Module : Naviguer en toute sécurité

Projet 1 - Un peu plus de sécurité, on n'en a jamais assez !

1/Introduction à la sécurité sur Internet
Article 1 : Swisscom – 10 conseils pour plus de sécurité sur internet
Article 2 : Economie.gouv - Dix règles pour vous prémunir contre le piratage de vos données personnelles
Article 3 : tf1info – Cybermenaces : 10 conseils à appliquer pour naviguer en toute sécurité

2/Créer des mots de passe forts
Lastpass ajouté à l'extension

3/Fonctionnalité de sécurité de votre navigateur

1-

- www.morvel.com : site non sécurisé
- www.dccomics.com : site sécurisé
- www.ironman.com : site sécurisé
- www.fessebook.com : accès refusé
- www.instagam.com : site non sécurisé

2- Chrome et firefox mis à jour

4/Éviter le spam et le phishing
Exercice de détection de spam et phishing

5/Comment éviter les logiciels malveillants

- Site n°1
  - Indicateur de sécurité
    - HTTPS
  - Analyse Google
    - Aucun contenu suspect
- Site n°2
  - Indicateur de sécurité
    - Not secure
  - Analyse Google
    - Aucun contenu suspect
- Site n°3
  - Indicateur de sécurité
    - Not secure
  - Analyse Google
    - Vérifier un URL en particulier
- Site n°4 (site non sécurisé)

6/Achats en ligne sécurisés
Création des libellés correspondant à mes besoins afin d'organiser mes mails

7/Comprendre le suivi du navigateur

8/Principes de base de la confidentialité des médias sociaux

1-facebook parmétré

9/Que faire si votre ordinateur est infecté par un virus

1- exercice(s) pour vérifier la sécurité en fonction de l'appareil utilisé

- Sécuriser votre terminal informatique : mise à jour, verrouillage et sauvegarde :

*Mettre à jour régulièrement les appareils
*Utiliser un anti-virus et un pare-feu (bloque les connexions non désirées depuis l'appareil)
*Réaliser des analyses (ou scans) des appareils pour identifier la présence de programmes malveillants.
*Sécuriser l'accès au wifi, éviter de se connecter sur un wifi non sécurisé (sinon, utiliser du réseau privé virtuel VPN)
* Verrouillez l'accès de vos appareils et à votre profil utilisateur : par un code ou mot de passe, afin de protéger vos documents.
* Activer un écran de verrouillage automatique
* Utiliser l'authentification à deux facteurs
* Sauvegardez régulièrement vos fichiers en utilisant un clef USB, un disque dur externe ou du cloud
*Séparer vos usages personnels et professionnels

- Sécuriser les mots de passe

* Varier les mots de passe et réserver chacun à un usage unique
* Changer les mots de passe au moindre doute d'utilisation frauduleuse
*Utiliser, si nécessaire, des logiciels qui aident à la gestion des mots de passe (ex : LastPass)

- Sécurisez vos achats en ligne

* Faire les achats sur un site web disposant d'une sécurité « https »
*****Ne partager jamais des informations personnelles (mot de passe, informations bancaires)
*N'installer des applications que depuis les sites ou magasins officiels des éditeurs

- Utiliser la messagerie de façon sécurisée

* Lire attentivement les informations contenues dans les courriels : déceler les spams et les phishing
* S'interroger sur la pertinence et la crédibilité du contenu, sur l'identité de l'expéditeur et son langage, etc.
* Se méfier des extensions de pièces jointes qui paraissent douteuses
* Voir figurer des logos qui paraissent officiels ne veut pas nécessairement dire qu'il s'agit d'un courriel officiel.

- Se méfier des faux sites et non sécurisés

*Savoir reconnaitre les faux sites et non sécurisés
* Vérifier l'identité du site et ses mentions légales avant de réaliser le moindre achat ou téléchargement.
* Utiliser un bloqueur de fenêtres contextuelles avec le navigateur (ex : Adblock) La plupart sont créées par des publicitaires, mais elles peuvent également contenir du code malveillant ou dangereux.
*Etre attentif aux notifications du navigateur

- Maîtriser les réseaux sociaux

*être prudents sur ce qu'on communique

*Ne contribuer pas à notre propre piratage
*Définir les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour nous nuire

Tester votre niveau de sécurité informatique et internet sur 4 points essentiels de votre système d'information : Test en ligne de cybersécurité pour les TPE et PME en 4 étapes et moins de 10 minutes (par le Service du Haut Fonctionnaire de Défense et de Sécurité du Ministère de l'économie et des finances en France)

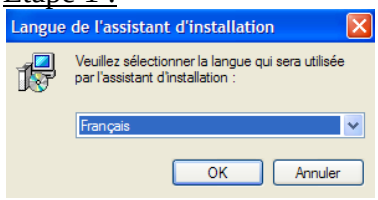
2- Un exercice pour installer et utiliser un antivirus+antimalware en fonction de l'appareil utilisé

Les mots « antivirus » et « anti-malware » ont presque le même sens. Tous deux se réfèrent à un logiciel conçu pour détecter les logiciels malveillants, assurer la protection contre ces logiciels et les supprimer.
Mais ils ne sont pas les mêmes. Ils se complètent pour agir comme le plus haut niveau de défense contre les logiciels malveillants, en complément d'une bonne hygiène de comportement en ligne. L'antimalware détecte les formes plus avancées de malwares, tandis que le logiciel antivirus se défend contre les menaces traditionnelles plus établies.

Nous allons utiliser la version gratuite de Malwarebytes Anti-Malware.
Cette version permet de scanner votre PC et de supprimer les logiciels malveillants. La différence avec la version PRO est que vous devrez mettre à jour le logiciel et lancer les analyses manuellement.

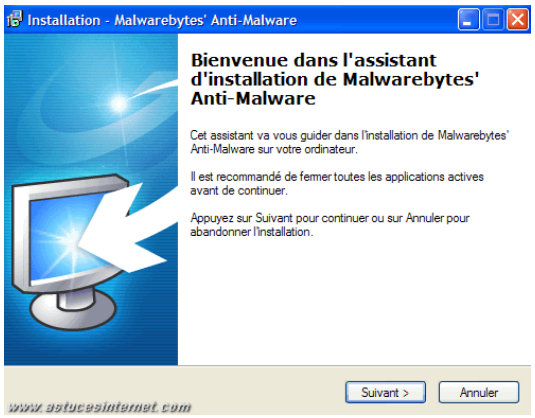
- Télécharger la dernière version disponible de Malwarebytes Anti-Malware. Une fois téléchargé, exécutez le fichier pour démarrer l'installation du logiciel.

Étape 1 :



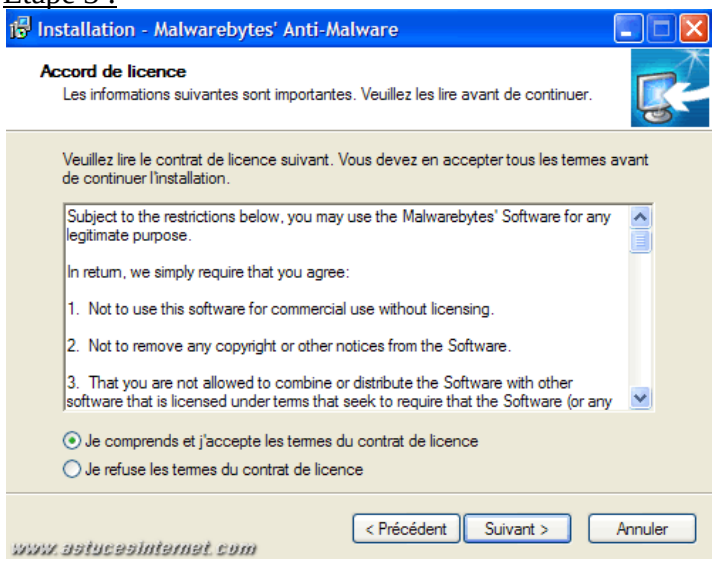
Sélectionnez *Français* puis cliquez sur OK.

Étape 2 :



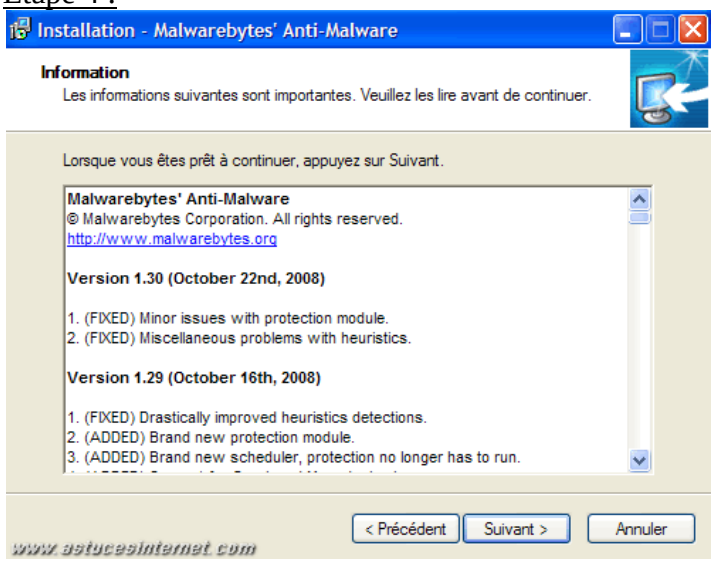
Cliquez sur *Suivant*.

Étape 3 :



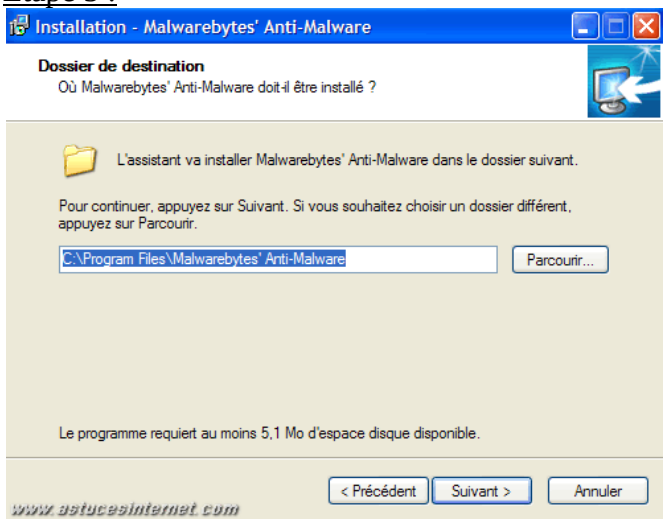
Pour utiliser le logiciel, vous devez accepter les conditions d'utilisation. Cochez *Je comprends et j'accepte les termes du contrat de licence* et cliquez sur *Suivant* pour continuer.

Étape 4 :



Cliquez sur *Suivant*.

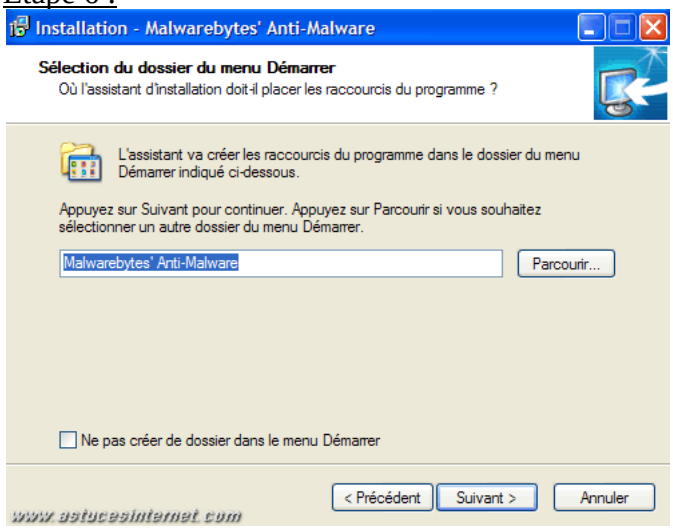
Étape 5 :



Vous avez la possibilité de choisir le répertoire d'installation du logiciel. Par défaut, le logiciel s'installe dans le dossier **C:\Program Files\Malwarebytes Anti-Malware**.

- Si vous voulez choisir un autre répertoire, cliquez sur *Parcourir*, sélectionnez le répertoire désiré et cliquez sur *Suivant.*
- Pour installer le logiciel dans son répertoire par défaut, cliquez directement sur *Suivant.*
-

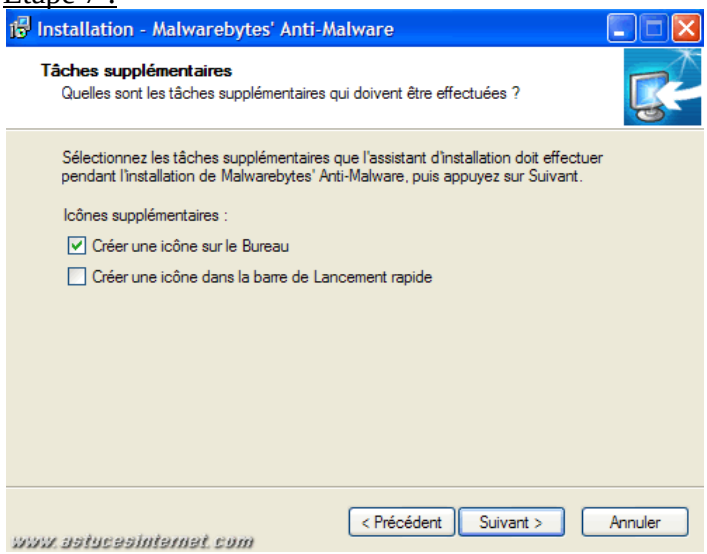
Étape 6 :



Vous avez la possibilité de créer un raccourci dans le menu Démarrer. Par défaut, le dossier qui sera créé dans votre menu Démarrer s'intitulera Malwarebytes Anti-Malware. Pour modifier l'emplacement de ce raccourci, cliquez sur *Parcourir* et sélectionnez un autre répertoire.
Si vous ne désirez pas créer de raccourci dans le menu Démarrer, cochez la case *Ne pas créer de dossier dans le menu Démarrer.*

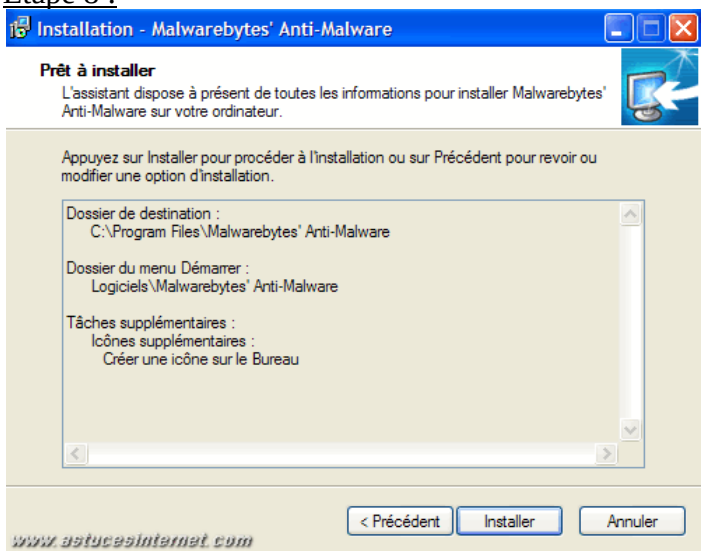
Cliquez sur *Suivant* pour continuer.

Étape 7 :



Vous pouvez créer des raccourcis sur votre bureau et dans la barre de lancement rapide de Windows. Cochez les cases selon les raccourcis que vous désirez créer et cliquez sur *Suivant* pour poursuivre l'installation.

Étape 8 :

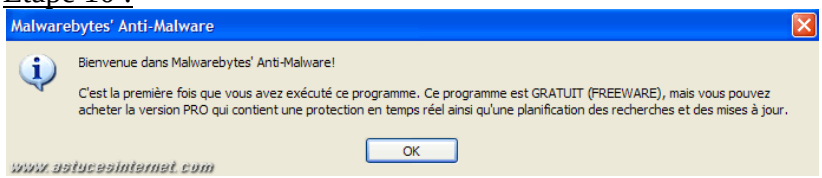


Le logiciel est prêt à être installé. Cliquez sur *Installer* pour lancer l'installation.

Étape 9 :

Cliquez sur *Terminer*. Malwarebytes Anti-Malware va se mettre à jour automatiquement.

Étape 10 :



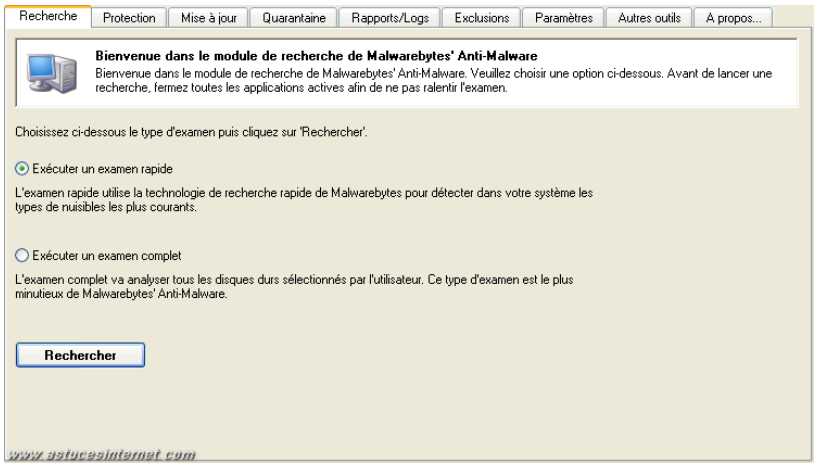
Malwarebytes Anti-Malware vous rappelle qu'une version PRO est disponible. Cliquez sur *OK* pour passer le message.

Étape 11 :

Malwarebytes Anti-Malware va se mettre à jour. Veuillez patienter durant le téléchargement des mises à jour du logiciel.

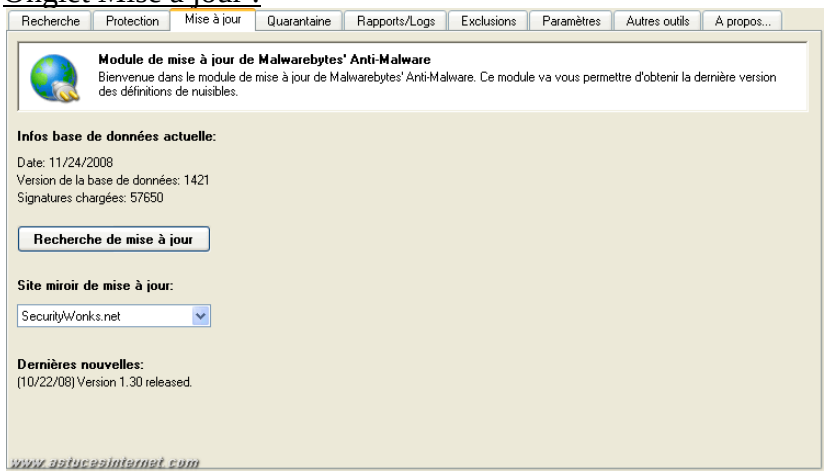
Descriptions des onglets disponibles dans l'interface du logiciel :

Onglet Recherche :



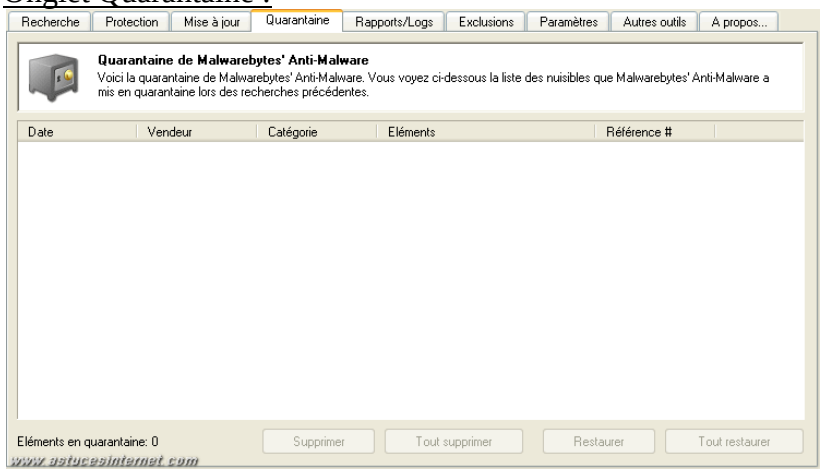
L'onglet Recherche permet de lancer une analyse de votre ordinateur. Sélectionnez le type d'analyse que vous voulez effectuer et cliquez sur *Rechercher*.

Onglet Mise à jour :



Pour mettre à jour la base de données du logiciel, cliquez sur *Recherche de mise à jour*. Si vous rencontrez des difficultés lors du téléchargement de la mise à jour (*lenteur du téléchargement*), vous avez la possibilité de sélectionner un autre site de téléchargement. Pour cela, sélectionnez une autre adresse dans la liste de *Site miroir de mise à jour*.

Onglet Quarantaine :

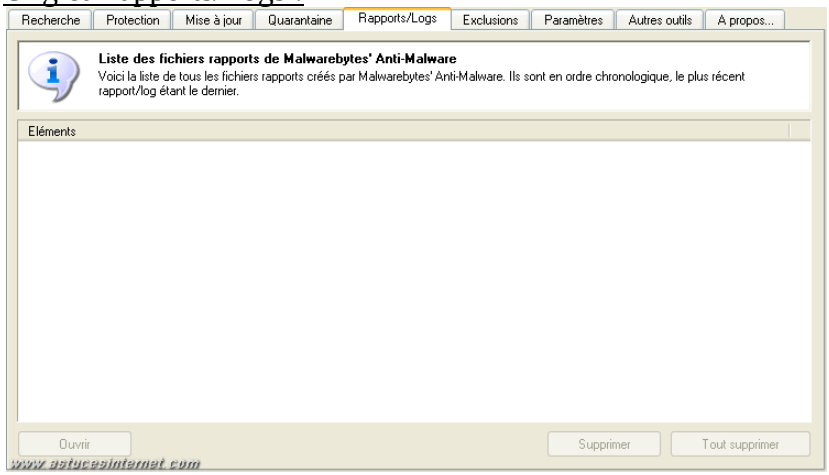


Cet onglet affiche la totalité des malwares qui ont été détecté sur votre ordinateur. Les

éléments présents dans cette fenêtre sont en quarantaine. Cela signifie qu'ils ne sont plus en activité sur votre ordinateur. Vous avez la possibilité de supprimer le contenu de la quarantaine en cliquant sur *Supprimer* pour effacer un élément sélectionné ou cliquer sur *Tout supprimer* pour vider totalement la zone la quarantaine.

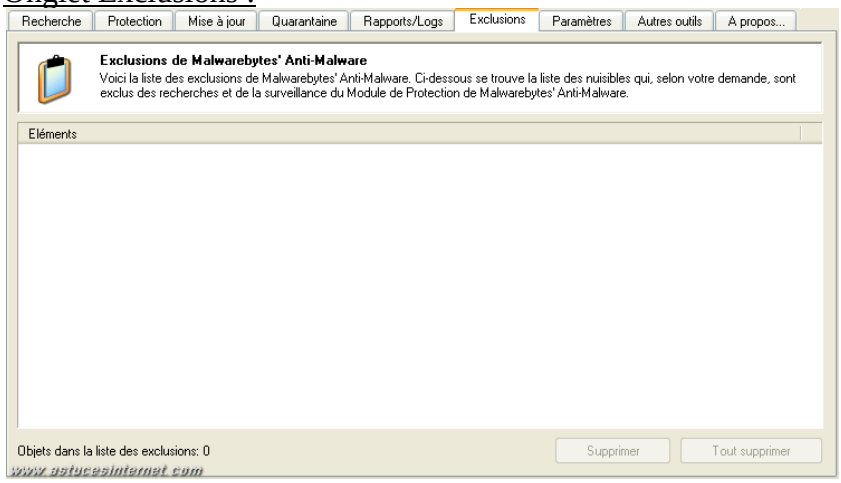
Si vous pensez qu'un élément a été filtré à tort et qu'il ne s'agit pas d'un malware *(faux positif)*, vous avez la possibilité de le restaurer en cliquant sur *Restaurer*. Vous disposez également d'une fonction *Tout restaurer, mais* nous vous la déconseillons. Si vous avez des éléments à restaurer, il vaut mieux les analyser au cas par cas plutôt que de faire une restauration complète qui remettrait par la même occasion les vrais malwares qui se trouveraient dans la quarantaine.

Onglet Rapports/Logs :



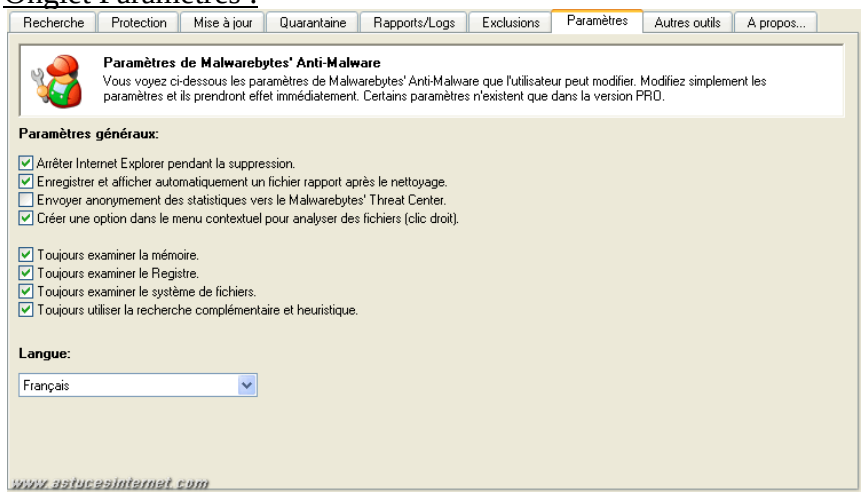
Cet onglet vous permet de visualiser les rapports d'analyse que vous avez effectué sur votre ordinateur.

Onglet Exclusions :



Cet onglet affiche tous les éléments qui ont été détecté comme étant malveillants mais que vous avez décider d'exclure de la recherche et de conserver sur votre PC. Si vous avez filtré un élément à tort, vous avez la possibilité de le retirer de la liste des exclusions en le sélectionnant puis en cliquant sur *Supprimer*. Cet élément sera de nouveau reconnu comme malveillant lors de la prochaine analyse.

Onglet Paramètres :

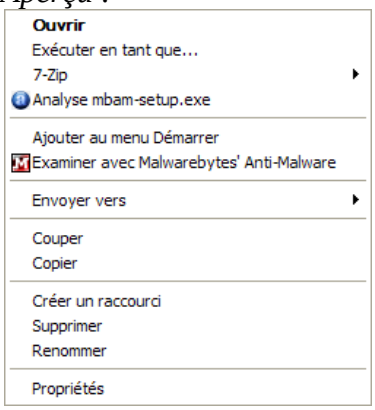


Cet onglet permet de définir les paramètres de fonctionnement de Malwarebytes' Anti-Malware.

Liste des options disponibles :

- **Arrêter Internet Explorer** pendant la suppression : Permet de couper le navigateur Internet Explorer lors de l'analyse.
- **Enregistrer et afficher automatiquement** un fichier rapport après le nettoyage : Permet d'enregistrer les fichiers logs à la fin de l'analyse. Ces fichiers logs seront disponibles dans l'onglet Rapports/Logs.
- **Envoyer anonymement** des statistiques vers le Malwarebytes' Threat Center : Si vous ne désirez pas que votre PC envoie des informations concernant l'utilisation de Malwarebytes' Anti-Malware et la détection de malware, décochez cette case.
- **Créer une option dans le menu contextuel** pour analyser des fichiers (clic droit) : Permet d'ajouter un lien dans le menu contextuel de Windows. Si vous activez cette option, vous pourrez lancer une analyse sur un fichier en faisant un clic droit sur ce dernier.

Aperçu :

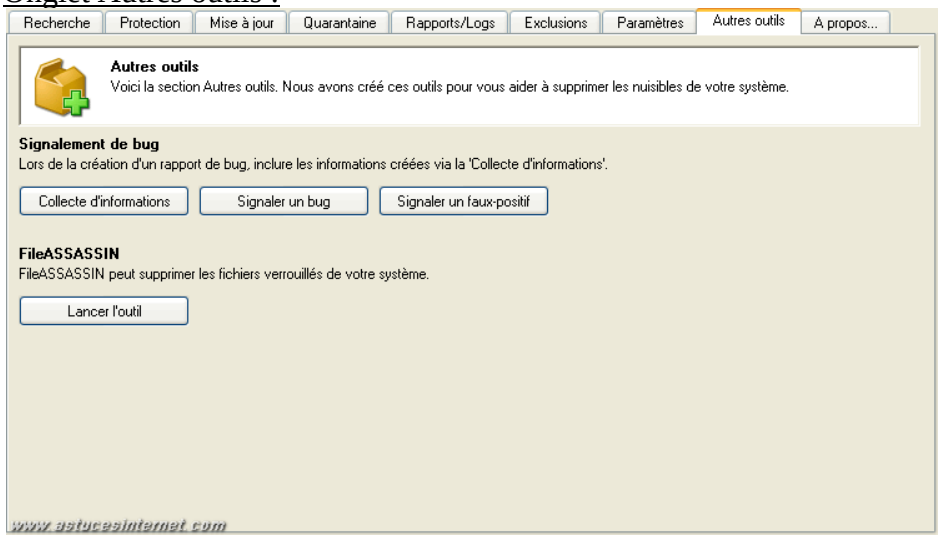


- **Toujours examiner la mémoire.**
- **Toujours examiner le Registre.**
- **Toujours examiner le système de fichiers.**
- **Toujours utiliser la recherche complémentaire et heuristique.**

Il est possible de désactiver certains types d'analyse *(Mémoire, Registre, Système de fichier ou détection heuristique*). Il est conseillé de laisser ces options actives.

- **Langue** : Permet de définir la langue utilisée dans Malwarebytes' Anti-Malware.

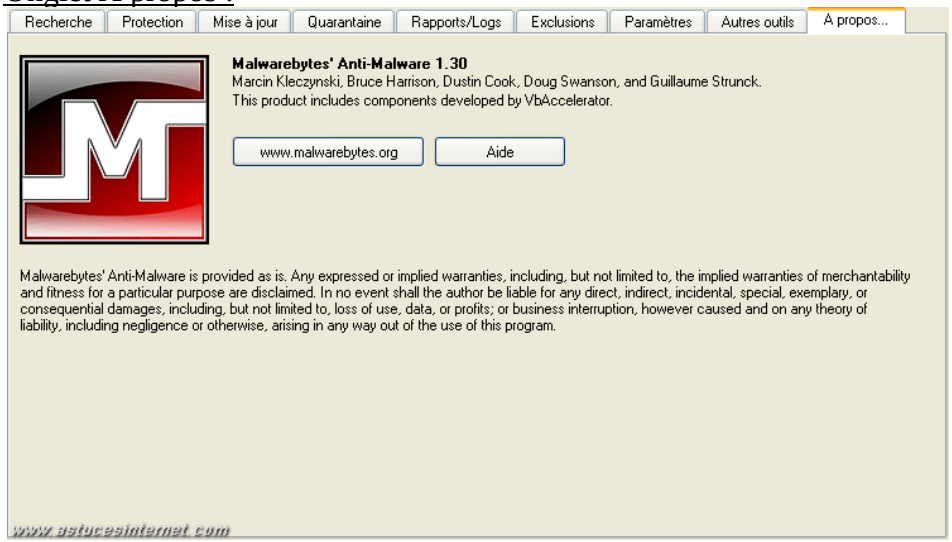
Onglet Autres outils :



L'onglet *Autres outils* vous permet d'envoyer diverses informations à l'éditeur du logiciel. Ainsi, vous avez la possibilité d'envoyer un rapport de bug *(Signaler un bug)* et d'envoyer un fichier log pour illustrer le bug *(Collecte d'informations).* Vous avez également la possibilité de signaler une fausse alerte détectée par le logiciel *(Signaler un faux-positif).*

FileASSASSIN est un outil fourni avec Malwarebytes' Anti-Malware. Il permet de déverrouiller un fichier qui ne pourrait pas être supprimé car toujours en cours d'utilisation sur l'ordinateur. Pour utiliser FileASSASSIN, cliquez sur *Lancer l'outil.*

Onglet A propos :

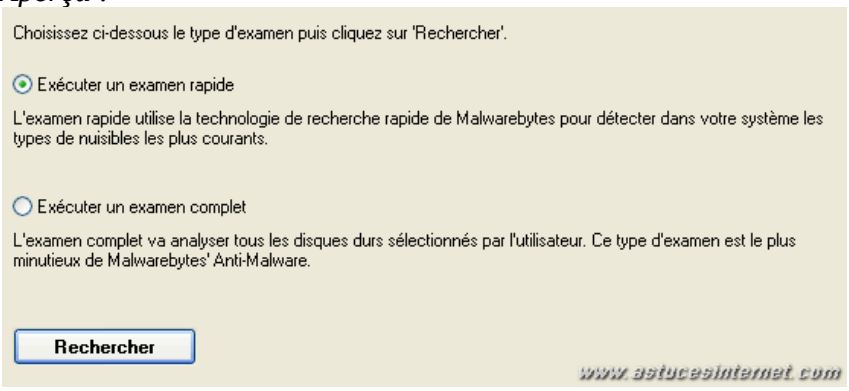


Cet onglet affiche les liens vers le site officiel de Malwarebytes' Anti-Malware et vers l'aide du logiciel.

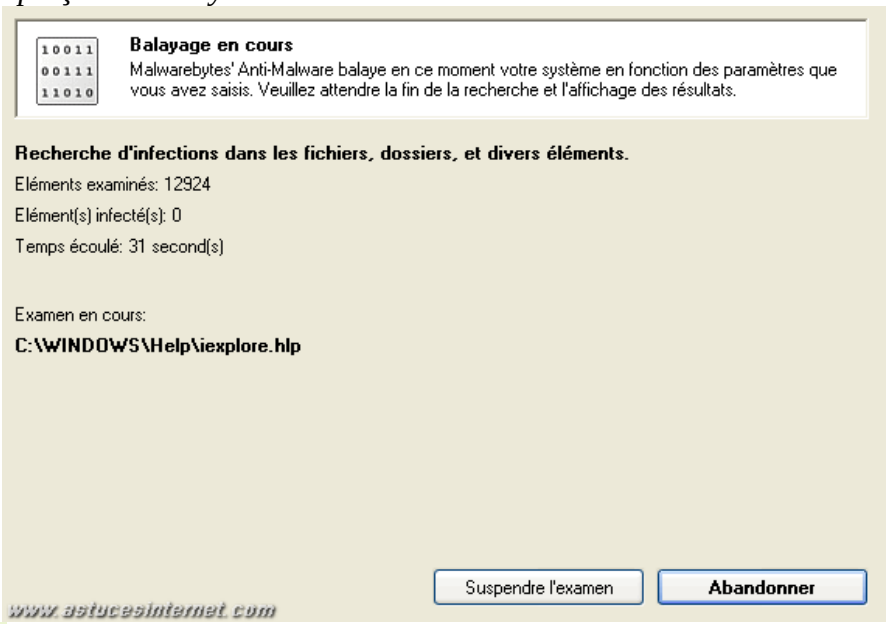
Utilisation du logiciel :

Pour effectuer une analyse de votre ordinateur, rendez-vous dans l'onglet *Recherche*, cochez le type de recherche que vous désirez effectuer et cliquez sur *Rechercher.*

Aperçu :



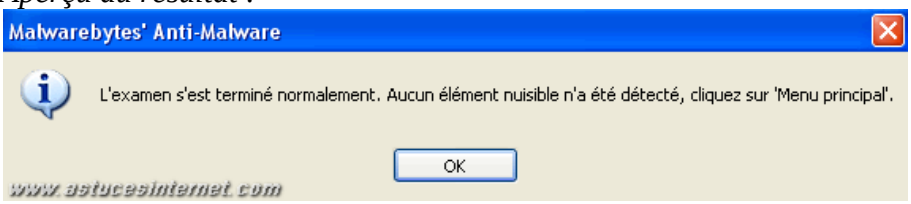
Aperçu de l'analyse en cours :



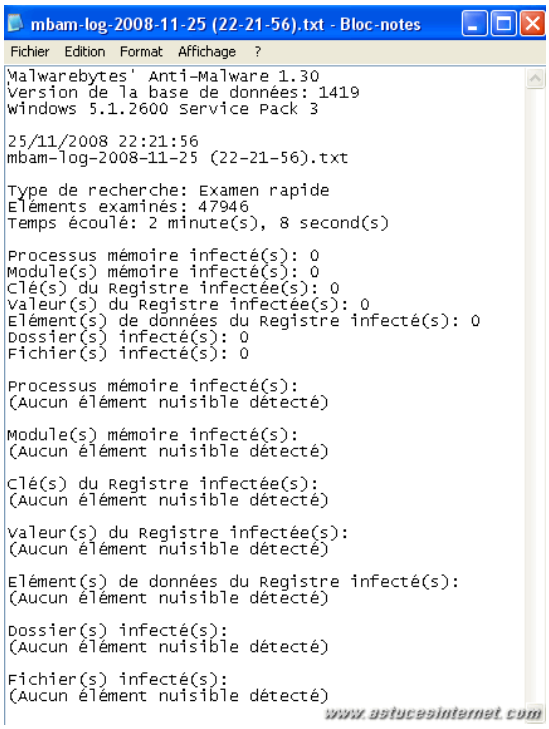
Note : Vous pouvez suspendre ou abandonner l'analyse en cours.

Une fois l'analyse terminée, Malwarebytes' Anti-Malware affiche le rapport d'analyse (sauf si vous avez désactivé l'option dans l'onglet *Paramètres).*

Aperçu du résultat :



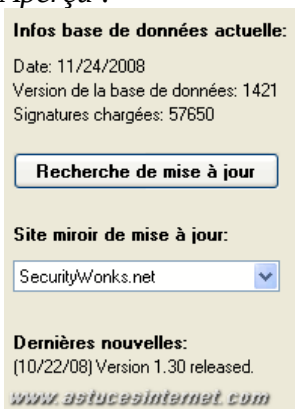
Aperçu d'un rapport d'analyse :



Mise à jour du logiciel :

Pour mettre à jour le logiciel, rendez-vous dans l'onglet *Mise à jour* et cliquez sur *Recherche de mise à jour*.

Aperçu :



Malwarebytes' Anti-Malware va télécharger les nouvelles signatures de malware qui ont été détectées depuis la mise à jour précédente.

Aperçu du résultat :