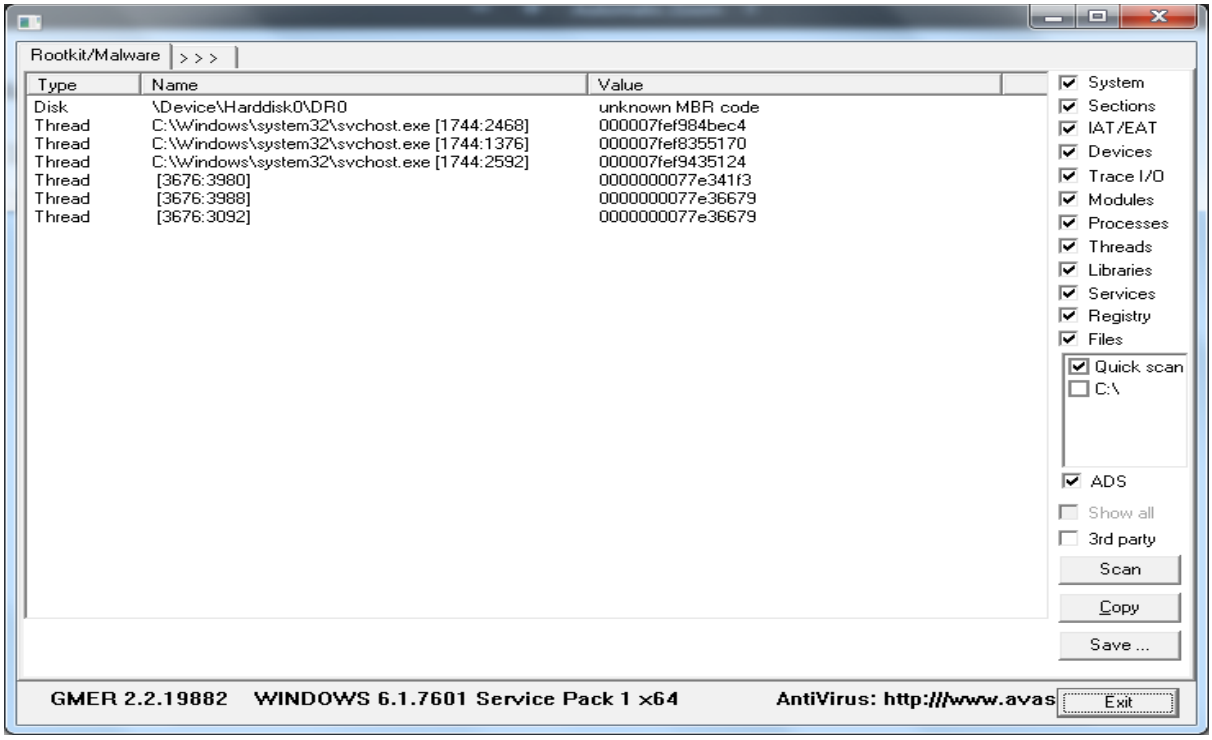
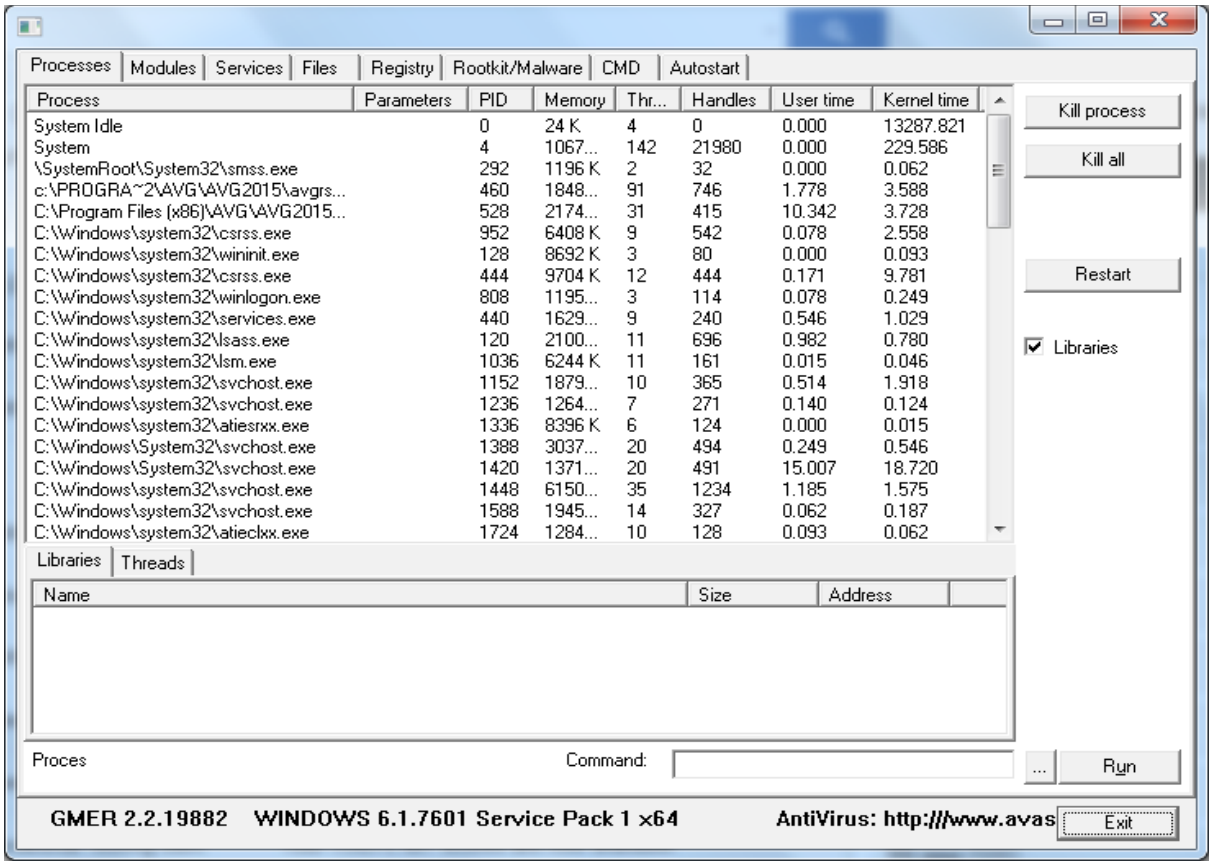
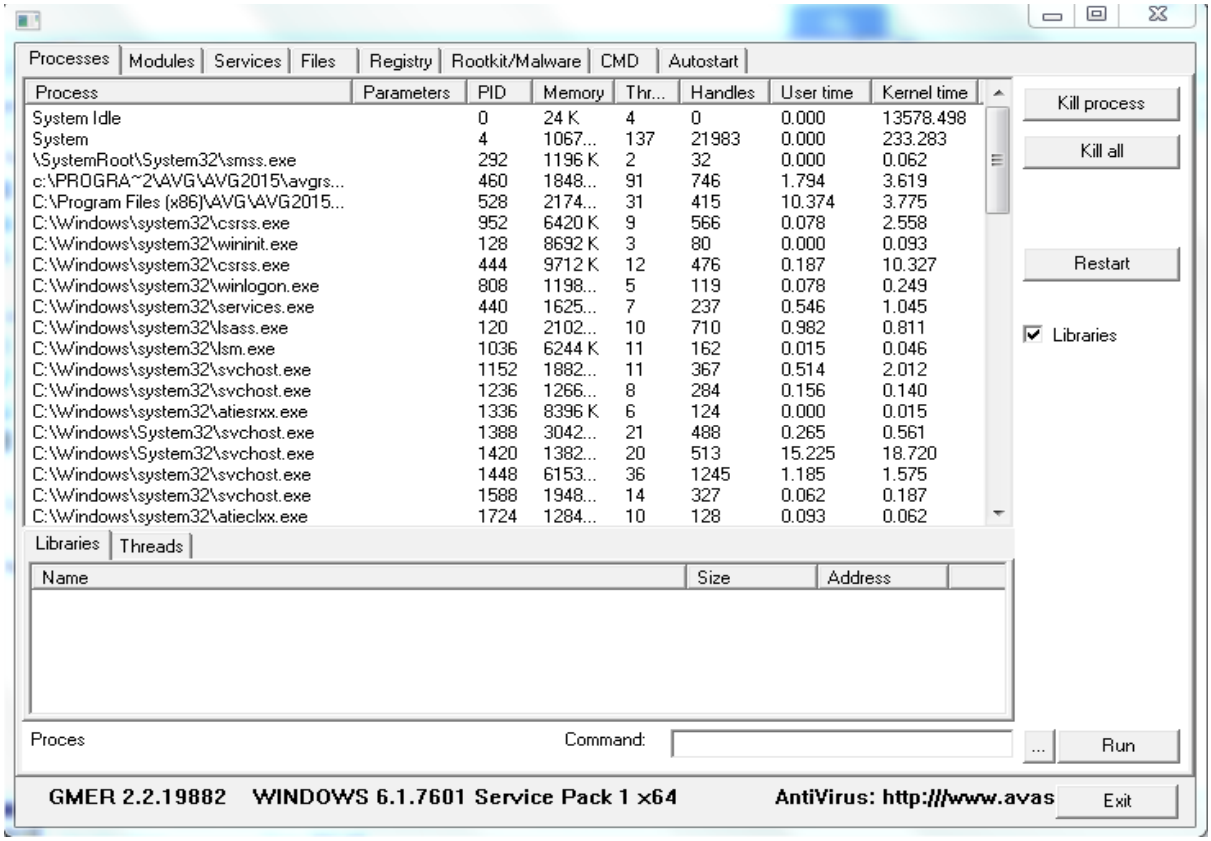
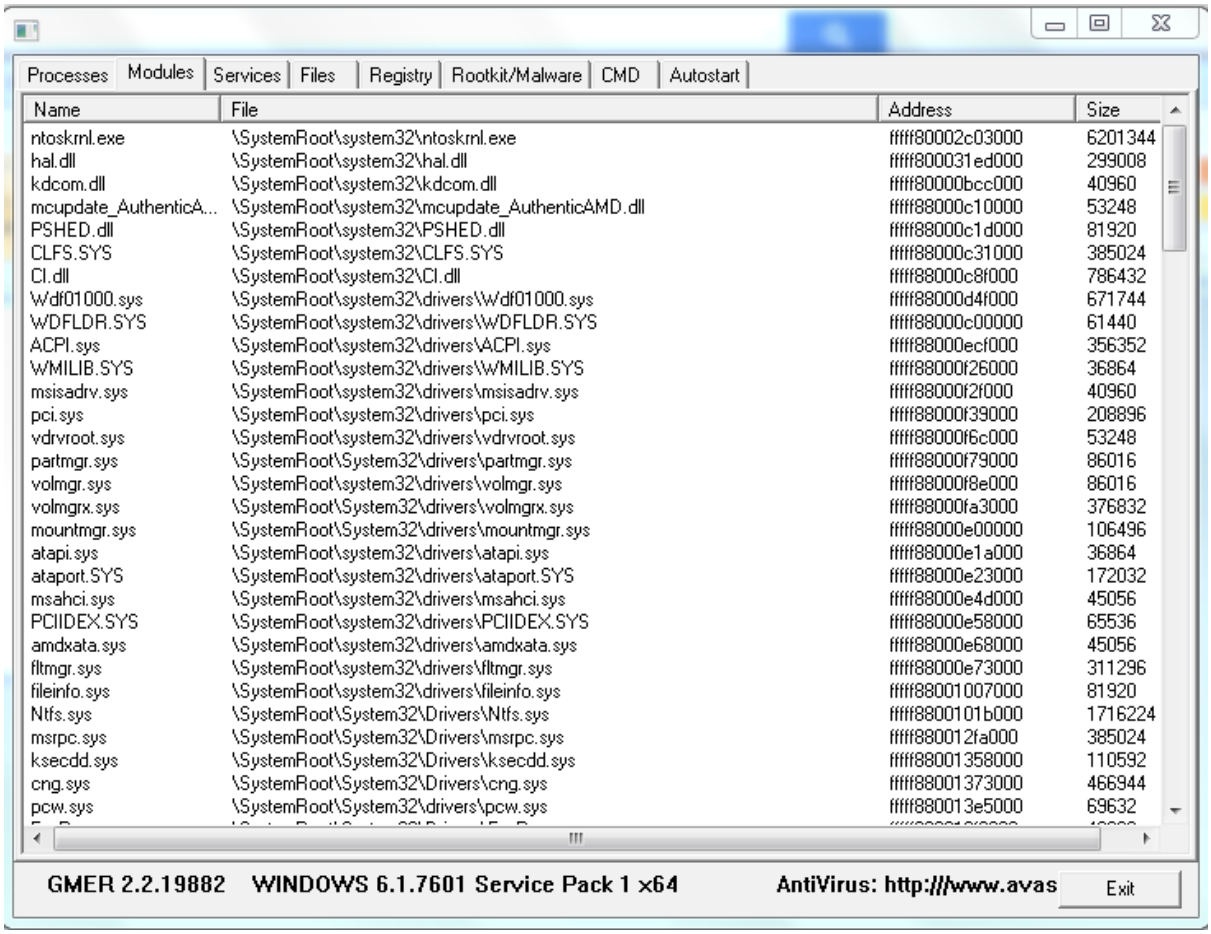
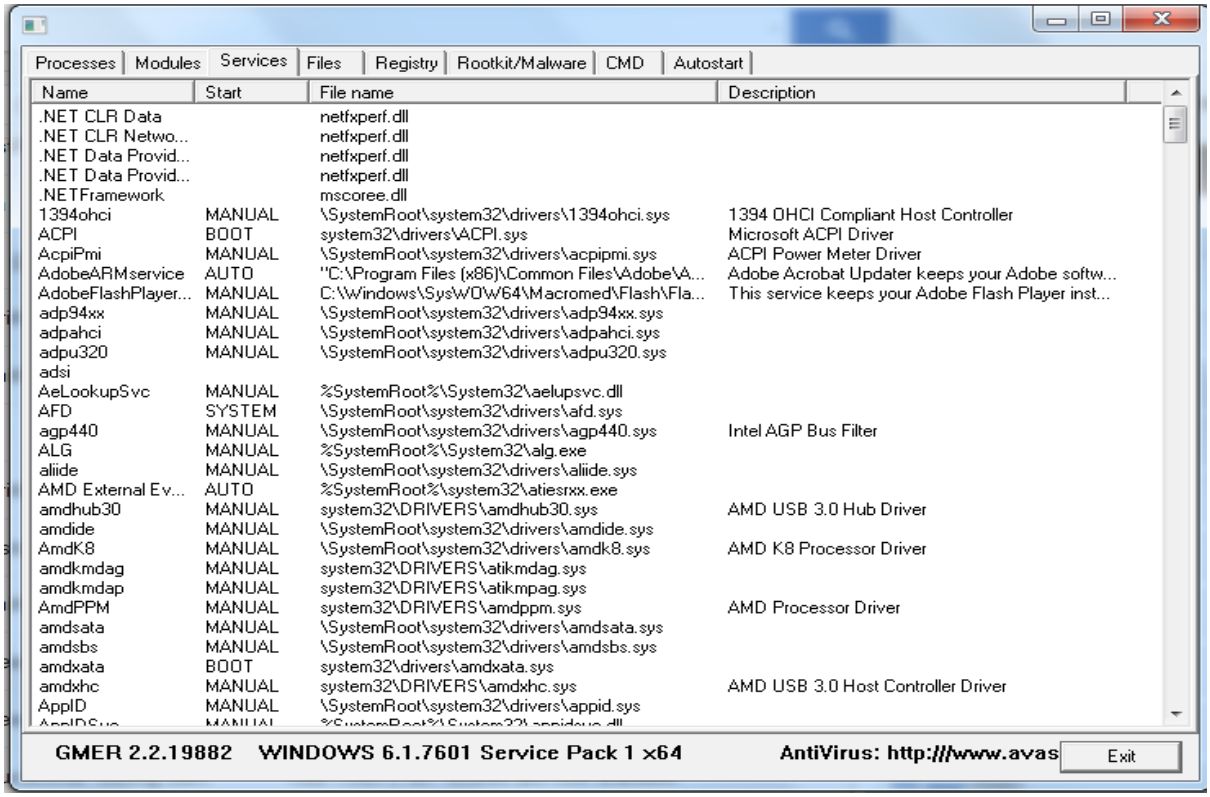
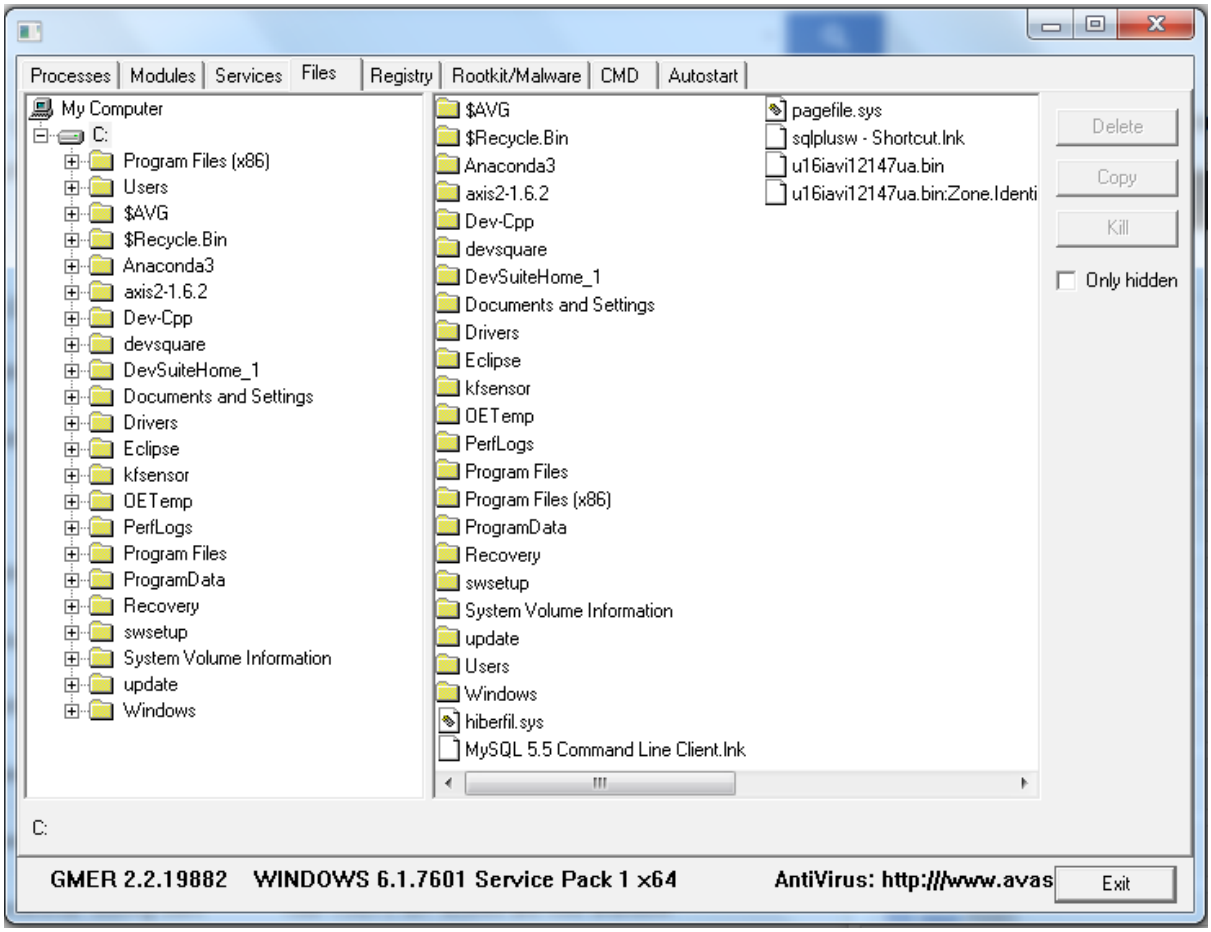

Rootkit/Malware
> > >
Type
Name
Value
Disk
\Device\Harddisk0\DR0
unknown MBR code
Thread
C:\Windows\system32\svchost.exe [1744:2468]
000007fef984bec4
Thread
C:\Windows\system32\svchost.exe [1744:1376]
000007fef8355170
Thread
C:\Windows\system32\svchost.exe [1744:2592]
000007fef9435124
Thread
[3676:3980]
0000000077e341f3
Thread
[3676:3988]
0000000077e36679
Thread
[3676:3092]
0000000077e36679
System
Sections
IAT/EAT
Devices
Trace I/O
Modules
Processes
Threads
Libraries
Services
Registry
Files
Quick scan
C:\
ADS
Show all
3rd party
Scan
Copy
Save ...
GMER 2.2.19882
WINDOWS 6.1.7601 Service Pack 1 x64
AntiVirus: http:///www.avas
Exit

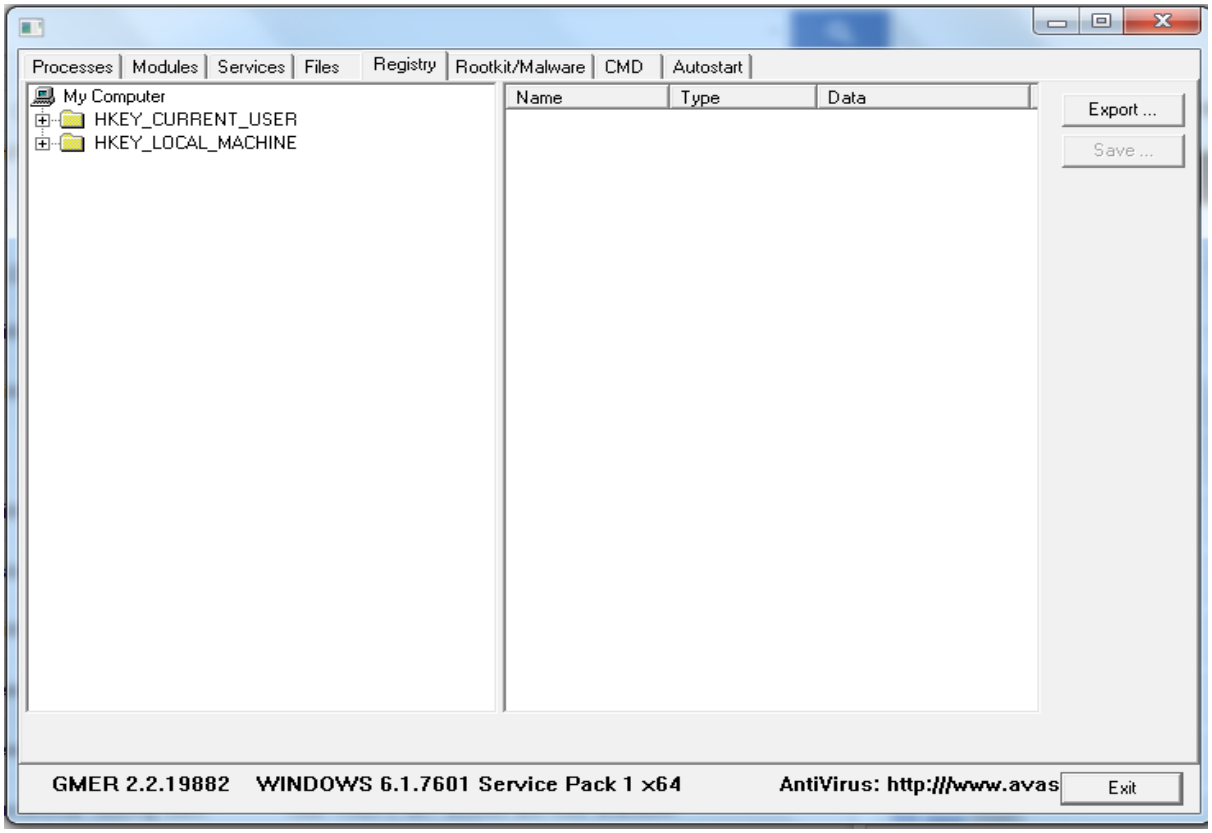

Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
Process
Parameters
PID
Memory
Thr...
Handles
User time
Kernel time
System Idle
0
24 K
4
0
0.000
13287.821
System
4
1067...
142
21980
0.000
229.586
\SystemRoot\System32\smss.exe
292
1196 K
2
32
0.000
0.062
c:\PROGRA~2\AVG\AVG2015\avgrs...
460
1848...
91
746
1.778
3.588
C:\Program Files (x86)\AVG\AVG2015...
528
2174...
31
415
10.342
3.728
C:\Windows\system32\csrss.exe
952
6408 K
9
542
0.078
2.558
C:\Windows\system32\wininit.exe
128
8692 K
3
80
0.000
0.093
C:\Windows\system32\csrss.exe
444
9704 K
12
444
0.171
9.781
C:\Windows\system32\winlogon.exe
808
1195...
3
114
0.078
0.249
C:\Windows\system32\services.exe
440
1629...
9
240
0.546
1.029
C:\Windows\system32\lsass.exe
120
2100...
11
696
0.982
0.780
C:\Windows\system32\lsm.exe
1036
6244 K
11
161
0.015
0.046
C:\Windows\system32\svchost.exe
1152
1879...
10
365
0.514
1.918
C:\Windows\system32\svchost.exe
1236
1264...
7
271
0.140
0.124
C:\Windows\system32\atiesrxx.exe
1336
8396 K
6
124
0.000
0.015
C:\Windows\System32\svchost.exe
1388
3037...
20
494
0.249
0.546
C:\Windows\System32\svchost.exe
1420
1371...
20
491
15.007
18.720
C:\Windows\system32\svchost.exe
1448
6150...
35
1234
1.185
1.575
C:\Windows\system32\svchost.exe
1588
1945...
14
327
0.062
0.187
C:\Windows\system32\atieclxx.exe
1724
1284...
10
128
0.093
0.062
Kill process
Kill all
Restart
Libraries
Libraries
Threads
Name
Size
Address
Proces
Command:
...
Run
GMER 2.2.19882
WINDOWS 6.1.7601 Service Pack 1 x64
AntiVirus: http:///www.avas
Exit

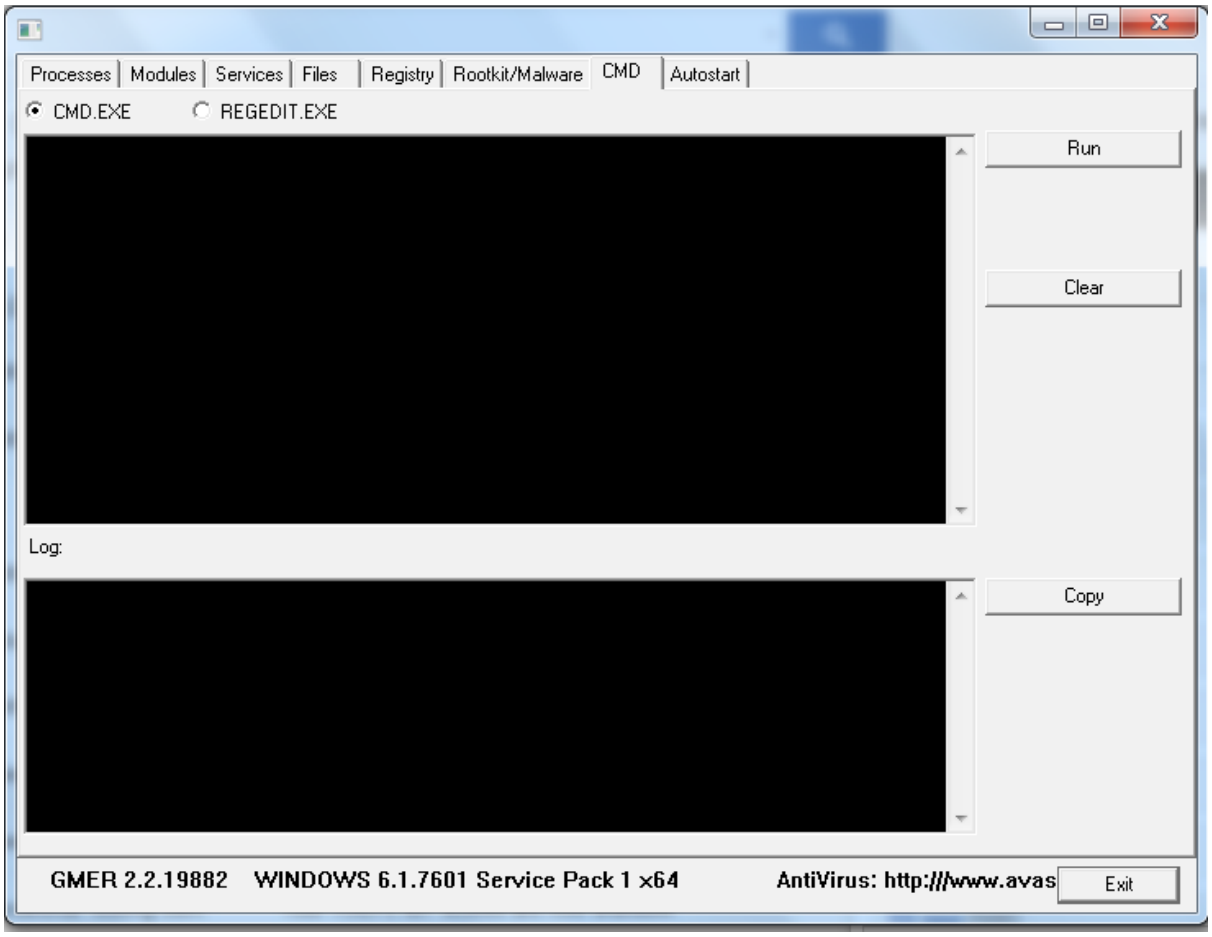

Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
Process
Parameters
PID
Memory
Thr...
Handles
User time
Kernel time
System Idle 0 24 K 4 0 0.000 13578.498
System 4 1067... 137 21983 0.000 233.283
\SystemRoot\System32\smss.exe 292 1196 K 2 32 0.000 0.062
c:\PROGRA~2\AVG\AVG2015\avgrs... 460 1848... 91 746 1.794 3.619
C:\Program Files (x86)\AVG\AVG2015... 528 2174... 31 415 10.374 3.775
C:\Windows\system32\csrss.exe 952 6420 K 9 566 0.078 2.558
C:\Windows\system32\wininit.exe 128 8692 K 3 80 0.000 0.093
C:\Windows\system32\csrss.exe 444 9712 K 12 476 0.187 10.327
C:\Windows\system32\winlogon.exe 808 1198... 5 119 0.078 0.249
C:\Windows\system32\services.exe 440 1625... 7 237 0.546 1.045
C:\Windows\system32\lsass.exe 120 2102... 10 710 0.982 0.811
C:\Windows\system32\lsm.exe 1036 6244 K 11 162 0.015 0.046
C:\Windows\system32\svchost.exe 1152 1882... 11 367 0.514 2.012
C:\Windows\system32\svchost.exe 1236 1266... 8 284 0.156 0.140
C:\Windows\system32\atiesrxx.exe 1336 8396 K 6 124 0.000 0.015
C:\Windows\System32\svchost.exe 1388 3042... 21 488 0.265 0.561
C:\Windows\System32\svchost.exe 1420 1382... 20 513 15.225 18.720
C:\Windows\system32\svchost.exe 1448 6153... 36 1245 1.185 1.575
C:\Windows\system32\svchost.exe 1588 1948... 14 327 0.062 0.187
C:\Windows\system32\atieclxx.exe 1724 1284... 10 128 0.093 0.062
Kill process
Kill all
Restart
Libraries
Libraries
Threads
Name
Size
Address
Proces
Command:
...
Run
GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http:///www.avas
Exit

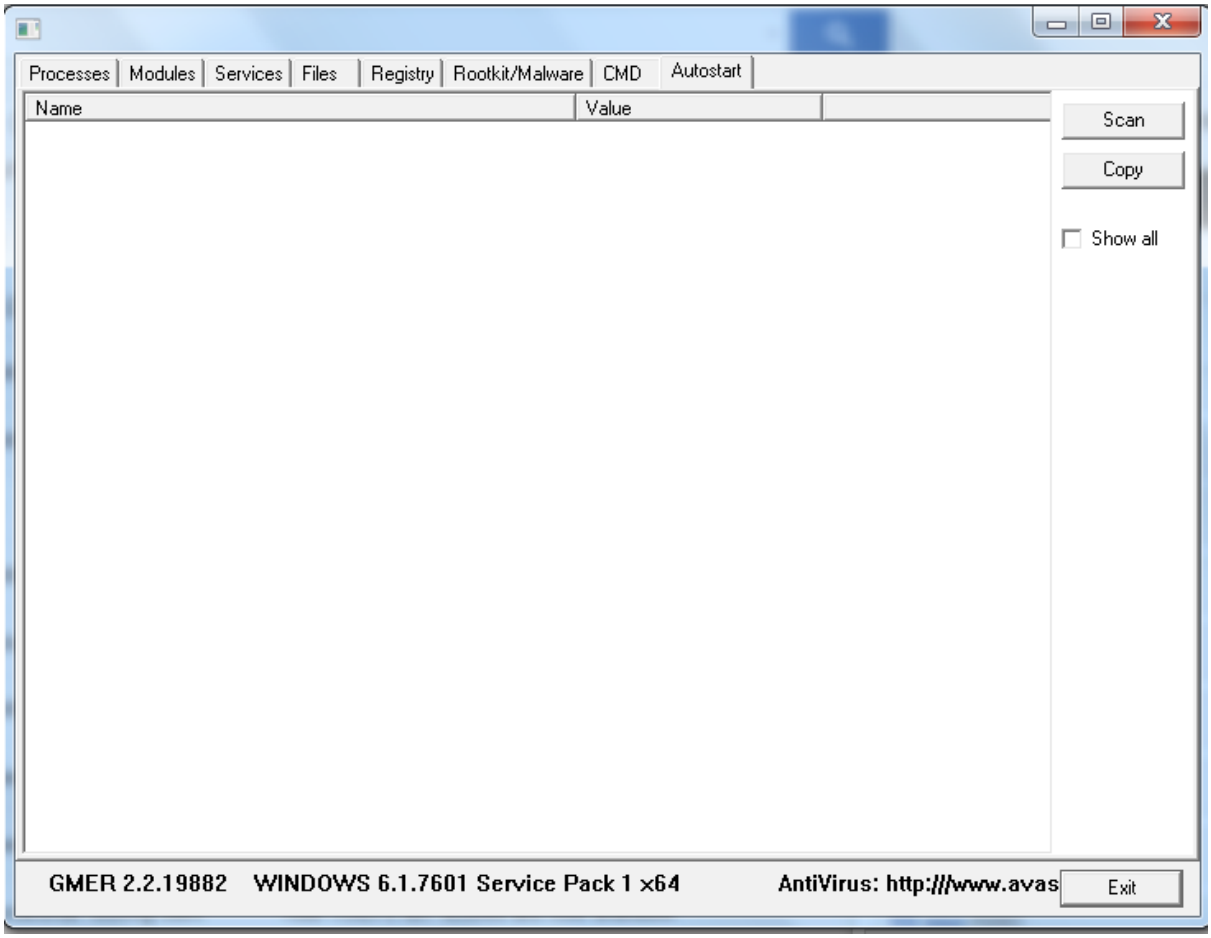

Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
Name
File
Address
Size
ntoskrnl.exe \SystemRoot\system32\ntoskrnl.exe fffff80002c03000 6201344
hal.dll \SystemRoot\system32\hal.dll fffff800031ed000 299008
kdcom.dll \SystemRoot\system32\kdcom.dll fffff80000bcc000 40960
mcupdate_AuthenticA... \SystemRoot\system32\mcupdate_AuthenticAMD.dll fffff88000c10000 53248
PSHED.dll \SystemRoot\system32\PSHED.dll fffff88000c1d000 81920
CLFS.SYS \SystemRoot\system32\CLFS.SYS fffff88000c31000 385024
CI.dll \SystemRoot\system32\CI.dll fffff88000c8f000 786432
Wdf01000.sys \SystemRoot\system32\drivers\Wdf01000.sys fffff88000d4f000 671744
WDFLDR.SYS \SystemRoot\system32\drivers\WDFLDR.SYS fffff88000c00000 61440
ACPI.sys \SystemRoot\system32\drivers\ACPI.sys fffff88000ecf000 356352
WMILIB.SYS \SystemRoot\system32\drivers\WMILIB.SYS fffff88000f26000 36864
msisadrv.sys \SystemRoot\system32\drivers\msisadrv.sys fffff88000f2f000 40960
pci.sys \SystemRoot\system32\drivers\pci.sys fffff88000f39000 208896
vdrvroot.sys \SystemRoot\system32\drivers\vdrvroot.sys fffff88000f6c000 53248
partmgr.sys \SystemRoot\System32\drivers\partmgr.sys fffff88000f79000 86016
volmgr.sys \SystemRoot\system32\drivers\volmgr.sys fffff88000f8e000 86016
volmgrx.sys \SystemRoot\System32\drivers\volmgrx.sys fffff88000fa3000 376832
mountmgr.sys \SystemRoot\System32\drivers\mountmgr.sys fffff88000e00000 106496
atapi.sys \SystemRoot\system32\drivers\atapi.sys fffff88000e1a000 36864
ataport.SYS \SystemRoot\system32\drivers\ataport.SYS fffff88000e23000 172032
msahci.sys \SystemRoot\system32\drivers\msahci.sys fffff88000e4d000 45056
PCIIDEX.SYS \SystemRoot\system32\drivers\PCIIDEX.SYS fffff88000e58000 65536
amdxata.sys \SystemRoot\system32\drivers\amdxata.sys fffff88000e68000 45056
fltmgr.sys \SystemRoot\system32\drivers\fltmgr.sys fffff88000e73000 311296
fileinfo.sys \SystemRoot\system32\drivers\fileinfo.sys fffff88001007000 81920
Ntfs.sys \SystemRoot\System32\Drivers\Ntfs.sys fffff8800101b000 1716224
msrpc.sys \SystemRoot\System32\Drivers\msrpc.sys fffff880012fa000 385024
ksecdd.sys \SystemRoot\System32\Drivers\ksecdd.sys fffff88001358000 110592
cng.sys \SystemRoot\System32\Drivers\cng.sys fffff88001373000 466944
pcw.sys \SystemRoot\System32\drivers\pcw.sys fffff880013e5000 69632
GMER 2.2.19882 WINDOWS 6.1.7601 Service Pack 1 x64 AntiVirus: http:///www.avas
Exit


Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
Name
Start
File name
Description
.NET CLR Data
netfxperf.dll
.NET CLR Netwo...
netfxperf.dll
.NET Data Provid...
netfxperf.dll
.NET Data Provid...
netfxperf.dll
.NETFramework
mscoree.dll
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
AdobeARMservice
AUTO
"C:\Program Files (x86)\Common Files\Adobe\A...
Adobe Acrobat Updater keeps your Adobe softw...
AdobeFlashPlayer...
MANUAL
C:\Windows\SysWOW64\Macromed\Flash\Fla...
This service keeps your Adobe Flash Player inst...
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\aelupsvc.dll
AFD
SYSTEM
\SystemRoot\system32\drivers\afd.sys
agp440
MANUAL
\SystemRoot\system32\drivers\agp440.sys
Intel AGP Bus Filter
ALG
MANUAL
%SystemRoot%\System32\alg.exe
aliide
MANUAL
\SystemRoot\system32\drivers\aliide.sys
AMD External Ev...
AUTO
%SystemRoot%\system32\atiesrxx.exe
amdhub30
MANUAL
system32\DRIVERS\amdhub30.sys
AMD USB 3.0 Hub Driver
amdide
MANUAL
\SystemRoot\system32\drivers\amdide.sys
AmdK8
MANUAL
\SystemRoot\system32\drivers\amdk8.sys
AMD K8 Processor Driver
amdkmdag
MANUAL
system32\DRIVERS\atikmdag.sys
amdkmdap
MANUAL
system32\DRIVERS\atikmpag.sys
AmdPPM
MANUAL
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
amdxhc
MANUAL
system32\DRIVERS\amdxhc.sys
AMD USB 3.0 Host Controller Driver
AppID
MANUAL
\SystemRoot\system32\drivers\appid.sys
GMER 2.2.19882
WINDOWS 6.1.7601 Service Pack 1 x64
AntiVirus: http:///www.avas
Exit


Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
My Computer
C:
Program Files (x86)
Users
$AVG
$Recycle.Bin
Anaconda3
axis2-1.6.2
Dev-Cpp
devsquare
DevSuiteHome_1
Documents and Settings
Drivers
Eclipse
kfsensor
OETemp
PerfLogs
Program Files
ProgramData
Recovery
swsetup
System Volume Information
update
Windows
$AVG
$Recycle.Bin
Anaconda3
axis2-1.6.2
Dev-Cpp
devsquare
DevSuiteHome_1
Documents and Settings
Drivers
Eclipse
kfsensor
OETemp
PerfLogs
Program Files
Program Files (x86)
ProgramData
Recovery
swsetup
System Volume Information
update
Users
Windows
hiberfil.sys
MySQL 5.5 Command Line Client.lnk
pagefile.sys
sqlplusw - Shortcut.lnk
u16iavi12147ua.bin
u16iavi12147ua.bin:Zone.Identi
Delete
Copy
Kill
Only hidden
C:
GMER 2.2.19882
WINDOWS 6.1.7601 Service Pack 1 x64
AntiVirus: http:///www.avas
Exit


Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
My Computer
HKEY_CURRENT_USER
HKEY_LOCAL_MACHINE
Name
Type
Data
Export ...
Save ...
GMER 2.2.19882
WINDOWS 6.1.7601 Service Pack 1 x64
AntiVirus: http:///www.avas
Exit


Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
CMD.EXE
REGEDIT.EXE
Run
Clear
Log:
Copy
GMER 2.2.19882
WINDOWS 6.1.7601 Service Pack 1 x64
AntiVirus: http:///www.avas
Exit


Processes
Modules
Services
Files
Registry
Rootkit/Malware
CMD
Autostart
Name
Value
Scan
Copy
Show all
GMER 2.2.19882
WINDOWS 6.1.7601 Service Pack 1 x64
AntiVirus: http:///www.avas
Exit