

## 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

**DISCLAIMER :** *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.*

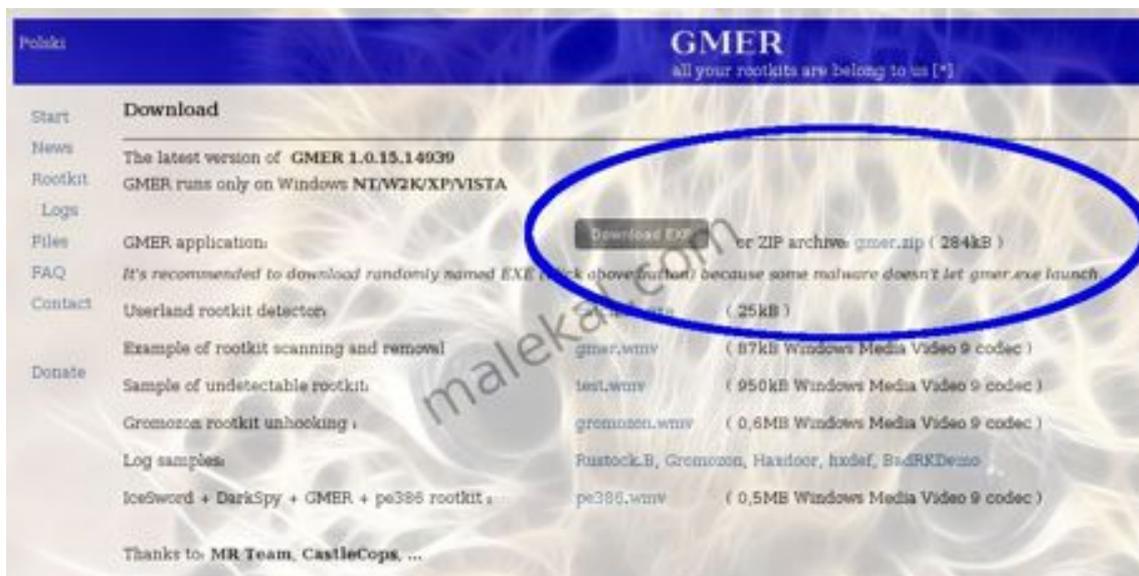
*On utilise pas un programme si on ne comprend pas le rapport ou pour le plaisir ou par excès de paranoïa.*

### Téléchargement de GMER

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

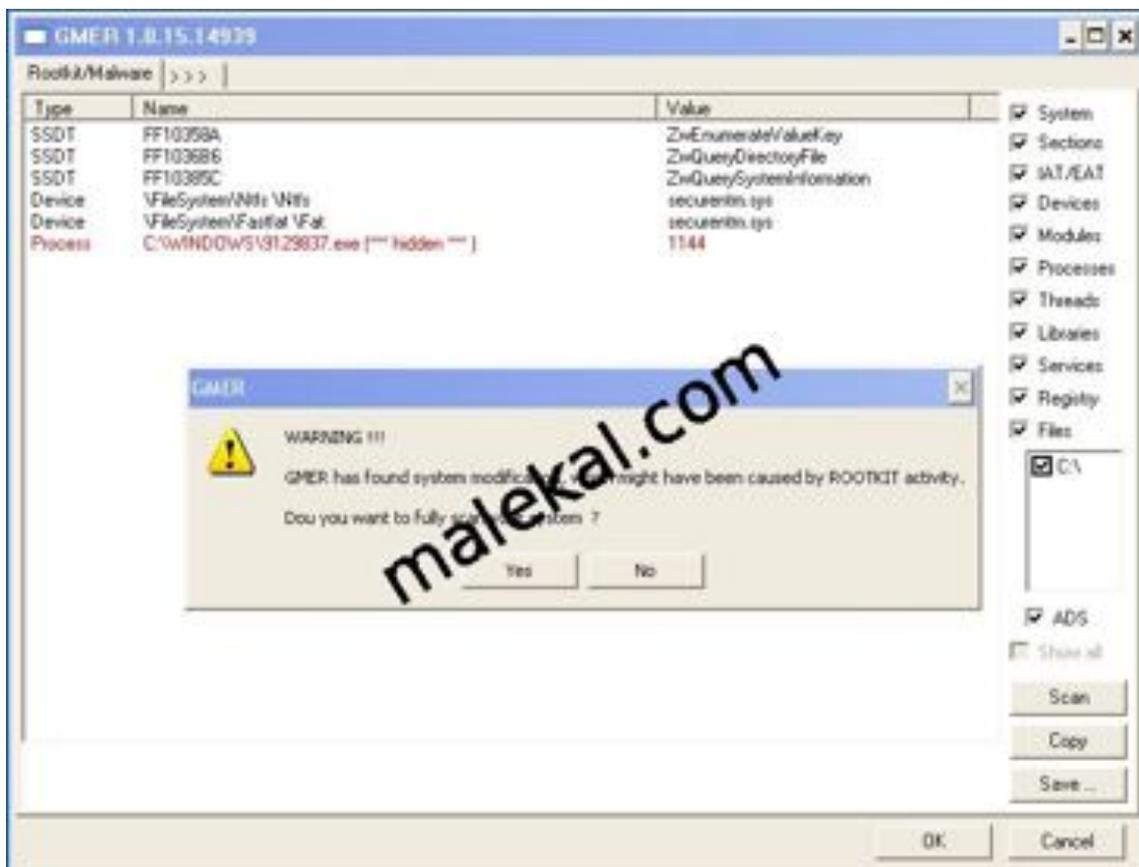
Le téléchargement du programme se fait à partir du menu *Files* à gauche.

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 strict 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.

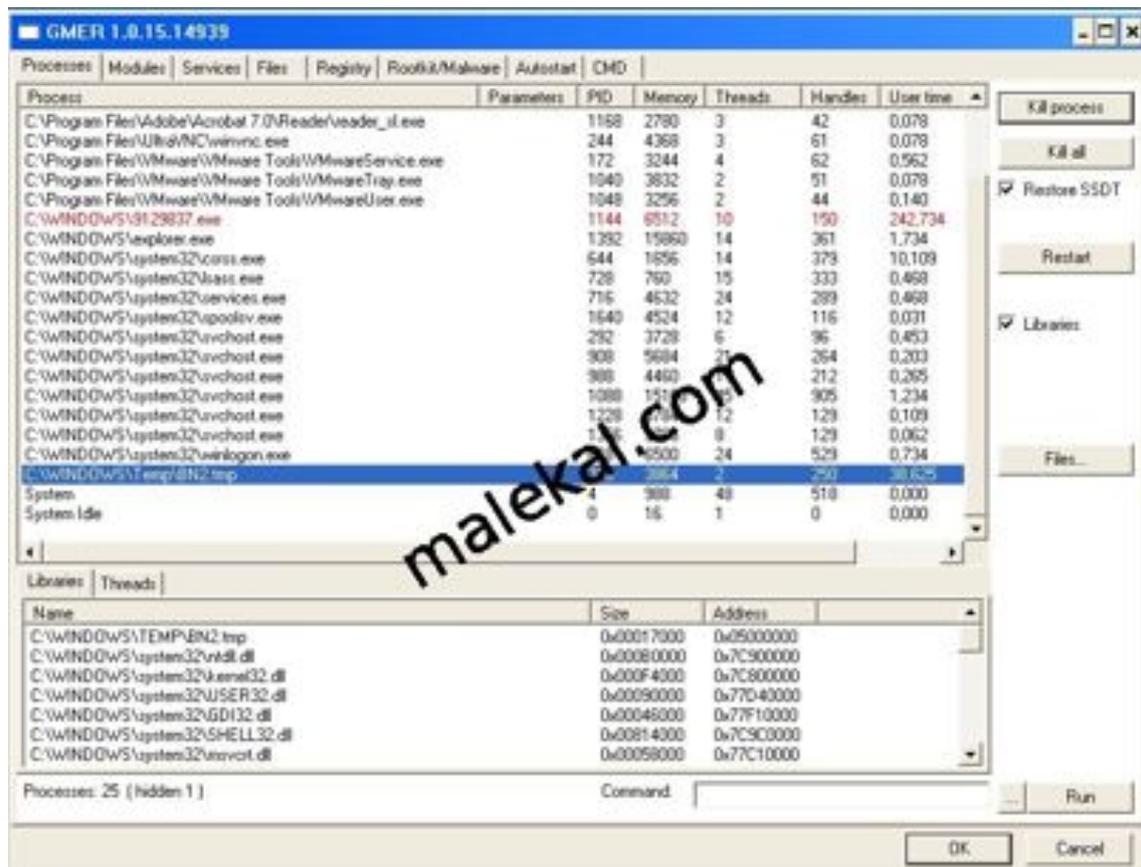
Dans la partie basse GMER affiche les librairies et Thread (si le

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



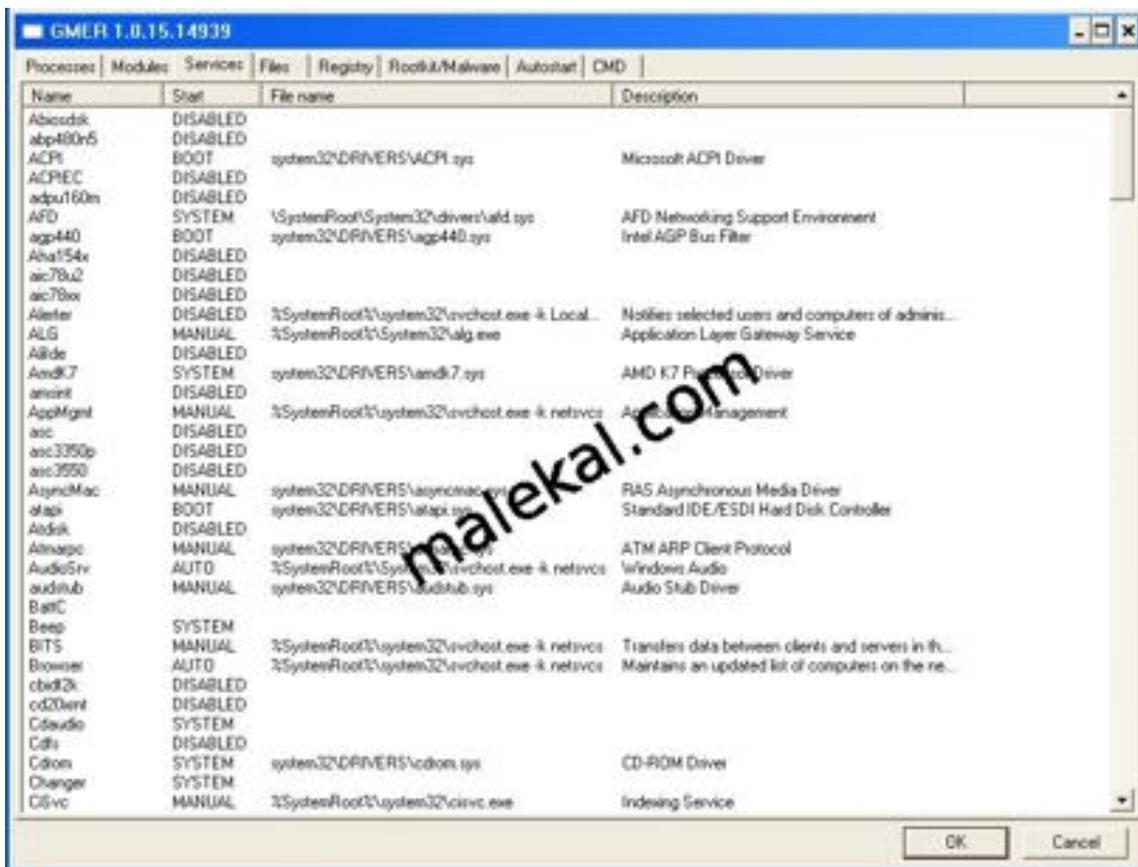
## Modules

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

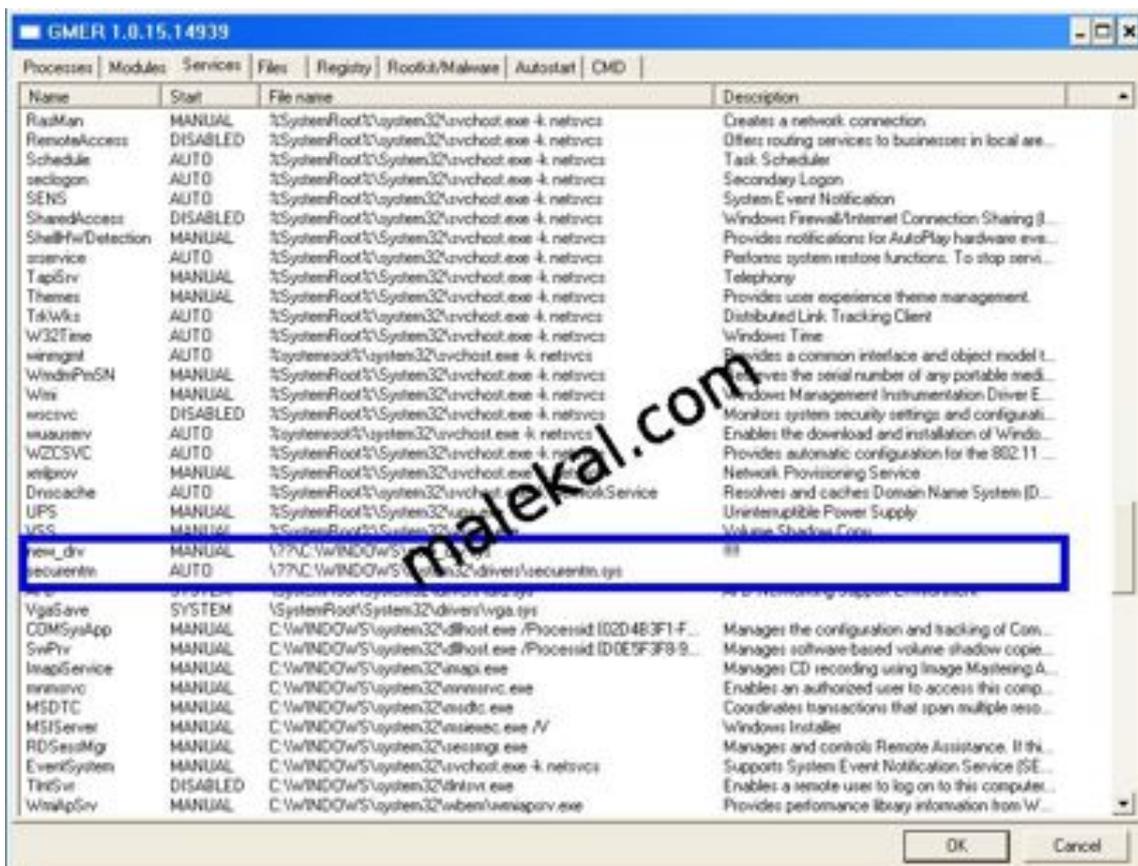
Name	File	Address	Size
ACPI.sys	ACPI.sys	F9E5C000	180416
afd.sys	\SystemRoot\System32\drivers\afd.sys	F871E000	139264
agp440.sys	agp440.sys	F9F0B000	45056
atapi.sys	atapi.sys	F9D EE 0000	98304
audhub.sys	\SystemRoot\System32\DRIVERS\audhub.sys	FA490000	4096
aujzsnk.sys (GM...	V:\?C:\DOCUMENT~1\MALEKA~1\LOCALS~1\Temp\aujz...	F7C54000	81920
BATT.C.SYS	W:\WINDOWS\System32\DRIVERS\BATT.C.SYS	FA2C3000	16384
Beep.SYS	\SystemRoot\System32\Drivers\Beep.SYS	FA3C3000	8192
BOOTVID.dll	W:\WINDOWS\System32\BOOTVID.dll	FA2B8000	12288
Cdfs.SYS	\SystemRoot\System32\Drivers\Cdfs.SYS	FA0B8000	65536
cdrom.sys	\SystemRoot\System32\DRIVERS\cdrom.sys	F9F8B000	53248
CLASSPNP.SYS	W:\WINDOWS\System32\DRIVERS\CLASSPNP.SYS	F9E9B000	53248
CirBatt.sys	\SystemRoot\System32\DRIVERS\CirBatt.sys	FA357000	16384
compbatt.sys	compbatt.sys	FA2BF000	16384
disk.sys	disk.sys	F9EEB000	16384
dmio.sys	dmio.sys	F9E06000	13548
dmload.sys	dmload.sys	3B110000	8192
dump_atapi.sys	\SystemRoot\System32\Drivers\dump_atapi.sys	F9E13000	98304
dump_WMILIB.S...	\SystemRoot\System32\Drivers\dump_WMILIB.SYS	3D100000	8192
Dxapi.sys	\SystemRoot\System32\Drivers\Dxapi.sys	F9E8F000	12288
deg.sys	\SystemRoot\System32\Drivers\deg.sys	BF9C1000	73728
degthk.sys	\SystemRoot\System32\Drivers\degthk.sys	FA599000	4096
Fanfat.SYS	\SystemRoot\System32\Drivers\Fanfat.SYS	F8300000	143360
fdc.sys	\SystemRoot\System32\DRIVERS\fdc.sys	FA168000	28672
Fips.SYS	\SystemRoot\System32\Drivers\Fips.SYS	FA098000	36864
flpydisk.sys	\SystemRoot\System32\DRIVERS\flpydisk.sys	FA1A3000	20480
BMgr.sys	BMgr.sys	F50B7000	126976
Fx_Rec.SYS	\SystemRoot\System32\Drivers\Fx_Rec.SYS	FA3C1000	8192
fdisk.sys	fdisk.sys	F9E2C000	126976
hal.dll	W:\WINDOWS\System32\hal.dll	806EC000	131968
8042prt.sys	\SystemRoot\System32\DRIVERS\8042prt.sys	F9F8B000	53248
intelide.sys	intelide.sys	FA3AF000	8192
intelppm.sys	\SystemRoot\System32\DRIVERS\intelppm.sys	F9FAB000	36864
ipsec.sys	\SystemRoot\System32\DRIVERS\ipsec.sys	F87C0000	77824
isapnp.sys	isapnp.sys	F9EAB000	36864
kbdclass.sys	\SystemRoot\System32\DRIVERS\kbdclass.sys	FA158000	24576

## 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](http://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)



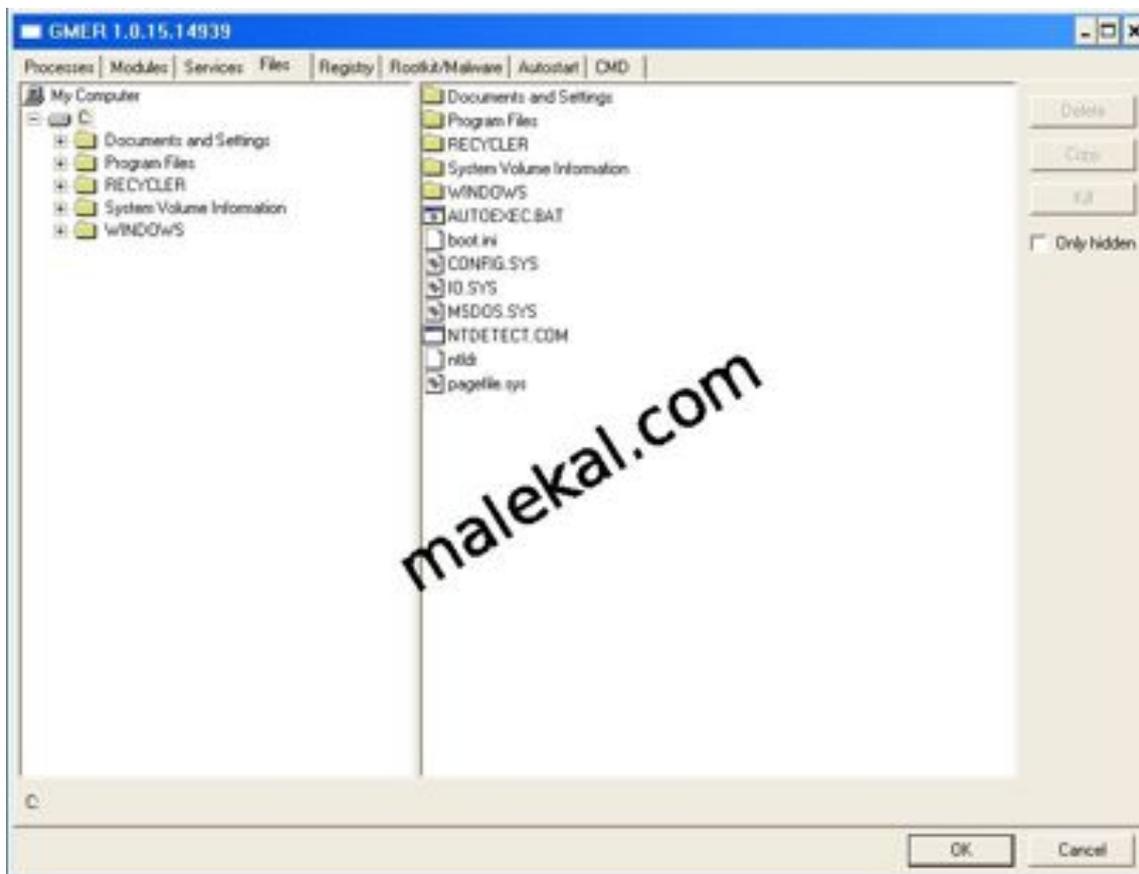
mais bien souvent cela ne fonctionne pas et GMER affiche un message d'erreur. La suppression d'un service appartenant à un rootkit ne peut se faire si ce dernier est actif sur le système (se reporter plus bas).



## Files

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

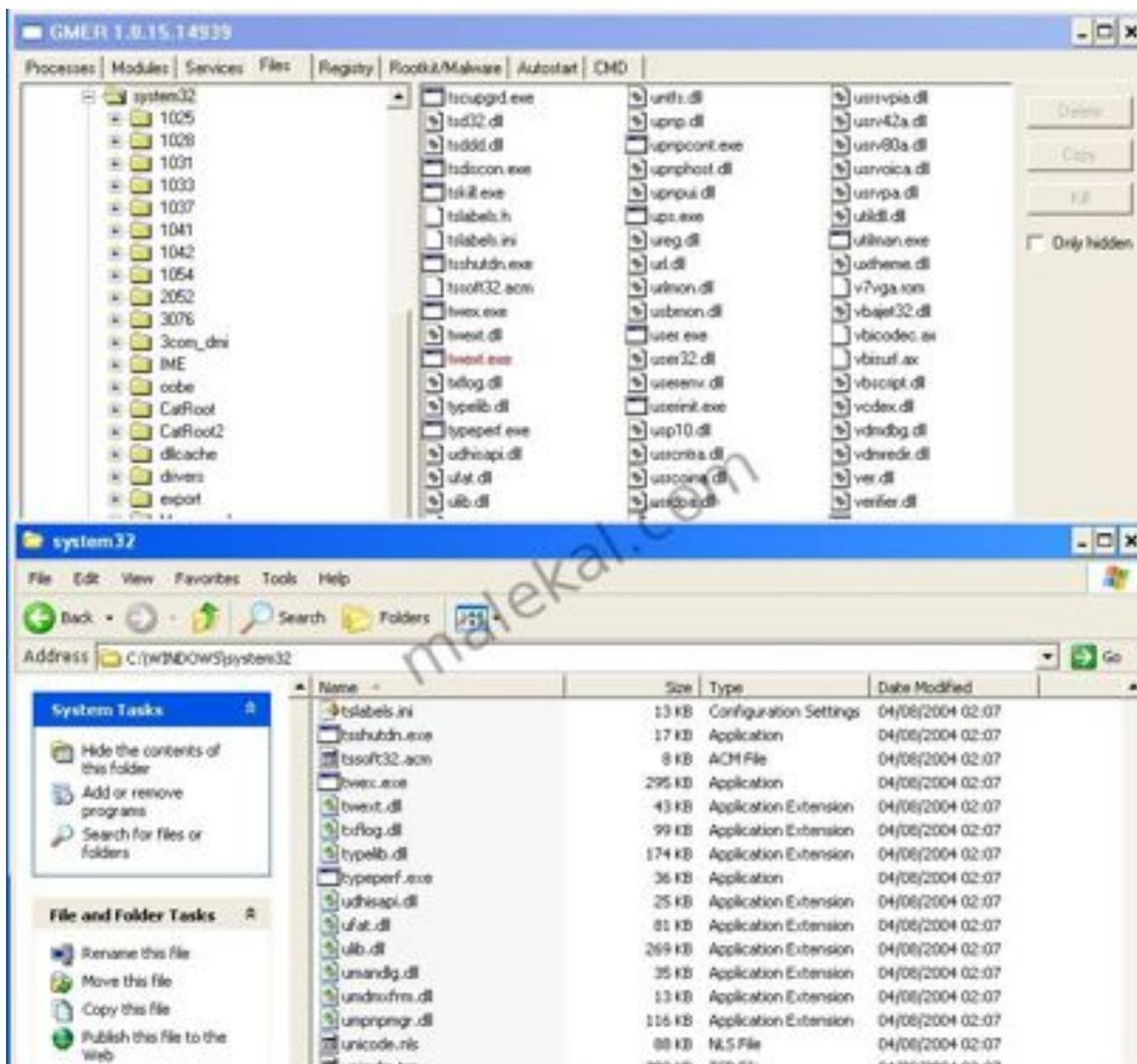
- *Delete* : Supprime le fichier sélectionné
- *Copy* : Copie le fichier sélectionné (ce qui peut être pratique pour récupérer un fichier rootkité)
- *Kill* : Détruit la structure du PE, le fichier n'est pas supprimé mais endommagé, il devient alors non exécutable (erreur Win32 lors de l'exécution).



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).



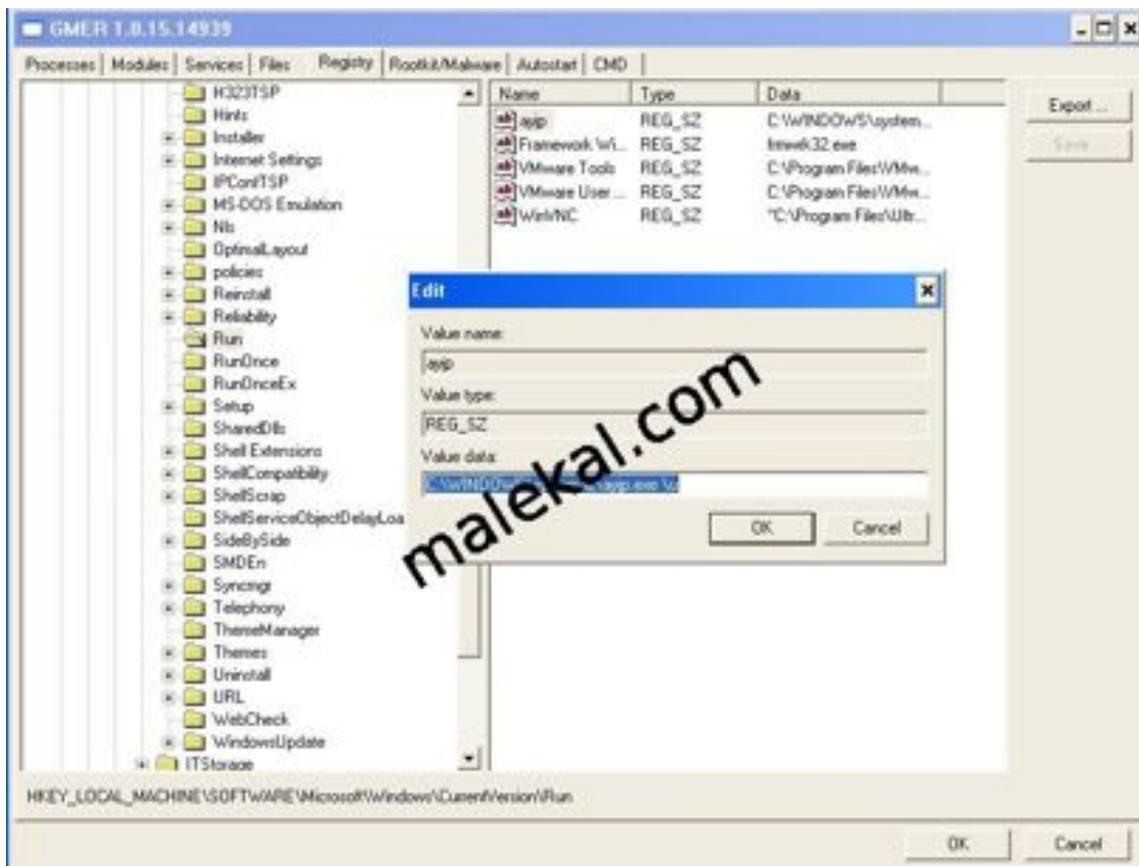
## Registry

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

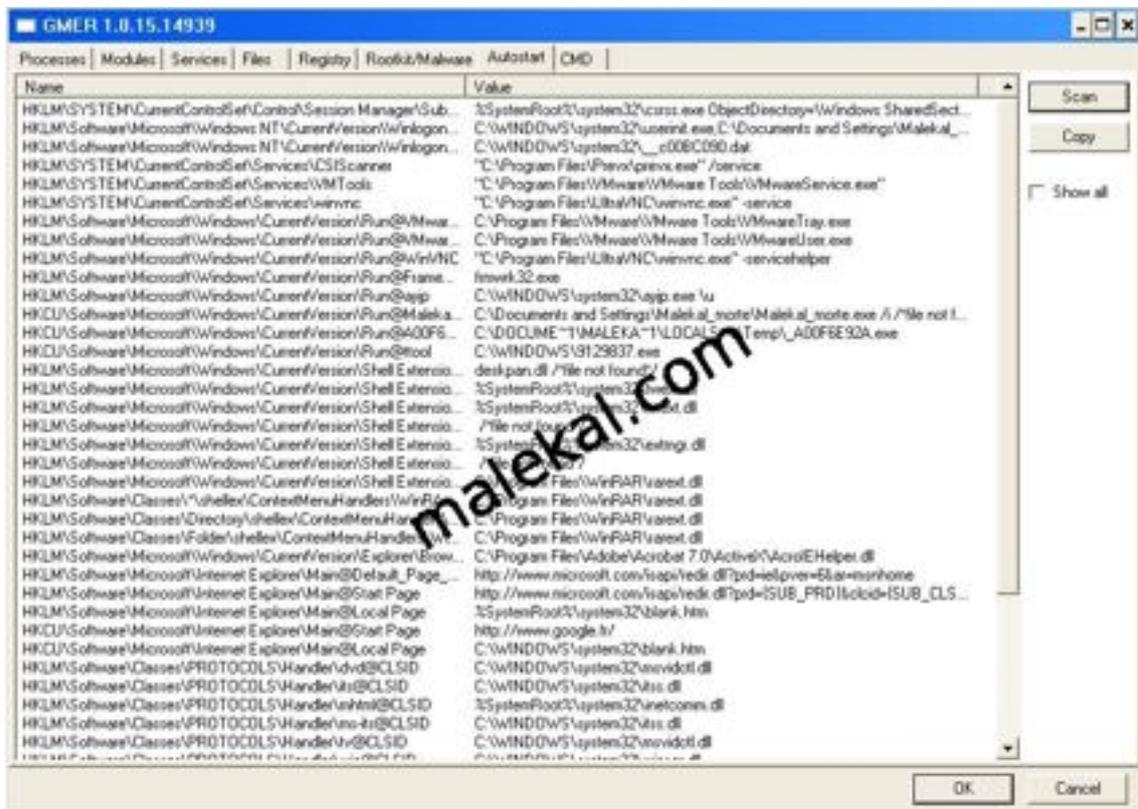
ystème). Avant de jouer avec GMER, il est conseillé de faire une copie du registre (dossier C:\Windows\System32config) ou un export via ERUNT (se reporter au tutorial ERUNT)



## 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.

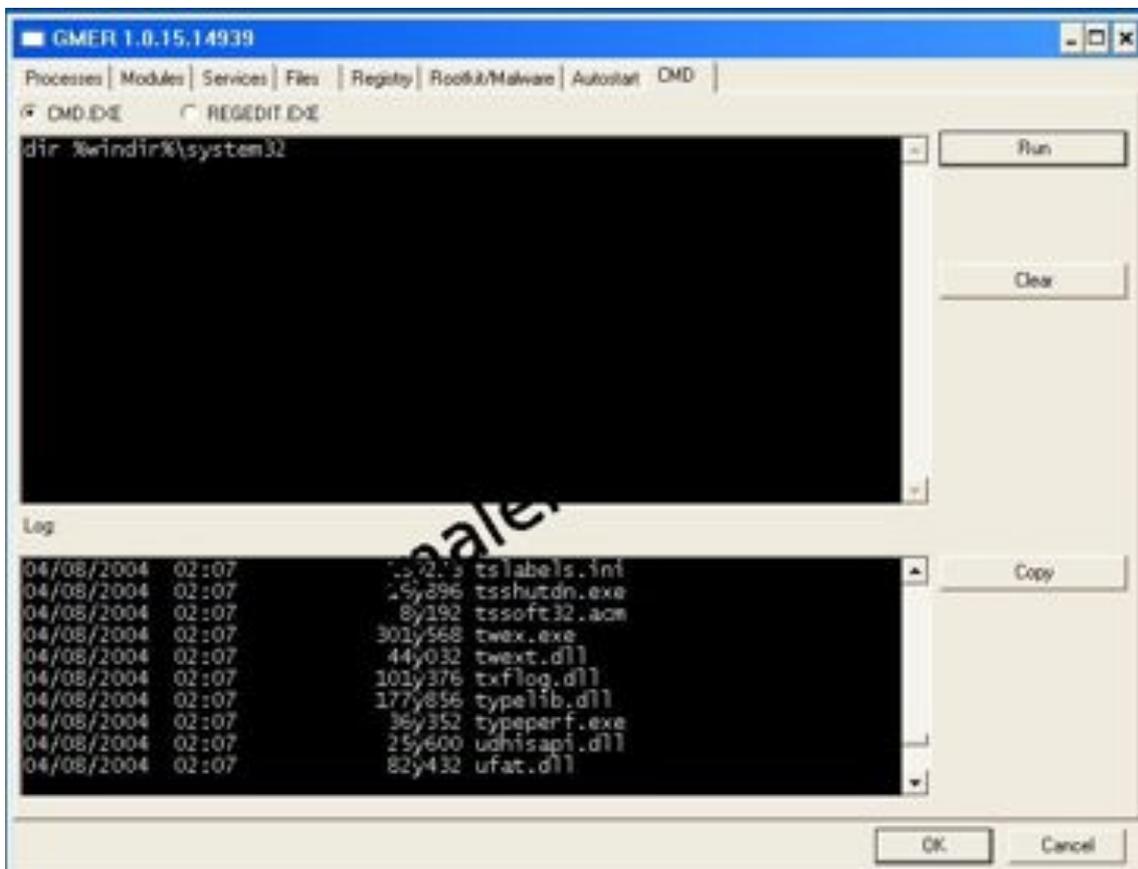


## CMD

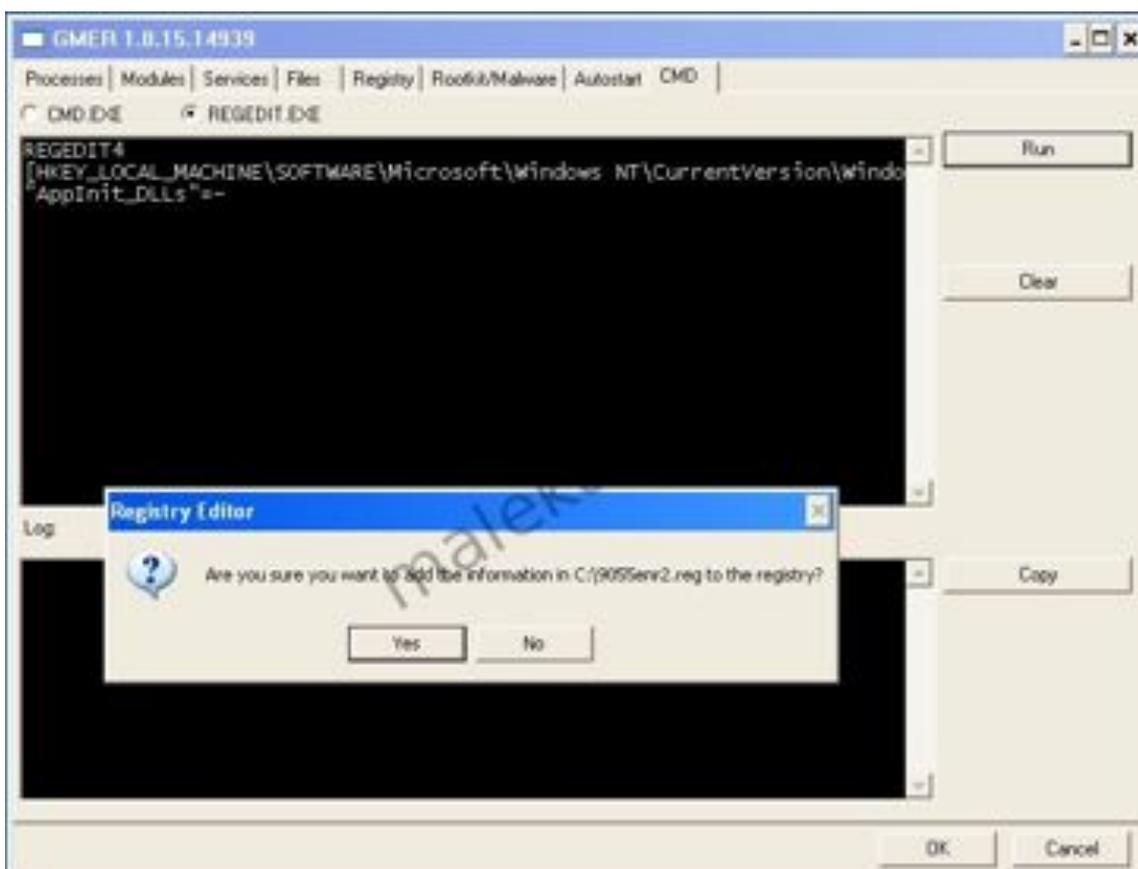
L'onglet CMD permet d'exécuter des commandes CMD lorsque l'onglet CMD.EXE est coché.

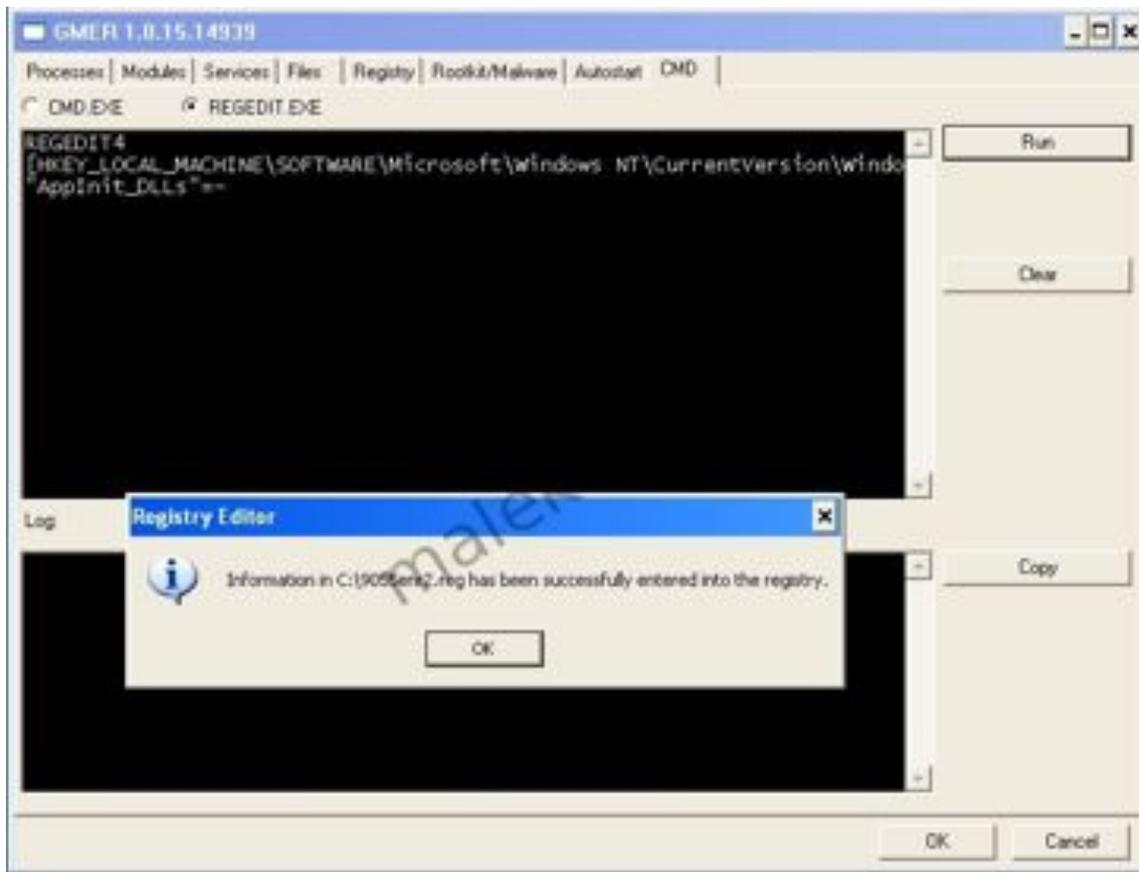
Tapez la commande dans la partie haute et cliquez dur *Run* à droite, le résultat de la commande apparaît dans la partie basse de la fenêtre.

Le bouton *Copy* permet de récupérer le résultat dans un copier/coller.



En cochant l'onglet *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.

Type	Name	Value
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31274	Details
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@C:\WINDOWS\system32\SHELL32.dll-22913	Shows the disk drives and hardware ...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@C:\WINDOWS\system32\SHELL32.dll-31361	Provides options for you to customize ...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31317	System Tasks
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31319	Show the contents of this drive
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31292	Search for files or folders
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31321	Hide the contents of this drive
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31233	File and Folder Tasks
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31236	Make a new folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31260	Publish this folder to the Web
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31374	Share this folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31256	Move this folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31258	Copy this folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31380	E-mail this folder's files
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31262	Delete this folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31323	Show the contents of this folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31325	Hide the contents of this folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31329	Provides the steps necessary to add ...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31254	Rename this folder
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@C:\WINDOWS\system32\usermgr.exe	Setup Information
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31242	Rename this file
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31244	Move this file
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31246	Copy this file
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31275	Publish this file to the Web
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31273	E-mail this file
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31274	Delete this file
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@C:\WINDOWS\system32\cleanmgr.exe	Disk Space Cleanup Manager for Win...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-12710	Run
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@C:\WINDOWS\regedit.exe	Registry Editor
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31249	Transfers copies of the selected items...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31275	This section displays the size, file type...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@C:\WINDOWS\system32\SHELL32.dll-22912	Shows shortcuts to Web sites, network...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31273	These links open other folders and fa...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31274	These tasks apply to the files and fold...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@shell32.dll-31375	Makes the selected folder available to...
Reg	HKCU\Software\Microsoft\Windows\Shell\NoRoam\MUICache@C:\WINDOWS\system32\SHELL32.dll-22914	Contains letters, reports, and other do...
File	C:\WINDOWS\S19129837.exe	35940 bytes executable
File	C:\WINDOWS\new_drv.zip	8192 bytes executable
File	C:\WINDOWS\system32\lsasrv_32	0 bytes
File	C:\WINDOWS\system32\lsasrv_32\local ds	0 bytes
File	C:\WINDOWS\system32\lsasrv_32\user dr	10430 bytes
File	C:\WINDOWS\system32\lsasrv.exe	348672 bytes
Service	C:\WINDOWS\new_drv.zip	[MANUAL] new_drv

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 apparaissent 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] 0x10000000

Library C:\Windows\System32bmtdhh.dll (\*\* hidden \*\*) @

C:\WINDOWSgmer.exe [504] 0x10000000

Library C:\Windows\System32bmtdhh.dll (\*\* hidden \*\*) @

C:\Windows\System32cmd.exe [672] 0x10000000

Library C:\Windows\System32bmtdhh.dll (\*\* hidden \*\*) @

C:\Windows\System32spoolsv.exe [1108] 0x10000000

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

-- Services – GMER 1.0.11 --

Service C:\Windows\System32bmtdhh.sys [BOOT] bmtdhh <–

ROOTKIT !!!

**Fichiers considérés comme rootkités :**

-- Files – GMER 1.0.11 --

File C:\Windows\System32bmtdhh.dll

File C:\Windows\System32bmtdhh.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, Alcohol 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](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 reconnaît facilement ces derniers aux devices relatifs au SCSI :

*-- Devices – GMER 1.0.15 --*

*Device Driversptd Device1875799320 spjp.sys*

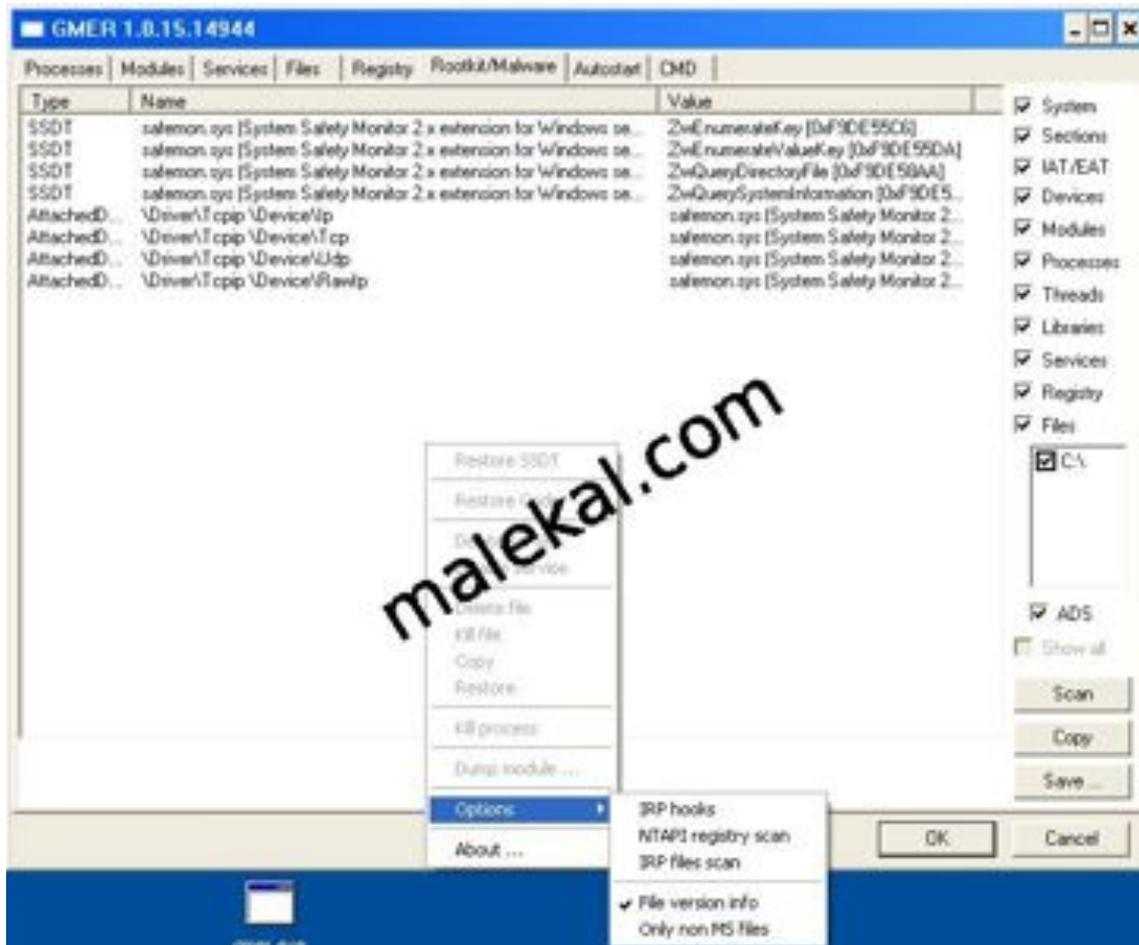
*Device Driverascafl5y DeviceScsiascafl5y1Port3Path0Target0Lun0  
82D171F8*

*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 totalité des malwares en cours d'exécution.

