2013

Microsoft Security Essentials

Écrit par **malekalmorte**
http://www.malekal.com

Microsoft security essentials

L'installation

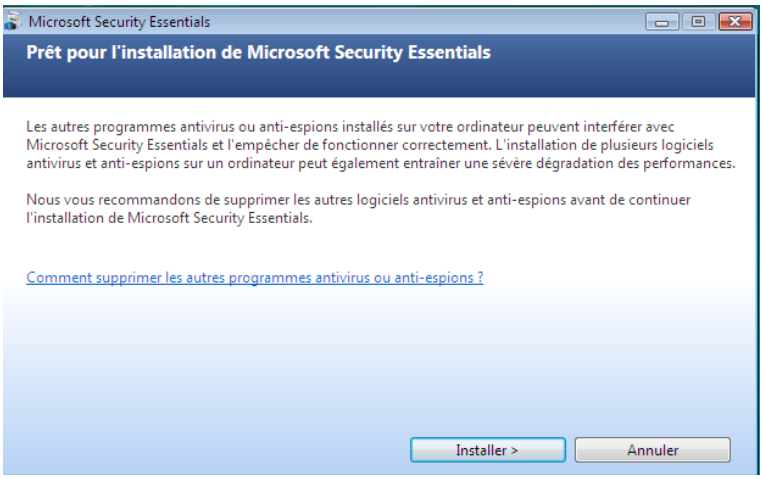
Vous pouvez télécharger Microsoft Security Essentials à partir de ce lien : Télécharger Microsoft Security Essentials

- Choisissez *Français* comme langue et cliquez sur le système d'exploitation.
- Le programme d'installation se lance, cliquez sur le bouton *Suivant* pour continuer

- Vous devez accepter la licence d'utilisation en cliquant sur le bouton *Accepter*

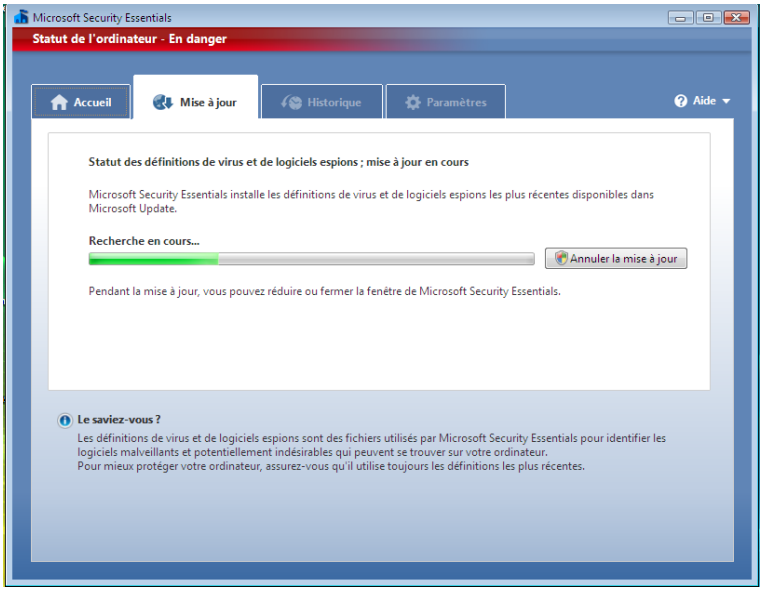
- Le programme d'installation vérifie via WGA que votre Windows est authentique et non une version pirate
- Cliquez sur le bouton *Vérifier* pour continuer.

- L’installation est prête, cliquez sur le bouton *installer* pour commencer.

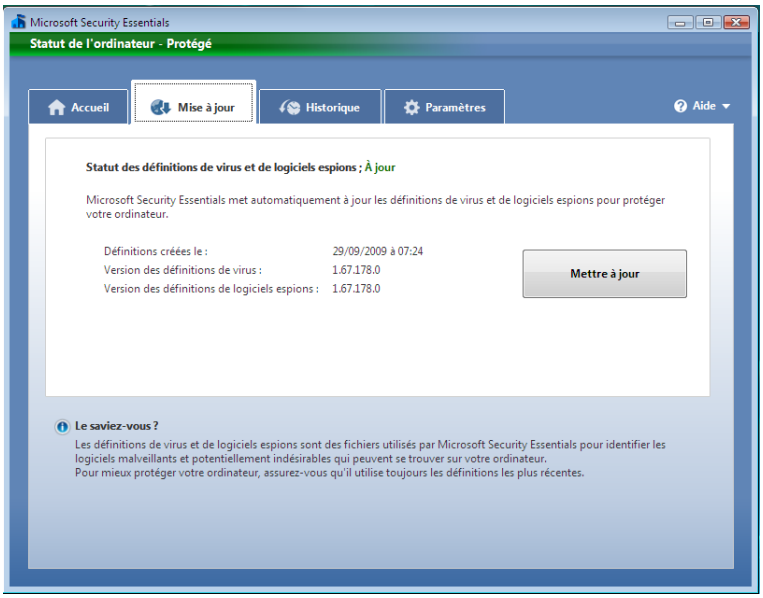


Mise à jour de Microsoft Security Essentials

L’interface de Microsoft Security Essentials est très simple et se compose de quatre onglets. La mise à jour de Microsoft Security Essentials est automatique après l’installation. Celle-ci se fait à partir de l’onglet *Mise à jour*, si la mise à jour a réussi, une bande verte s’affiche en haut pour vous le signaler.



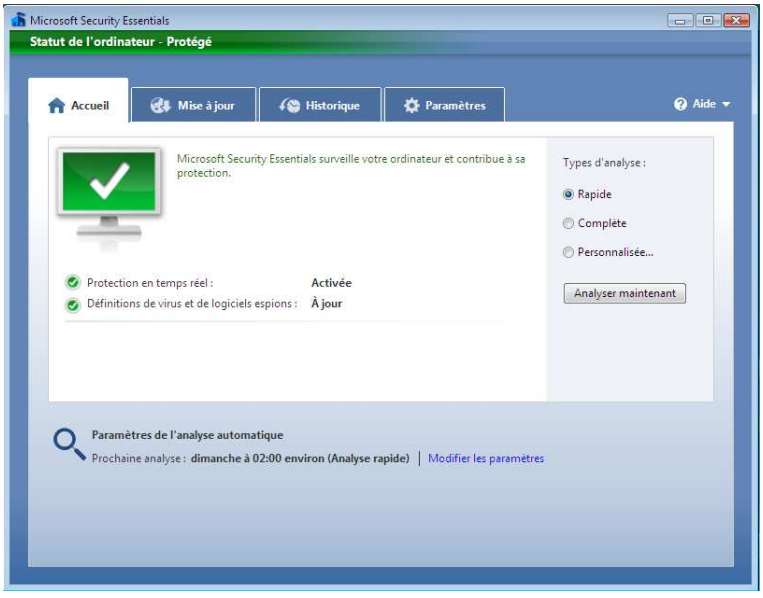
Si vous voulez lancer une mise à jour manuelle, il vous suffit de cliquer sur le bouton Mettre à jour à droite.



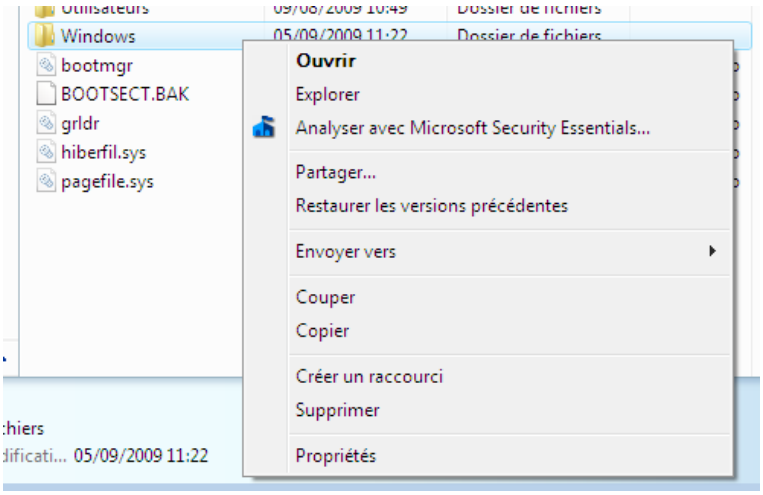
Scan de l'ordinateur

Le scan de l'ordinateur se fait à partir de l'onglet *Accueil*.
Trois scans sont possibles :

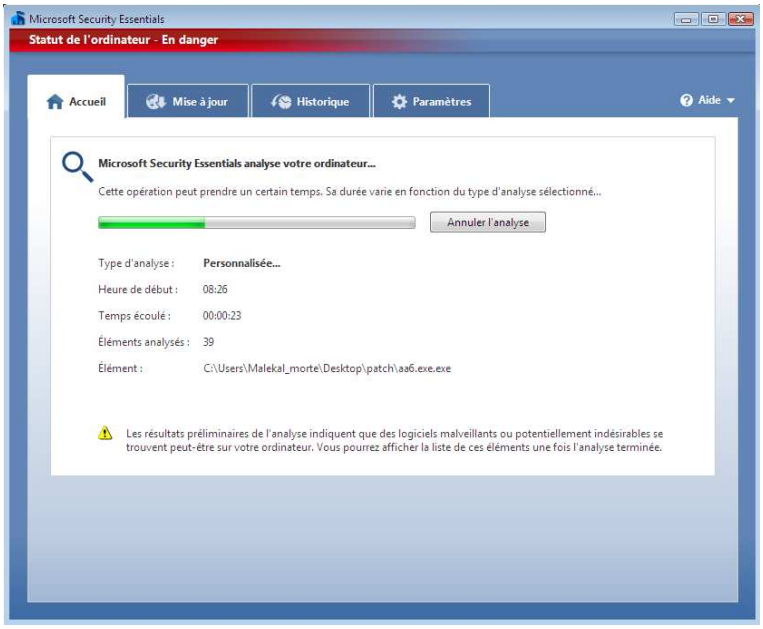
- Un scan rapide qui analyse seulement les zones sensibles succeptibles de contenir des malwares
- Scan complet qui scanne tous les fichiers du disques.
- Scan personnalisé, vous choisissez les emplacements (dossiers/fichiers à scanner).



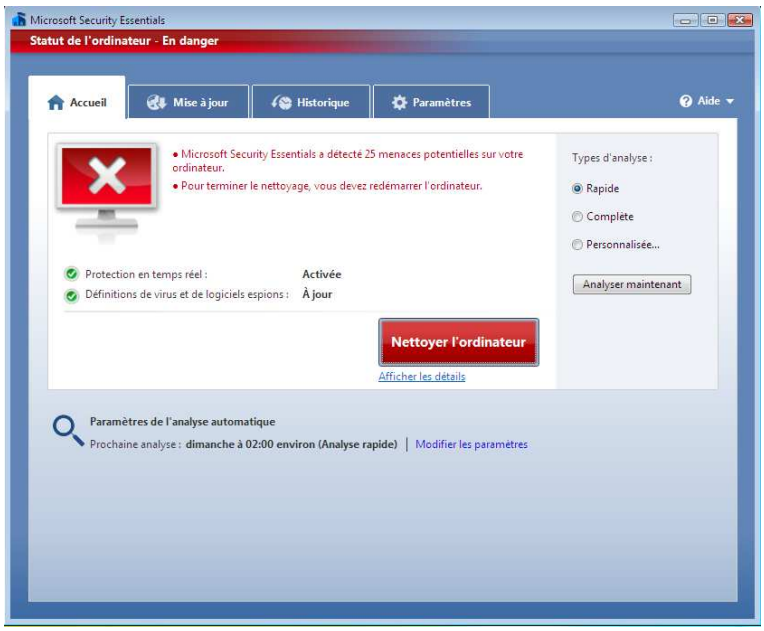
A noter que vous pouvez aussi lancer un scan par un clic droit sur un dossier ou fichier à partir de l'explorateur de fichiers :



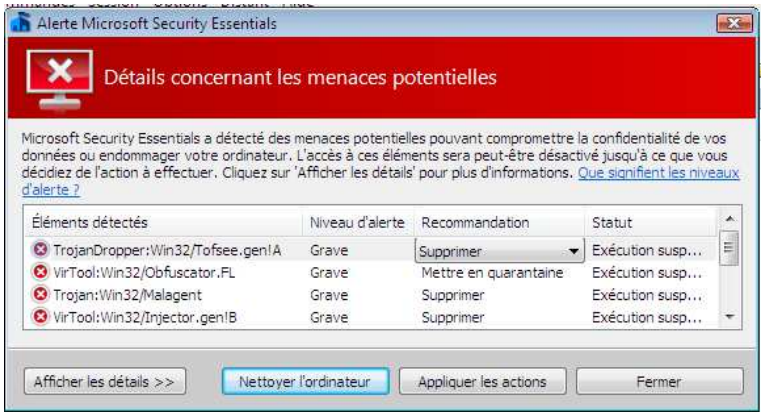
Le scan peut prendre plusieurs minutes. Si des éléments infectieux sont détectés, une alerte en bas du scan apparaît : *Les résultats préliminaires de l'analyse indiquent que des logiciels malveillants ou potentiellements indésirables se trouvent peut-être sur votre ordinateur. Vous pourrez afficher la liste de ces éléments une fois l'analyse terminée.*
Des éléments infectieux détectés ne veut pas forcément dire que votre ordinateur est infecté (infection active), encore faut-il comprendre les alertes, lire la page : Comprendre les rapports de scan des antivirus



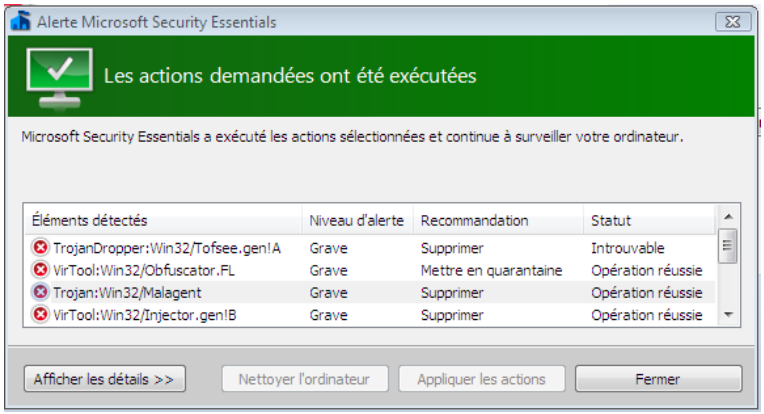
Une fois le scan terminé, Microsoft Security Essentials vous indique le nombre de menaces détectées, le bouton Nettoyer l'ordinateur permet de mettre en quarantaine ces menaces.



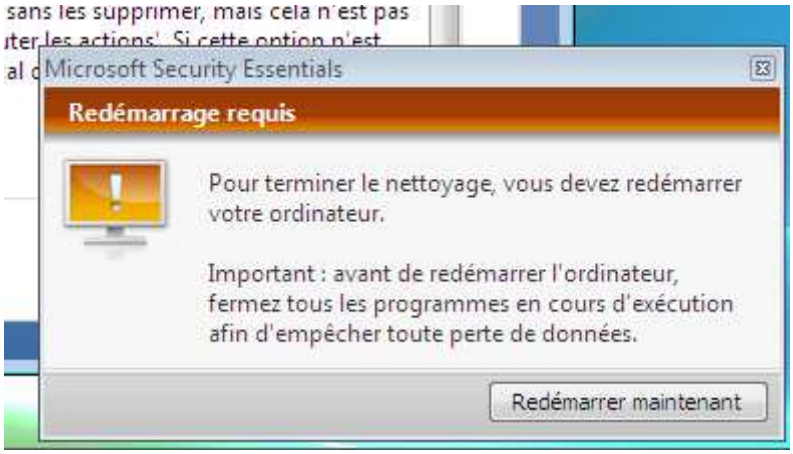
Le bouton *Afficher les détails* permet de lister les menaces détectées



Enfin, le bouton *Afficher les détails* donne les informations sur la menace et notamment son emplacement sur le disque dur.
Le bouton *Nettoyer l'ordinateur* va supprimer toutes les menaces détectées, sinon il est possible de paramétrer une action pour chaque menace à partir des menus déroulants (Supprimer, mettre en quarantaine etc).
Cliquez alors sur le bouton *Appliquer les actions.*
Lorsque les actions sont effectuées avec succès, un bandeau vert vous l'indique.

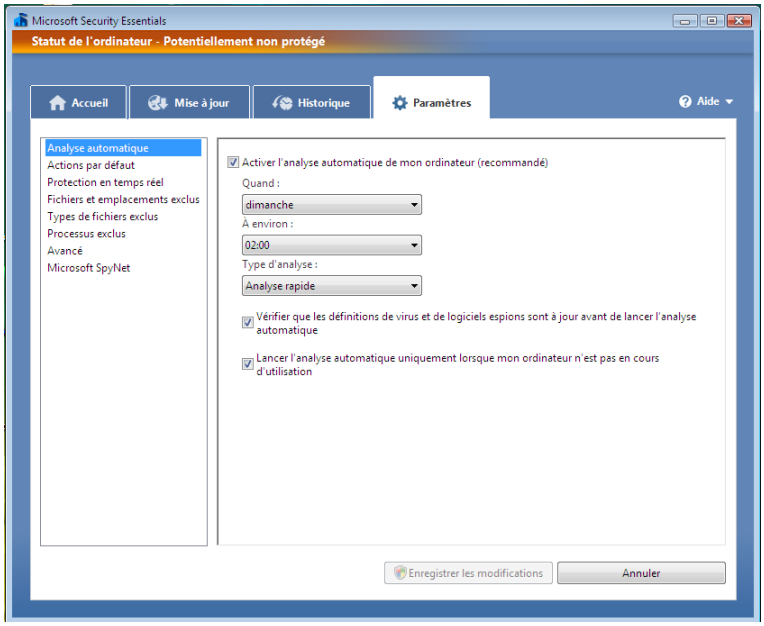


Le nettoyage de l'ordinateur peut necessiter un redémarrage, si c'est le cas, une fenêtre d'alerte vous en informe. Si vous désirez redémarrer l'ordinateur, cliquez alors sur le bouton *Redémarrer maintenant*



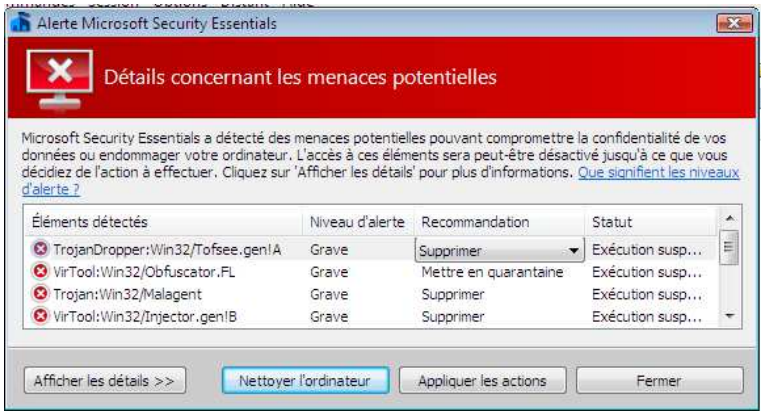
A noter que Microsoft Security Essentials configure une analyse automatique de l'ordinateur le dimanche, vous pouvez modifier cette analyse de l'ordinateur à partir de l'onglet *Paramètres* puis *Analyse automatique*

This image has been resized. Click this bar to view the full image. The original image is sized 840x686px.



Le gardien : protection en temps réel

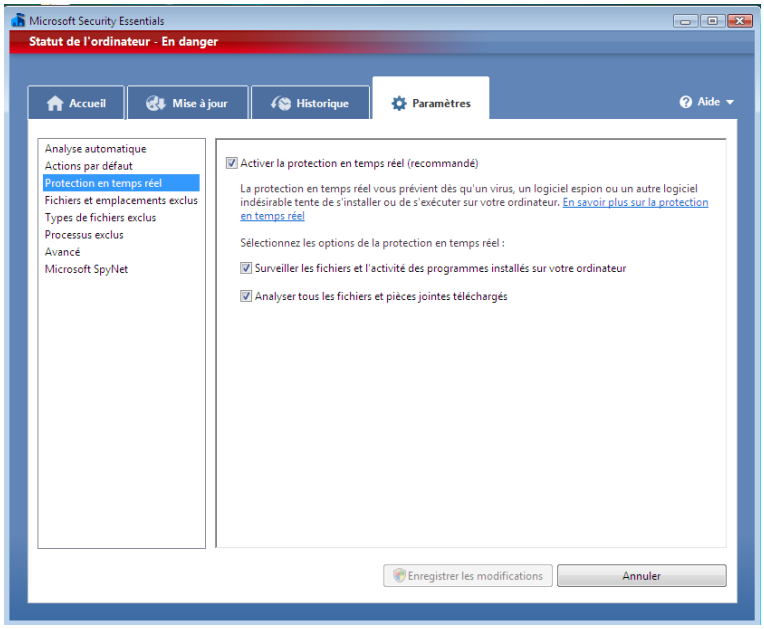
Le gardien scanne en temps réel les fichiers que vous tentez d'ouvrir ou lire afin de détecter d'éventuelles menaces, il permet donc de protéger votre ordinateur.
Dans le cas où celui-ci détecte une menace, une alerte, comme dans la capture suivante, apparaît en bas à droite à côté de l'horloge :



On retrouve alors les mêmes actions, fenêtres et informations que lors du scan manuel.

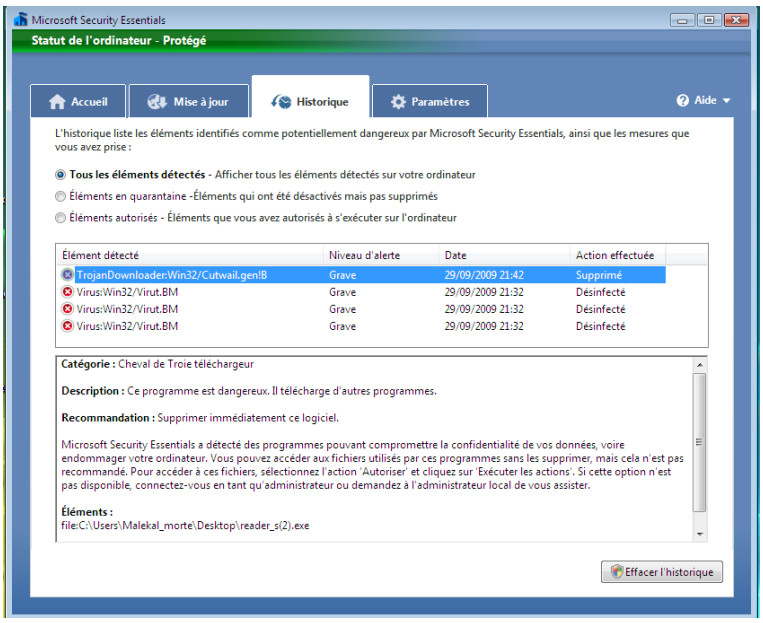
Il est bien sûr possible de désactiver la protection en temps (ce qui n'est pas recommandé, sauf si vous savez ce que vous faites), cela se fait à partir de l'onglet *Paramètres* puis *Protection en temps réel.*

⚠ This image has been resized. Click this bar to view the full image. The original image is sized 836x686px.



Historique et quarantaine

L'onglet Historique permet de lister les éléments qui ont été détectés lors des scans ou par la protection en temps réel (Guard/Gardien).
Si vous souhaitez vider l'historique, cliquez sur le bouton en bas à droite *Effacer l'Historique.*

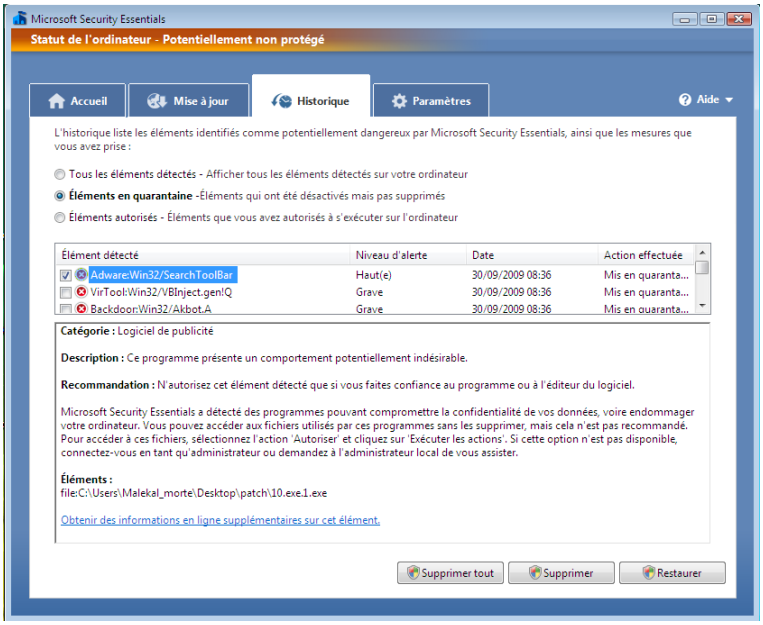


Pour afficher et gérer les éléments mis en quarantaine, cliquez en haut de la fenêtre sur *Eléments en quarantaine*.

Pour rappel : La quarantaine permet d'empêcher un fichier d'être exécuté ou supprimé, dans le cas d'un malware, cela peut donc l'empêcher d'être actif au sein du système.
Pour toutes questions sur la quarantaine, se reporter à la page : FAQ : la quarantaine de antivirus Pour avoir accès à la quarantaine, cliquez sur l'onglet quarantaine.
Vous obtenez sous forme de liste, les fichiers mis en quarantaine avec la date, le fichier incriminé.

Vous pouvez alors :

- Supprimer tout le contenu de la quarantaine – bouton *Supprimer tout*.
- Supprimer les éléments que vous aurez cochés dans la liste puis cliquez sur le bouton *Supprimer*.
- Restaurer les éléments cochés à leurs emplacements d'origine puis cliquez sur le bouton *Restaurer*.

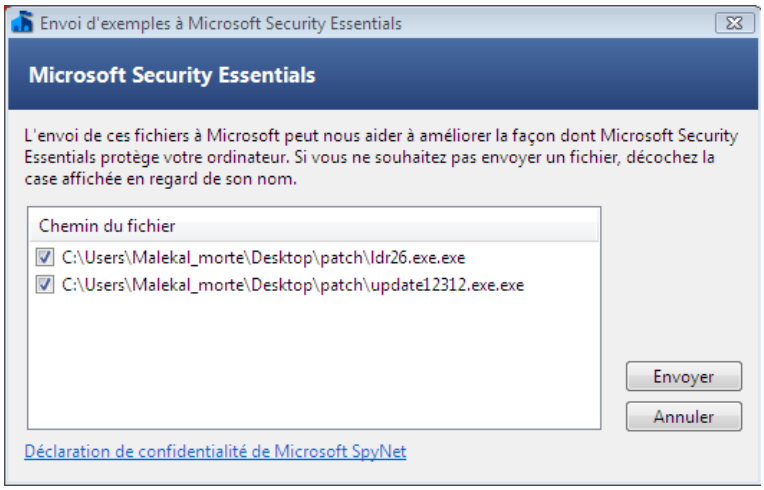


Microsoft SpyNet

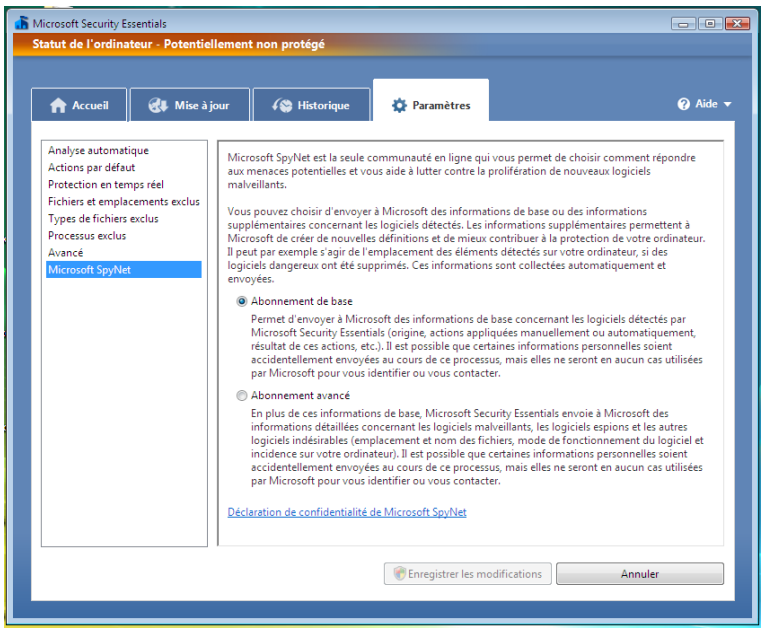
Microsoft SpyNet est un programme qui permet d'envoyer les malwares inconnus ainsi que des informations comme l'origine, les actions que vous avez effectués (supprimer, mis en quarantaine etc) par Microsoft Security Essentials aux laboratoires de Microsoft ceci afin :

- D'ajouter une définition virales et donc de permettre à Microsoft Security Essentials de détecter la menace.
- Eventuellement, si c'est une menace importe ajouter (ou mettre à jour) le MSRT afin de supprimer ce malware des ordinateurs infectés.
- Améliorer Microsoft Security Essentials selon les actions effectuées.
- Eventuellement détecter et corriger des faux positifs.

Lorsque Microsoft Security Essentials détecte des éléments à envoyer au programme Microsoft SpyNet, la fenêtre suivante s'ouvre alors, vous pouvez cliquer sur le bouton *Envoyer* pour envoyer ces fichiers aux laboratoires Microsoft.



A noter qu'à partir de l'onglet *Paramètres* puis Microsoft SpyNet, vous pouvez choisir le type d'abonnement et la manière dont les informations sont collectées



Exclusions de fichiers

Il est possible d'exclure des fichiers lors du scan de l'ordinateur ou par le gardien, cela peut-être intéressant par exemple pour exclure un dossier de vidéos afin de rendre l'analyse de l'ordinateur plus rapide ou dans le cas d'un faux positif d'exclure le fichier en question afin de ne plus obtenir d'alerte.

L'exclusion est paramétrable à partir de l'onglet *Paramètres*, vous pouvez alors à partir de :

- l'onglet fichiers et emplacements exclus ajouter des fichiers ou dossiers qui seront exclus du scan de l'ordinateur et du gardien
- l'onglet types de fichiers exclus : exclure le scan de certains de fichiers, par exemple les vidéos de type avi en ajoutant l'extension .avi
- l'onglet processus exclus : exclure des processus qui seront en cours d'exécution sur l'ordinateur de l'analyse de l'ordinateur ou par le gardien.

Il vous suffit d'ajouter le fichier ou l'extension et enregistrer les nouveaux paramètres.