Bonjour,

Si vous avez l'impression que votre PC est infecté, il faut effectuer une première recherche de nuisibles puis créer deux rapports détaillés (alias "logs" en anglais) qui vont décrire l'état du PC.

Cette procédure s'applique aux ordinateurs tournant sous Windows 2000, Windows NT, Windows XP, Windows Vista et Windows 7 (32bit et 64bit).
Elle doit être réalisée avec les droits Administrateur.

Tous les programmes utilisés ici sont sûrs: il faut ignorer toute alerte de votre antivirus/antispyware.

Procédure:

Étape 1: OTL (de OldTimer), téléchargement
Télécharger **OTL.exe** depuis http://oldtimer.geekstogo.com/OTL.exe
Enregistrer ce fichier **sur le Bureau**.
Important: même si OTL.exe est déjà présent sur le PC, il faut toujours télécharger la dernière version (qui devra remplacer toute version antérieure),

Télécharger le fichier **scan.zip** depuis **ce lien**.
Extraire de cette archive le fichier **scan.txt** et placer ce fichier **sur le Bureau**.

Étape 2: Malwarebytes' Anti-Malware, installation
Télécharger Malwarebytes' Anti-Malware depuis la page ci-dessous:
http://www.malwarebytes.org/products/malwarebytes_free
(cliquer sur le bouton gris "Download Now")

Enregistrer ce fichier sur le Bureau.
Faire un double clic sur **mbam-setup.exe** pour lancer l'installation (Accepter le contrat de licence, puis valider les options par défaut).
Sur le dernier écran de la procédure d'installation, cocher la case située devant "**Mettre à jour Malwarebytes' Anti-Malware**", puis cliquer sur le bouton "**Terminer**".

Étape 3: ERUNT (de Lars Hederer): sauvegarde du Registre
Télécharger **ERUNT** depuis la page: http://www.larshederer.homepage.t-online.de/erunt/
Sous **Download ERUNT:**, télécharger **erunt-setup.exe**
Télécharger également le fichier de langue française: sous **French** télécharger le fichier **erunt-loc_fr.zip**

Installer ERUNT en faisant un double clic sur **erunt-setup.exe**
Décompresser l'archive **erunt-loc_fr.zip** (sous XP, clic droit puis Extraire tout) et placer les fichiers extraits dans le dossier d'installation de ERUNT: ***%SystemDrive%*\Program Files\ERUNT**
[*%SystemDrive%* représente la partition sur laquelle est installé le système, généralement C:]

Lancer ERUNT par un double clic sur **ERUNT.EXE**
Sous Windows Vista/7, faire un clic droit sur **ERUNT.EXE** puis choisir "Exécuter en tant qu'Administrateur" pour lancer l'outil.
Sur le message de Bienvenue, cliquer sur **OK**
Dans la fenêtre intitulée "ERU pour Windows NT", cocher toutes les options de sauvegarde (Registre système, Registre utilisateur courant et Autres registres utilisateur)
Cliquer ensuite sur **OK**

Accepter la création du dossier (dans le dossier Windows\ERDNT\) en cliquant sur **Oui**.
Attendre la fin de la sauvegarde, signalée par le message "Sauvegarde du registre effectuée", et cliquer sur **OK**.

Étape 4: Pas de processus de contrôle en temps réel
Désactiver le module résident de l'antivirus et celui de l'antispyware.
Voir **Désactiver le module résident de l'antivirus.**
Voir **Désactiver le module résident de l'antispyware.**
Note: si vous n'y arrivez pas, sautez cette étape ainsi que l'étape 6, mais signalez-le dans votre réponse.

Étape 5: Malwarebytes' Anti-Malware, recherche
Fermer toutes les fenêtres de programme ouvertes.
Lancer Malwarebytes' Anti-Malware via le Menu Démarrer.
Dans l'onglet **Paramètres**, vérifier que toutes les cases sont cochées sauf "Créer une option dans le menu contextuel pour analyser des fichiers (clic droit)".
Dans l'onglet **Mise à jour**, cliquer sur le bouton **Recherche de mise à jour** et installer toutes les mises à jour trouvées.
Dans l'onglet **Recherche**, cocher le bouton radio situé devant "**Exécuter un examen rapide**" puis cliquer sur le bouton **Rechercher**.
Attendre sans rien faire d'autre la fin de la recherche; dans la fenêtre annonçant la fin de l'analyse, cliquer sur OK; puis cliquer sur le bouton "**Afficher les résultats**".
Note: à ce stade du nettoyage, il ne faut pas utiliser l'option "Supprimer la sélection".

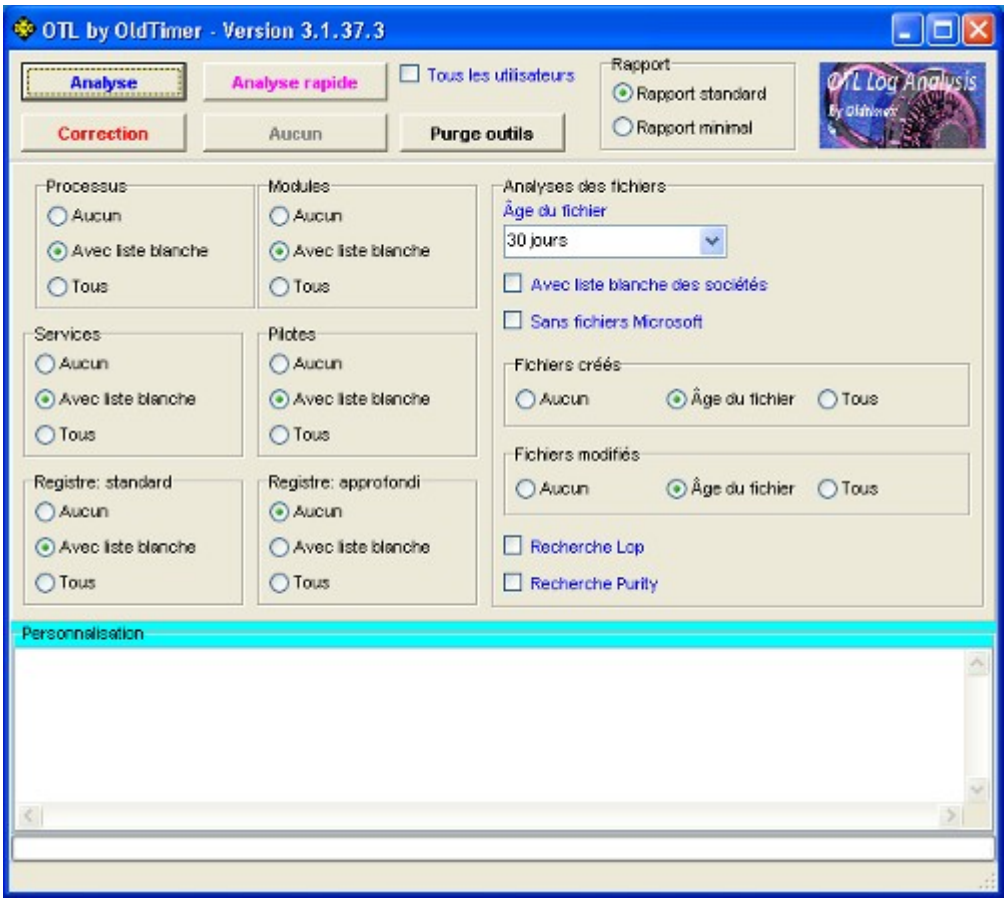
Cliquer sur le bouton "**Enregistrer le rapport**", valider la sauvegarde, puis cliquer sur le bouton "**Quitter**"

Étape 6: Processus de contrôle en temps réel
Important: Réactiver le module résident de l'antivirus et celui de l'antispyware.

Étape 7: OTL (de OldTimer), analyse
Fermer toutes les fenêtres de programme ouvertes.

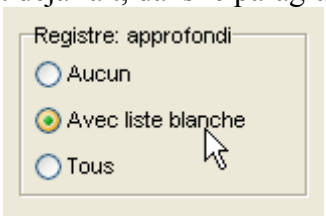
Faire un double clic sur **OTL.exe** pour lancer l'outil.
Sous Windows Vista/7, faire un clic droit sur **OTL.exe** puis choisir "Exécuter en tant qu'Administrateur" pour lancer l'outil.

L'écran principal de OTL s'affiche:



Sous Vista/7 64bit, vérifier que la case située devant "Avec analyses 64Bit" est cochée (en haut).

Si ce n'est déjà fait, dans le paragraphe **Registre: approfondi**, cocher le bouton-radio **Avec liste blanche**:



Cocher (en haut) la case située devant **Tous les utilisateurs**: 

Cocher les deux cases situées devant **Recherche Lop** et **Recherche Purity**:

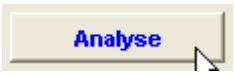
Faire un **double clic** dans la zone blanche située en bas et nommée "Personnalisation": 

Il y a ouverture d'une petite fenêtre "OTL":

Cliquer sur le bouton **Ok**.

A partir de la nouvelle fenêtre "Ouvrir", naviguer jusqu'à l'emplacement de sauvegarde du fichier **scan.txt** puis cliquer sur le bouton **Ouvrir**.

Le contenu du fichier **scan.txt** est ainsi inséré dans le panneau "Personnalisation" 

Enfin cliquer sur le bouton **Analyse**: 

Laisser l'outil travailler sans l'interrompre.
Lorsque l'outil a terminé, il y a ouverture d'une fenêtre du Bloc-notes contenant un rapport (log).
Fermer le Bloc-notes.
Le second rapport est visible dans la Barre des tâches. Le fermer également.
Fermer la fenêtre de OTL.

Étape 8: Résultats
Ouvrir un nouveau sujet dans **le sous-forum "Demandes d'étude de rapports d'analyse"**

Envoyer dans ce sujet un premier message contenant:
*- **une description détaillée des symptômes d'infection**
*- le rapport de Malwarebytes' Anti-Malware (contenu du fichier **mbam-log-******-**-** (**-**-**)**.txt** situé dans le dossier:

> *pour XP:* ***%SystemDrive%*\Documents and Settings\<*profil*>\Application Data\Malwarebytes\Malwarebytes' Anti-Malware\Logs**
> *pour Vista et 7:* ***%SystemDrive%*\Users\<*profil*>\AppData\Roaming\Malwarebytes\Malwarebytes' Anti-Malware\Logs**
> ****-**-** (**-**-**) représente la date [année-mois-jour] et l'heure [hh-mn-ss])
> [%*SystemDrive*% représente la partition sur laquelle est installé le système, généralement C:]

Envoyer ensuite toujours dans ce sujet dans deux messages distincts *(à cause de la longueur des fichiers)*:

*- les deux rapports de OTL (contenu des fichiers **OTL.Txt** et **Extras.Txt** situés sur le Bureau).
Les rapports envoyés sur le forum doivent se terminer par une ligne contenant <End>. Si ce n'est pas le cas, ils sont incomplets, et doivent alors être découpés en plusieurs messages.

Note importante: Pour l'envoi de ces deux derniers rapports, il ne faut pas créer de nouveaux sujets, mais cliquer sur le bouton "Répondre" 

pour continuer dans le même fil de discussion.

Remarques:
Après l'envoi des rapports ci-dessus, ne pas effectuer d'installation de nouveau logiciel, ne pas utiliser de son propre chef d'utilitaire de nettoyage/désinfection.

Bien évidemment, ne pas suivre simultanément les conseils d'un autre forum - *ce qui entraînerait la fermeture immédiate de votre fil de discussion*.

A bientôt,