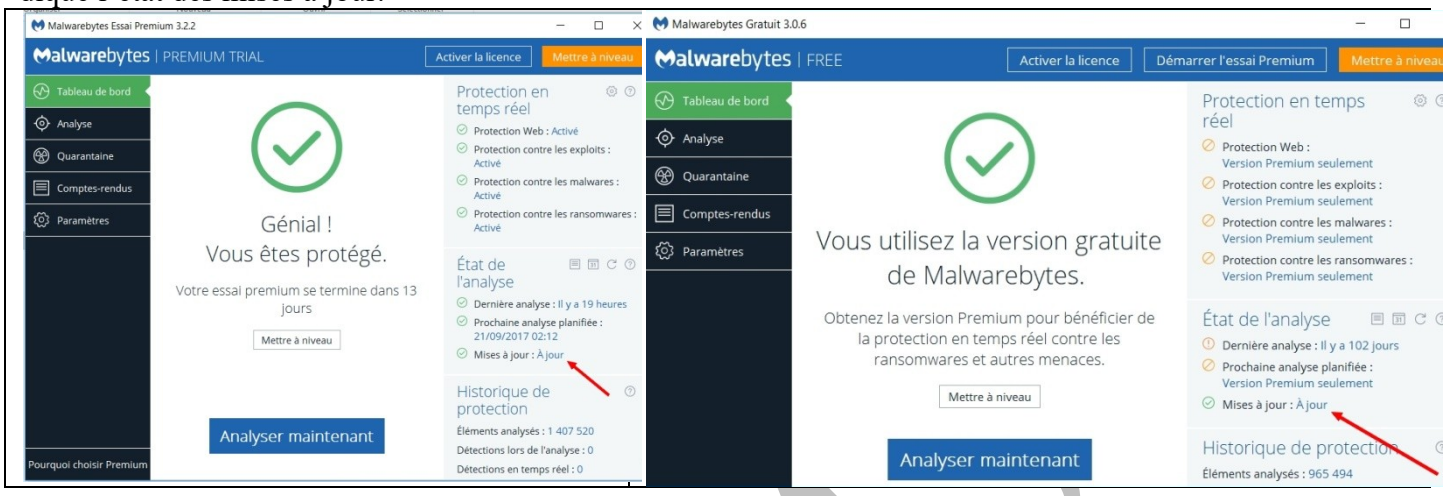




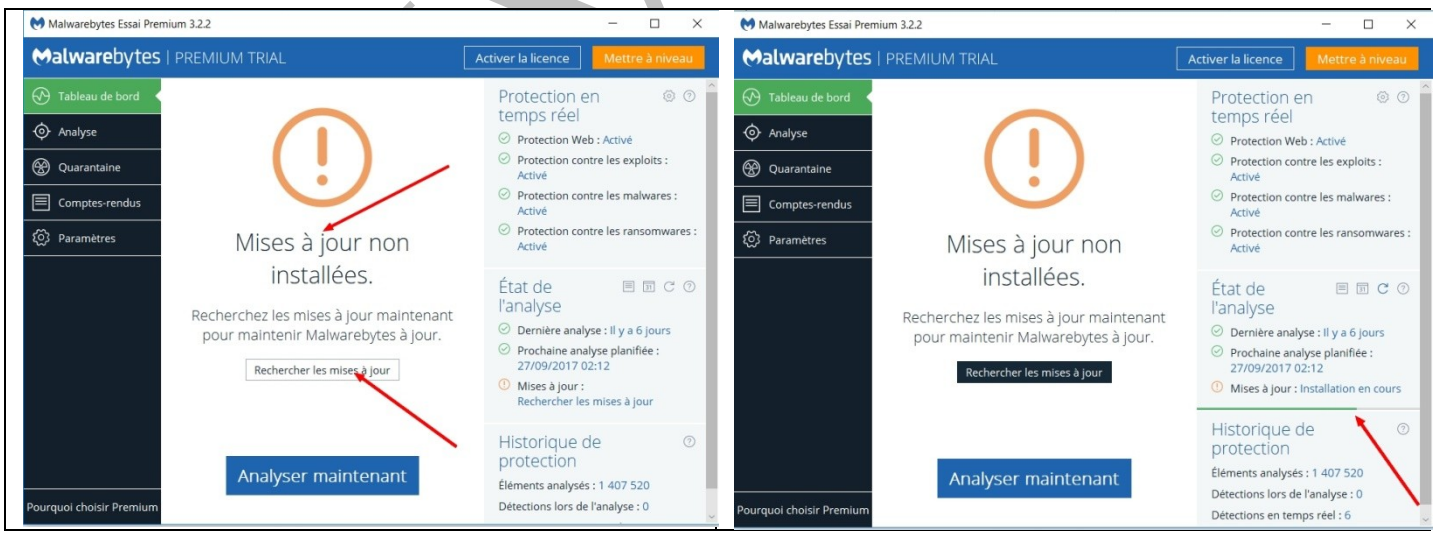
3 Détection et éradication des malwares

3.1 Mise à jour à faire selon les indications du logiciel

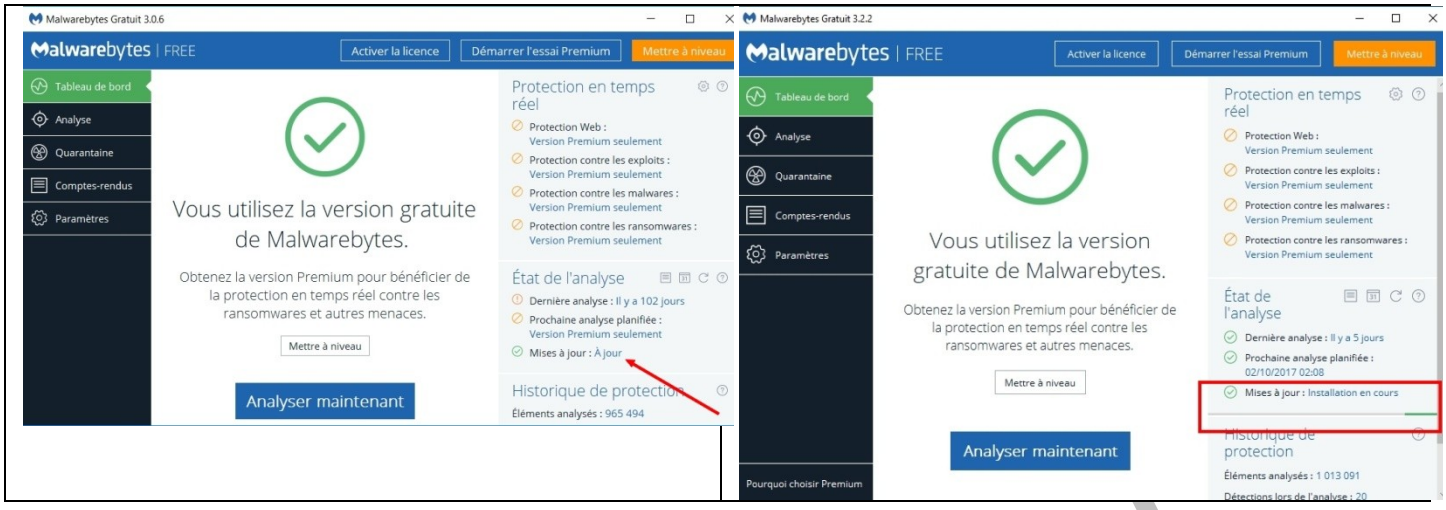
Selon la version, le texte d'introduction change mais le bouton de mise à jour est à la même place : il indique l'état des mises à jour.



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

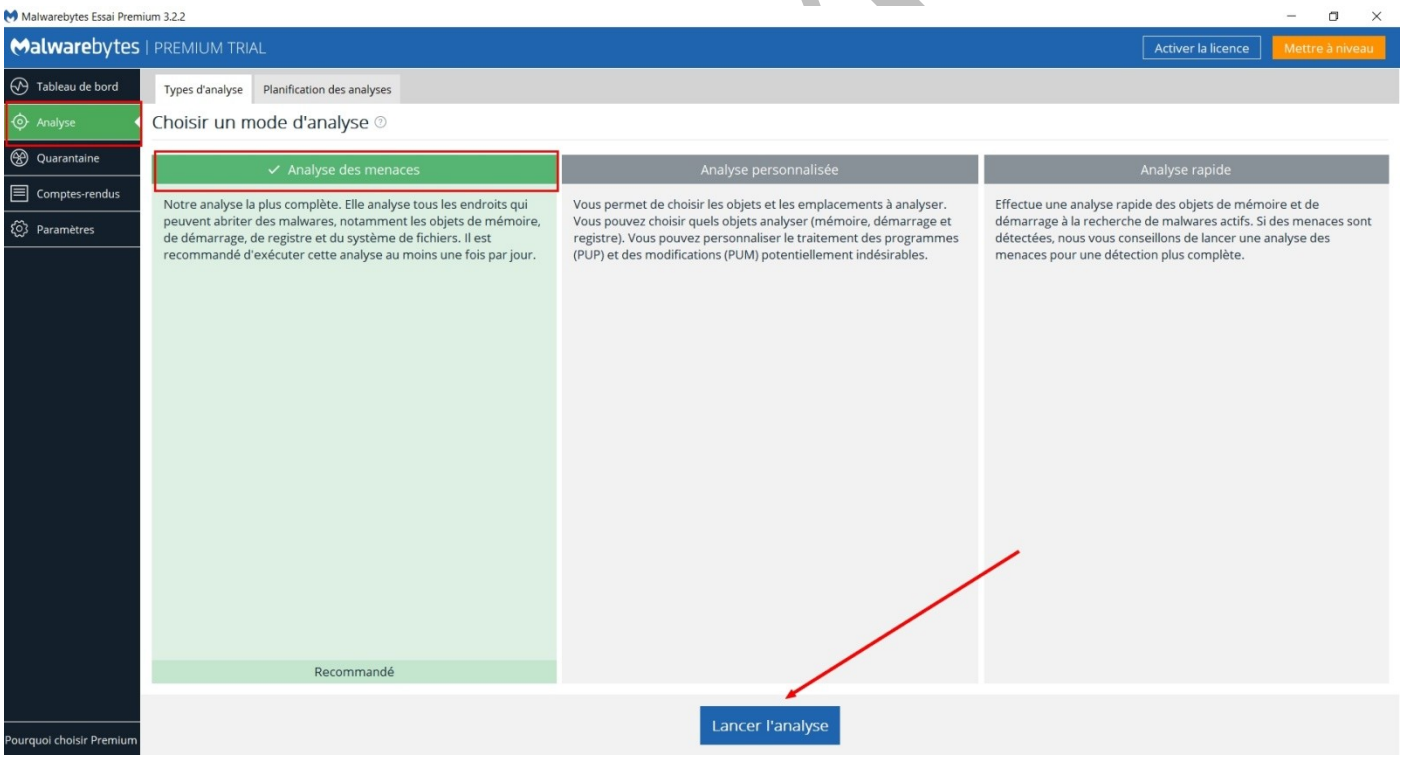


Dans la version gratuite, aller systématiquement chercher la mise à jour du logiciel (même si la mention A jour est là)

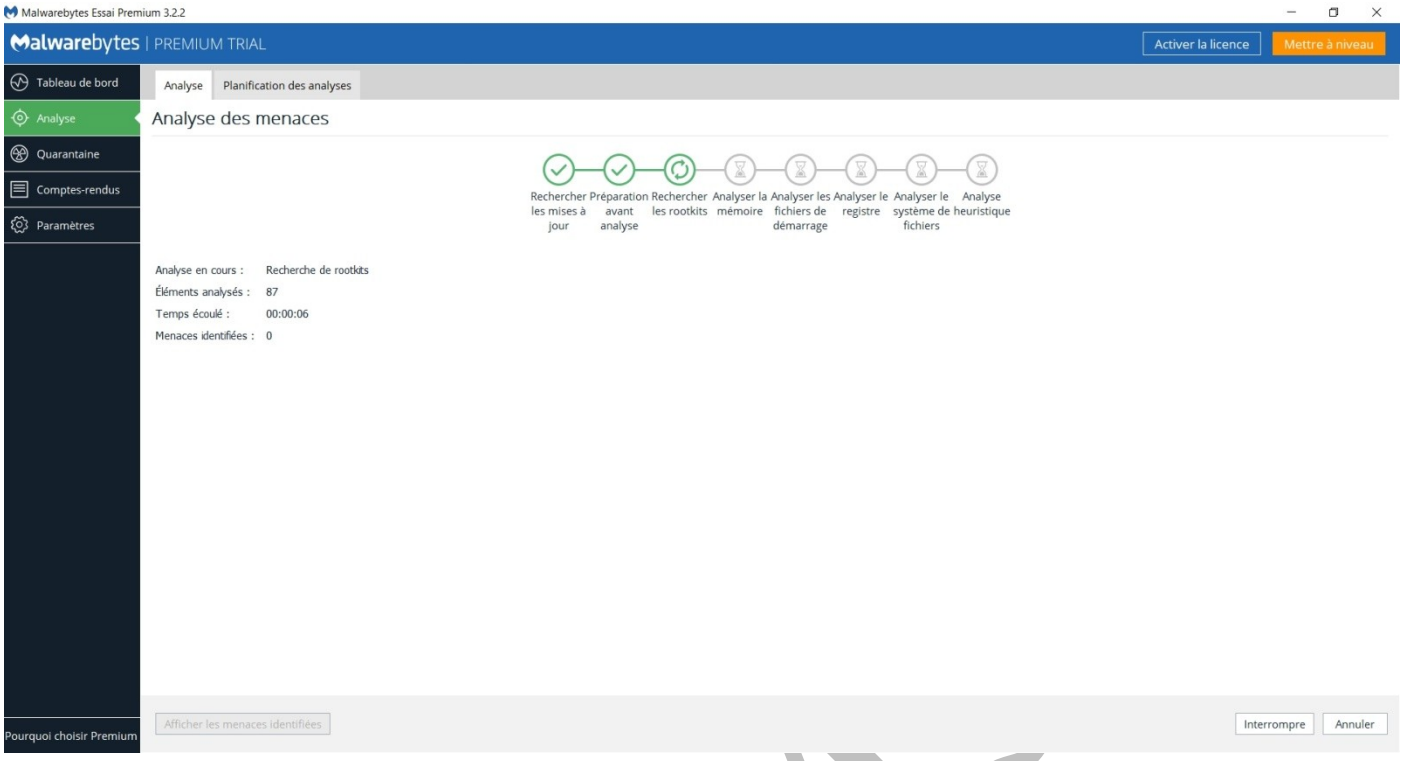


3.2 Détection

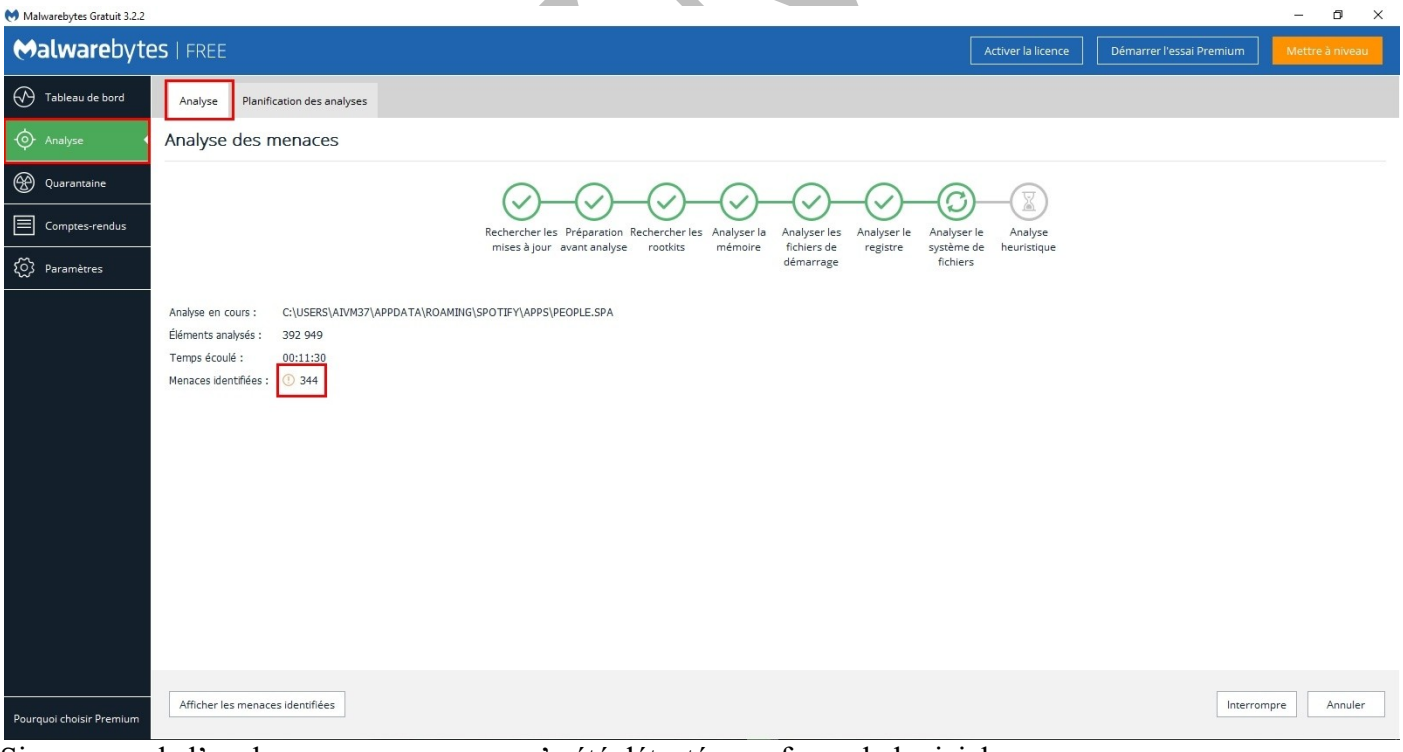
Onglet **Analyse**: trois types d'analyse sont proposés
Choisir **Analyse des menaces** et cliquer sur **Lancer l'analyse**



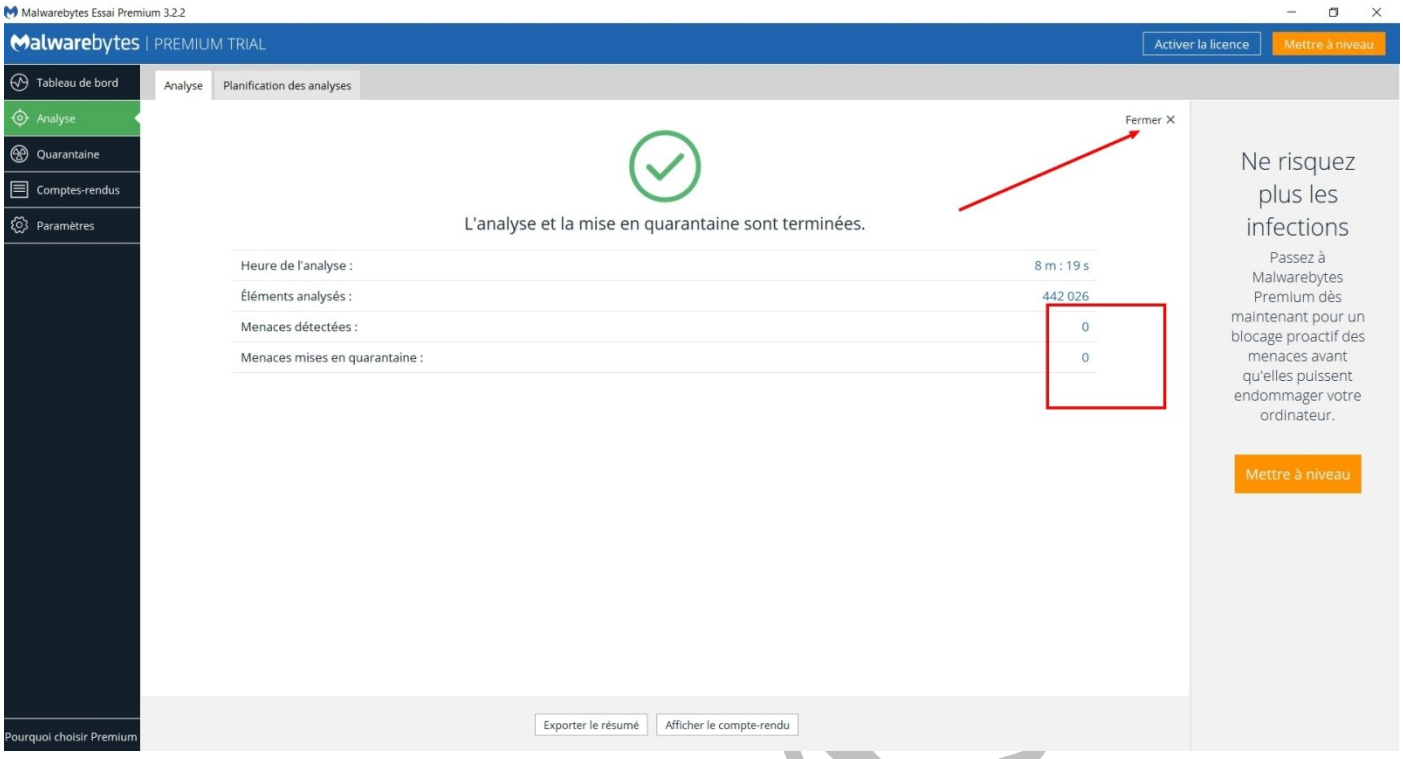
Déroulement de l'examen : analyse des menaces



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

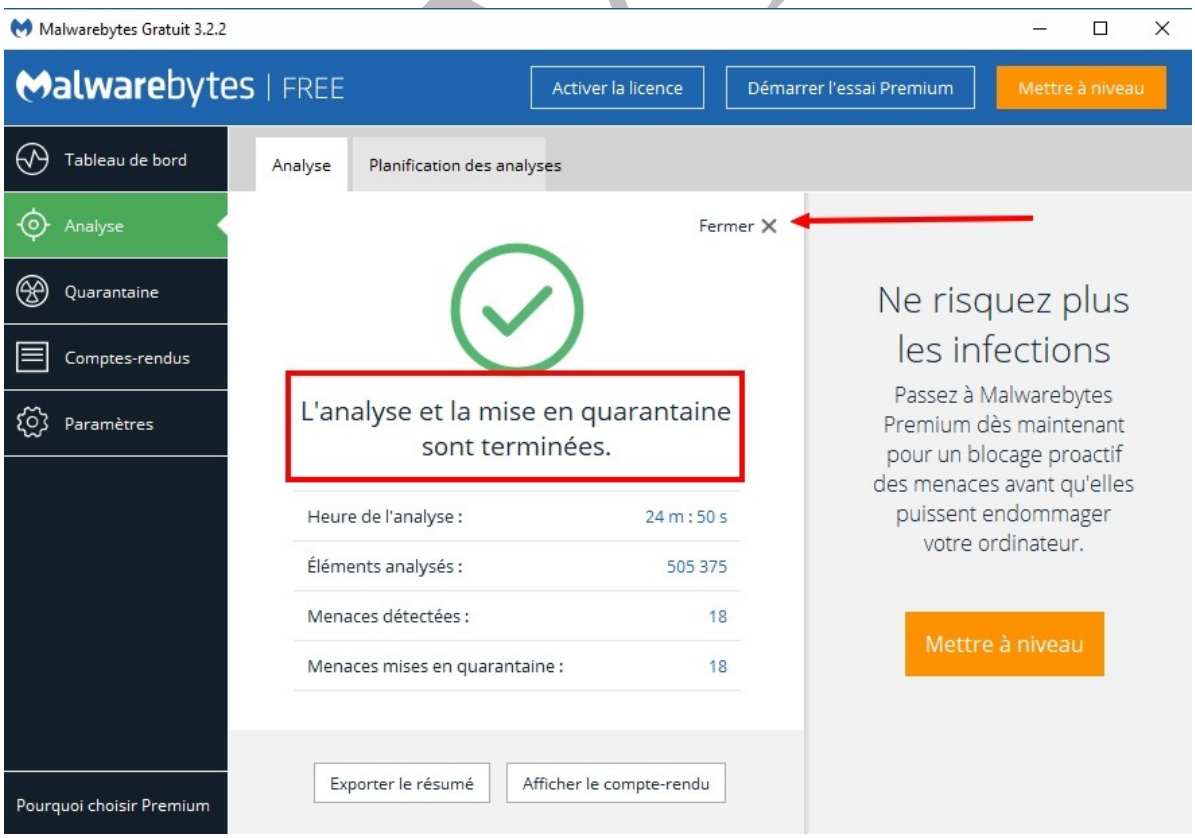


Si au cours de l'analyse, aucune menace n'a été détectée, on ferme le logiciel

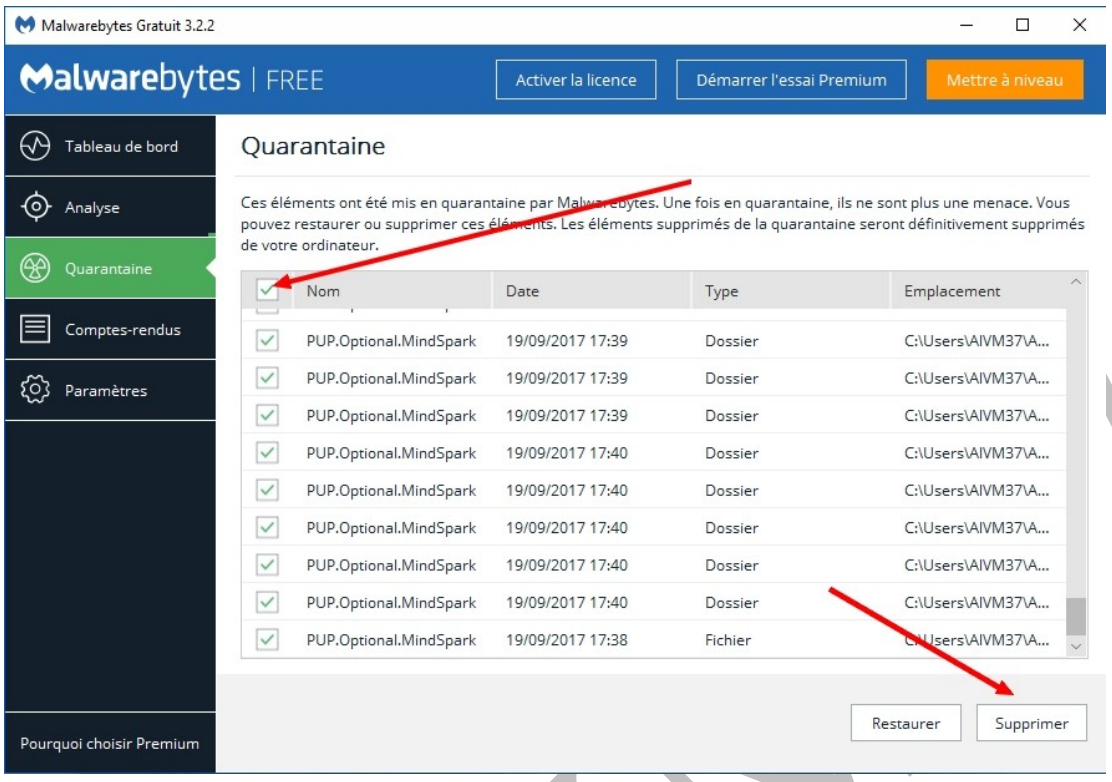


3.3 Eradication

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.



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