

# Digital Forensics

2021SM\_CS\_6419\_FRE1A

## Assignment-03

Prepared by:  
Mohammadali Rahnama

Student number:  
3709515



# 1. Volatility commands and snapshot of the Virustotal detection results for the 4 PIDs

- volatility -f Desktop/ cridex.vmem dlllist -p 788
- volatility -f Desktop/ cridex.vmem ldrmodules -p 788
- volatility -f Desktop/cridex.vmem dlldump --pid=788 --dump-dir ~/Desktop/788/

```
0x820e8da0 alg.exe 0x077fe0000 Secur32.dll OK: module.788.22e8da0.77fe0000.dll
root@fcs-security-attacker:~# volatility -f Desktop/cridex.vmem dlldump --pid=788 --dump-dir ~/Desktop/788/
Volatility Foundation Volatility Framework 2.6
Process(V) Name Module Base Module Name Result
-----
0x820e8da0 alg.exe 0x001000000 alg.exe OK: module.788.22e8da0.10000000.dll
0x820e8da0 alg.exe 0x07c900000 ntdll.dll OK: module.788.22e8da0.7c900000.dll
0x820e8da0 alg.exe 0x076b40000 WINMM.dll OK: module.788.22e8da0.76b40000.dll
0x820e8da0 alg.exe 0x077f60000 SHLWAPI.dll OK: module.788.22e8da0.77f60000.dll
0x820e8da0 alg.exe 0x05ad70000 UxTheme.dll OK: module.788.22e8da0.5ad70000.dll
0x820e8da0 alg.exe 0x0769c0000 USERENV.dll OK: module.788.22e8da0.769c0000.dll
0x820e8da0 alg.exe 0x077dd0000 ADVAPI32.dll OK: module.788.22e8da0.77dd0000.dll
0x820e8da0 alg.exe 0x077be0000 MSACM32.dll OK: module.788.22e8da0.77be0000.dll
0x820e8da0 alg.exe 0x077c00000 VERSION.dll OK: module.788.22e8da0.77c00000.dll
0x820e8da0 alg.exe 0x076fd0000 CLBCATQ.DLL OK: module.788.22e8da0.76fd0000.dll
0x820e8da0 alg.exe 0x06f880000 AcGenral.DLL OK: module.788.22e8da0.6f880000.dll
0x820e8da0 alg.exe 0x000680000 xpsp2res.dll OK: module.788.22e8da0.680000.dll
0x820e8da0 alg.exe 0x071a50000 MSWSOCK.DLL OK: module.788.22e8da0.71a50000.dll
0x820e8da0 alg.exe 0x077e70000 RPCRT4.dll OK: module.788.22e8da0.77e70000.dll
0x820e8da0 alg.exe 0x071a90000 wshtcpip.dll OK: module.788.22e8da0.71a90000.dll
0x820e8da0 alg.exe 0x071ab0000 WS2_32.dll OK: module.788.22e8da0.71ab0000.dll
0x820e8da0 alg.exe 0x071ad0000 WSOCK32.dll OK: module.788.22e8da0.71ad0000.dll
0x820e8da0 alg.exe 0x0774e0000 ole32.dll OK: module.788.22e8da0.774e0000.dll
0x820e8da0 alg.exe 0x077f10000 GDI32.dll OK: module.788.22e8da0.77f10000.dll
0x820e8da0 alg.exe 0x077120000 OLEAUT32.dll OK: module.788.22e8da0.77120000.dll
0x820e8da0 alg.exe 0x077c10000 msvcrt.dll OK: module.788.22e8da0.77c10000.dll
0x820e8da0 alg.exe 0x07c9c0000 SHELL32.dll OK: module.788.22e8da0.7c9c0000.dll
0x820e8da0 alg.exe 0x07c800000 kernel32.dll OK: module.788.22e8da0.7c800000.dll
0x820e8da0 alg.exe 0x0773d0000 comctl32.dll OK: module.788.22e8da0.773d0000.dll
0x820e8da0 alg.exe module. 0x0662b0000 hnetcfg.dll mod OK: module.788.22e8da0.662b0000.dll
0x820e8da0 alg.exe 22e8da0... 78 0x07e410000 USER32.dll 788/22e OK: module.788.22e8da0.7e410000.dll
```

```

root@fcs-security-attacker:~# volatility -f Desktop/cridex.vmem ldrmodules -p 788
Volatility Foundation Volatility Framework 2.6

```

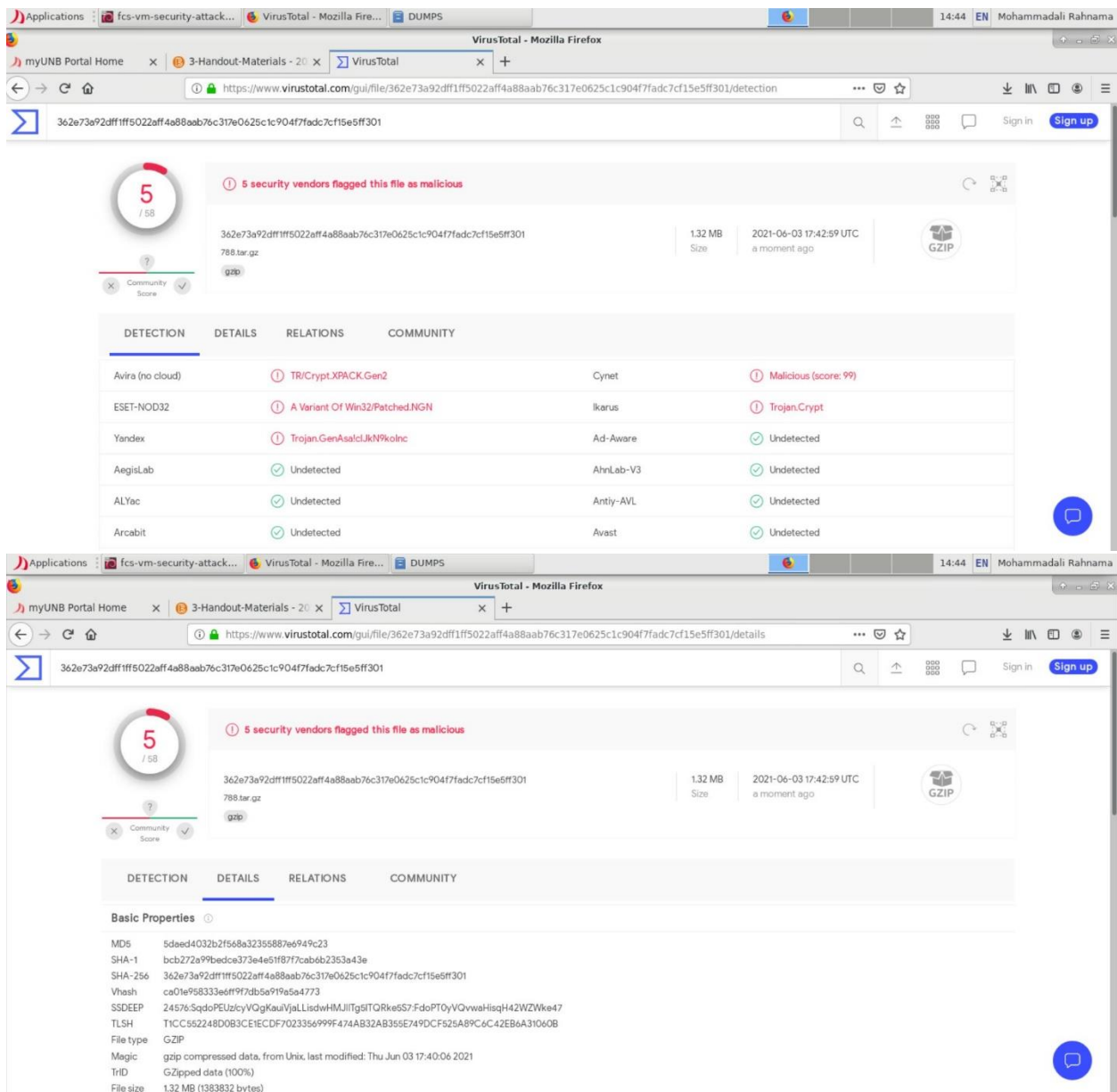
Pid	Process	Base	InLoad	InInit	InMem	MappedPath
788	alg.exe	0x01000000	True	False	True	\WINDOWS\system32\alg.exe
788	alg.exe	0x00680000	True	True	True	\WINDOWS\system32\xpsp2res.dll
788	alg.exe	0x76b40000	True	True	True	\WINDOWS\system32\winmm.dll
788	alg.exe	0x77f60000	True	True	True	\WINDOWS\system32\shlwapi.dll
788	alg.exe	0x77c00000	True	True	True	\WINDOWS\system32\version.dll
788	alg.exe	0x5ad70000	True	True	True	\WINDOWS\system32\uxtheme.dll
788	alg.exe	0x77dd0000	True	True	True	\WINDOWS\system32\advapi32.dll
788	alg.exe	0x77be0000	True	True	True	\WINDOWS\system32\msacm32.dll
788	alg.exe	0x7c800000	True	True	True	\WINDOWS\system32\kernel32.dll
788	alg.exe	0x6f880000	True	True	True	\WINDOWS\AppPatch\AcGenral.dll
788	alg.exe	0x773d0000	True	True	True	\WINDOWS\WinSxS\x86_Microsoft.Windows.Com
788	alg.exe	0x71a50000	True	True	True	\WINDOWS\system32\mswsock.dll
788	alg.exe	0x77e70000	True	True	True	\WINDOWS\system32\rpcrt4.dll
788	alg.exe	0x71a90000	True	True	True	\WINDOWS\system32\wshtcpip.dll
788	alg.exe	0x71ab0000	True	True	True	\WINDOWS\system32\ws2_32.dll
788	alg.exe	0x71ad0000	True	True	True	\WINDOWS\system32\wsnmp32.dll
788	alg.exe	0x774e0000	True	True	True	\WINDOWS\system32\ole32.dll
788	alg.exe	0x7c900000	True	True	True	\WINDOWS\system32\ntdll.dll
788	alg.exe	0x77f10000	True	True	True	\WINDOWS\system32\gdi32.dll
788	alg.exe	0x77120000	True	True	True	\WINDOWS\system32\oleaut32.dll
788	alg.exe	0x5cb70000	True	True	True	\WINDOWS\system32\shimeng.dll
788	alg.exe	0x769c0000	True	True	True	\WINDOWS\system32\userenv.dll
788	alg.exe	0x76fd0000	True	True	True	\WINDOWS\system32\clbcatq.dll
788	alg.exe	0x662b0000	True	True	True	\WINDOWS\system32\hnetcfg.dll
788	alg.exe	0x7e410000	True	True	True	\WINDOWS\system32\user32.dll

```

volatility: error: no such option: -p
root@fcs-security-attacker:~# volatility -f Desktop/cridex.vmem dlllist -p 788
Volatility Foundation Volatility Framework 2.6
*****
alg.exe pid: 788
Command line : C:\WINDOWS\System32\alg.exe
Service Pack 3

```

Base	Size	LoadCount	LoadTime	Path
0x01000000	0xd000	0xffff		C:\WINDOWS\System32\alg.exe
0x7c900000	0xaf000	0xffff		C:\WINDOWS\system32\ntdll.dll
0x7c800000	0xf6000	0xffff		C:\WINDOWS\system32\kernel32.dll
0x77c10000	0x58000	0xffff		C:\WINDOWS\system32\msvcrt.dll
0x76b20000	0x11000	0xffff		C:\WINDOWS\System32\ATL.DLL
0x7e410000	0x91000	0xffff		C:\WINDOWS\system32\USER32.dll
0x77f10000	0x49000	0xffff		C:\WINDOWS\system32\GDI32.dll
0x77dd0000	0x9b000	0xffff		C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x92000	0xffff		C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000	0x11000	0xffff		C:\WINDOWS\system32\Secur32.dll



The top screenshot shows the VirusTotal detection results for a file. The file is flagged as malicious by 5 security vendors. The detection results are as follows:

DETECTION	DETAILS	RELATIONS	COMMUNITY
Avira (no cloud)	TR/Crypt.XPACK.Gen2	Cynet	Malicious (score: 99)
ESET-NOD32	A Variant Of Win32/Patched.NGN	Ikarus	Trojan.Crypt
Yandex	Trojan.GenAsa/cJkN9koInc	Ad-Aware	Undetected
AegisLab	Undetected	AhnLab-V3	Undetected
ALYac	Undetected	Antiy-AVL	Undetected
Arcabit	Undetected	Avast	Undetected

The bottom screenshot shows the basic properties of the file:

Property	Value
MD5	5deed4032b2f568a3235887e6949c23
SHA-1	bcb272a99bedce373e4e5f877cab6b2353a43e
SHA-256	362e73a92dff1ff5022aff4a88aab76c317e0625c1c904f7fadc7cf15e5ff301
Vhash	ca01e95833ed9f7db5e919a5e4773
SSDEEP	24576:SqdoPEUzcyVQgKauVjaLLisdwHMJlITgsITORkeS57:FdoPTOyVQvwaHsqH4ZWZwke47
TLSH	T1CC562248D083CE1ECDF7023356999F474AB32AB355E749DCF525A89C6C42EBAA31060B
File type	GZIP
Magic	gzip compressed data, from Unix, last modified: Thu Jun 03 17:40:06 2021
TriD	GZipped data (100%)
File size	1.32 MB (138382 bytes)

- volatility -f Desktop/stuxnet.vmem dlllist -p 680
- volatility -f Desktop/stuxnet.vmem ldrmodules -p 680
- volatility -f Desktop/ stuxnet.vmem dlldump --pid=680 --dump-dir ~/Desktop/680/



```

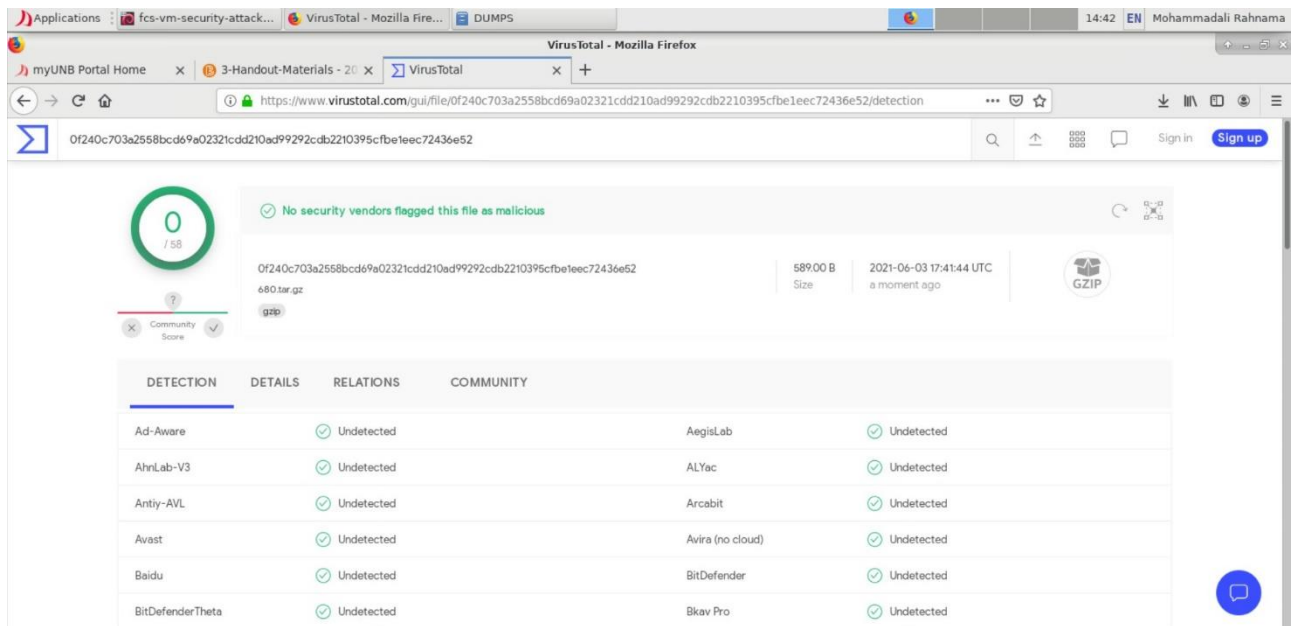
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem dlldump --pid=680 --dump-dir ~/Desktop/680/
Volatility Foundation Volatility Framework 2.6
Process(V) Name Module Base Module Name Result
-----
0x81e70020 lsass.exe 0x001000000 lsass.exe OK: module.680.2070020.1000000.dll
0x81e70020 lsass.exe 0x07c900000 Error: DllBase is paged
0x81e70020 lsass.exe 0x0743c0000 psbase.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x076b40000 WINMM.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x075730000 LSASRV.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x076f60000 WLDAP32.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x077c00000 VERSION.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x05ad70000 UxTheme.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x074380000 wdigest.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x068000000 rsaenh.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x0769c0000 USERENV.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x0767a0000 NTDSAPI.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x0767c0000 w32time.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x077dd0000 ADVAPI32.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x077a80000 CRYPT32.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x077fe0000 Secur32.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x074410000 scecli.dll Error: DllBase is paged
0x81e70020 lsass.exe 0x071b20000 MPR.dll Error: DllBase is paged

root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem ldrmodules -p 680
Volatility Foundation Volatility Framework 2.6
Pid Process Base InLoad InInit InMem MappedPath
-----
680 lsass.exe module. 0x01000000 True False True \WINDOWS\system32\lsass.exe

root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem dlllist -p 680
Volatility Foundation Volatility Framework 2.6
*****
lsass.exe pid: 680
Command line : C:\WINDOWS\system32\lsass.exe
Service Pack 3
7882

Base Size LoadCount LoadTime Path
-----
0x01000000 0x6000 0xffff C:\WINDOWS\system32\lsass.exe
0x7c900000 0xaf000 0xffff C:\WINDOWS\system32\ntdll.dll
0x7c800000 0xf6000 0xffff C:\WINDOWS\system32\kernel32.dll
0x77dd0000 0x9b000 0xffff C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000 0x92000 0xffff C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000 0x11000 0xffff C:\WINDOWS\system32\Secur32.dll
0x75730000 0xb5000 0xffff C:\WINDOWS\system32\LSASRV.dll
0x71b20000 0x12000 0xffff C:\WINDOWS\system32\MPR.dll
0x7e410000 0x91000 0xffff C:\WINDOWS\system32\USER32.dll
0x77f10000 0x49000 0xffff C:\WINDOWS\system32\GDI32.dll
0x77b20000 0x12000 0xffff C:\WINDOWS\system32\MSASN1.dll
0x77c10000 0x58000 0xffff C:\WINDOWS\system32\msvcrt.dll
0x5b860000 0x55000 0xffff C:\WINDOWS\system32\NETAPI32.dll
0x767a0000 0x13000 0xffff module. module. module. C:\WINDOWS\system32\NTDSAPI.dll
0x76f20000 0x27000 0xffff module. module. module. C:\WINDOWS\system32\DNSAPI.dll
0x71b20000 0x12000 0xffff C:\WINDOWS\system32\MPR.dll

```



- volatility -f Desktop/stuxnet.vmem dlldump -p 868
- volatility -f Desktop/stuxnet.vmem ldrmodules -p 868
- volatility -f Desktop/stuxnet.vmem dlldump --pid=868 --dump-dir ~/Desktop/868/

```
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem ldrmodules -p 868
Volatility Foundation Volatility Framework 2.6
Pid      Process      Base      InLoad InInit InMem MappedPath
-----
868 lsass.exe 0x00080000 False False False
868 lsass.exe 0x7c900000 True True True \WINDOWS\system32\ntdll.dll
868 lsass.exe 0x77e70000 True True True \WINDOWS\system32\RPCRT4.dll
868 lsass.exe 0x7c800000 True True True \WINDOWS\system32\kernel32.dll
868 lsass.exe 0x77fe0000 True True True \WINDOWS\system32\Secur32.dll
868 lsass.exe 0x7e410000 True True True \WINDOWS\system32\user32.dll
868 lsass.exe 0x01000000 True False True
868 lsass.exe 0x77f10000 True True True \WINDOWS\system32\GDI32.dll
868 lsass.exe 0x77dd0000 True True True \WINDOWS\system32\ADVAPI32.dll
root@fcs-security-attacker:~#
868 lsass.exe 0x77dd0000 True True True \WINDOWS\system32\ADVAPI32.dll
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem dlldump --pid=868 --dump-dir ~/Desktop/868/
Volatility Foundation Volatility Framework 2.6
Process(V) Name      Module Base Module Name      Result
-----
0x81c498c8 lsass.exe 0x00100000 lsass.exe OK: module.868.1e498c8.1000000.dll
0x81c498c8 lsass.exe 0x07c90000 ntdll.dll OK: module.868.1e498c8.7c90000.dll
0x81c498c8 lsass.exe 0x077e7000 RPCRT4.dll OK: module.868.1e498c8.77e7000.dll
0x81c498c8 lsass.exe 0x077f1000 GDI32.dll OK: module.868.1e498c8.77f1000.dll
0x81c498c8 lsass.exe 0x077dd000 ADVAPI32.dll OK: module.868.1e498c8.77dd000.dll
0x81c498c8 lsass.exe 0x07c80000 kernel32.dll OK: module.868.1e498c8.7c80000.dll
0x81c498c8 lsass.exe 0x07e41000 USER32.dll OK: module.868.1e498c8.7e41000.dll
0x81c498c8 lsass.exe 0x077fe000 Secur32.dll OK: module.868.1e498c8.77fe000.dll
root@fcs-security-attacker:~#
```

```

root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem dlllist -p 868
Volatility Foundation Volatility Framework 2.6
*****
lsass.exe pid: 868
Command line : "C:\WINDOWS\system32\lsass.exe"
Service Pack 3

```

Base	Size	LoadCount	LoadTime	Path
0x01000000	0x6000	0xffff		C:\WINDOWS\system32\lsass.exe
0x7c900000	0xaf000	0xffff		C:\WINDOWS\system32\ntdll.dll
0x7c800000	0xf6000	0xffff		C:\WINDOWS\system32\kernel32.dll
0x77dd0000	0x9b000	0xffff		C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x92000	0xffff		C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000	0x11000	0xffff		C:\WINDOWS\system32\Secur32.dll
0x7e410000	0x91000	0xffff		C:\WINDOWS\system32\USER32.dll
0x77f10000	0x49000	0xffff		C:\WINDOWS\system32\GDI32.dll

```

root@fcs-security-attacker:~#

```

32 / 58 security vendors flagged this file as malicious

441e010a8e870facbdb67b540ec83c9cf58e9e64a705a237e7563f7761dd7c7

356.84 KB Size

2021-06-03 17:45:20 UTC a moment ago

868.tar.gz

gZip

DETECTION	DETAILS	RELATIONS	COMMUNITY
AegisLab	Worm.Win32.Stuxnet.Iv3n	AhnLab-V3	Trojan.Win32.Genome.R150575
Antiy-AVL	Trojan.Generic.ASMalw.FH.7976F9	Arcabit	Trojan.Kazy.D12C0B
Avast	Win32:Duqu-F [Rtk]	AVG	Win32:Duqu-F [Rtk]
Avira (no cloud)	TR/Crypt.XPACK.Gen	BitDefender	Gen.Variant.Kazy.76811
BitDefenderTheta	AltPacker.C89F107B21	Comodo	Malware@#21c6ogu33uk1c
Cynet	Malicious (score: 99)	Cyren	W32/Duqu.OFNC-1922

- volatility -f Desktop/stuxnet.vmem dlllist -p 1928
- volatility -f Desktop/stuxnet.vmem ldrmodules -p 1928
- volatility -f Desktop/ stuxnet.vmem dlldump --pid=1928 --dump-dir ~/Desktop/1928/



```
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem dlldump --pid=1928 --dump-dir ~/Desktop/1928/
```

```
Volatility Foundation Volatility Framework 2.6
Process(V) Name Module Base Module Name Result
-----
0x81c47c00 lsass.exe 0x001000000 lsass.exe OK: module.1928.1e47c00.1000000.dll
0x81c47c00 lsass.exe 0x07c900000 ntdll.dll OK: module.1928.1e47c00.7c900000.dll
0x81c47c00 lsass.exe 0x077f60000 SHLWAPI.dll OK: module.1928.1e47c00.77f60000.dll
0x81c47c00 lsass.exe 0x0771b0000 WININET.dll OK: module.1928.1e47c00.771b0000.dll
0x81c47c00 lsass.exe 0x077dd0000 ADVAPI32.dll OK: module.1928.1e47c00.77dd0000.dll
0x81c47c00 lsass.exe 0x077a80000 CRYPT32.dll OK: module.1928.1e47c00.77a80000.dll
0x81c47c00 lsass.exe 0x077fe0000 Secur32.dll OK: module.1928.1e47c00.77fe0000.dll
0x81c47c00 lsass.exe 0x077c00000 VERSION.dll OK: module.1928.1e47c00.77c00000.dll
0x81c47c00 lsass.exe 0x076d60000 IPHLPAPI.DLL OK: module.1928.1e47c00.76d60000.dll
0x81c47c00 lsass.exe 0x05b860000 NETAPI32.dll OK: module.1928.1e47c00.5b860000.dll
0x81c47c00 lsass.exe 0x071ab0000 WS2_32.dll OK: module.1928.1e47c00.71ab0000.dll
0x81c47c00 lsass.exe 0x071ad0000 WSOCK32.dll OK: module.1928.1e47c00.71ad0000.dll
0x81c47c00 lsass.exe 0x0774e0000 ole32.dll OK: module.1928.1e47c00.774e0000.dll
0x81c47c00 lsass.exe 0x07e410000 USER32.dll OK: module.1928.1e47c00.7e410000.dll
0x81c47c00 lsass.exe 0x077f10000 GDI32.dll OK: module.1928.1e47c00.77f10000.dll
0x81c47c00 lsass.exe 0x077120000 OLEAUT32.dll OK: module.1928.1e47c00.77120000.dll
0x81c47c00 lsass.exe 0x0769c0000 USERENV.dll OK: module.1928.1e47c00.769c0000.dll
0x81c47c00 lsass.exe 0x07c800000 kernel32.dll OK: module.1928.1e47c00.7c800000.dll
0x81c47c00 lsass.exe 0x0773d0000 comctl32.dll OK: module.1928.1e47c00.773d0000.dll
0x81c47c00 lsass.exe 0x076bf0000 PSAPI.DLL OK: module.1928.1e47c00.76bf0000.dll
0x81c47c00 lsass.exe 0x077c10000 msvcrt.dll OK: module.1928.1e47c00.77c10000.dll
0x81c47c00 lsass.exe 0x077e70000 RPCRT4.dll OK: module.1928.1e47c00.77e70000.dll
0x81c47c00 lsass.exe 0x000870000 KERNEL32...0360b7ab OK: module.1928.1e47c00.870000.dll
0x81c47c00 lsass.exe 0x076f20000 DNSAPI.dll OK: module.1928.1e47c00.76f20000.dll
0x81c47c00 lsass.exe 0x07c9c0000 SHELL32.dll OK: module.1928.1e47c00.7c9c0000.dll
0x81c47c00 lsass.exe 0x071aa0000 WS2HELP.dll OK: module.1928.1e47c00.71aa0000.dll
```

```
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem ldrmodules -p 1928
```

```
Volatility Foundation Volatility Framework 2.6
Pid Process Base InLoad InInit InMem MappedPath
-----
1928 lsass.exe 0x00080000 False False False
1928 lsass.exe 0x7c900000 True True True \WINDOWS\system32\ntdll.dll
1928 lsass.exe 788 0x773d0000 True True True \WINDOWS\WinSxS\x86_Microsoft.Windows.C
.dll
1928 lsass.exe 0x77f60000 True True True \WINDOWS\system32\shlwapi.dll
1928 lsass.exe 0x771b0000 True True True \WINDOWS\system32\wininet.dll
1928 lsass.exe 0x77a80000 True True True \WINDOWS\system32\crypt32.dll
1928 lsass.exe 0x77fe0000 True True True \WINDOWS\system32\secur32.dll
1928 lsass.exe 0x77c00000 True True True \WINDOWS\system32\version.dll
1928 lsass.exe 0x01000000 True False True
1928 lsass.exe 0x5b860000 True True True \WINDOWS\system32\netapi32.dll
1928 lsass.exe 0x77e70000 True True True \WINDOWS\system32\rpcrt4.dll
1928 lsass.exe 0x71ab0000 True True True \WINDOWS\system32\ws2_32.dll
1928 lsass.exe 0x71ad0000 True True True \WINDOWS\system32\wsck32.dll
1928 lsass.exe 0x774e0000 True True True \WINDOWS\system32\ole32.dll
1928 lsass.exe 0x7e410000 True True True \WINDOWS\system32\user32.dll
1928 lsass.exe 0x77f10000 True True True \WINDOWS\system32\gdi32.dll
1928 lsass.exe 0x77120000 True True True \WINDOWS\system32\oleaut32.dll
1928 lsass.exe 0x76d60000 True True True \WINDOWS\system32\iphlpapi.dll
1928 lsass.exe 0x769c0000 True True True \WINDOWS\system32\userenv.dll
1928 lsass.exe 0x7c800000 True True True \WINDOWS\system32\kernel32.dll
1928 lsass.exe 0x76bf0000 True True True \WINDOWS\system32\psapi.dll
1928 lsass.exe 0x77c10000 True True True \WINDOWS\system32\msvcrt.dll
1928 lsass.exe 0x77dd0000 True True True \WINDOWS\system32\advapi32.dll
1928 lsass.exe 0x7c9c0000 True True True \WINDOWS\system32\shell32.dll
1928 lsass.exe 0x00870000 True True True
1928 lsass.exe 0x76f20000 True True True \WINDOWS\system32\dnsapi.dll
```

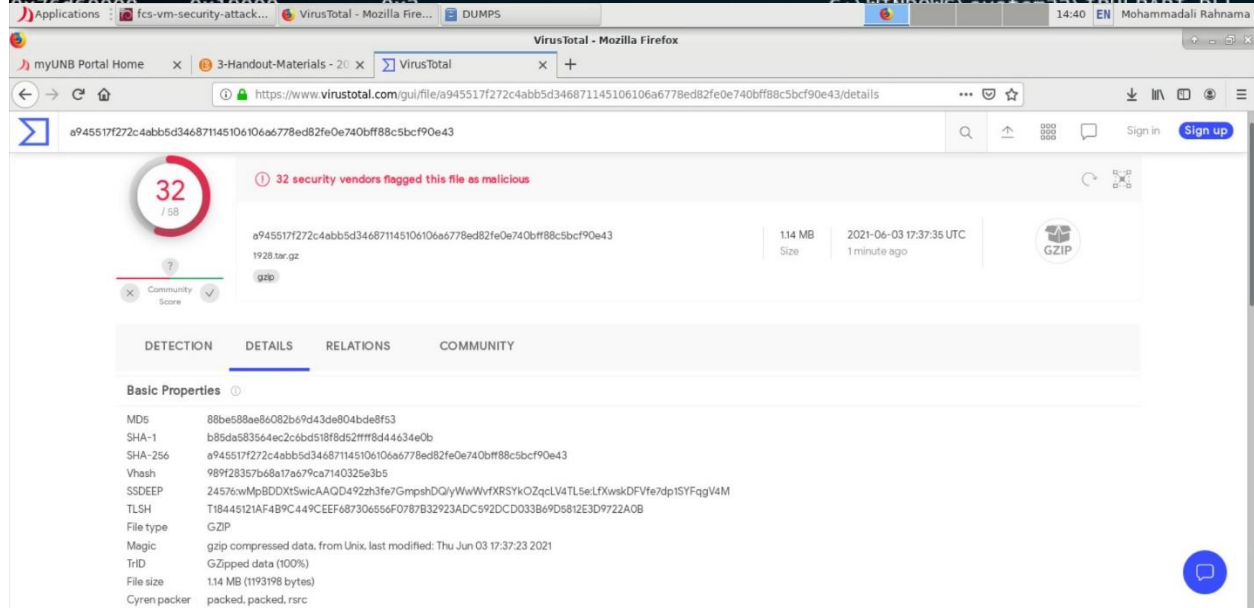


```

root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem dlllist -p 1928
Volatility Foundation Volatility Framework 2.6
*****
lsass.exe pid: 1928
Command line : "C:\WINDOWS\system32\lsass.exe"
Service Pack 3

```

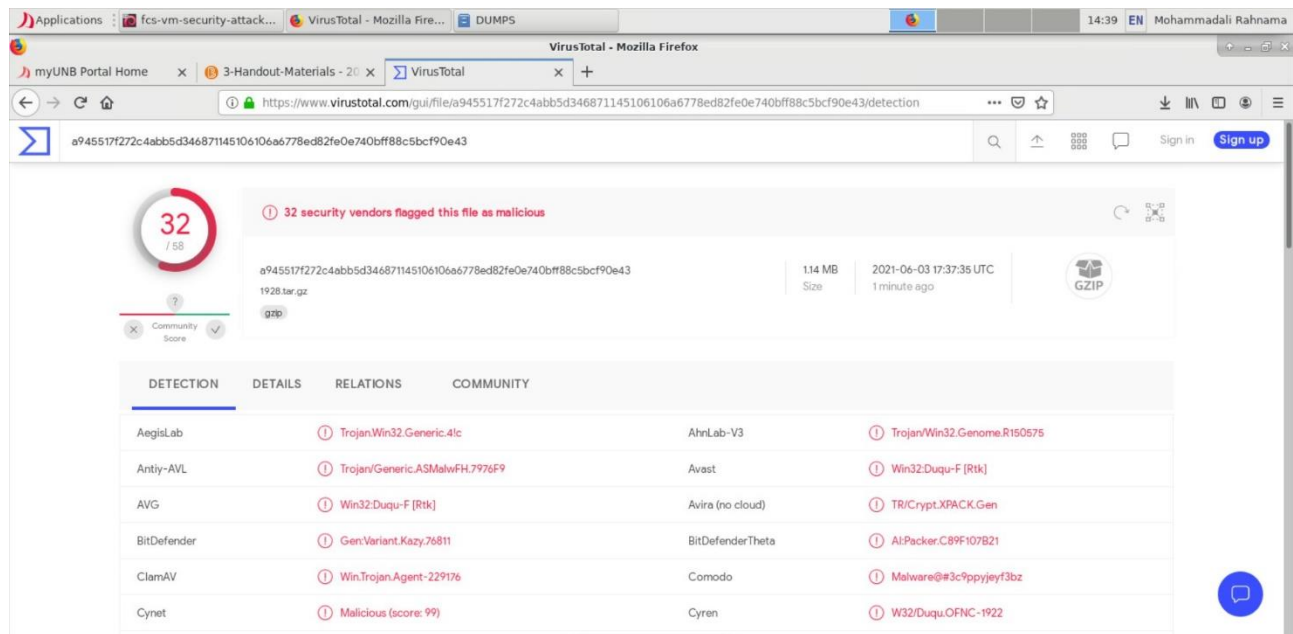
Base	Size	LoadCount	LoadTime	Path
0x01000000	0x6000	0xffff		C:\WINDOWS\system32\lsass.exe
0x7c900000	0xaf000	0xffff		C:\WINDOWS\system32\ntdll.dll
0x7c800000	0xf6000	0xffff		C:\WINDOWS\system32\kernel32.dll
0x77dd0000	0x9b000	0xffff		C:\WINDOWS\system32\ADVAPI32.dll
0x77e70000	0x92000	0xffff		C:\WINDOWS\system32\RPCRT4.dll
0x77fe0000	0x11000	0xffff		C:\WINDOWS\system32\Secur32.dll
0x7e410000	0x91000	0xffff		C:\WINDOWS\system32\USER32.dll
0x77f10000	0x49000	0xffff		C:\WINDOWS\system32\GDI32.dll
0x00870000	0x138000	0x1		C:\WINDOWS\system32\KERNEL32.DLL.ASL
0x76f20000	0x27000	0x2		C:\WINDOWS\system32\DNSAPI.dll
0x77c10000	0x58000	0x27		C:\WINDOWS\system32\msvcrt.dll
0x71ab0000	0x17000	0xa		C:\WINDOWS\system32\WS2_32.dll
0x71aa0000	0x8000	0x8		C:\WINDOWS\system32\WS2HELP.dll

**32** / 58  
32 security vendors flagged this file as malicious

File: 1928.tar.gz  
Size: 1.14 MB  
Date: 2021-06-03 17:37:35 UTC  
Format: GZIP

Property	Value
MD5	88be588ae86082b69d43de804bde8f53
SHA-1	b85da583544ec2c6bd518f8d52fff8d44634e0b
SHA-256	a945517f272c4abb5d346871145106106a6778ed82fe0e740bfb88c5bcf90e43
Vhash	989f28357b68a17a679ca7140325e3b5
SSDEEP	24576:WpBDDXt5wicAAQD49Zzh3f7GmpshDQlyWwVvFXRSYkOZqCLV4TL5eLFXwskDFVfe7dp1SYFqgV4M
TLSH	T18445121AF4B9C449CEEf687306556F0787B32923ADC592DCD033869D5812E3D9722A0B
File type	GZIP
Magic	gzip compressed data, from Unix, last modified: Thu Jun 03 17:37:23 2021
TrID	GZipped data (100%)
File size	1.14 MB (1193198 bytes)
Cyren packer	packed, packed, rsrc



## 2. How many register keys in Stuxnet case have been added to the computer?

According to [Panda Security](#) Stuxnet will create the following entries in the Windows Registry:

- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXCLS
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXCLS\0000
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXCLS\0000\Control
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXNET
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXNET\0000
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Enum\Root\LEGACY\_MRXNET\0000\Control
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxCls
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxCls\Enum
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxNet
- HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\MRxNet\Enum
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXCLS
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXCLS\0000
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXCLS\0000\Control
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXNET
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXNET\0000
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Enum\Root\LEGACY\_MRXNET\0000\Control
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxCls\Enum
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet
- HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MRxNet\Enum

We were able to find most of them in our file the screenshots are as follows:

```

Volatility: Error: Option -K: Invalid integer value: \\windows\\system32\\cmd.exe
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem printkey -K "Controlset001\\Enum\\Root"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

```

```

-----
Registry: \\Device\\HarddiskVolume1\\WINDOWS\\system32\\config\\system
Key name: Root (S)
Last updated: 2011-06-03 04:26:47 UTC+0000

```

```

Subkeys:
(S) *PNP0501
(S) ACPI_HAL
(S) COMPOSITE_BATTERY
(S) dmio
(S) ftdisk
(S) LEGACY_AFD
(S) LEGACY_ALG
(S) LEGACY_AUDIOSRV
(S) LEGACY_BEEP
(S) LEGACY_BITS
(S) LEGACY_BROWSER
(S) LEGACY_CDFS
(S) LEGACY_CLR_OPTIMIZATION_V2.0.50727_32
(S) LEGACY_CLR_OPTIMIZATION_V4.0.30319_32
(S) LEGACY_COMSYSAPP
(S) LEGACY_CRYPTSVC
(S) LEGACY_DCOMLAUNCH
(S) LEGACY_DHCP
(S) LEGACY_DMBOOT
(S) LEGACY_DMLOAD
(S) LEGACY_DMSERVER

```

```

(S) LEGACY_IPNAT
(S) LEGACY_IPSEC
(S) LEGACY_JAVAQUICKSTARTERSERVICE
(S) LEGACY_KSECDD
(S) LEGACY_LANMANSERVER
(S) LEGACY_LANMANWORKSTATION
(S) LEGACY_LMHOSTS
(S) LEGACY_MNMDD
(S) LEGACY_MOUNTMGR

```

```

(S) LEGACY_MRXCLS
(S) LEGACY_MRXDAV
(S) LEGACY_MRXNET
(S) LEGACY_MRXSMB
(S) LEGACY_MSDTC
(S) LEGACY_MSE

```

```

root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem printkey -K "Controlset001\\Enum\\Root\\LEGACY_MRXNET"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile

```

```

-----
Registry: \\Device\\HarddiskVolume1\\WINDOWS\\system32\\config\\system
Key name: LEGACY_MRXNET (S)
Last updated: 2011-06-03 04:26:47 UTC+0000

```

```

Subkeys:
(S) 0000

```

```

Values:
REG_DWORD NextInstance : (S) 1

```

```

root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem printkey -K "Software\\Microsoft\\Windows\\CurrentVersion

```



```

root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem hivelist
Volatility Foundation Volatility Framework 2.6
-----
Virtual Physical Name
-----
0xe1069008 0x14b8d008 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1077758 0x152b7758 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
0xe1bd9b9e 0x0e1959e8 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1bd5b60 0x0e027b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1bc26d8 0x0de626d8 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1bb5758 0x0df10758 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe1628b60 0x0a7a0b60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1638b60 0x0a7a0b60 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1638b60 0x0a7a0b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe1628008 0x0a7a0b60 \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0xe13feb60 0x02e6ab60 [no name]
0xe1035b60 0x02a9eb60 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe102e008 0x02a98008 [no name]
0xe102e008 0x02a98008 [no name]
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem printkey -K "Software\Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile
-----
Registry: \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
Key name: Run (S)
Last updated: 2010-08-22 17:37:49 UTC+0000

Subkeys:

Values:
-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\default
Key name: Run (S)
Last updated: 2010-08-22 13:32:52 UTC+0000

Subkeys:

Values:
-----
Registry: \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
Key name: Run (S)
Last updated: 2010-08-22 17:37:44 UTC+0000

Subkeys:

Values:
-----
root@fcs-security-attacker:~# volatility -f Desktop/stuxnet.vmem printkey -K "Controlset001\Enum\Root\LEGACY_MRXNET\0000"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable (V) = Volatile
-----
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: 0000 (S)
Last updated: 2011-06-03 04:26:47 UTC+0000

Subkeys:
(V) Control

Values:
REG_SZ Service : (S) MRxNet
REG_DWORD Legacy : (S) 1
REG_DWORD ConfigFlags : (S) 0
REG_SZ Class : (S) LegacyDriver
REG_SZ ClassGUID : (S) {8ECC055D-047F-11D1-A537-0000F8753ED1}
REG_SZ DeviceDesc : (S) MRXNET
root@fcs-security-attacker:~#

```

### 3. Why does Stuxnet need these register keys?

Stuxnet creates these entries so that the rootkits can register as a service and run whenever the computer boots. They are also injected into the lsass.exe process so that they cannot be viewed.