Malekal's forum • Process Explorer : Exemple d'utilisation avancée : Papiers / Articles

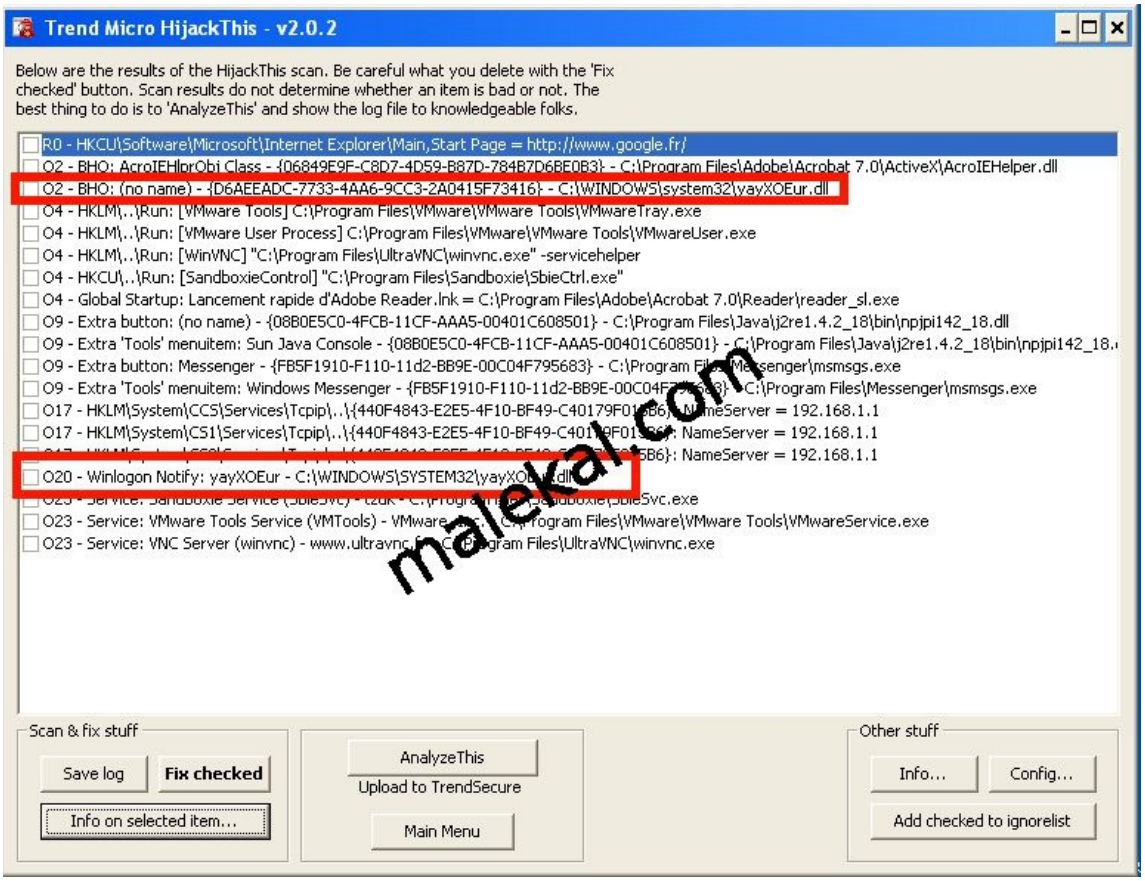
Ceci n'est pas une procédure de désinfection pour les infections Vundo/Virtumonde mais une démonstration des possibilité offerte par le programme Process Explorer - Pour supprimer les infections Vundo/Virtumonde, suivre la procédure donnée sur cette page : http://www.malekal.com/Trojan.vundo.php
Cette page vous montre les possibilités offertes par le programme Process Explorer en supprimant l'infection Vundo/Virtumonde.
Pour mieux apréhender cette page, il est conseillé d'avoir lu le tutorial Process Explorer :
http://www.malekal.com/tutorial_ProcessExplorer.php

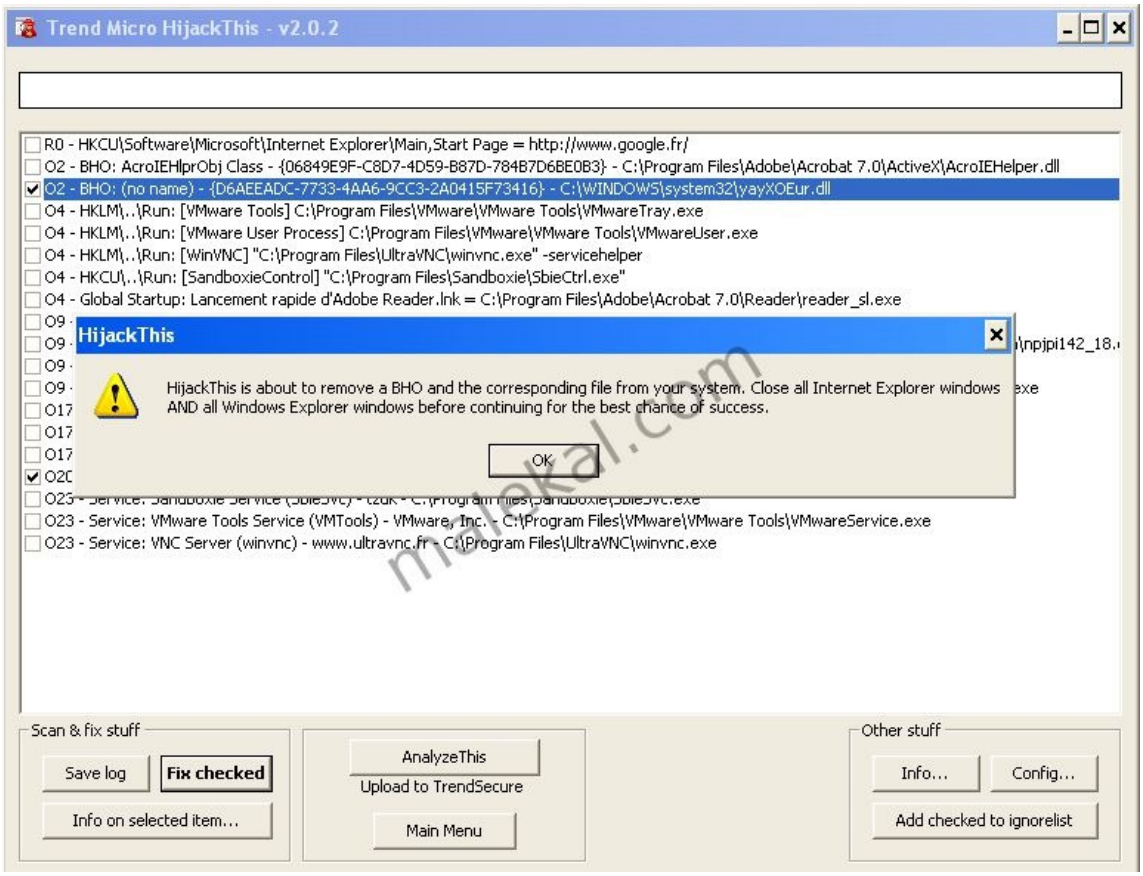
Présentation rapide de Vundo/Virtumonde
Vundo/Virtumonde est un adware qui affiche des popups de publicités et/ou effectuent des redirections lors des recherches Google.
Cet adware est en général installé par une infection tiers (Trojan/Backdoor) afin de rémunérer les auteurs de ces infections via les publicités ouvertes sur votre PC.

Voir les liens suivants pour le détails de l'infection :
http://www.malekal.com/Trojan.vundo.php
http://www.malekal.com/Win32_VBStat-c.php

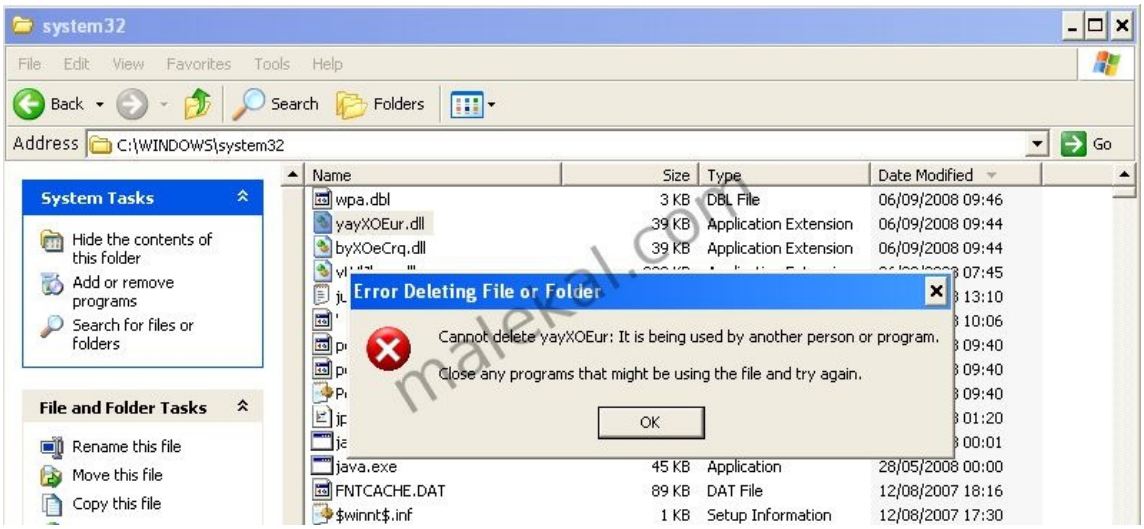
Vundo/Virtumonde se présente donc sous forme de fichiers DLL avec des noms aléatoires qui se chargent dans les processus Explorer.exe (sous forme de BHO) et Winlogon.exe ce qui pose de gros soucis à la majorité des antivirus pour supprimer cette infection (quand les antivirus en question la détectent).

Voici les lignes HijackThis.... tenter de fixer les lignes directement ne sert à rien, car l'infection monitore les entrées, si vous tentez de les supprimer/modifier, l'infection va les remettre.
Le but étant de s'assurer que l'infection sera bien chargée au redémarrage l'ordinateur.
La clef Notify Winlogon permet aussi le chargement de l'infection en mode sans échec et donc l'impossibilité de supprimer les fichiers DLL.

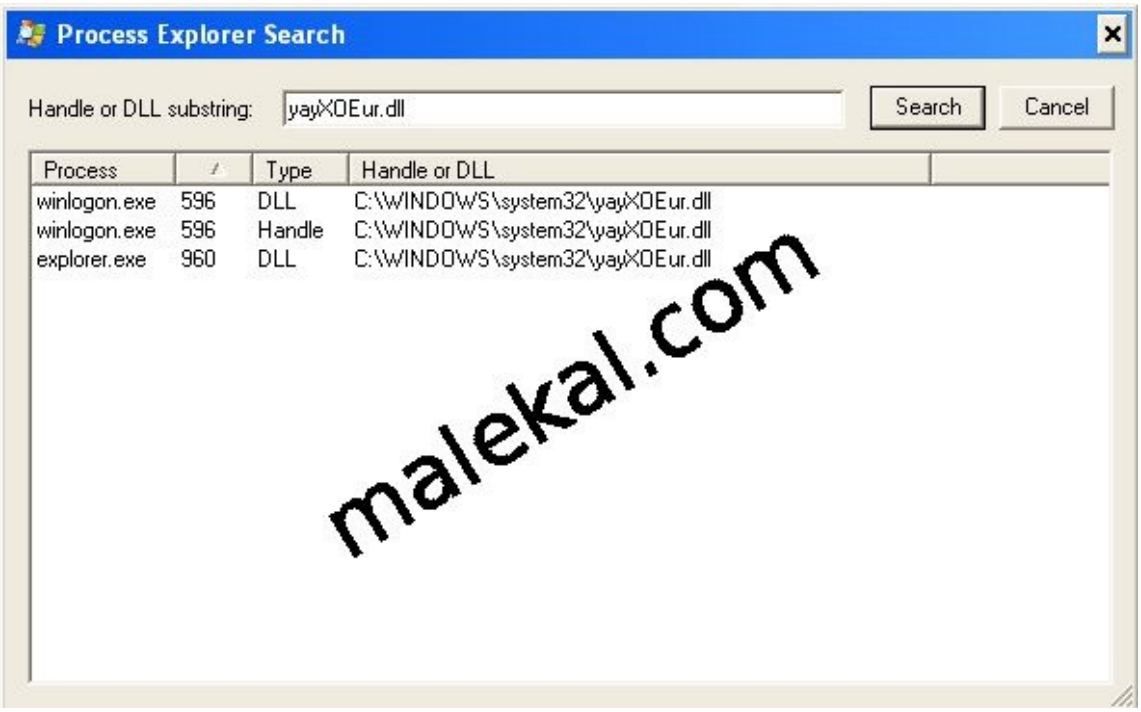




Tenter de supprimer directement les fichiers est aussi inutile puisque les ressources sont en cours d'utilisation.



Une recherche de la DLL en question sur Process Explorer nous montre qu'elle se charge bien dans les processus explorer.exe / winlogon.exe



Process Explorer VS Vundo/Virtumonde

Lorsque l'on souhaite supprimer une infection, on peux s'y prendre de deux manières :

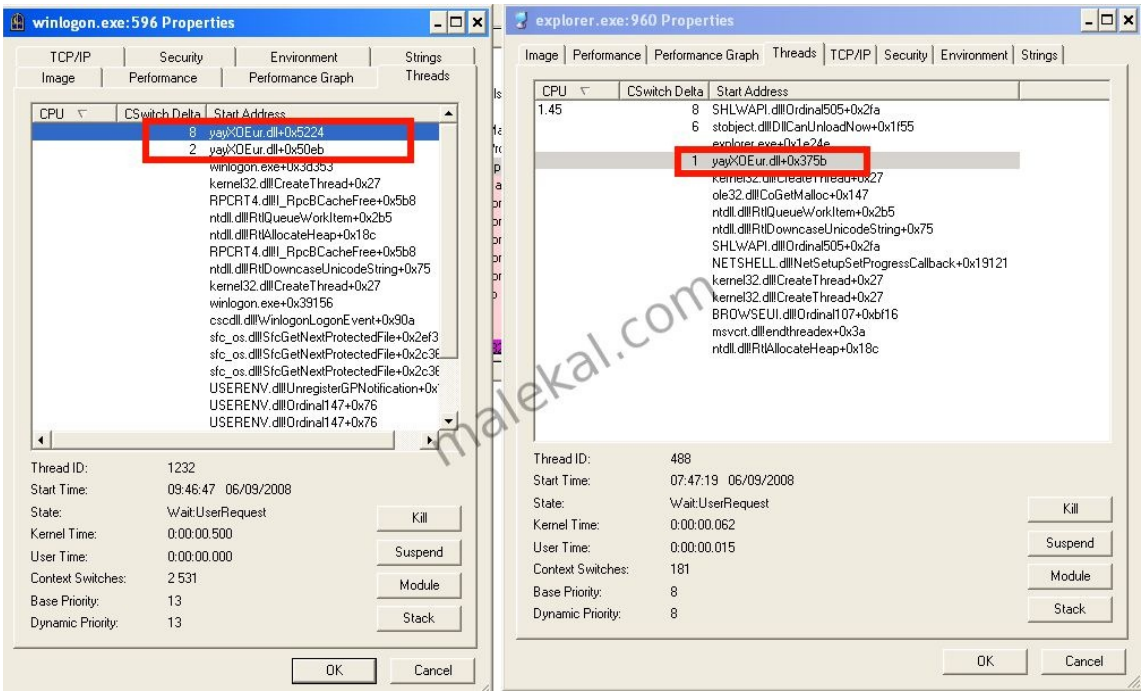
- Supprimer les points de chargement afin que l'infection ne se relance pas au redémarrage de l'ordinateur
- Supprimer le fichier chargés (DLL, driver ou fichiers .exe) afin encore une fois que l'infection ne puisse pas se relancer

Dans le dernier cas, en général, un utilisateur recevant le message disant que le fichier est utilisé va faire appel à un programme tiers du style Unlocker pour tenter d'exploser le fichier (voir aussi Visualiser et supprimer les fichiers cachés et lockés).
Dans notre exemple, nous allons utiliser la seconde méthode, supprimer les points de chargement de l'infection (BHO et clefs Notify Winlogon).
Nous avons vu que l'infection monitore l'infection, il nous faut donc désactiver l'infection afin de supprimer les clefs

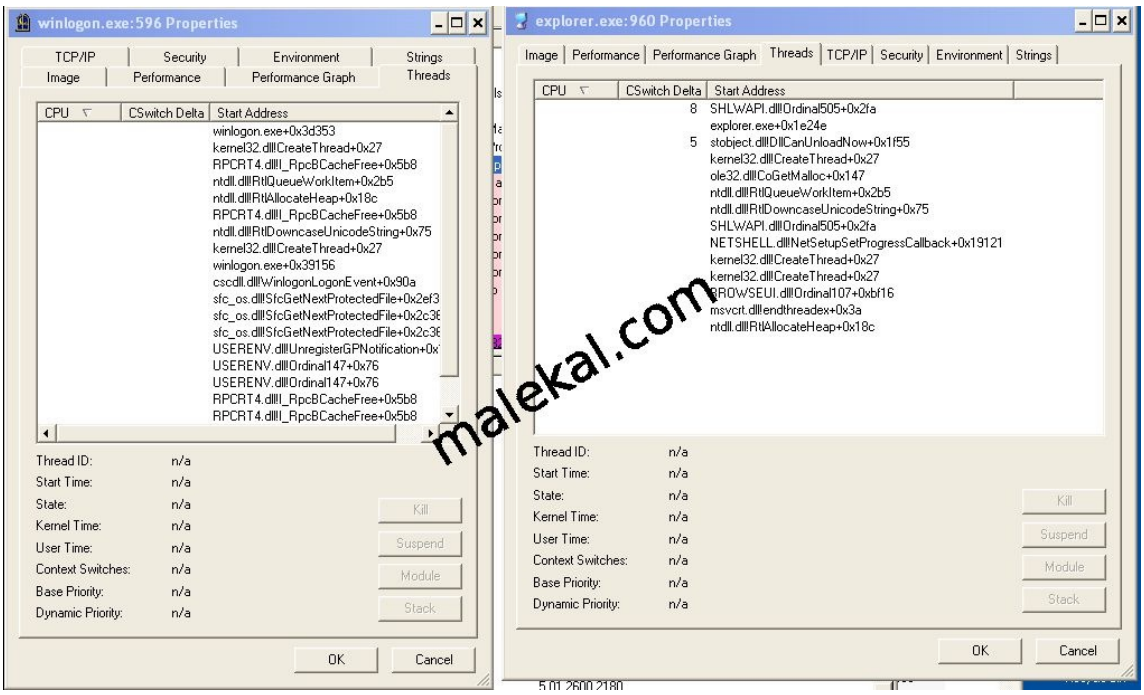
tranquillement.

Les DLL sont actives au seins des processus Winlogon.exe et Explorer.exe ce qui signifie qu'un thread est démarré pour que les DLL puissent faire leur boulot (en outre vous ouvrir des popups de publicités).

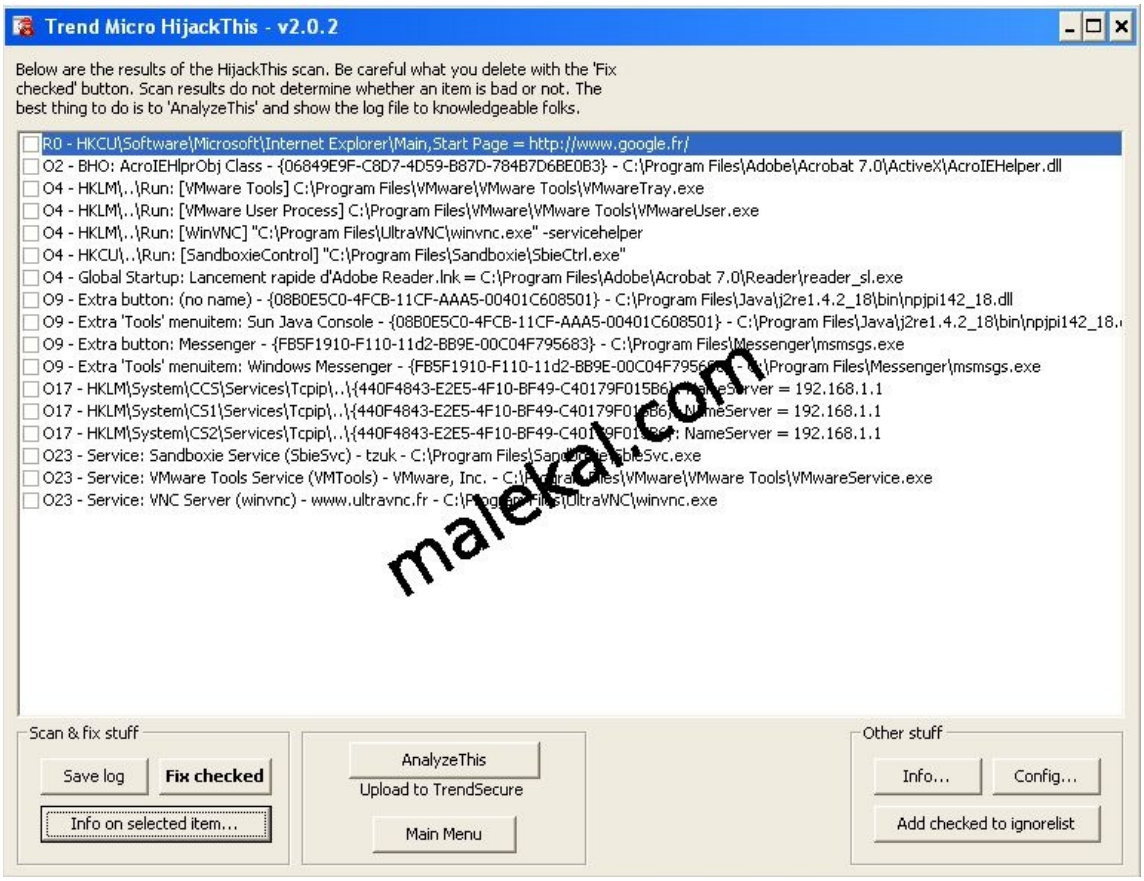
Process Explorer nous le montre bien :



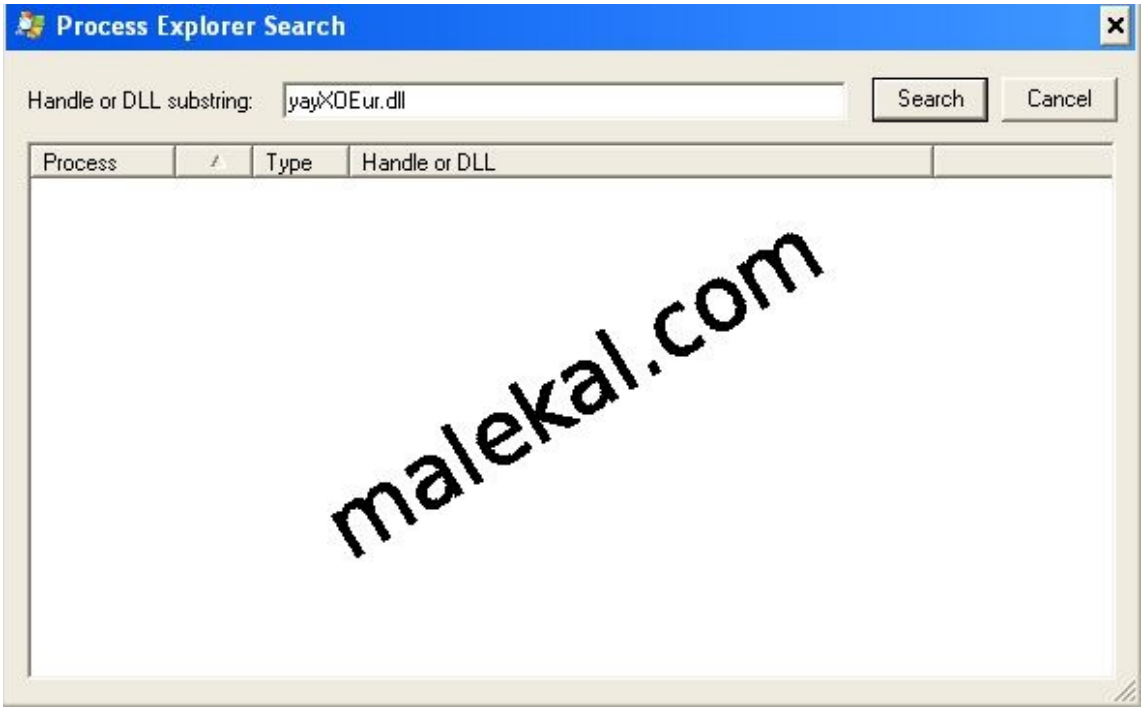
Il nous suffit alors d'arreter ces threads pour rendre l'infection inactive, ceci via le bouton Kill.



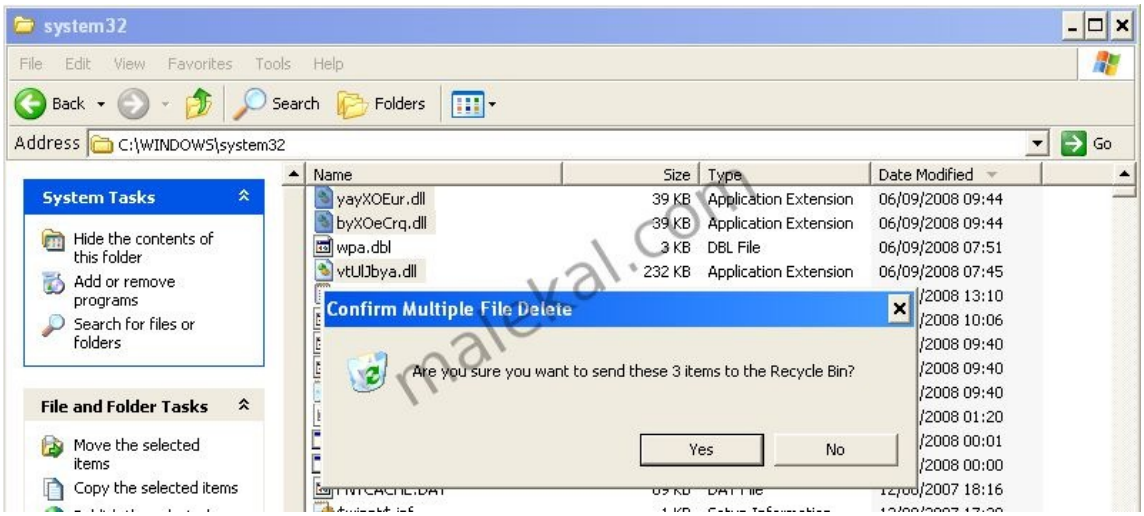
On détruit ensuite les points de chargements de l'infection via HijackThis en fixant les lignes (bouton Fix Checked).
Ô miracle, les lignes ne reviennent pas!

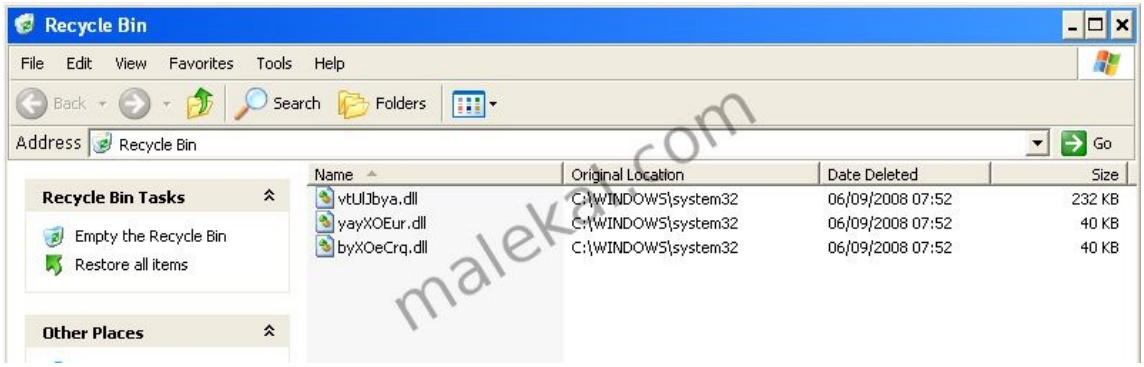


Les DLL sont encore chargées dans les processus mais inactives, il nous faut redémarrer le système.
Plus de point de chargement, plus rien sur Process Explorer.... plus d'infection active :



Il n'y a plus qu'à utiliser notre meilleur alliée pour terminer le boulot, c'est à dire le bouton Supprimer de votre clavier pour envoyer nos amis à la corbeille.





Conclusion

Cette page nous montre bien que Process Explorer peux s'avérer être un outil puissant à utiliser avec précaution.

Ceci nous montre aussi qu'n 4 lignes, il est possible de supprimer une infection qui pose de gros problèmes à de nombreux internautes.
Et ceci sans antivirus/antispywares.