Tutorial GMER

GMER est un des meilleurs scanner rootkit. Voici donc un tutorial pour GMER démystifier le programme.

Quelques liens relatifs à Gmer et Rootkit :

- Le danger et fonctionnement des Rootkits
- Gmer – Scanner Rootkit efficace »>Fiche de GMER dans les programmes utiles
- Les Anti-Rootkit / Scanner Rootkit
- Supprimer les rootkits sous Windows

DISLAIMER : *GMER est un outil puissant…*

Cette page est destinée aux personnes ayant un minimum de connaissance sur le fonctionnement de Windows. Si vous n'avez pas de connaissances, n'utilisez pas GMER.

Ce n'est pas la peine de scanner avec GMER et demander de l'aide sur le forum pour analyser le rapport.
On utilise pas un programme si on ne comprend pas le rapport ou pour le plaisir ou par excès de paranoïa.

Téléchargement de GMER

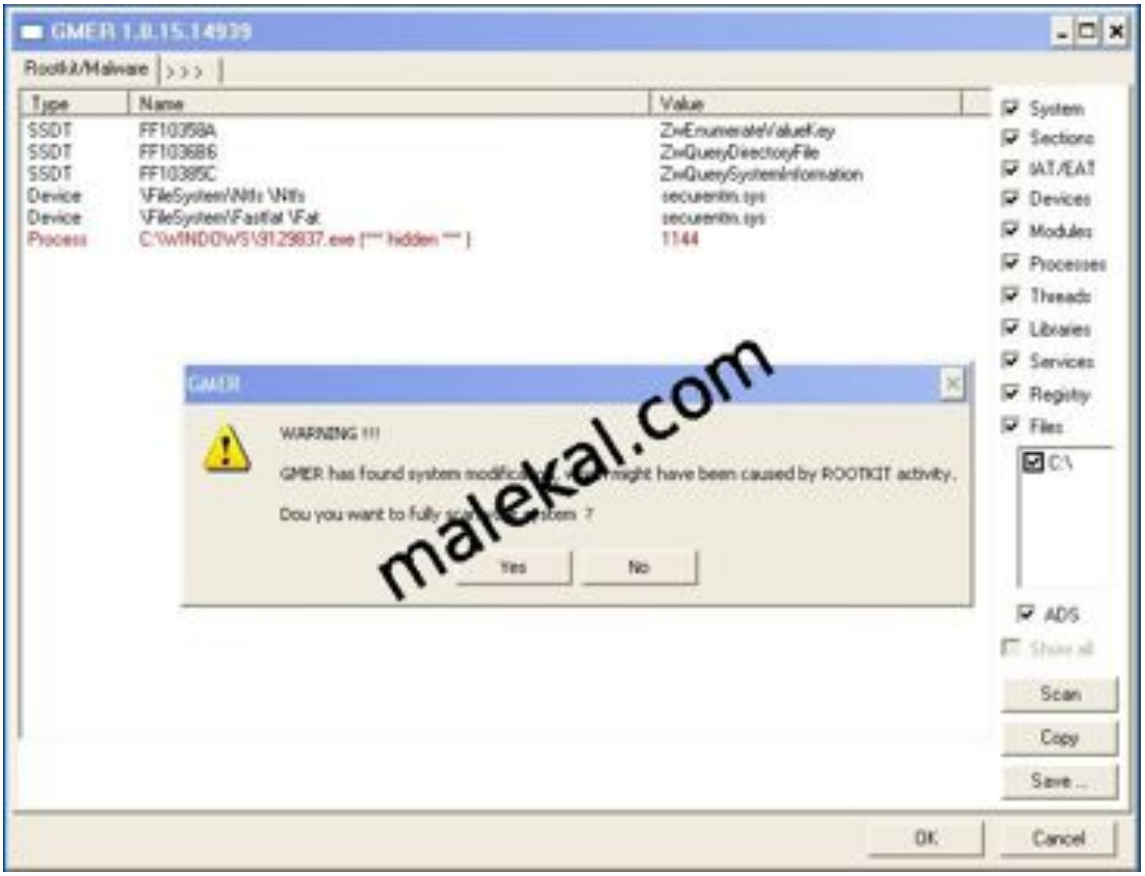
L'adresse du site officiel de GMER est : http://www.gmer.net

Le téléchargement du programme se fait à partir du menu *Files* à gauche.

GMER est disponible au format ZIP (*gmer.zip*) ou via un EXE avec un nom aléatoire (*Download EXE)*, ceci permet l'exécution sur des PC avec des infections bloquant l'exécution de fichiers portant le nom GMER.

Avant toute utilisation de GMER, veuillez désactiver votre antivirus, antispyware sous peine de vous prendre un BSOD.

L'exécution de GMER se fait simplement en double-cliquant sur le fichier téléchargé. Le programme se lance alors… si un rootkit est détecté dès le lancement du programme, une popup vous en informe.



Onglet GMER

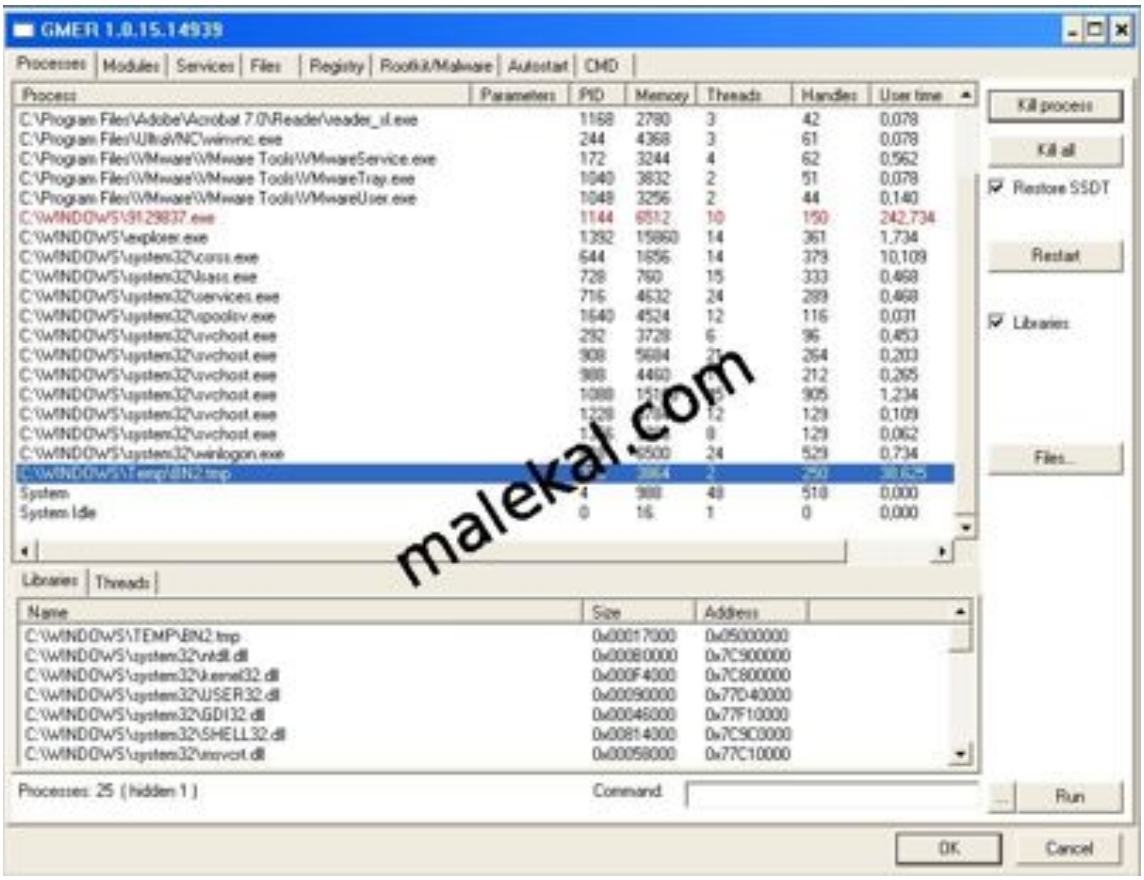
Processes

L'onglet Processes permet de lister les processus démarrés et éventuellement afficher les processus considérés comme rootkités.
Les boutons :

- *Kill Process* permet de tuer le processus sélectionné
- *Kill All* tue tous les processus et services, Windows ne tourne alors qu'avec le stric minimum (voir application plus bas).
- *Restart* redémarre l'ordinateur (à utiliser après Kill All par exemple)
- *Files* permet de naviguer dans les dossiers pour démarrer une application.

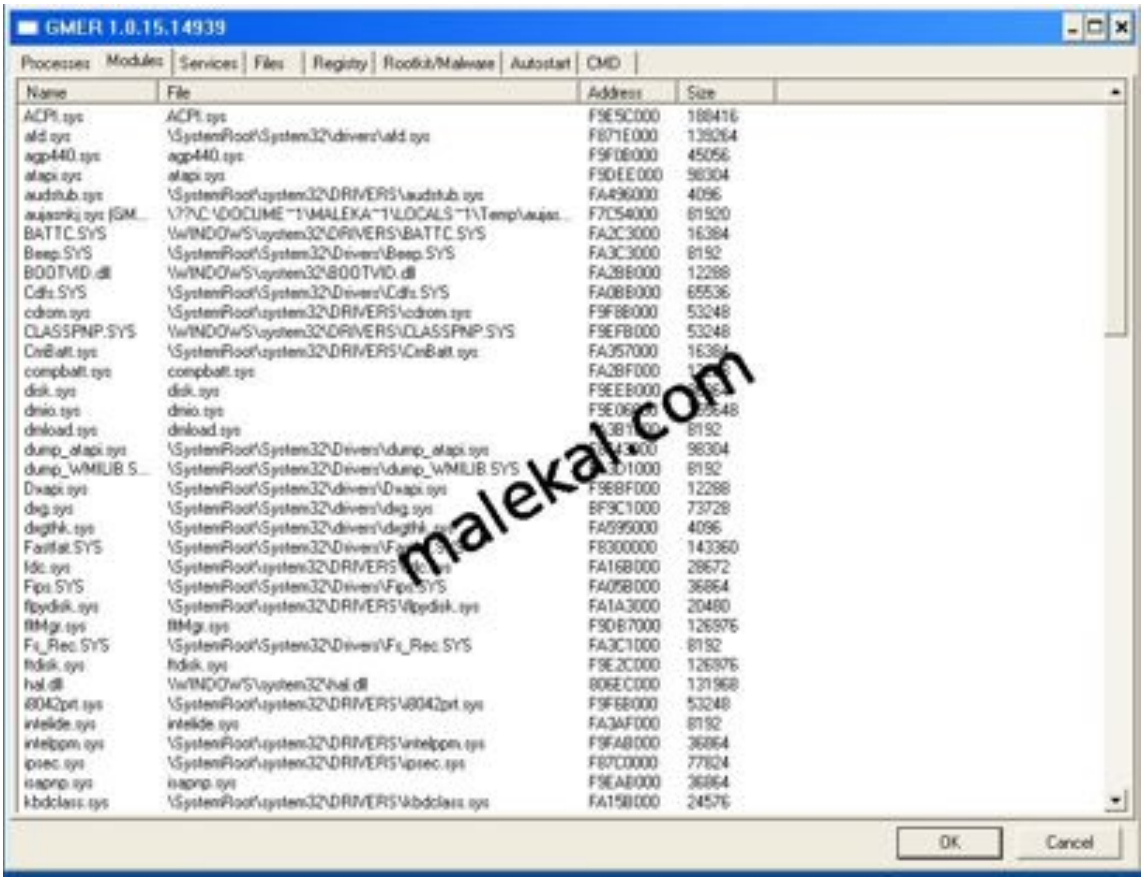
Dans la partie basse GMER affiche les libraries et Thread (si le

bouton Libraries à droite est coché).
GMER ne permet pas de manipuler ces derniers, Process Explorer permet cela, reportez-vous à la page virtumonde VS Process Explorer



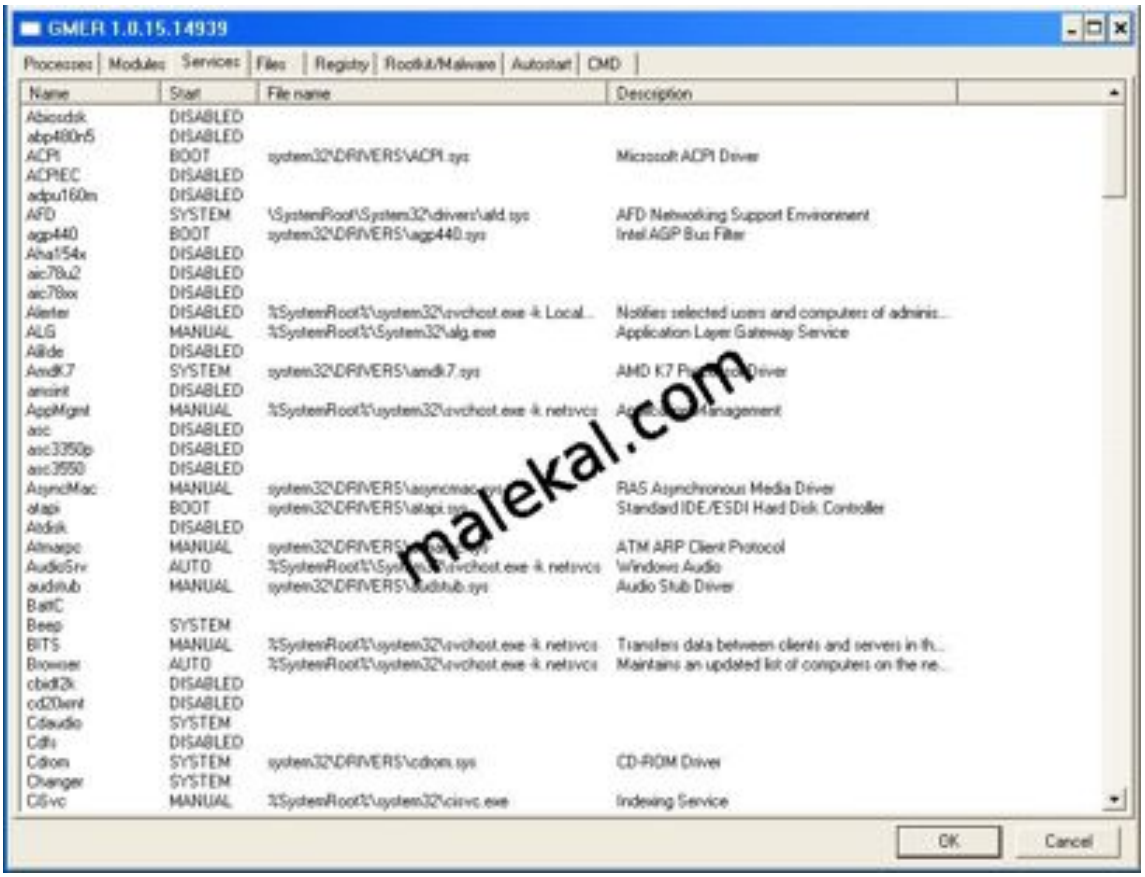
Modules

Affiche les modules chargés dans le kernel Windows. Aucune opération n’est possible, ceci est une fenêtre de consultation.

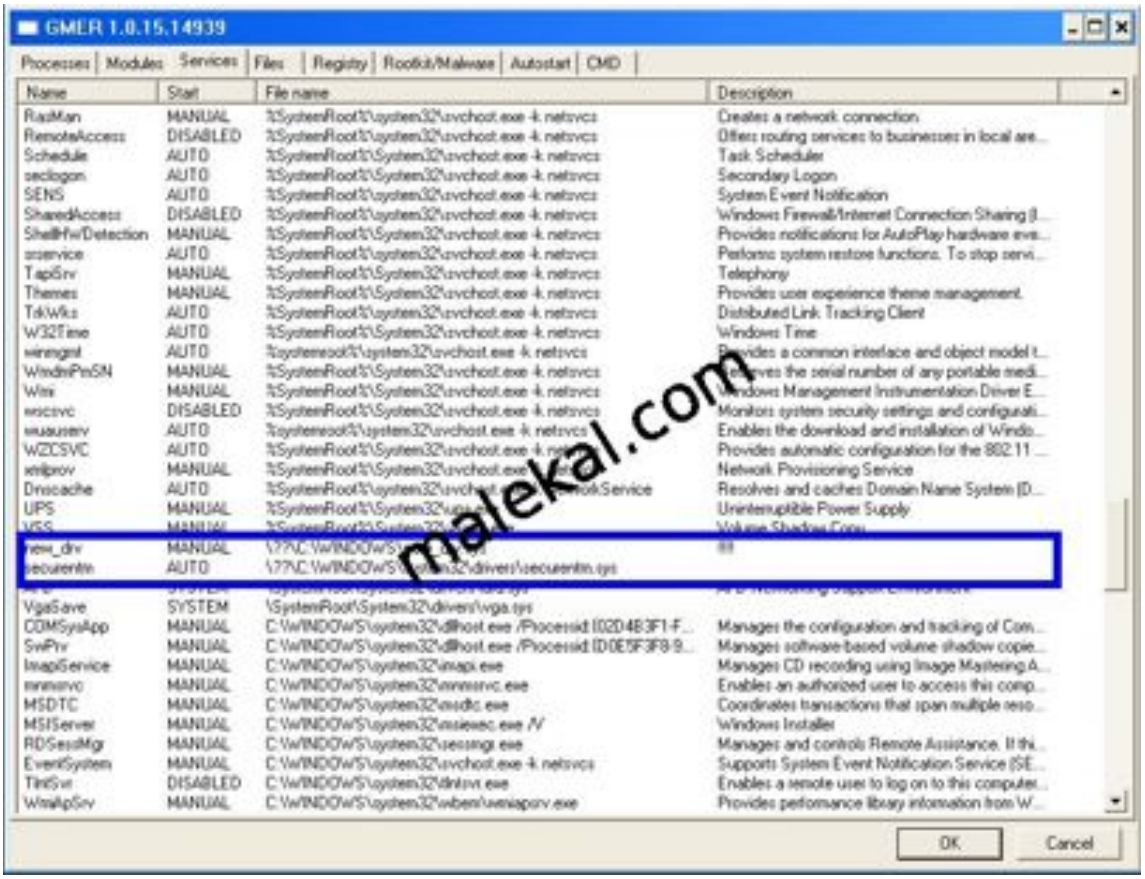


Services

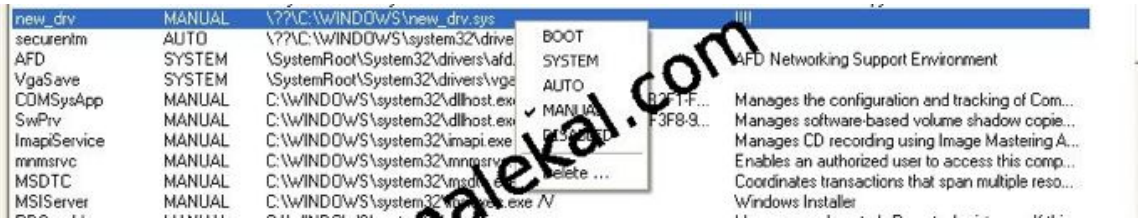
Liste les services, le mode de démarrage (colonne Start), le driver et la description. Pour plus d’informations sur les services Windows, se rendre à la page Dossier sur les processus et les services Windows



Voici deux services appartenant à des rootkits (plus d'infos sur new_drv.sys/Trojan-PSW.Win32.Small.bs)



Un clic droit sur le service sélectionné permet de modifier le mode de démarrage (AUTO, MANUAL, DISABLED etc)… ou supprimer (bouton Delete)

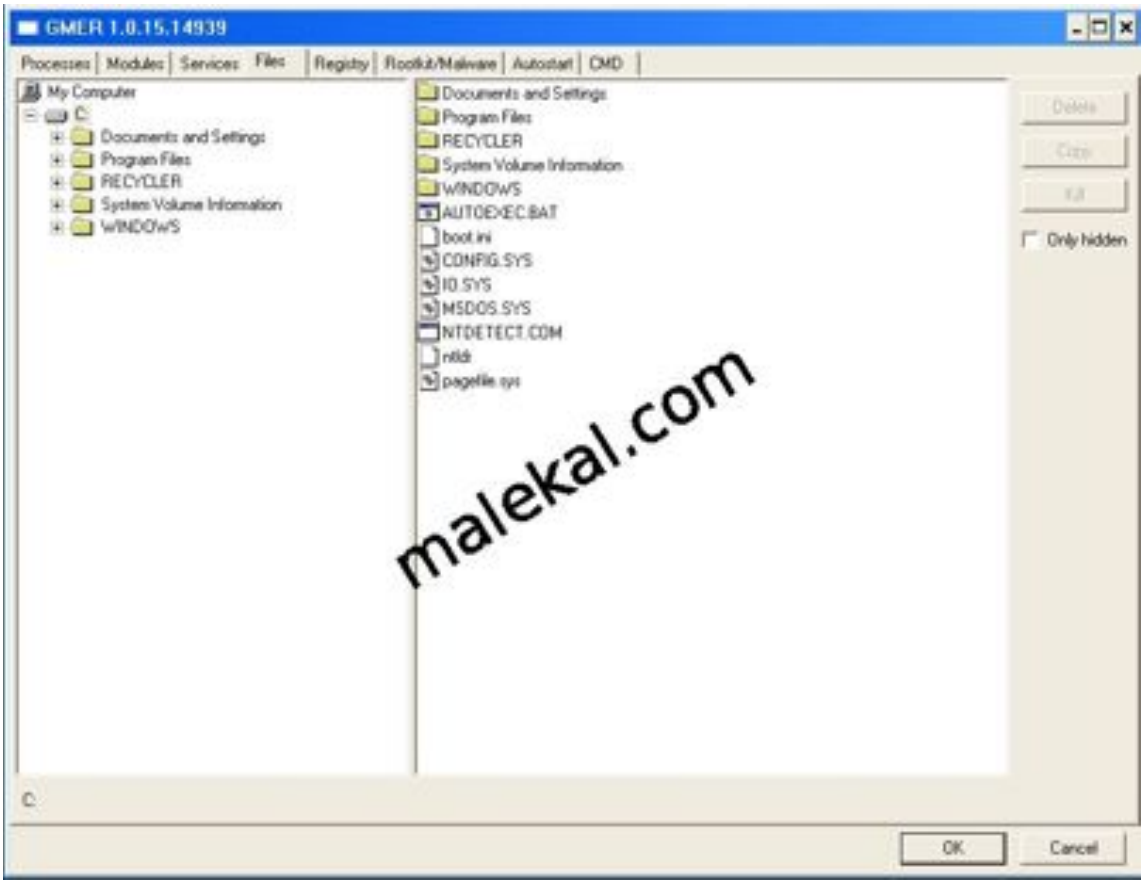


mais bien souvent cela ne fonctionne pas et GMER affiche un message d'erreur. La suppression d'un service appartenant à un rootkit ne peut se faire si ce dernier est actif sur le système (se reporter plus bas).

Files

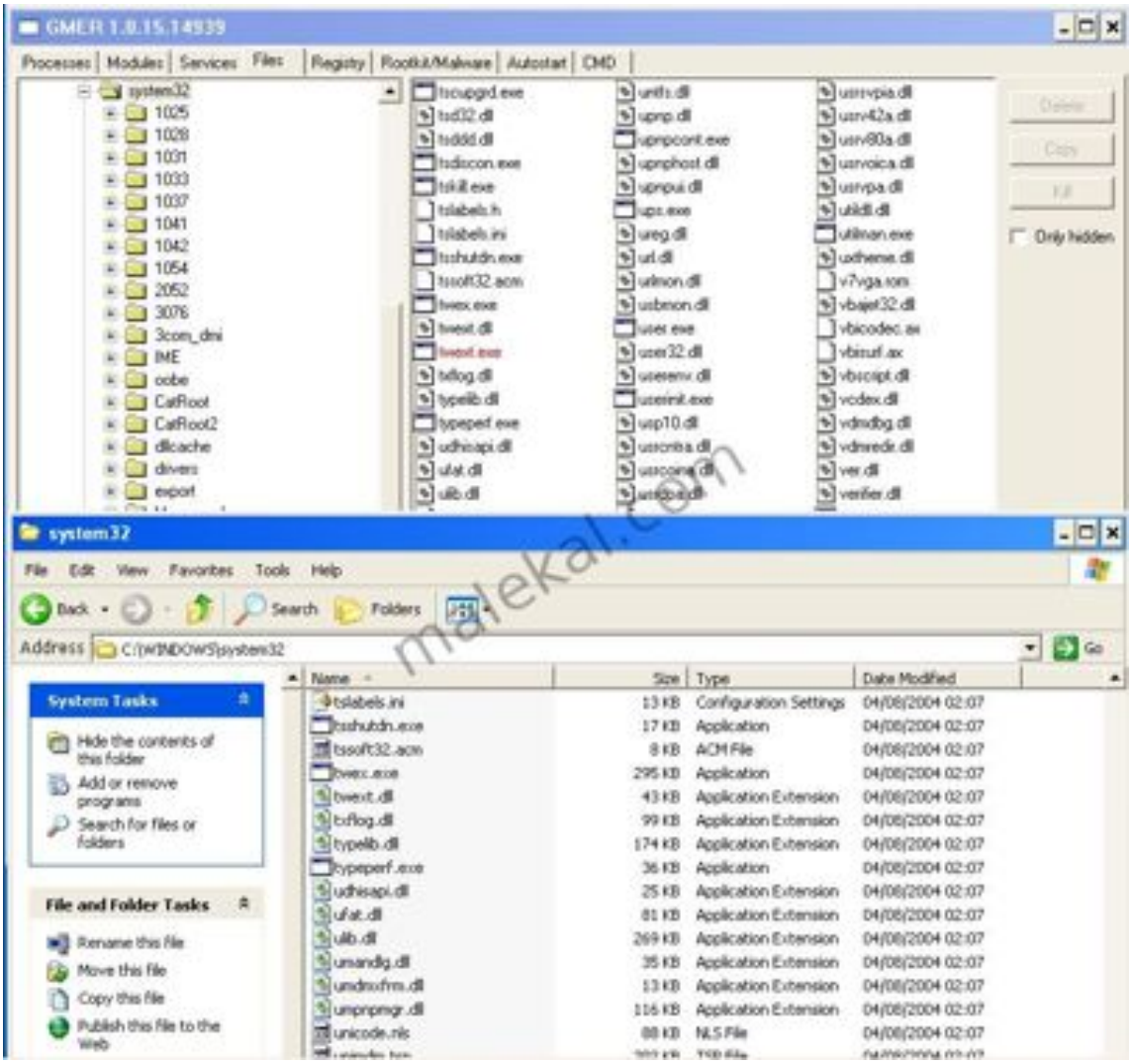
L'onglet Files est un explorateur de fichiers qui permet en autre d'afficher des fichiers rootkités. Les boutons :

- *Delete :* Supprime le fichier sélectionné
- *Copy :* Copie le fichier sélectionné (ce qui peut être pratique pour récupérer un fichier rootkité)
- *Kill :* Détruit la structure du PE, le fichier n'est pas supprimé mais endommagé, il devient alors non exécutable (erreur Win32 lors de l'exécution).



Dans la capture ci-dessous, le fichier twext.exe (variante Trojan.Zbot/Zeus) est rouge car il est rootkité.
Si vous jetez un coup d'oeil à l'explorateur de fichiers plus bas, vous verrez que ce dernier n'apparaît pas, il est donc caché de l'utilisateur et du système.

Le bouton *Only Hidden* permet d'afficher que les fichiers considérés comme rootkités (en rouge).



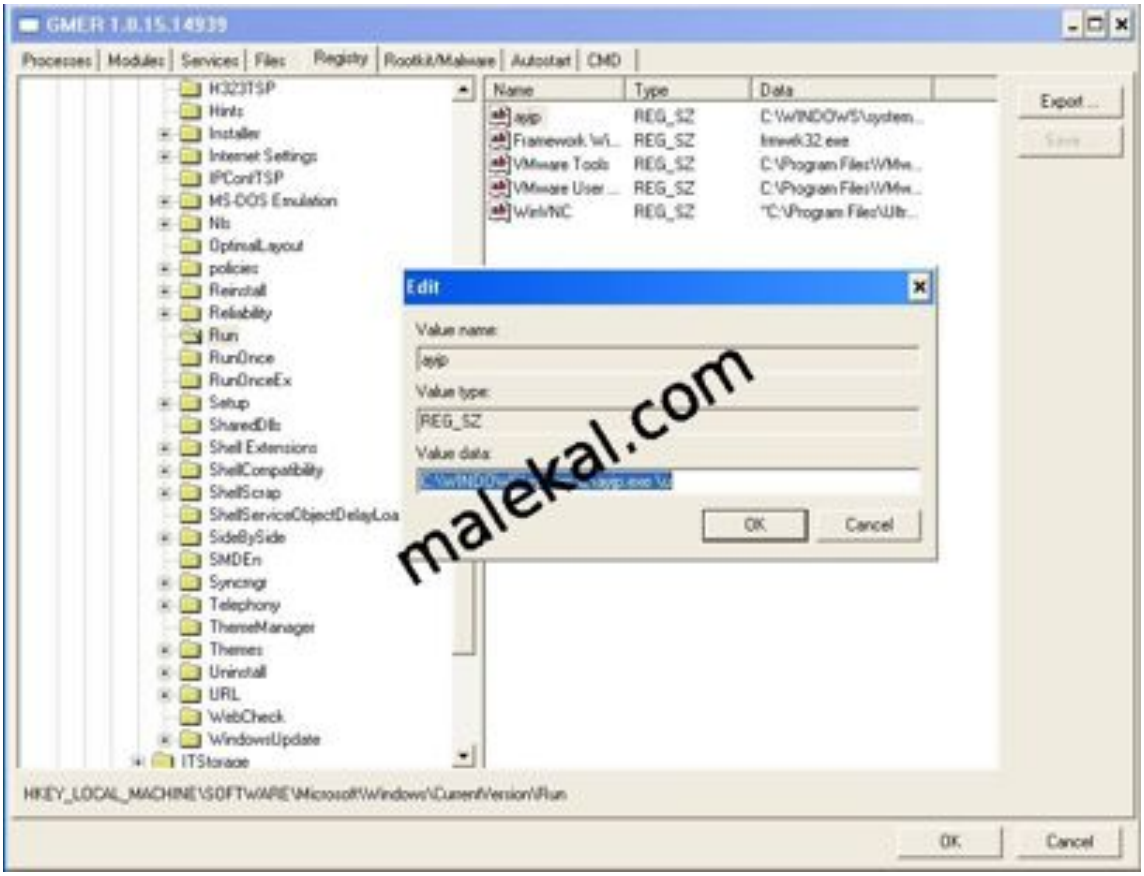
Registry

De même que l'onglet Files, GMER intègre un éditeur du registre Windows qui permet aussi de visualiser les clefs du registre rootkitées.

Le bouton *Export* permet d'exporter une clef vers un fichier reg. En double-cliquant sur une clef, il est possible de modifier les valeurs, la clef se grise et vous devez cliquer sur le bouton *Save* à droite pour enregistrer les modifications.

NOTE : J'ai déjà planté un ordinateur en effectuant des modifications du registre Windows via GMER (voir la FAQ Microsoft : Comment faire pour récupérer Windows XP à partir d'un Registre endommagé qui empêche le démarrage du

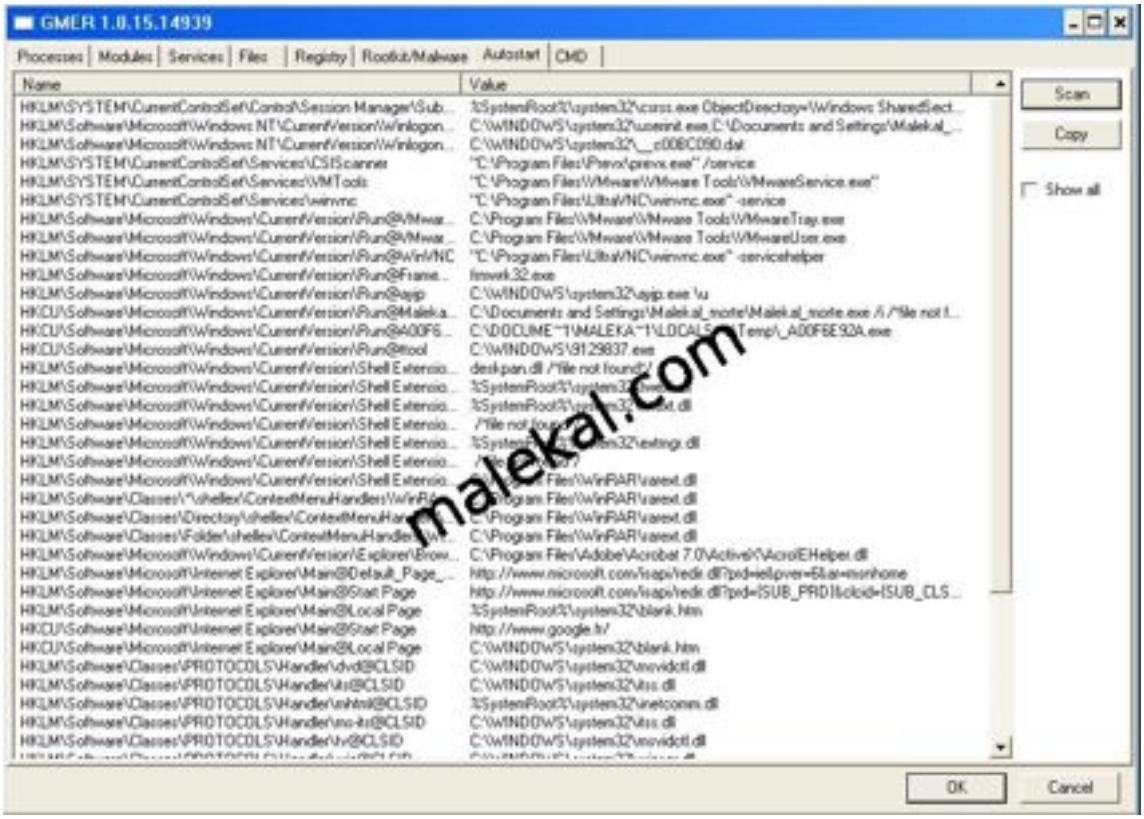
système). Avant de jouer avec GMER, il est conseillé de faire une copie du registre (dossier C:\Windows\System32config) ou un export via ERUNT (se reporter au tutorial ERUNT)



AutoStart

Liste les divers points de chargement du registre Windows et leurs contenus.

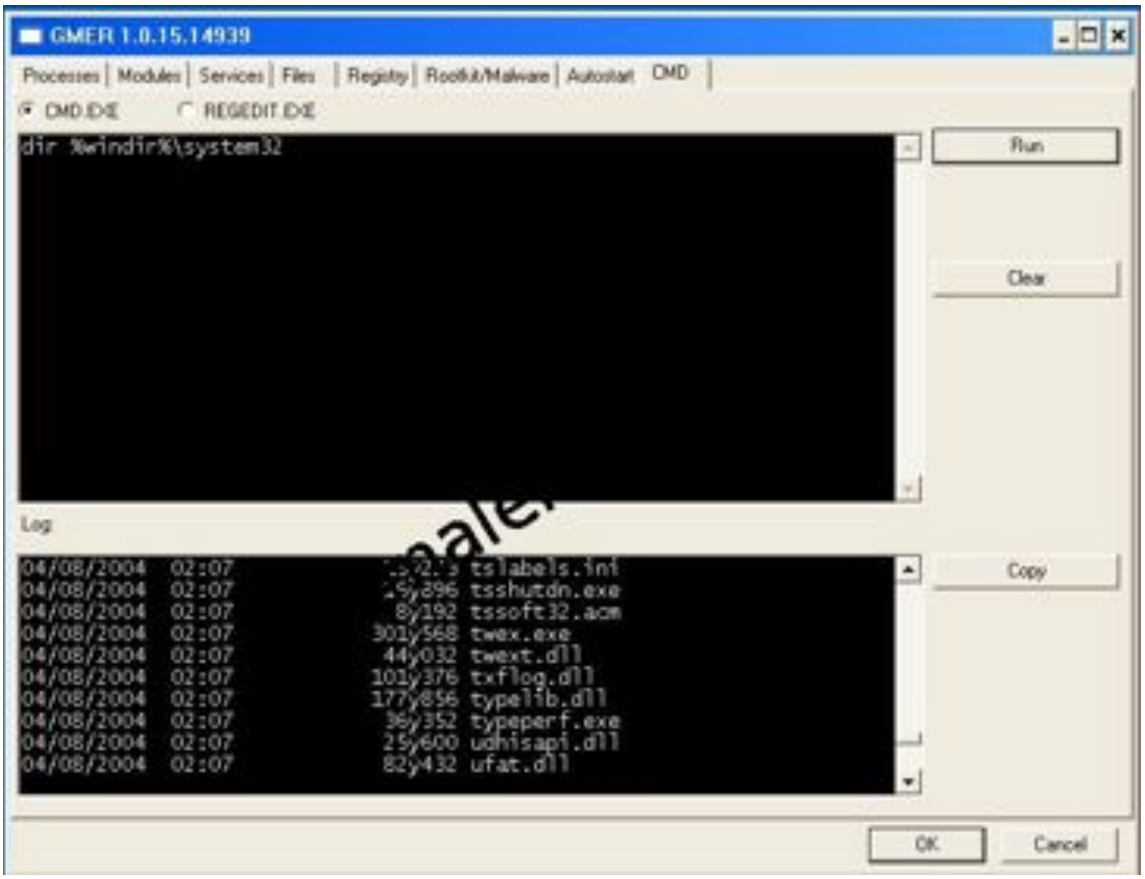
Le bouton *Copy* permet d'effectuer un copier/coller du contenu du rapport.



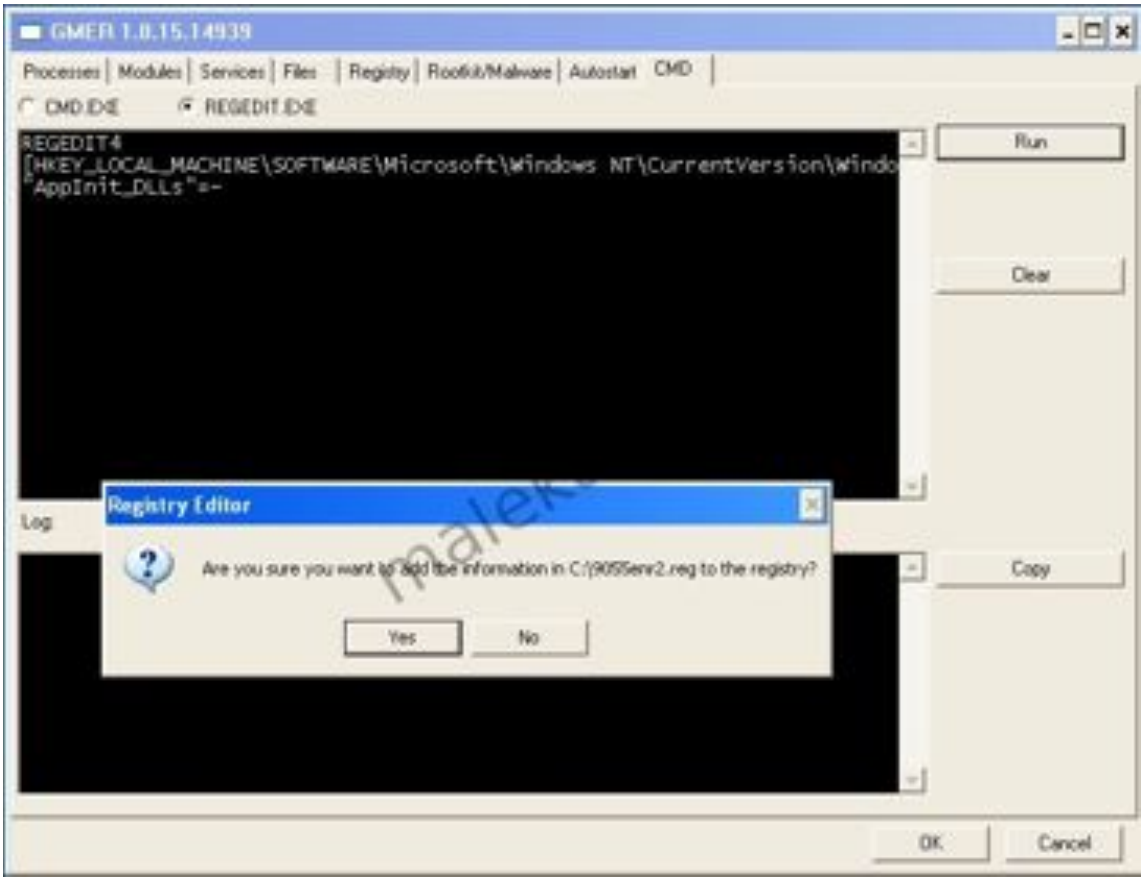
CMD

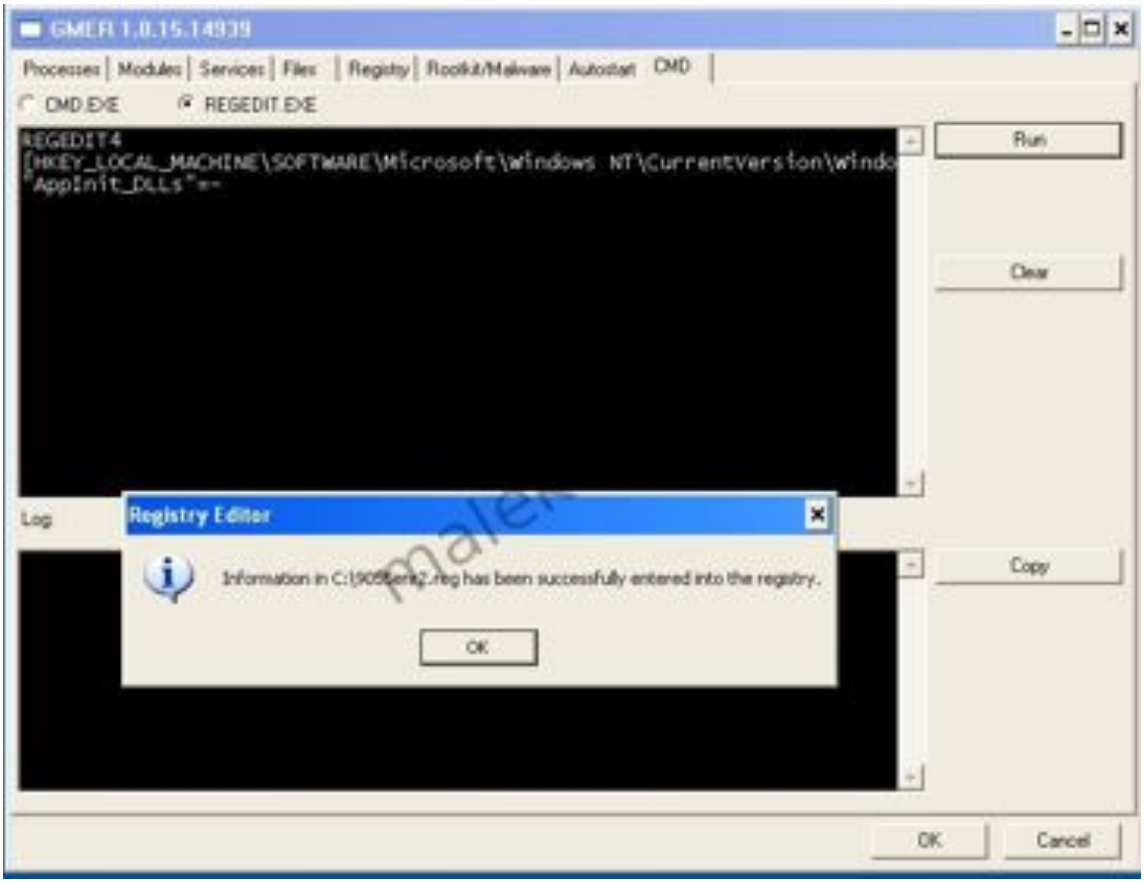
L'onglet CMD permet d'exécuter des commandes CMD lorsque l'onglet CMD.EXE est coché.

Tapez la commande dans la partie haute et cliquez dur *Run* à droite, le résultat de la commande apparaît dans la partie basse de la fenêtre.
Le bouton *Copy* permet de récupérer le résultat dans un copier/coller.



En cochant l'onget *REGEDIT.EXE*, il est possible d'exécuter des commandes reg pour modifier le registre Windows.





Scanner Rootkit de GMER

L'onglet Rootkit/Malware permet de lancer un scan anti-rootkit.

Dans la partie droite, vous pouvez choisir les éléments du système à scanner (IE/EAT, Modules, processus, Registre etc). Notez que pour les fichiers, vous pouvez déterminer les partitions à scanner. Eventuellement ne scanner que la partition système pour gagner du temps.

Les informations sur le scan s'affichent alors, les éléments détectés comme rootkit apparaissent en rouge dans chaque section.

Le bouton *Copy* permet de récupérer le résultat pour effectuer un copier/coller.
Le bouton *Save* permet l'enregistrement du rapport sur votre disque au format texte.

Voici quelques exemples de logs, encore une fois GMER peut afficher des informations sur des éléments légitimes puisque le rapport ne se contente pas de lister des éléments néfastes mais afficher les éléments chargés dans le système et surtout la manière dont ils se chargent… GMER peut donc lister des éléments néfastes comme des éléments légitimes.
Il convient donc d'effectuer une recherche sur le nom de fichier sur Google par exemple (voir le sujet Mieux Utiliser les moteurs de recherche), si vous avez un doute:

Exemple de SSDT Hook (les API apparaîssent à droite) :

SSDT SystemRootSystem32DRIVERSavpe32.sys ZwCreateProcess
SSDT SystemRootSystem32DRIVERSavpe32.sys ZwCreateProcessEx
SSDT SystemRootSystem32DRIVERSavpe32.sys ZwOpenProcess
SSDT SystemRootSystem32DRIVERSavpe32.sys ZwOpenThread
SSDT SystemRootSystem32DRIVERSavpe32.sys ZwQueryDirectoryFile
SSDT SystemRootSystem32DRIVERSavpe32.sys

ZwQuerySystemInformation

Certains programmes de sécurité peuvent effectuer des hook comme vsdatant.sys (ZoneAlarm), klif.sys (Kaspersky) etc.

Exemple de Devices…… ci-dessous des devices attachées aux drivers runtime2.sys (malware)

—- Devices – GMER 1.0.12 —-

Device FileSystemNtfs Ntfs IRP_MJ_CREATE [F82048FE] runtime2.sys
Device FileSystemNtfs Ntfs IRP_MJ_DIRECTORY_CONTROL [F820498A] runtime2.sys
Device DriverTcpip DeviceIp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys
Device DriverTcpip DeviceTcp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys
Device DriverTcpip DeviceUdp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys
Device DriverTcpip DeviceRawIp IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys
Device DriverTcpip DeviceIPMULTICAST IRP_MJ_DEVICE_CONTROL [F8D6EA92] runtime.sys
… et ici légitime vsdatant.sys étant le driver de ZoneAlarm

Device DriverTcpip DeviceIp IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys
Device DriverTcpip DeviceIp IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys
Device DriverTcpip DeviceTcp IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys
Device DriverTcpip DeviceTcp IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys

Device DriverTcpip DeviceUdp IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys
Device DriverTcpip DeviceUdp IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys
Device DriverTcpip DeviceRawIp IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys
Device DriverTcpip DeviceRawIp IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys
Device DriverTcpip DeviceIPMULTICAST IRP_MJ_CLOSEIRP_MJ_READ [BA437E90] vsdatant.sys
Device DriverTcpip DeviceIPMULTICAST IRP_MJ_INTERNAL_DEVICE_CONTROL [BA437E90] vsdatant.sys
Device DriverAFD DeviceAfd IRP_MJ_CREATE [BA431B50] vsdatant.sys
Device DriverAFD DeviceAfd IRP_MJ_CLOSEIRP_MJ_READ [BA431B50] vsdatant.sys
Device DriverAFD DeviceAfd IRP_MJ_INTERNAL_DEVICE_CONTROL [BA431B50] vsdatant.sys

Inline Hook (en mode userland) faite par l'infection Haxdoor :

User code sections :
.text C:WINDOWSgmer.exe[504] ntdll.dll!LdrLoadDll 7C9161CA 5 Bytes JMP 00010016
.text C:WINDOWSgmer.exe[504] USER32.dll!GetDlgItemTextA + 2 77D8AC08 5 Bytes JMP 000102B3
.text C:WINDOWSgmer.exe[504] WS2_32.dll!gethostbyname + 2 71A54FD6 5 Bytes JMP 00010C14
.text C:WINDOWSgmer.exe[504] WININET.dll!InternetConnectA 771B44DB 5 Bytes JMP 00010F44
.text C:WINDOWSgmer.exe[504] WININET.dll!HttpOpenRequestA + 2 771B4AC7 5 Bytes JMP 000110B9
.text C:WINDOWSgmer.exe[504] WININET.dll!InternetOpenA + 2 771B6D2C 5 Bytes JMP 00011042
.text C:WINDOWSgmer.exe[504] WININET.dll!HttpSendRequestA

+ 2 771B76BA 5 Bytes JMP 10001000
C:\Windows\System32bmtdhh.dll

Exemple de log avec une librairie bmtdhh.dll cachée (hidden) chargée dans divers processus :

—- Processes – GMER 1.0.11 —-

*Process C:\Windows\System32winlogon.exe (*** hidden ***) 484*
*Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @*
C:\Windows\System32winlogon.exe [484] 0×10000000
*Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @*
C:WINDOWSgmer.exe [504] 0×10000000
*Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @*
C:\Windows\System32cmd.exe [672] 0×10000000
*Library C:\Windows\System32bmtdhh.dll (*** hidden ***) @*
C:\Windows\System32spoolsv.exe [1108] 0×10000000

Service considéré comme rootkité, le type de démarrage est indique entre [ ] :

—- Services – GMER 1.0.11 —-
Service C:\Windows\System32bmtdhk.sys [BOOT] bmtdhk <– ROOTKIT !!!

Fichiers considérés comme rootkités :

—- Files – GMER 1.0.11 —-

File C:\Windows\System32bmtdhh.dll
File C:\Windows\System32bmtdhk.sys <– ROOTKIT !!!
File C:\Windows\System32klgcptini.dat
File C:\Windows\System32rd.dll
File C:\Windows\System32rd.sys

File C:\Windows\System32st889.dat

spdt (Daemon Tools, Alchohol 120% etc)

Le cas spXX.sys où X sont des lettres aléatoires avec le service spdt – Les programmes Dameon Tools, Alcohol 120% etc installent un driver commençant par sp et un driver aléatoire. Beaucoup de scanner rootkit d'éditeur de sécurité détectent ce dernier comme étant un rootkit alors qu'il est tout à fait légitime.

Voici un rapport GMER complet :
http://www.malekal.com/fichiers/GMER/GMER_spdt.txt

Dans le rapport ci-dessus le driver est spjp.sys et le driver aléatoire est ascafl5y.SYS
On reconnait facilement ces derniers aux devices relatifs au SCSI :

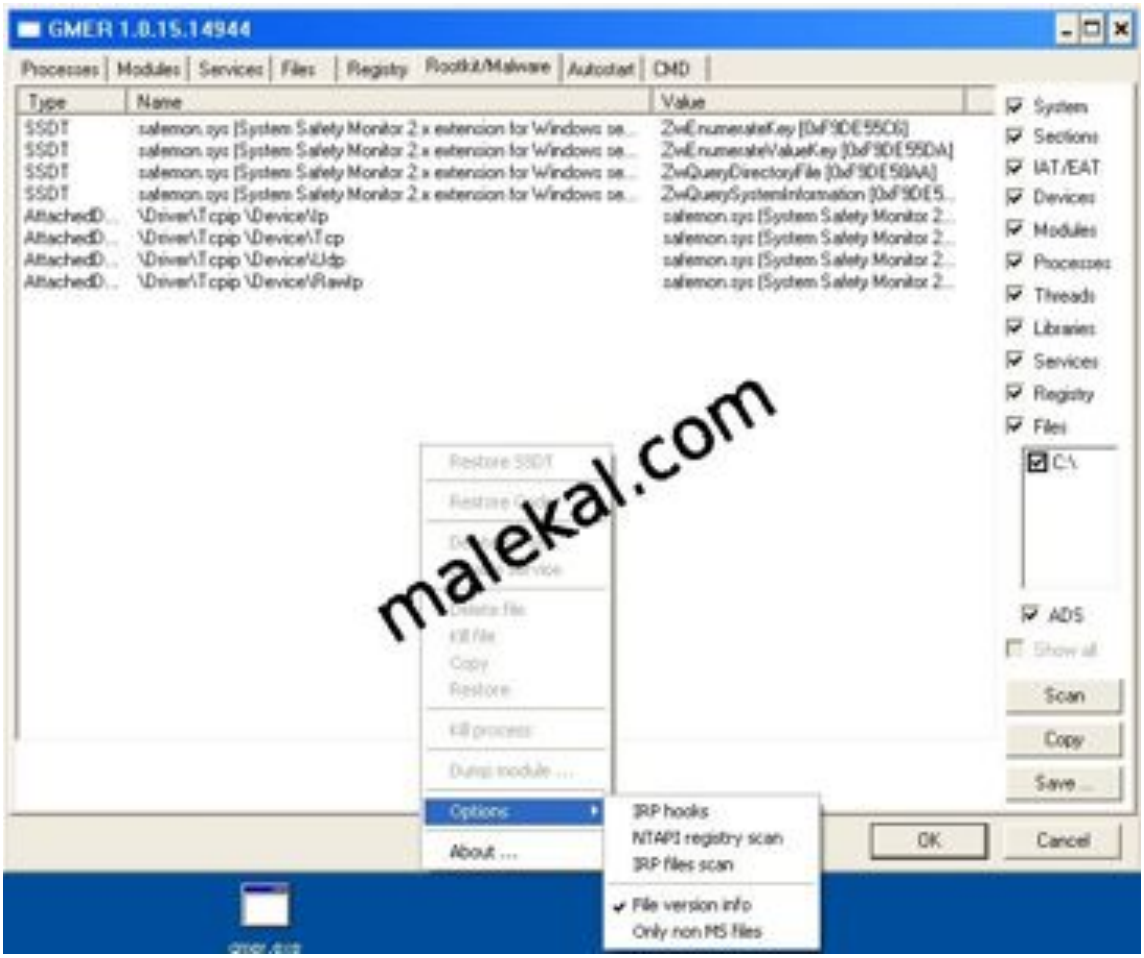
—- Devices – GMER 1.0.15 —-

Device Driversptd Device1875799320 spjp.sys
Device Driverascafl5y DeviceScsiascafl5y1Port3Path0Target0Lun0 82D171F8
Device Driverascafl5y DeviceScsiascafl5y1 82D171F8

En outre pour la partie Registry du scan GMER nous indique clairement entre parenthèses que le service spd appartient à Daemon Tools.

Type de Scan

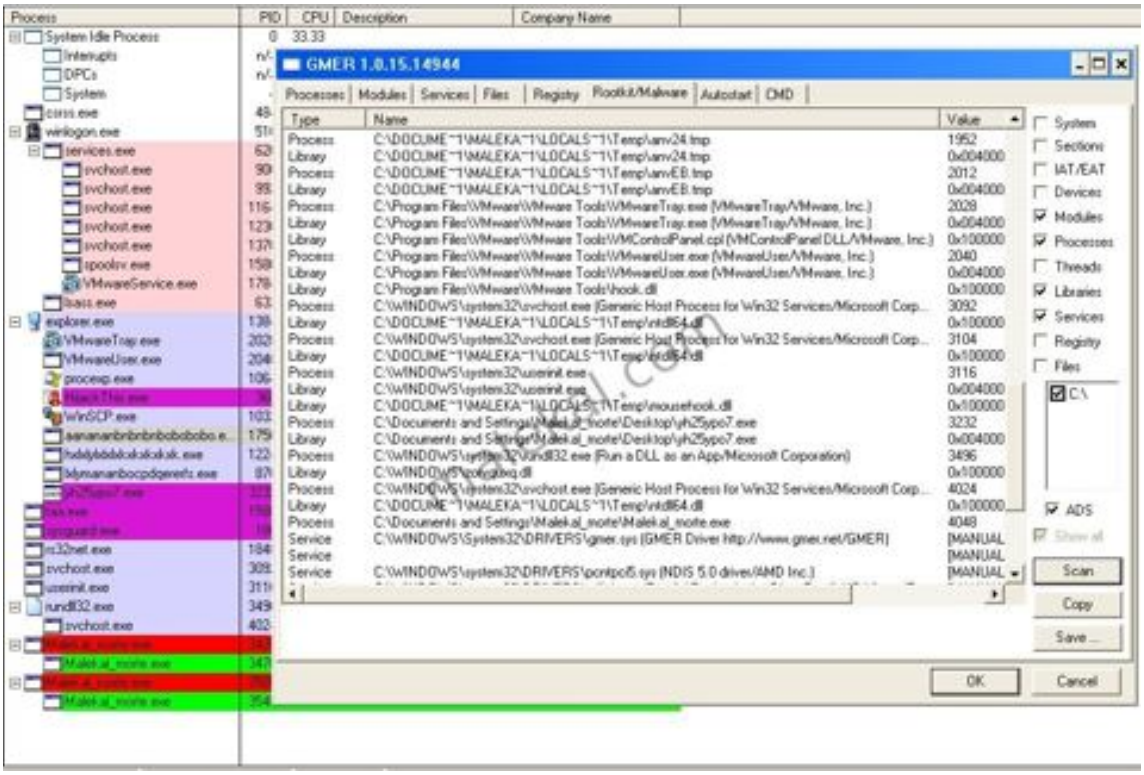
Dans l'onglet Rootkit/Malware en effectuant un clic droit sur la fenêtre, il est possible de choisir le type de scan.



La dernière option « *Only non MS files* » permet un scan rapide de l'ordinateur et ne lister que les fichiers non Microsoft.

Vous aurez donc aussi les fichiers de vos applications en cours d'exécution. Cela peut donner un rapide aperçu de ce qui tourne sur la machine et donc les malwares comme le montre la capture ci-dessus (pour un oeil averti).

L'avantage est que le scan dure 15s contrairement à un scan complet GMER mais permet tout de même de lister une bonne partie voire la totalié des malwares en cours d'exécution.



Suppression de Rootkit avec GMER

Se reporter à la page : Supprimer les Rootkits sous Windows

[Translate]