Rootkit is a stealth type of malicious software designed to hide the existence of certain process from normal methods of detection and enables continued privileged access to a computer.

INTRODUCTION:

Breaking the term rootkit into the two component words, root and kit, is a useful way to define it. Root is a UNIX/Linux term that's the equivalent of Administrator in Windows.

The word kit denotes programs that allow someone to obtain root/admin-level access to the computer by executing the programs in the kit — all of which is done without end-user consent or knowledge.

A rootkit is a type of malicious software that is activated each time your system boots up. Rootkits are difficult to detect because they are activated before your system's Operating System has completely booted up. A rootkit often allows the installation of hidden files, processes, hidden user accounts, and more in the systems OS. Rootkits are able to intercept data from terminals,network connections, and the keyboard.

Rootkits have two primary functions: remote command/control (back door) and software eavesdropping. Rootkits allow someone, legitimate or otherwise, to administratively control a computer. This means executing files, accessing logs, monitoring user activity, and even changing the computer's configuration.

Therefore, in the strictest sense, even versions of VNC are rootkits. This surprises most people, as they consider rootkits to be solely malware, but in of themselves they aren't malicious at all.

The presence of a rootkit on a network was first documented in the early 1990s. At that time, Sun and Linux operating systems were the primary targets for a hacker looking to install a rootkit. Today, rootkits are available for a number of operating systems, including Windows, and are increasingly difficult to detect on any network.

PROCEDURE:

STEP-1: Download Rootkit Tool from GMER website www.gmer.net.

STEP-2: This displays the Processes, Modules, Services, Files, Registry, RootKit Malwares, Autostart, CMD of local host.

STEP-3: Select Processes menu and kill any unwanted process if any.

STEP-4: Modules menu displays the various system files like .sys, .dll

STEP-5: Services menu displays the complete services running with Autostart, Enable, Disable, System, Boot.

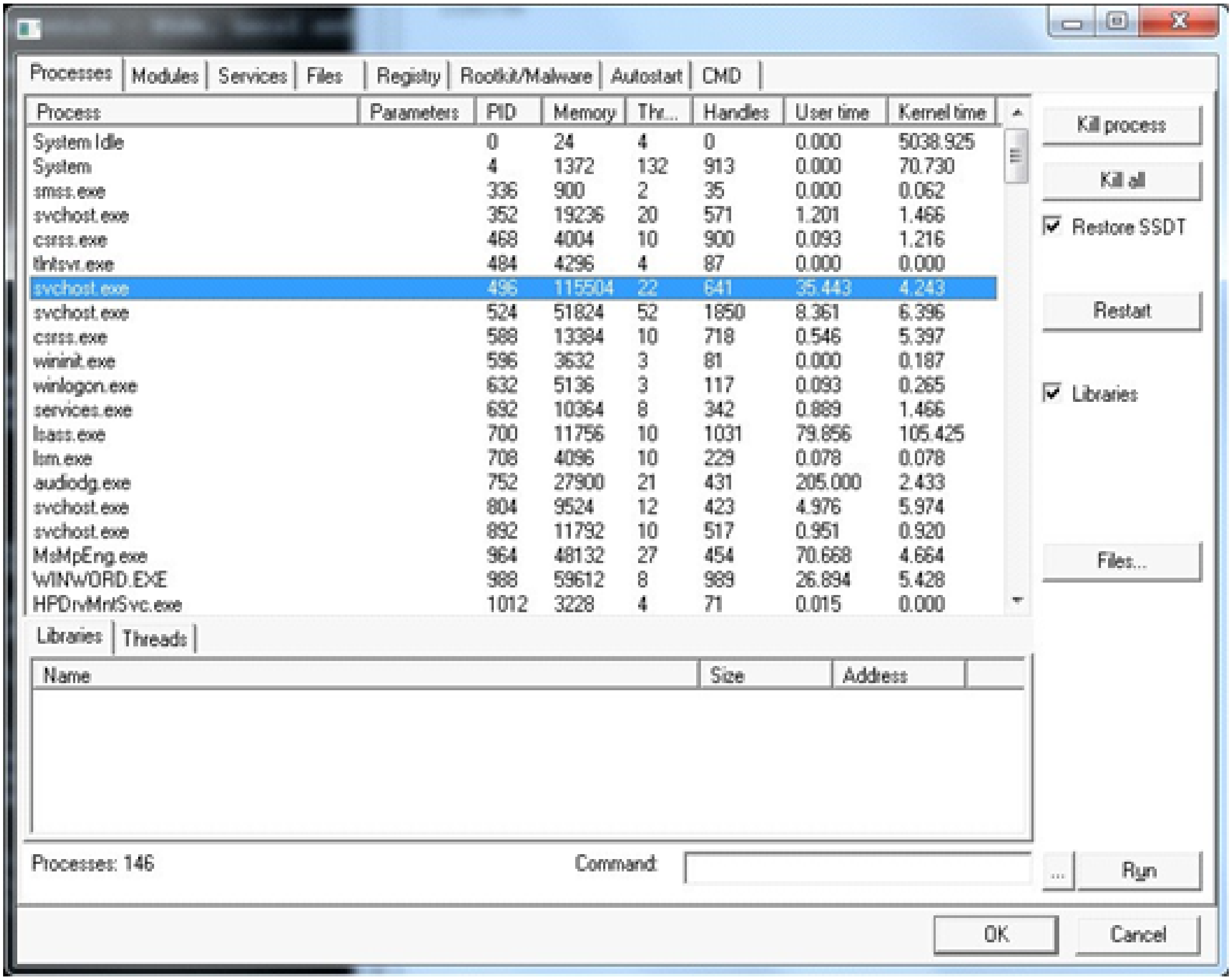
STEP-6: Files menu displays full files on Hard-Disk volumes.

STEP-7: Registry displays Hkey_Current_user and Hkey_Local_Machine.

STEP-8: Rootkits / Malwares scans the local drives selected.

STEP-9: Autostart displays the registry base Autostart applications.

STEP-10:CMD allows the user to interact with command line utilities or Registry



Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
System Idle		0	24	4	0	0.000	5038.925
System		4	1372	132	913	0.000	70.730
smss.exe		336	900	2	35	0.000	0.062
svchost.exe		352	19236	20	571	1.201	1.466
csrss.exe		468	4004	10	900	0.093	1.216
tlntsvr.exe		484	4296	4	87	0.000	0.000
svchost.exe		496	115504	22	641	35.443	4.243
svchost.exe		524	51824	52	1850	8.361	6.396
csrss.exe		588	13384	10	718	0.546	5.397
wininit.exe		596	3632	3	81	0.000	0.187
winlogon.exe		632	5136	3	117	0.093	0.265
services.exe		692	10364	8	342	0.889	1.466
lsass.exe		700	11756	10	1031	79.856	105.425
lsm.exe		708	4096	10	229	0.078	0.078
audiodg.exe		752	27900	21	431	205.000	2.433
svchost.exe		804	9524	12	423	4.976	5.974
svchost.exe		892	11792	10	517	0.951	0.920
MsMpEng.exe		964	48132	27	454	70.668	4.664
WINWORD.EXE		988	59612	8	989	26.894	5.428
HPDrvMntSvc.exe		1012	3228	4	71	0.015	0.000

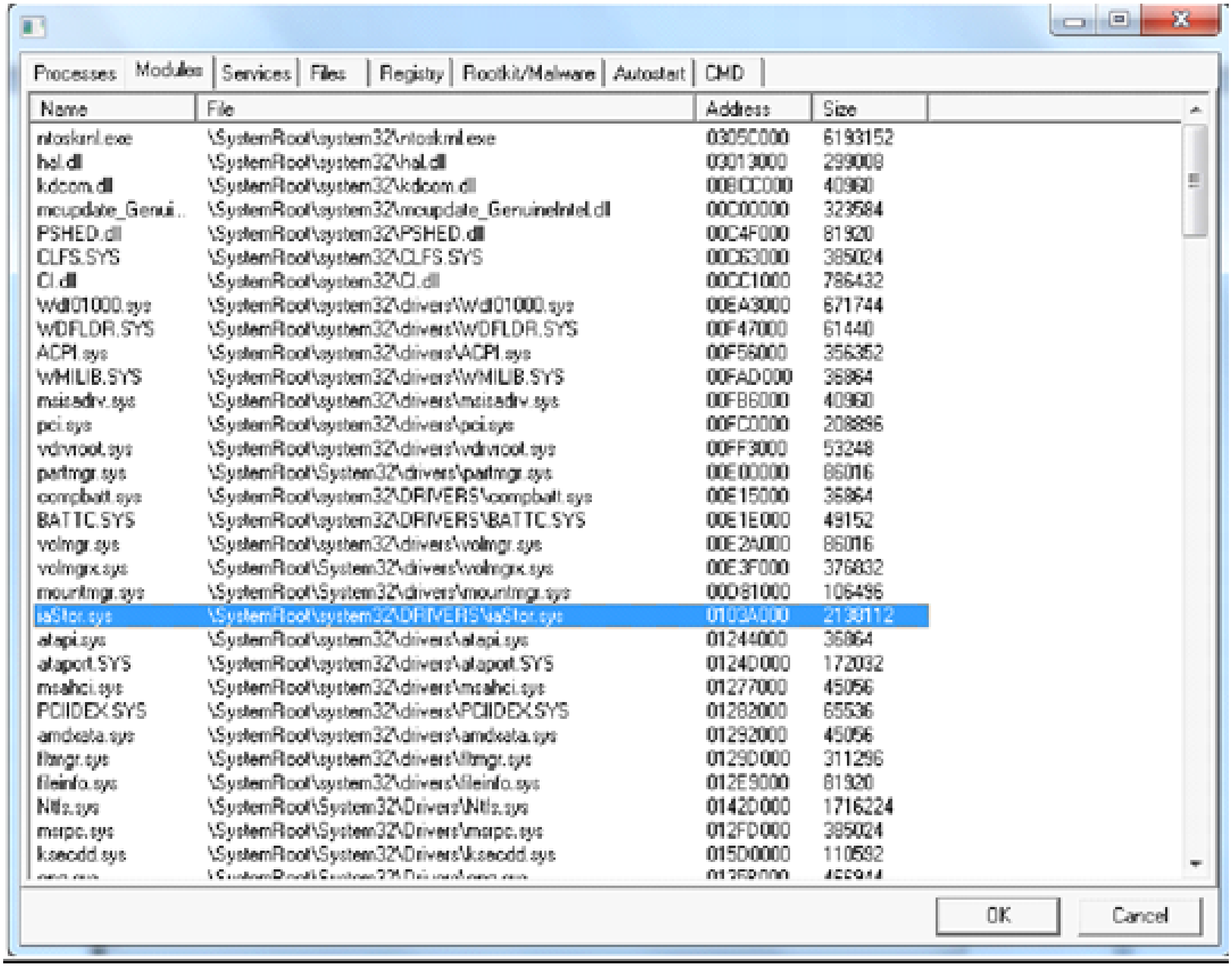
☑ Restore SSDT

☑ Libraries

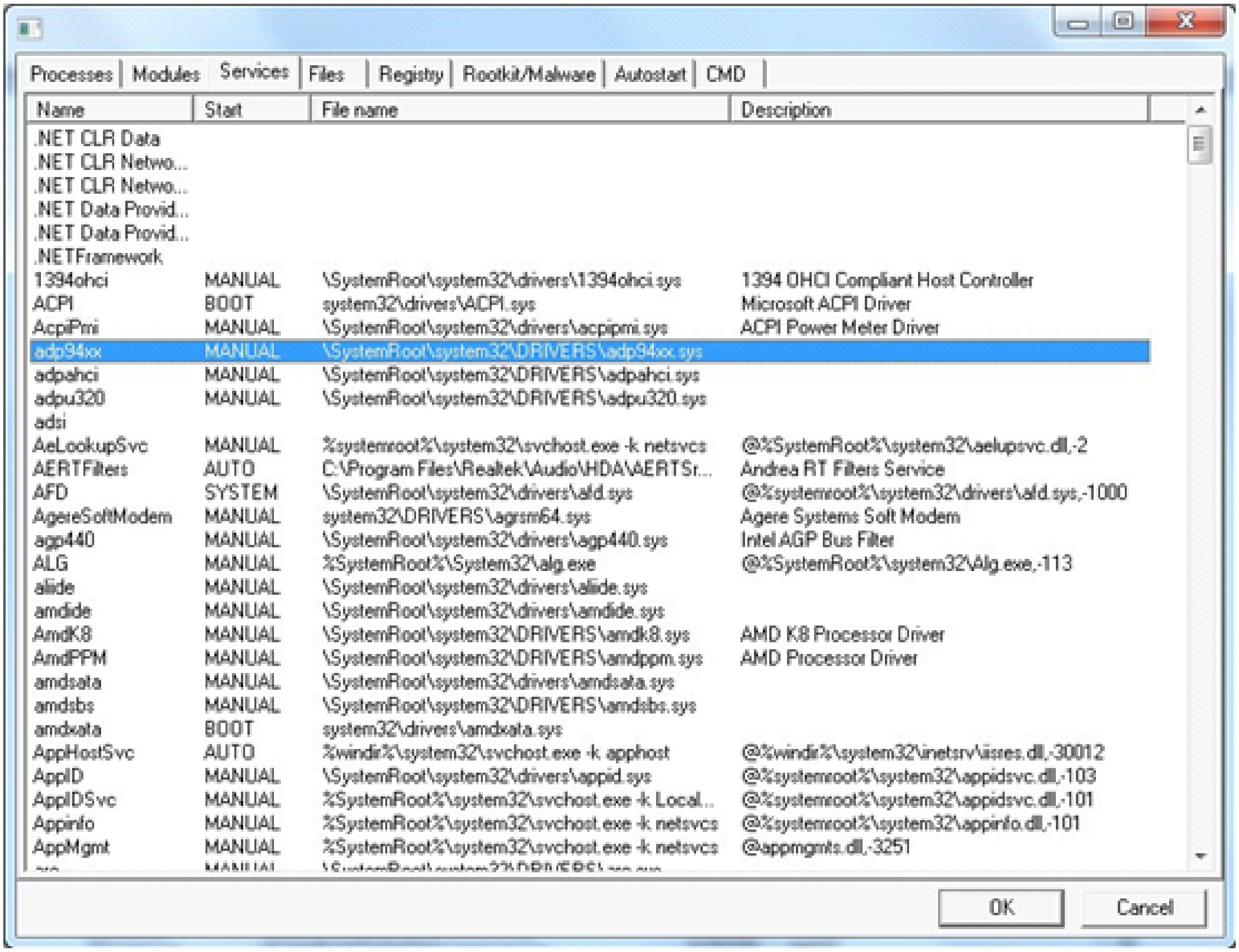
Name	Size	Address

Processes: 146

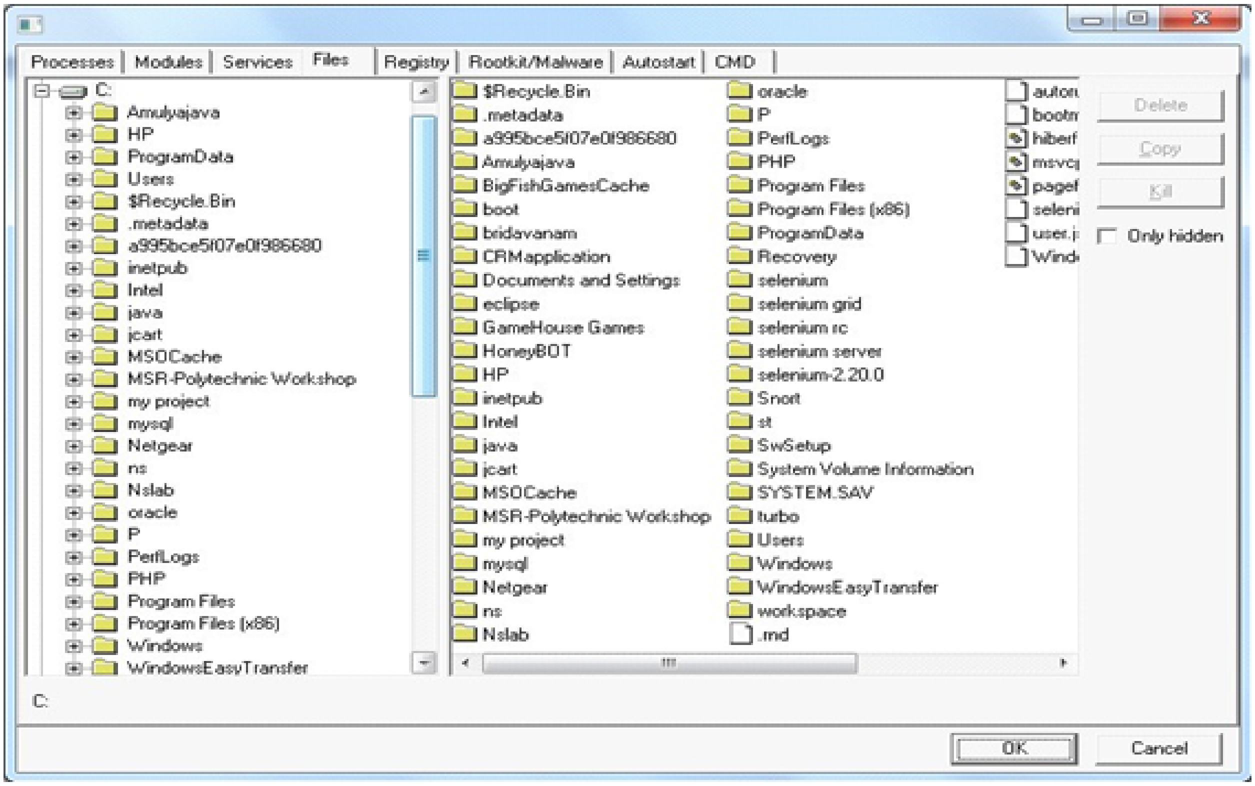
Command:



Name	File	Address	Size
ntoskrnl.exe	\SystemRoot\system32\ntoskrnl.exe	0305C000	6193152
hal.dll	\SystemRoot\system32\hal.dll	03013000	299008
kdcom.dll	\SystemRoot\system32\kdcom.dll	00BCC000	40960
mcupdate_Genui...	\SystemRoot\system32\mcupdate_GenuineIntel.dll	00C00000	323584
PSHED.dll	\SystemRoot\system32\PSHED.dll	00C4F000	81920
CLFS.SYS	\SystemRoot\system32\CLFS.SYS	00C63000	385024
CI.dll	\SystemRoot\system32\CI.dll	00CC1000	786432
Wdf01000.sys	\SystemRoot\system32\drivers\Wdf01000.sys	00EA3000	671744
WDFLDR.SYS	\SystemRoot\system32\drivers\WDFLDR.SYS	00F47000	61440
ACPI.sys	\SystemRoot\system32\drivers\ACPI.sys	00F56000	356352
WMILIB.SYS	\SystemRoot\system32\drivers\WMILIB.SYS	00FAD000	36864
msisadrv.sys	\SystemRoot\system32\drivers\msisadrv.sys	00FB6000	40960
pci.sys	\SystemRoot\system32\drivers\pci.sys	00FC0000	208896
vdrvroot.sys	\SystemRoot\system32\drivers\vdrvroot.sys	00FF3000	53248
partmgr.sys	\SystemRoot\System32\drivers\partmgr.sys	00E00000	86016
compbatt.sys	\SystemRoot\system32\DRIVERS\compbatt.sys	00E15000	36864
BATTC.SYS	\SystemRoot\system32\DRIVERS\BATTC.SYS	00E1E000	49152
volmgr.sys	\SystemRoot\system32\drivers\volmgr.sys	00E2A000	86016
volmgrx.sys	\SystemRoot\System32\drivers\volmgrx.sys	00E3F000	376832
mountmgr.sys	\SystemRoot\System32\drivers\mountmgr.sys	00D81000	106496
iaStor.sys	\SystemRoot\system32\DRIVERS\iaStor.sys	0103A000	2138112
atapi.sys	\SystemRoot\system32\drivers\atapi.sys	01244000	36864
ataport.SYS	\SystemRoot\system32\drivers\ataport.SYS	0124D000	172032
msahci.sys	\SystemRoot\system32\drivers\msahci.sys	01277000	45056
PCIIDEX.SYS	\SystemRoot\system32\drivers\PCIIDEX.SYS	01282000	65536
amdxata.sys	\SystemRoot\system32\drivers\amdxata.sys	01292000	45056
fltmgr.sys	\SystemRoot\system32\drivers\fltmgr.sys	0129D000	311296
fileinfo.sys	\SystemRoot\system32\drivers\fileinfo.sys	012E9000	81920
Ntfs.sys	\SystemRoot\System32\Drivers\Ntfs.sys	0142D000	1716224
msrpc.sys	\SystemRoot\System32\Drivers\msrpc.sys	012FD000	385024
ksecdd.sys	\SystemRoot\System32\Drivers\ksecdd.sys	015D0000	110592
cng.sys	\SystemRoot\System32\Drivers\cng.sys	0135B000	458944



Name	Start	File name	Description
.NET CLR Data			
.NET CLR Netwo...			
.NET CLR Netwo...			
.NET Data Provid...			
.NET Data Provid...			
.NETFramework			
1394ohci	MANUAL	\SystemRoot\system32\drivers\1394ohci.sys	1394 OHCI Compliant Host Controller
ACPI	BOOT	system32\drivers\ACPI.sys	Microsoft ACPI Driver
AcpiPmi	MANUAL	\SystemRoot\system32\drivers\acpipmi.sys	ACPI Power Meter Driver
adp94xx	MANUAL	\SystemRoot\system32\DRIVERS\adp94xx.sys	
adpahci	MANUAL	\SystemRoot\system32\DRIVERS\adpahci.sys	
adpu320	MANUAL	\SystemRoot\system32\DRIVERS\adpu320.sys	
adsi			
AeLookupSvc	MANUAL	%systemroot%\system32\svchost.exe -k netsvcs	@%SystemRoot%\system32\aelupsvc.dll,-2
AERTFilters	AUTO	C:\Program Files\Realtek\Audio\HDA\AERTSr...	Andrea RT Filters Service
AFD	SYSTEM	\SystemRoot\system32\drivers\afd.sys	@%systemroot%\system32\drivers\afd.sys,-1000
AgereSoftModem	MANUAL	system32\DRIVERS\agrsm64.sys	Agere Systems Soft Modem
agp440	MANUAL	\SystemRoot\system32\drivers\agp440.sys	Intel AGP Bus Filter
ALG	MANUAL	%SystemRoot%\System32\alg.exe	@%SystemRoot%\system32\Alg.exe,-113
aliide	MANUAL	\SystemRoot\system32\drivers\aliide.sys	
amdide	MANUAL	\SystemRoot\system32\drivers\amdide.sys	
AmdK8	MANUAL	\SystemRoot\system32\DRIVERS\amdk8.sys	AMD K8 Processor Driver
AmdPPM	MANUAL	\SystemRoot\system32\DRIVERS\amdppm.sys	AMD Processor Driver
amdsata	MANUAL	\SystemRoot\system32\drivers\amdsata.sys	
amdsbs	MANUAL	\SystemRoot\system32\DRIVERS\amdsbs.sys	
amdxata	BOOT	system32\drivers\amdxata.sys	
AppHostSvc	AUTO	%windir%\system32\svchost.exe -k apphost	@%windir%\system32\inetsrv\iisres.dll,-30012
AppID	MANUAL	\SystemRoot\system32\drivers\appid.sys	@%systemroot%\system32\appidsvc.dll,-103
AppIDSvc	MANUAL	%SystemRoot%\system32\svchost.exe -k Local...	@%systemroot%\system32\appidsvc.dll,-101
Appinfo	MANUAL	%SystemRoot%\system32\svchost.exe -k netsvcs	@%systemroot%\system32\appinfo.dll,-101
AppMgmt	MANUAL	%SystemRoot%\system32\svchost.exe -k netsvcs	@appmgmts.dll,-3251



GMER is an application that detects and removes rootkits .

It scans for:

1. hidden processes
2. hidden threads
3. hidden modules
4. hidden services
5. hidden files
6. hidden disk sectors (MBR)
7. hidden Alternate Data Streams
8. hidden registry keys
9. drivers hooking SSDT
10. drivers hooking IDT
11. drivers hooking IRP calls
12. inline hooks

Frequently Asked Questions

Question : *Do I have a rootkit?*

Answer: You can scan the system for rootkits using GMER. Run **gmer.exe**, select **Rootkit** tab and click the "Scan" button.
If you don't know how to interpret the output, please **Save** the log and send it to my email address.
Warning ! Please, do not select the "Show all" checkbox during the scan.

Question : *How to create "3rd party" log ?*

Answer: Tick **"3rd party"** option and then click the "Scan" button. After the scan you can use "Remove signed" and "Remove duplicates" options to filter the scan results.

Question : *How to install the GMER software ?*

Answer: Just run **gmer.exe.** All required files will be copied to the system during the first lanuch.

Question : *How to uninstall/remove the GMER software from my machine ?*

Answer: Just delete the **exe** file.

Question : *My computer is infected and GMER won't start:*

Answer: Try to rename gmer.exe to iexplore.exe and then run it.

Question : *How do I remove the Rustock rootkit ?*

Answer: When GMER detects hidden service click "**Delete the service**" and answer **YES** to all questions.

Question: How do I show all NTFS Streams ?

Answer: On the "Rootkit Tab" select only: Files + ADS + Show all options and then click the Scan button.

Question: Can I launch GMER in Safe Mode ?

Answer: Yes, you can launch GMER in Safe Mode, however rootkits which don't work in Safe Mode won't be detected.

Question: I am confused as to use delete or disable the hidden "service".

Answer: Sometimes "delete the service" option wont work because the rootkit protects its service. So, in such case use: 1) "disable the service", 2) reboot your machine, and 3) "delete the service".

link

http://www.gmer.net/#files