

## Exercise 12a:

To build a Trojan and know the harmness of the trojan malwares in a computer system.

### Trojan.bat:

@echo off

:X

start mspaint

start notepad

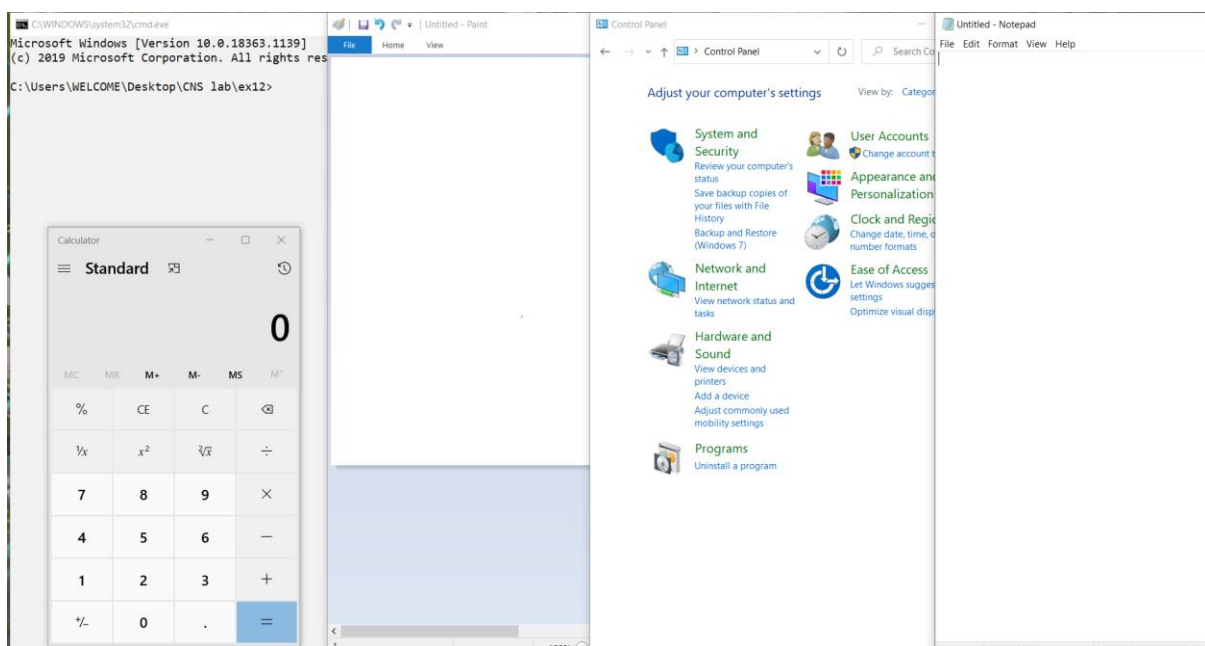
start cmd

start explorer

start control

start calc

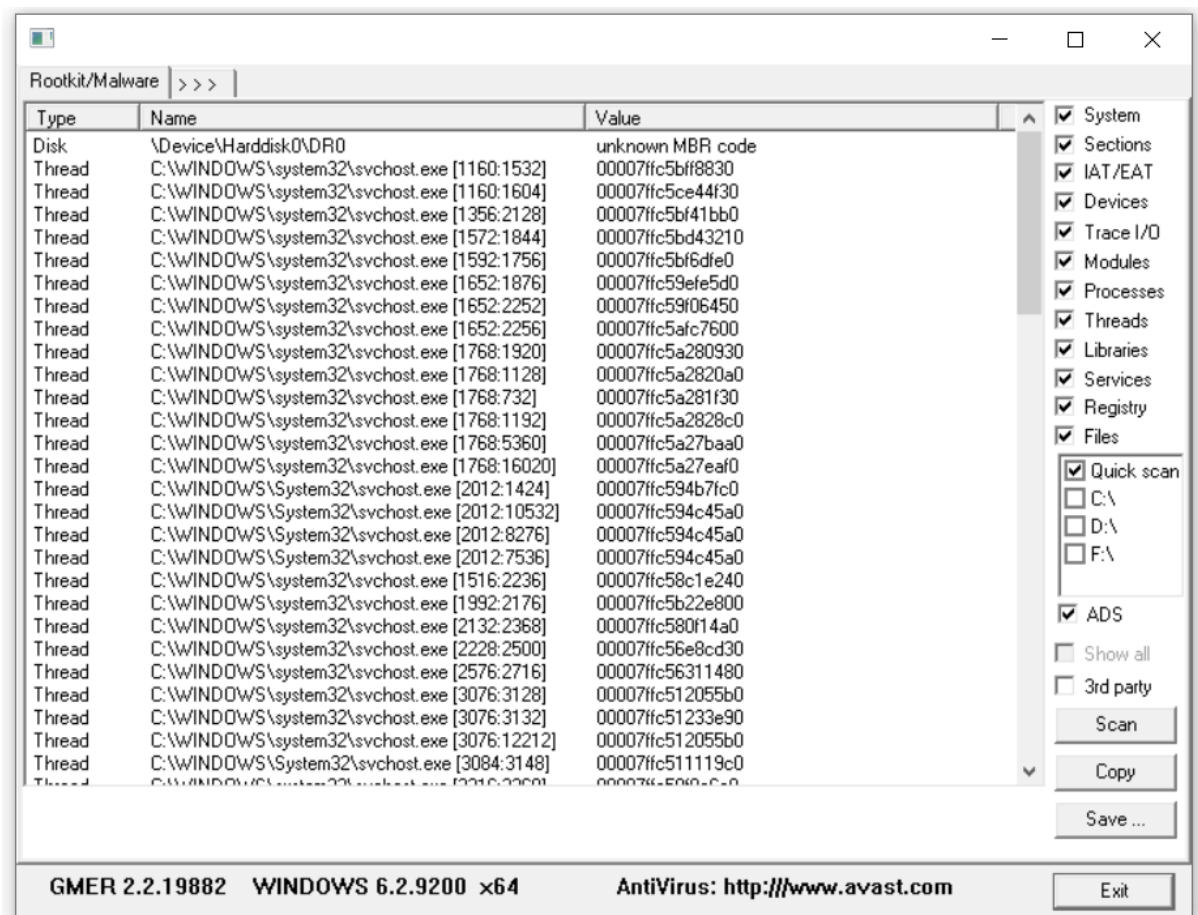
When the above file is executed, it opens all the mentioned applications.



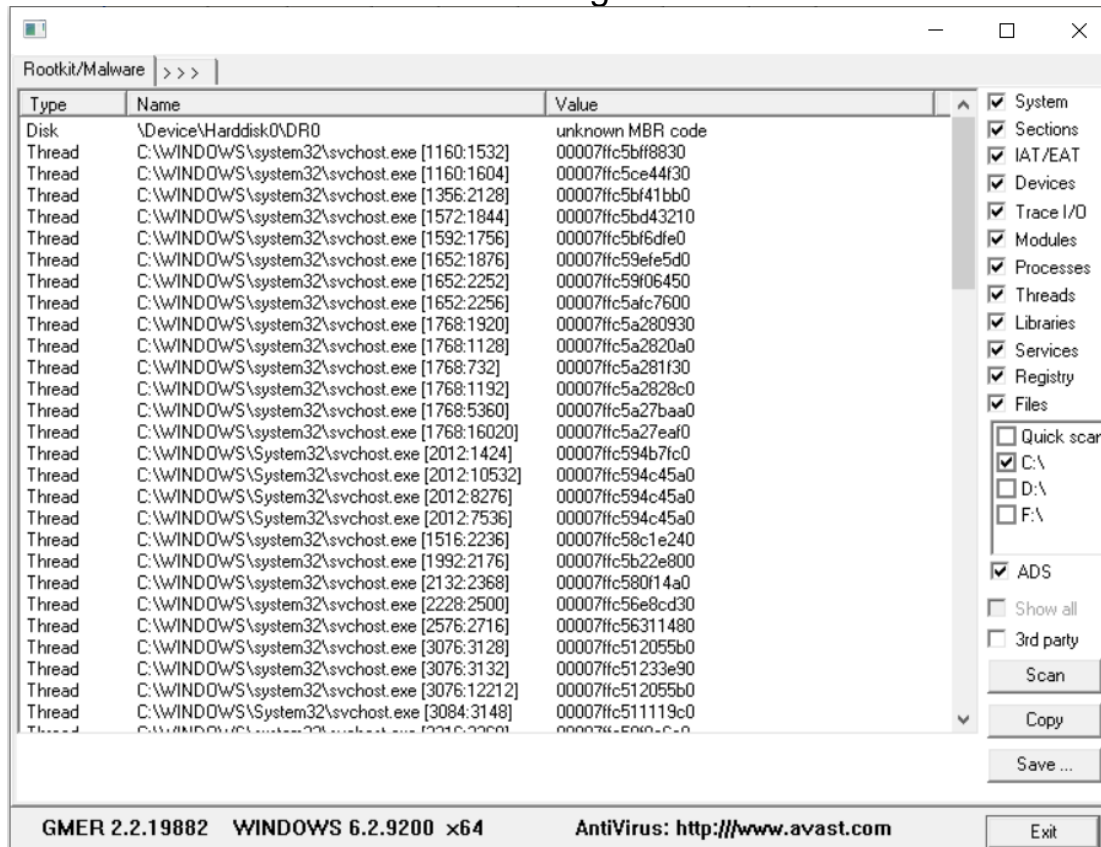
## Exercise 12b:

To install rootkit and to study about the variety of options.

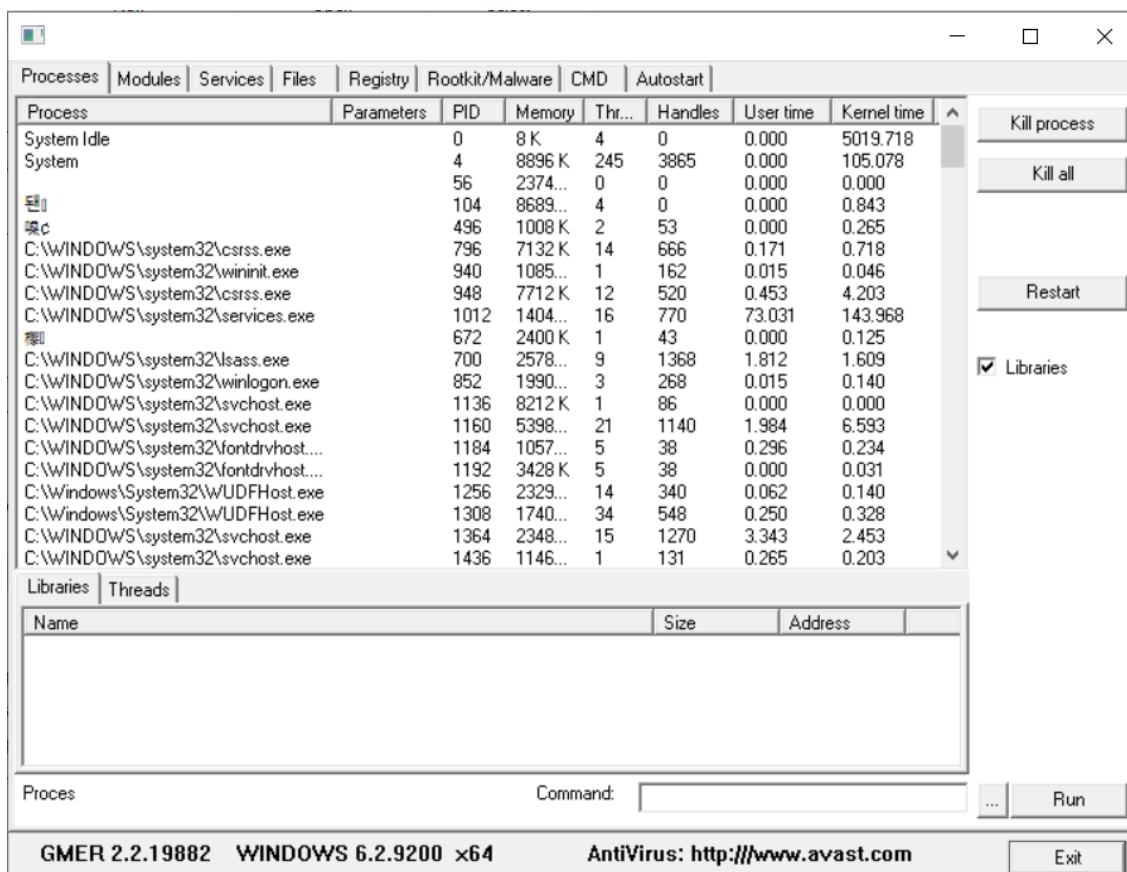
Rootkit screen :



The C: drive is selected for scanning



Processes tab:



## Modules tab:

Processes Modules Services Files Registry Rootkit/Malware CMD Autostart				
Name	File	Address	Size	
ntosknl.exe	\SystemRoot\system32\ntosknl.exe	ffff80663e00000	11227136	
hal.dll	\SystemRoot\system32\hal.dll	ffff80663d5c000	671744	
kd.dll	\SystemRoot\system32\kd.dll	ffff8065f85d000	45056	
msrpc.sys	\SystemRoot\System32\drivers\msrpc.sys	ffff8065f8bd000	393216	
ksecdd.sys	\SystemRoot\System32\drivers\ksecdd.sys	ffff8065f88d000	167936	
werkernel.sys	\SystemRoot\System32\drivers\werkern.sys	ffff8065f86d000	69632	
CLFS.SYS	\SystemRoot\System32\drivers\CLFS.SYS	ffff8065f95d000	425984	
tm.sys	\SystemRoot\System32\drivers\tm.sys	ffff8065f92d000	159744	
PSHED.dll	\SystemRoot\system32\PSHED.dll	ffff8065f9cd000	106496	
BOOTVID.dll	\SystemRoot\system32\BOOTVID.dll	ffff8065f9ed000	45056	
FLTMGR.SYS	\SystemRoot\System32\drivers\FLTMGR.SYS	ffff8065fb0d000	462848	
clips.sys	\SystemRoot\System32\drivers\clips.sys	ffff8065f9fd000	1069056	
cmimcext.sys	\SystemRoot\System32\drivers\cmimcext.sys	ffff8065fb8d000	57344	
ntosext.sys	\SystemRoot\System32\drivers\ntosext.sys	ffff8065fb9d000	49152	
CI.dll	\SystemRoot\system32\CI.dll	ffff80665000000	909312	
cng.sys	\SystemRoot\System32\drivers\cng.sys	ffff806650e0000	770048	
Wdf01000.sys	\SystemRoot\system32\drivers\Wdf01000.sys	ffff806651a0000	872448	
WDFLDR.SYS	\SystemRoot\system32\drivers\WDFLDR.SYS	ffff8065fbad000	77824	
WppRecorder.sys	\SystemRoot\system32\drivers\WppRecorder.sys	ffff8065fbdd000	65536	
SleepStudyHelper.sys	\SystemRoot\system32\drivers\SleepStudyHelper.sys	ffff8065fbcdd000	61440	
acpiex.sys	\SystemRoot\System32\drivers\acpiex.sys	ffff8065fbd0000	151552	
mssecflt.sys	\SystemRoot\system32\drivers\mssecflt.sys	ffff80665280000	294912	
SgmaAgent.sys	\SystemRoot\system32\drivers\SgmaAgent.sys	ffff8065fc2d000	106496	
ACPI.sys	\SystemRoot\System32\drivers\ACPI.sys	ffff806652d0000	835584	
WMILIB.SYS	\SystemRoot\System32\drivers\WMILIB.SYS	ffff8065fc4d000	49152	
msisadv.sys	\SystemRoot\System32\drivers\msisadv.sys	ffff806653a0000	45056	
pci.sys	\SystemRoot\System32\drivers\pci.sys	ffff80665400000	454656	
tpm.sys	\SystemRoot\System32\drivers\tpm.sys	ffff806653b0000	262144	
intelpep.sys	\SystemRoot\System32\drivers\intelpep.sys	ffff80665480000	372736	
WindowsTrustedRT.sys	\SystemRoot\system32\drivers\WindowsTrustedRT.sys	ffff806654e0000	94208	

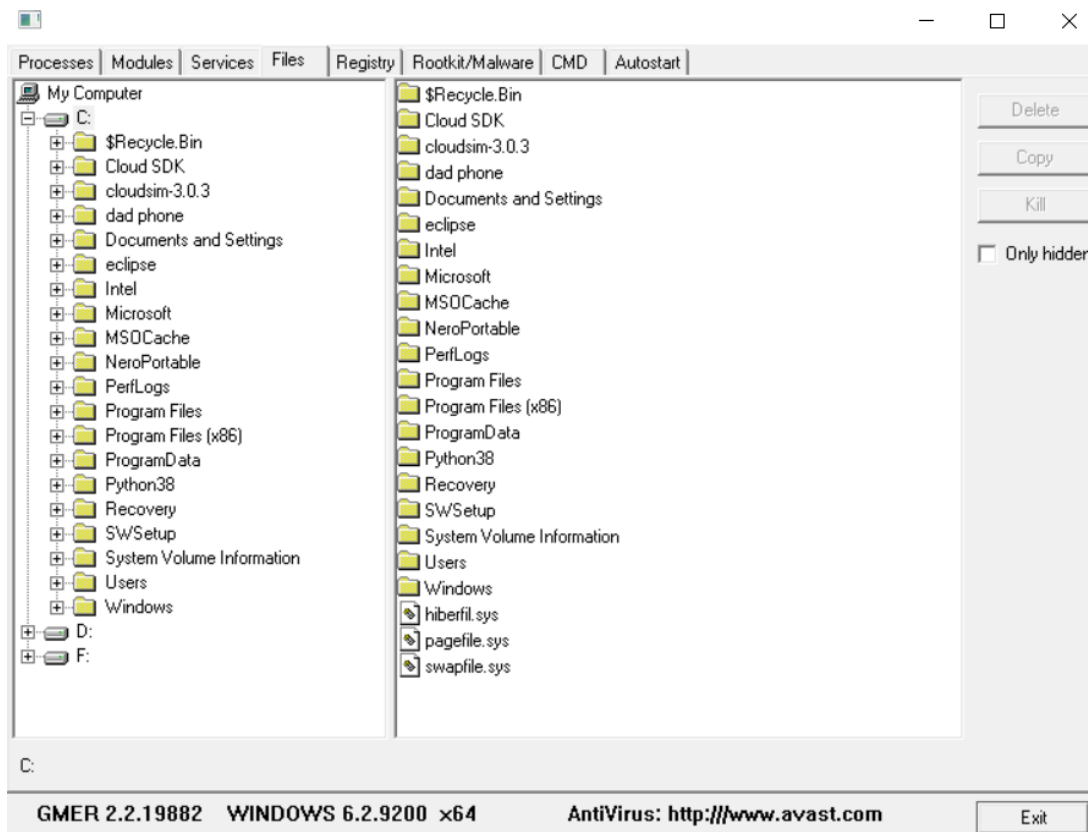
GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com Exit

## Services tab:

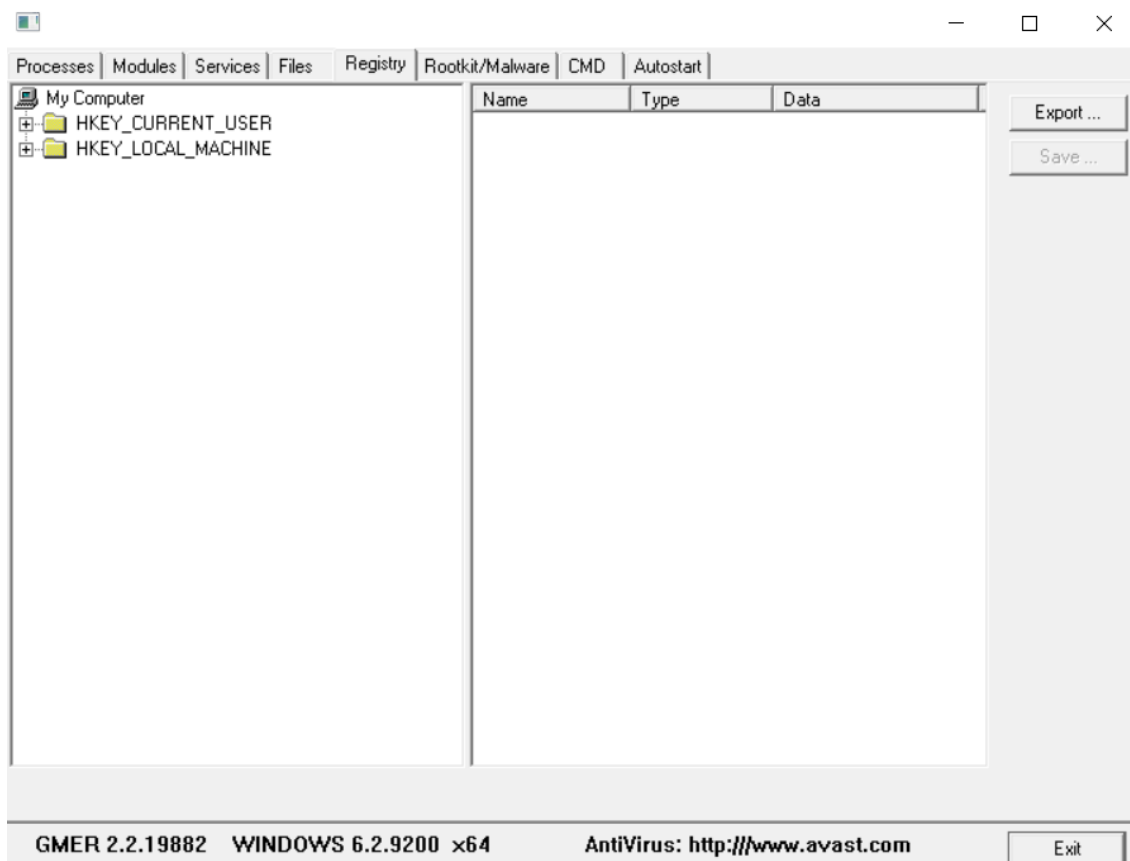
Processes Modules Services Files Registry Rootkit/Malware CMD Autostart				
Name	Start	File name	Description	
.NET CLR Data		%systemroot%\system32\netfxperf.dll		
.NET CLR Netwo...		%systemroot%\system32\netfxperf.dll		
.NET CLR Netwo...		%systemroot%\system32\netfxperf.dll		
.NET Data Provid...		netfxperf.dll		
.NET Data Provid...		%systemroot%\system32\netfxperf.dll		
.NET Memory Ca...		%systemroot%\system32\netfxperf.dll		
.NET Framework		%systemroot%\system32\mscoree.dll		
1394ohci	MANUAL	\SystemRoot\System32\drivers\1394ohci.sys		
3ware	BOOT	System32\drivers\3ware.sys		
AarSvc	MANUAL	%SystemRoot%\System32\AarSvc.dll		
AarSvc_27728d36	MANUAL	C:\WINDOWS\system32\svchost.exe -k AarSvc...	Agent Activation Runtime_27728d36	
ACPI	BOOT	System32\drivers\ACPI.sys		
AcpiDev	MANUAL	\SystemRoot\System32\drivers\AcpiDev.sys		
acpiex	BOOT	System32\drivers\acpiex.sys	Microsoft ACPIex Driver	
acpipagr	MANUAL	\SystemRoot\System32\drivers\acpipagr.sys		
AcpiPmi	MANUAL	\SystemRoot\System32\drivers\acpipmi.sys		
acptime	MANUAL	\SystemRoot\System32\drivers\acptime.sys		
Acx01000	MANUAL	system32\drivers\Acx01000.sys		
AdobeARMservice	AUTO	"C:\Program Files (x86)\Common Files\Adobe\A...	Adobe Acrobat Updater keeps your Adobe softw...	
AdobeFlashPlaye...	MANUAL	C:\Windows\System32\WindowsCommon\Flash\Fla...	This service keeps your Adobe Flash Player inst...	
ADOVMPPackage				
ADP80XX	BOOT	System32\drivers\ADP80XX.SYS		
adsis				
AFD	SYSTEM	\SystemRoot\system32\drivers\afd.sys		
afunix	SYSTEM	\SystemRoot\system32\drivers\afunix.sys	afunix	
ahcache	SYSTEM	system32\DRIVERS\ahcache.sys		
AJRouter	MANUAL	%SystemRoot%\System32\AJRouter.dll		
ALG	MANUAL	%SystemRoot%\System32\alg.exe		
AMD External Ev...	AUTO	%SystemRoot%\System32\DriverStore\FileRepo...		
amdgp2	MANUAL	\SystemRoot\System32\drivers\amdgp2.sys		

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com Exit

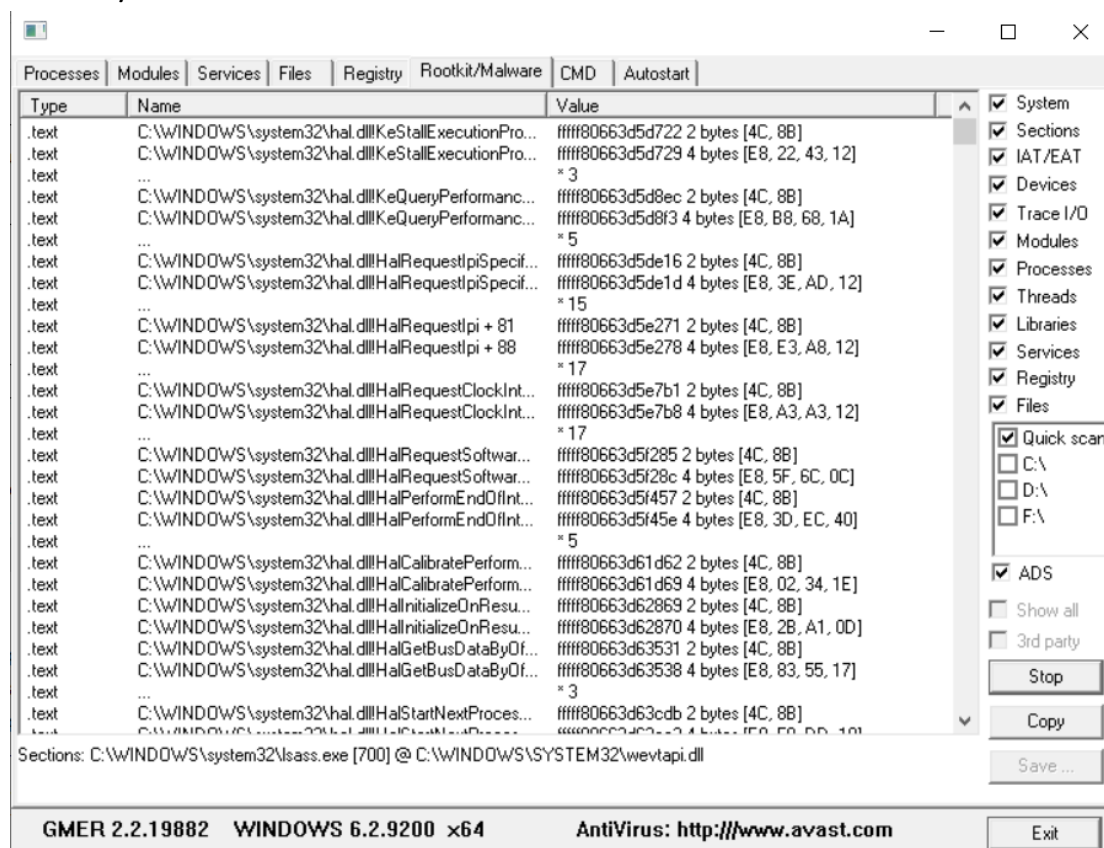
## Files tab:



## Registry tab:



## Rootkit/Malware tab:



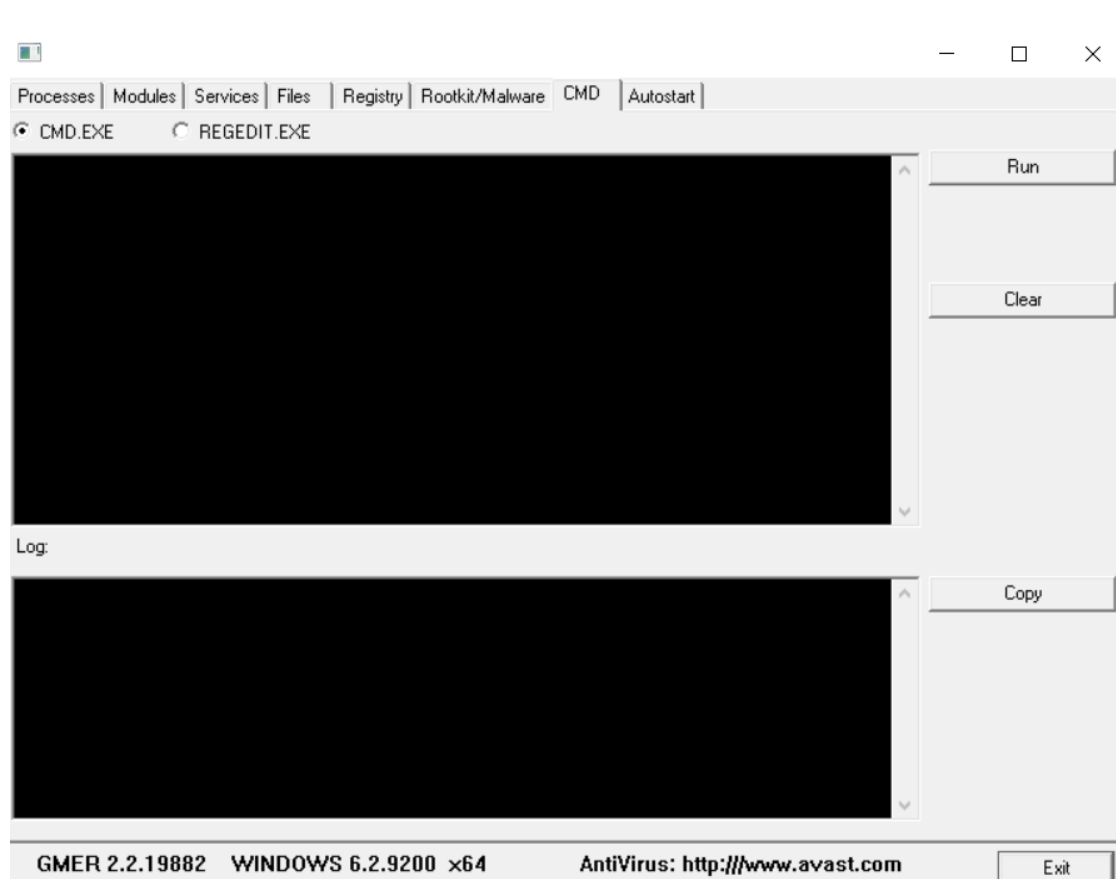
The screenshot shows the 'Rootkit/Malware' tab in the GMER application. The main window displays a list of system files and their values. The right-hand pane contains various scan options, including 'System', 'Sections', 'IAT/EAT', 'Devices', 'Trace I/O', 'Modules', 'Processes', 'Threads', 'Libraries', 'Services', 'Registry', and 'Files'. The 'Quick scan' option is checked, and the 'Show all' and '3rd party' options are unchecked. The 'Stop' button is visible.

Type	Name	Value
.text	C:\WINDOWS\system32\hal.dll\KeStallExecutionPro...	ffff80663d5d722 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\KeStallExecutionPro...	ffff80663d5d729 4 bytes [E8, 22, 43, 12]
.text	...	* 3
.text	C:\WINDOWS\system32\hal.dll\KeQueryPerformanc...	ffff80663d5d8ec 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\KeQueryPerformanc...	ffff80663d5d8f3 4 bytes [E8, B8, 68, 1A]
.text	...	* 5
.text	C:\WINDOWS\system32\hal.dll\HalRequestpiSpecif...	ffff80663d5de16 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalRequestpiSpecif...	ffff80663d5de1d 4 bytes [E8, 3E, AD, 12]
.text	...	* 15
.text	C:\WINDOWS\system32\hal.dll\HalRequestpi + 81	ffff80663d5e271 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalRequestpi + 88	ffff80663d5e278 4 bytes [E8, E3, A8, 12]
.text	...	* 17
.text	C:\WINDOWS\system32\hal.dll\HalRequestClockInt...	ffff80663d5e7b1 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalRequestClockInt...	ffff80663d5e7b8 4 bytes [E8, A3, A3, 12]
.text	...	* 17
.text	C:\WINDOWS\system32\hal.dll\HalRequestSoftwar...	ffff80663d5f285 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalRequestSoftwar...	ffff80663d5f28c 4 bytes [E8, 5F, 6C, 0C]
.text	C:\WINDOWS\system32\hal.dll\HalPerformEndOfInt...	ffff80663d5f457 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalPerformEndOfInt...	ffff80663d5f45e 4 bytes [E8, 3D, EC, 40]
.text	...	* 5
.text	C:\WINDOWS\system32\hal.dll\HalCalibratePerform...	ffff80663d61d62 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalCalibratePerform...	ffff80663d61d69 4 bytes [E8, 02, 34, 1E]
.text	C:\WINDOWS\system32\hal.dll\HalInitializeOnResu...	ffff80663d62869 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalInitializeOnResu...	ffff80663d62870 4 bytes [E8, 2B, A1, 0D]
.text	C:\WINDOWS\system32\hal.dll\HalGetBusDataByOf...	ffff80663d63531 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalGetBusDataByOf...	ffff80663d63538 4 bytes [E8, 83, 55, 17]
.text	...	* 3
.text	C:\WINDOWS\system32\hal.dll\HalStartNextProces...	ffff80663d63cdb 2 bytes [4C, 8B]
.text	C:\WINDOWS\system32\hal.dll\HalStartNextProces...	ffff80663d63cda 4 bytes [E8, 5B, 0D, 10]

Sections: C:\WINDOWS\system32\lsass.exe [700] @ C:\WINDOWS\SYSTEM32\wextapi.dll

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: <http://www.avast.com> Exit

## CMD tab:

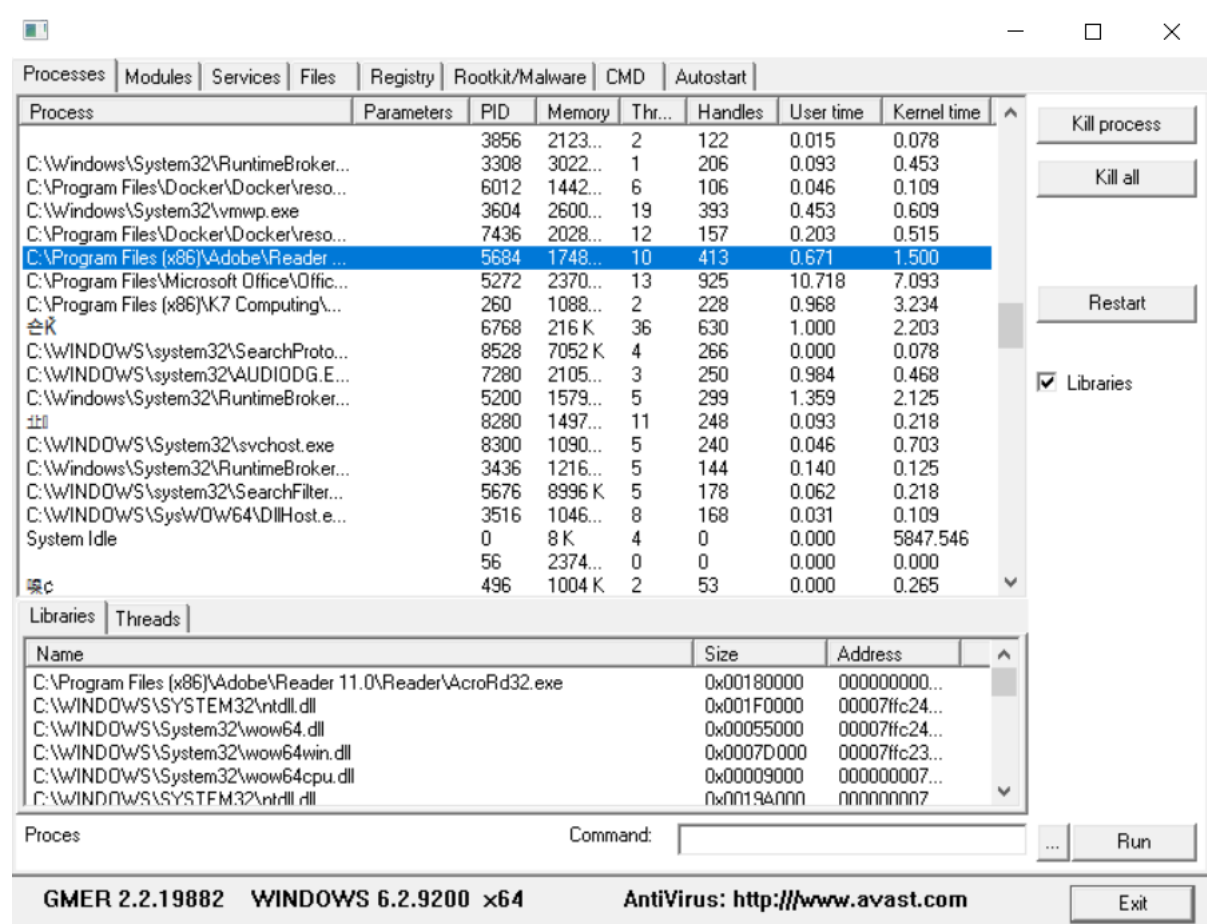


The screenshot shows the 'CMD' tab in the GMER application. The main window displays a command prompt interface. The right-hand pane contains buttons for 'Run', 'Clear', and 'Copy'. The 'Log' section is visible at the bottom.

Log:

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: <http://www.avast.com> Exit

Killing the Adobe process:



The screenshot shows the GMER 2.2.19882 interface. The 'Processes' tab is active, displaying a list of running processes. The process 'C:\Program Files (x86)\Adobe\Reader\Reader.exe' is highlighted in blue. The 'Libraries' tab is also visible, showing a list of loaded DLLs. The bottom status bar indicates 'GMER 2.2.19882 WINDOWS 6.2.9200 x64' and 'AntiVirus: http://www.avast.com'.

Process	Parameters	PID	Memory	Thr...	Handles	User time	Kernel time
C:\Windows\System32\RuntimeBroker...		3856	2123...	2	122	0.015	0.078
C:\Program Files\Docke\Docke\reso...		3308	3022...	1	206	0.093	0.453
C:\Windows\System32\vmwp.exe		6012	1442...	6	106	0.046	0.109
C:\Program Files\Docke\Docke\reso...		3604	2600...	19	393	0.453	0.609
C:\Program Files\Docke\Docke\reso...		7436	2028...	12	157	0.203	0.515
C:\Program Files (x86)\Adobe\Reader...		5684	1748...	10	413	0.671	1.500
C:\Program Files\Microsoft Office\Offic...		5272	2370...	13	925	10.718	7.093
C:\Program Files (x86)\K7 Computing\...		260	1088...	2	228	0.968	3.234
C:\WINDOWS\system32\SearchProto...		6768	216 K	36	630	1.000	2.203
C:\WINDOWS\system32\AUDIOODG.E...		8528	7052 K	4	266	0.000	0.078
C:\Windows\System32\RuntimeBroker...		7280	2105...	3	250	0.984	0.468
C:\Windows\System32\RuntimeBroker...		5200	1579...	5	299	1.359	2.125
C:\WINDOWS\System32\svchost.exe		8280	1497...	11	248	0.093	0.218
C:\Windows\System32\RuntimeBroker...		8300	1090...	5	240	0.046	0.703
C:\WINDOWS\system32\SearchFilter...		3436	1216...	5	144	0.140	0.125
C:\WINDOWS\SysWOW64\DllHost.e...		5676	8996 K	5	178	0.062	0.218
System Idle		3516	1046...	8	168	0.031	0.109
		0	8 K	4	0	0.000	5847.546
		56	2374...	0	0	0.000	0.000
		496	1004 K	2	53	0.000	0.265

Name	Size	Address
C:\Program Files (x86)\Adobe\Reader 11.0\Reader\AcroRd32.exe	0x00180000	00000000...
C:\WINDOWS\SYSTEM32\ntdll.dll	0x001F0000	00007ffc24...
C:\WINDOWS\System32\wow64.dll	0x00055000	00007ffc24...
C:\WINDOWS\System32\wow64win.dll	0x0007D000	00007ffc23...
C:\WINDOWS\System32\wow64cpu.dll	0x00009000	000000007...
C:\WINDOWS\SYSTEM32\ntdll.dll	0x0019A000	000000007...

Process: Command: Run

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com Exit

