Lab 7 Solutions - The Case of Zegost

Lab 7 - The Case of Zegost

Your security device alerts on a malware callback connection from ***192.168.1.60*** to the C2 domain "***xntk0520.9966.org***" on port ***8000*** (as shown in the screenshot), the C2 domain resolves to IP ***192.168.1.22***. You suspect the host ***192.168.1.60*** to be infected. You collect the memory image from the host (***zegost.vmem***).

- Which process is connecting to the C2 server?
- What is the full path of the process?
- Is this a legitimate process?
- If it is a legitimate process then why is the process connecting to the C2 ip and can you identify the component that is malicious and dump it to disk?
- Can you establish any relationship between the dumped component and the C2 domain?

Answers

01. Which process is connecting to the C2 server?

Running the netscan plugin shows a closed connection to the C2 server on port ***8000*** and it is associated with the process ***svchost.exe*** (***pid 880***)

```
root@kratos:~/Volatility# python vol.py -f zegost.vmem --profile=Win7SP0x86 netscan
Volatility Foundation Volatility Framework 2.5
Offset(P)          Proto    Local Address                  Foreign Address      State          Pid      Owner          Created
0xf51a30          TCPv4    0.0.0.0:49155                  0.0.0.0:0            LISTENING        396 services.exe
0xf51a30          TCPv6    :::49155                       :::0                 LISTENING        396 services.exe
0xeddf6b0         TCPv6    :::49152                       :::0                 LISTENING        396 wininit.exe
0xeddf758         TCPv4    0.0.0.0:49152                  0.0.0.0:0            LISTENING        396 wininit.exe
0xf57f3d8         TCPv4    192.168.1.60:49157             192.168.1.22:8000    CLOSED           880 svchost.exe
```

02. What is the full path of the process?

The full path of the process is "**C:\Windows\System32\svchost.exe**" as shown in the screenshot

03. Is this a legitimate process?

The output from the ***dlllist*** plugin shows that this is a legitimate executable loaded from the standard path.

```
root@kratos:~/Volatility# python vol.py -f zegost.vmem --profile=Win7SP0x86 dlllist -p 880
Volatility Foundation Volatility Framework 2.5
************************************************************************
svchost.exe pid:    880
Command line : C:\Windows\system32\svchost.exe -k netsvcs


Base             Size  LoadCount Path
---------- ---------- ---------- ----
0x00f30000     0x8000     0xffff C:\Windows\system32\svchost.exe
0x76f60000   0x13c000     0xffff C:\Windows\SYSTEM32\ntdll.dll
0x75530000    0xd4000     0xffff C:\Windows\system32\kernel32.dll
0x75160000    0x4a000     0xffff C:\Windows\system32\KERNELBASE.dll
```

04. If it is a legitimate process then why is the process connecting to the C2 ip and can you identify the component that is malicious and dump it to disk?

Even though this is a legitimate svchost.exe process but it is possible that svchost.exe is loading a DLL which is running as service. Running the dlllist plugin shows a suspicious module (with .ddf extension) as shown below.

```
0x6b890000     0x12000         0x1 c:\windows\system32\aelupsvc.dll
0x74fe0000     0x4b000     0xffff C:\Windows\system32\apphelp.dll
0x6bbb0000      0xf000         0x1 c:\windows\system32\appinfo.dll
0x10000000     0x26000         0x1 c:\users\test\application data\acd systems\acdsee\imageik.ddf
0x71200000     0x32000         0x3 C:\Windows\system32\WINMM.dll
0x76e50000      0x5000         0x1 C:\Windows\system32\psapi.dll
0x76e60000     0xf4000         0x1 C:\Windows\system32\wininet.dll
```

Dumping this module to disk and submitting to VirusTotal confirms it to be the malicious component.

```
root@kratos:~/Volatility# python vol.py -f zegost.vmem --profile=Win7SP0x86 dlldump -p 880
 -b 0x10000000 -D dump/
Volatility Foundation Volatility Framework 2.5
Process(V) Name                 Module Base Module Name          Result
---------- -------------------- ----------- -------------------- ------
0x86213030 svchost.exe          0x010000000 imageik.ddf          OK: module.880.ea13030.10
000000.dll
root@kratos:~/Volatility#
```

Analysis | File detail | Additional information | Comments 0 | Votes

Antivirus	Result	Update
Ad-Aware	Trojan.Zegost.A	20170304
AhnLab-V3	Win-Trojan/Biz.2875392	20170304
ALYac	Trojan.Zegost.A	20170304
Antiy-AVL	Trojan[PSW]/Win32.Bjlog	20170304
Arcabit	Trojan.Zegost.A	20170304
Avast	Win32:Zegost-C [Trj]	20170304

05. Can you establish any relationship between the dumped component and the C2 domain?

Extracting strings from the dumped component shows reference to the C2 domain as shown below

```
root@kratos:~/Volatility/dump# strings -a module.880.ea13030.10000000.dll
!This program cannot be run in DOS mode.
Rich
.text
`.rdata
.data
.reloc
```

```
SYSTEM\CurrentControlSet\Services\%s
\setup.exe
@$0000jkdkfMA2@
xntk0520.9966.org
webshell
Default
%USERPROFILE%\Application Data\ACD Systems\ACDSee\Image??.ddf
0000
divxSoftware\GNU
Software\GNU\xvid
```