

Bu çalışmada BlackEnergy zararlı yazılımı tarafından enfekte edilmiş bir sistemin alınan ram imajı analiz edilecektir.

İmaj alınırken sistemde çalışan processlerin neler olduğunu görmek için Windows.pstree komutunu kullanacağız. Bu komut ile çalışan processlerin parent-child ilişkilerini inceleyeceğiz. Bunun için aşağıdaki komutu çalıştırıyoruz.

```
1 Volatility 3 Framework 2.7.0
2
3 PID PPID ImageFileName Offset(V) Threads Handles SessionId Wow64 CreateTime ExitTime Audit Cmd Path
4
5 4 0 System 0x89c037f8 55 245 N/A N/A - -
6 368 4 smss.exe 0x89965020 3 19 N/A False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\smss.exe \SystemRoot\System32\smss.exe \SystemRoot\System32\smss.exe
7 592 368 csrss.exe 0x89a98da0 11 321 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\csrss.exe C:\WINDOWS\system32\csrss.exe ObjectDirectory\Windows
SharedSection=1024,3072,512 Windows-On SubsystemType=Windows ServerDll=basesrv,1 ServerDll=winlsrv:UserServerDllInitialization,3 ServerDll=winlsrv:ConServerDllInit
MaxRequestThreads=16 \??\C:\WINDOWS\system32\csrss.exe
8 616 368 winlogon.exe 0x89a88da0 18 508 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\winlogon.exe winlogon.exe \??\C:\WINDOWS\system32\winlogon.exe
9 672 616 lsass.exe 0x89aa0020 21 335 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\lsass.exe C:\WINDOWS\system32\lsass.exe C:\WINDOWS\system32\lsass.exe
10 660 616 services.exe 0x89938908 15 240 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\services.exe C:\WINDOWS\system32\services.exe C:\WINDOWS\system32\services.exe
11 832 660 VBoxService.exe 0x899aa3d8 9 115 0 False 2023-02-14 04:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\VBoxService.exe C:\WINDOWS\system32\VBoxService.exe C:
\WINDOWS\system32\VBoxService.exe
12 1060 660 svchost.exe 0x89730da0 51 1072 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs C:
\WINDOWS\system32\svchost.exe
13 1156 1060 wscntfy.exe 0x89694388 1 20 0 False 2023-02-13 17:54:39.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\wscntfy.exe C:\WINDOWS\system32\wscntfy.exe C:\WINDOWS\system32\wscntfy.exe
14 1156 660 svchost.exe 0x899adda0 13 192 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService C:
\WINDOWS\system32\svchost.exe
15 968 660 svchost.exe 0x89a9f6f8 10 244 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k rpcss C:\WINDOWS\system32\svchost.exe
16 1060 660 spoolsv.exe 0x897075d0 10 106 0 False 2023-02-13 17:54:18.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\spoolsv.exe C:\WINDOWS\system32\spoolsv.exe C:\WINDOWS\system32\spoolsv.exe
17 800 660 svchost.exe 0x89aa0590 21 295 0 False 2023-02-13 17:54:16.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch C:
\WINDOWS\system32\svchost.exe
18 1108 660 svchost.exe 0x897289a8 5 78 0 False 2023-02-13 17:54:17.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkService C:
\WINDOWS\system32\svchost.exe
19 540 660 alg.exe 0x8969d2a0 5 102 0 False 2023-02-13 17:54:30.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\alg.exe C:\WINDOWS\system32\alg.exe C:\WINDOWS\system32\alg.exe
20 1484 1484 explorer.exe 0x897f3908 24 489 0 False 2023-02-13 17:54:15.000000 N/A \Device\HarddiskVolume1\WINDOWS\Explorer.EXE C:\WINDOWS\Explorer.EXE C:\WINDOWS\Explorer.EXE
21 964 1484 rootkit.exe 0x899dd740 0 0 False 2023-02-13 18:25:26.000000 2023-02-13 18:25:26.000000 \Device\HarddiskVolume1\Documents and Settings\CyberDefenders\Desktop\rootkit.exe - -
22 1960 964 cmd.exe 0x89a18da0 0 0 False 2023-02-13 18:25:26.000000 2023-02-13 18:25:26.000000 \Device\HarddiskVolume1\WINDOWS\system32\cmd.exe - -
23 1432 1484 notepad.exe 0x89a0d180 0 0 False 2023-02-13 18:28:25.000000 2023-02-13 18:28:40.000000 \Device\HarddiskVolume1\WINDOWS\system32\notepad.exe - -
24 1444 1484 notepad.exe 0x8996bd00 0 0 False 2023-02-13 18:28:42.000000 2023-02-13 18:28:47.000000 \Device\HarddiskVolume1\WINDOWS\system32\notepad.exe - -
25 528 1484 notepad.exe 0x896c3020 0 0 False 2023-02-13 18:26:55.000000 2023-02-13 18:27:46.000000 \Device\HarddiskVolume1\WINDOWS\system32\notepad.exe - -
26 1608 1484 taskmgr.exe 0x89a0a2f0 0 0 False 2023-02-13 18:29:13.000000 2023-02-13 18:29:22.000000 \Device\HarddiskVolume1\WINDOWS\system32\taskmgr.exe - -
27 276 1484 DumpIt.exe 0x89a0fda0 1 25 0 False 2023-02-13 18:29:08.000000 N/A - "C:\Documents and Settings\CyberDefenders\Desktop\dumpit-moonsols\DumpIt.exe" C:\Documents and
Settings\CyberDefenders\Desktop\dumpit-moonsols\DumpIt.exe
28 376 1484 VBoxTray.exe 0x899d2da0 13 125 0 False 2023-02-13 17:54:30.000000 N/A \Device\HarddiskVolume1\WINDOWS\system32\VBoxTray.exe "C:\WINDOWS\system32\VBoxTray.exe" C:\WINDOWS\system32\VBoxTray.exe
29 600 1484 mmsgs.exe 0x8994a020 2 157 0 False 2023-02-13 17:54:30.000000 N/A \Device\HarddiskVolume1\Program Files\Messenger\mmsgs.exe "C:\Program Files\Messenger\mmsgs.exe" /background C:\Program
Files\Messenger\mmsgs.exe
```

```
python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw
windows.pstree
```

Bu çıktıda explorer.exe tarafından oluşturulan, rootkit.exe ve cmd.exe arasındaki ilişki şüphe uyandırıcı. Aynı zamanda yine explorer.exe tarafından oluşturulan notepad.exe süreçleri de şüphe uyandırıcı. Tüm bunlar akla dll injection saldırısını getiriyor.

Burada windows.cmdline komutunu çalıştırarak süreçlere ait komut satırı argümanlarını inceleyelim.

```
(kali@kali) - [~/Downloads/volatility3]
$ python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw windows.cmdline
Volatility 3 Framework 2.7.0
Progress: 100.00 PDB scanning finished
PID Process Args
4 System Required memory at 0x10 is not valid (process exited?)
368 smss.exe \SystemRoot\System32\smss.exe
592 csrss.exe C:\WINDOWS\system32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,3072,512 Windows-On SubsystemType=Windows ServerDll=basesrv,1 ServerDll=winlsrv:UserServerDllInitialization,3 ServerDll=winlsrv:ConServerDllInit
616 winlogon.exe winlogon.exe
660 services.exe C:\WINDOWS\system32\services.exe
672 lsass.exe C:\WINDOWS\system32\lsass.exe
832 VBoxService.exe C:\WINDOWS\system32\VBoxService.exe
880 svchost.exe C:\WINDOWS\system32\svchost.exe -k DcomLaunch
968 svchost.exe C:\WINDOWS\system32\svchost.exe -k rpcss
1060 svchost.exe C:\WINDOWS\system32\svchost.exe -k netsvcs
1108 svchost.exe C:\WINDOWS\system32\svchost.exe -k NetworkService
1156 svchost.exe C:\WINDOWS\system32\svchost.exe -k LocalService
1484 explorer.exe C:\WINDOWS\Explorer.EXE
1608 spoolsv.exe C:\WINDOWS\system32\spoolsv.exe
480 wscntfy.exe C:\WINDOWS\system32\wscntfy.exe
540 alg.exe C:\WINDOWS\system32\alg.exe
376 VBoxTray.exe "C:\WINDOWS\system32\VBoxTray.exe"
636 mmsgs.exe "C:\Program Files\Messenger\mmsgs.exe" /background
1880 taskmgr.exe Required memory at 0x7ffdf010 is not valid (process exited?)
964 rootkit.exe Required memory at 0x7ffdf010 is not valid (process exited?)
1960 cmd.exe Required memory at 0x7ffdf010 is not valid (process exited?)
528 notepad.exe Required memory at 0x7ffdf010 is not valid (process exited?)
1432 notepad.exe Required memory at 0x7ffdf010 is not valid (process exited?)
1444 notepad.exe Required memory at 0x7ffdf010 is not valid (process exited?)
276 DumpIt.exe "C:\Documents and Settings\CyberDefenders\Desktop\dumpit-moonsols\DumpIt.exe"
```

```
python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw  
windows.cmdline
```

Bazen kötü amaçlı yazılımlar, kötü amaçlı kod enjekte etmek veya sistemde yetkisiz eylemler gerçekleştirmek için svchost.exe -k DcomLaunch sistem işlemini kullanır. Yukarıdaki çıktıda pid değeri 880 olan svchost.exe süreci bu amaç için çalışıyor olabilir. Bu sebeple svchost.exe için windows.malfind aracını çalıştırarak olası bir injection saldırı durumu var mı inceleyelim.

```
(kali@kali)-[~/Downloads/volatility3]
$ python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw windows.malfind --pid 880
Volatility 3 Framework 2.7.0
Progress: 100.00
PDB scanning finished
PID Process Start VPN End VPN Tag Protection CommitCharge PrivateMemory File output Notes Hexdump Disasm
880 svchost.exe 0x980000 0x988fff VadS PAGE_EXECUTE_READWRITE 9 1 Disabled MZ header
4d 5a 90 00 03 00 00 00 MZ.....
04 00 00 00 ff ff 00 00 .....
b8 00 00 00 00 00 00 00 .....
40 00 00 00 00 00 00 00 @.....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 .....
00 00 00 00 f8 00 00 00 .....
0x980000: dec ebp
0x980001: pop edx
0x980002: nop
0x980003: add byte ptr [ebx], al
0x980005: add byte ptr [eax], al
0x980007: add byte ptr [eax + eax], al
0x98000a: add byte ptr [eax], al
```

```
python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw  
windows.malfind --pid 880
```

Görünüşe göre bu svchost.exe dosyası sistem tarafından oluşturulmamış. O halde bu dosya svchost.exe 'nin adını kullanan bir zararlı yazılım olabilir. Bu aşamada Windows.ldrmodules aracını kullanarak gizlenmiş dll dosyalarını tespit etmeye çalışalım.

```
(kali@kali)-[~/Downloads/volatility3]
$ python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw windows.ldrmodules | grep -i false
4progressSystem.00x7c900000 False False False \WINDOWS\system32\ntdll.dll
368 smss.exe 0x48580000 True False True \WINDOWS\system32\smss.exe
592 csrss.exe 0x4600000 False False False \WINDOWS\Fonts\vgasys.fon
592 csrss.exe 0x4a680000 True False True \WINDOWS\system32\csrss.exe
592 csrss.exe 0x1210000 False False False \WINDOWS\Fonts\vgaoem.fon
592 csrss.exe 0x1230000 False False False \WINDOWS\Fonts\ega40woa.fon
592 csrss.exe 0x1220000 False False False \WINDOWS\Fonts\dosapp.fon
592 csrss.exe 0x1250000 False False False \WINDOWS\Fonts\cga40woa.fon
592 csrss.exe 0x1240000 False False False \WINDOWS\Fonts\cga80woa.fon
616 winlogon.exe 0x1000000 True False True \WINDOWS\system32\winlogon.exe
660 services.exe 0x1000000 True False True \WINDOWS\system32\services.exe
672 lsass.exe 0x1000000 True False True \WINDOWS\system32\lsass.exe
832 VBoxService.exe 0x4000000 True False True \WINDOWS\system32\VBoxService.exe
880 svchost.exe 0x1000000 True False True \WINDOWS\system32\svchost.exe
880 svchost.exe 0x9a0000 False False False \WINDOWS\system32\msxml3r.dll
968 svchost.exe 0x1000000 True False True \WINDOWS\system32\svchost.exe
1060 svchost.exe 0x1000000 True False True \WINDOWS\system32\svchost.exe
1108 svchost.exe 0x1000000 True False True \WINDOWS\system32\svchost.exe
1156 svchost.exe 0x1000000 True False True \WINDOWS\system32\svchost.exe
1484 explorer.exe 0x1000000 True False True \WINDOWS\explorer.exe
1484 explorer.exe 0x1f50000 False False False \WINDOWS\Resources\Themes\Luna\Shell\NormalColor\shellstyle.dll
1484 explorer.exe 0x25e0000 False False False \WINDOWS\system32\msxml3r.dll
1608 spoolsv.exe 0x1000000 True False True \WINDOWS\system32\spoolsv.exe
480 wscntfy.exe 0x1000000 True False True \WINDOWS\system32\wscntfy.exe
540 alg.exe 0x1000000 True False True \WINDOWS\system32\alg.exe
376 VBoxTray.exe 0x4000000 True False True \WINDOWS\system32\VBoxTray.exe
636 msmsgs.exe 0x1000000 True False True \Program Files\Messenger\msmsgs.exe
276 DumpIt.exe 0x4000000 True False True \Documents and Settings\CyberDefenders\Desktop\dumpit-moonsols\DumpIt.exe
```

```
python3 vol.py -f /home/kali/Downloads/CYBERDEF-567078-20230213-171333.raw  
windows.ldrmodules | grep -i false
```

msxml3r.dll dosyasının bağlantıları kesilmiş, o halde msxml3r.dll dosyası gizlenmiş olabilir.