

NintendoHunt Challenge

Scenario:

You have been hired as a soc analyst to investigate a potential security breach at a company. The company has recently noticed unusual network activity and suspects that there may be a malicious process running on one of their computers. Your task is identifying the malicious process and gathering information about its activity.

Task 1:

What is the process ID of the currently running malicious process?

I used the pstree plugin and tried to find the PID, I noticed several of suspicious processes and took me sometime to figure it out but at the end I noticed the svchost.exe was running under explorer.exe which is suspicious

.. 0xffffc20c69d00580:userinit.exe	4756	732	0	-----	2018-08-01	19:20:57	UTC+0000
.. 0xffffc20c69cfe580:explorer.exe	4824	4756	125	0	2018-08-01	19:20:58	UTC+0000
... 0xffffc20c6ddad580:svchost.exe	8560	4824	10	0	2018-08-01	20:13:10	UTC+0000
... 0xffffc20c6e495080:cmd.exe	8868	4824	0	-----	2018-08-01	19:40:14	UTC+0000

Answer: 8560

Task 2:

What is the md5 hash hidden in the malicious process memory?

I used the memdump plugin on the process PID 8560 and used strings on it

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 memdump --pid=8560 --dump-dir='/home/remnux/Malware'
Volatility Foundation Volatility Framework 2.6.1
*****
Writing svchost.exe [ 8560 ] to 8560.dmp
```

Then I found some string which says "the flag is" and a Base64.

After decoding I found the MD5

```
{
  "contents": "da391kdasdaadssssss t.h.e.fl.ag.is.M2ExOTY5N2YyOTA5NWJlMjg5YTk2ZTQ1MDQ2Nzk2ODA=",
  "settings": {
    "buffer size": 85,
    "line ending": "Windows"
  }
}
```

Answer: 3a19697f29095bc289a96e4504679680

Task 3:

What is the process name of the malicious process parent?

Same like task 1

.. 0xffffc20c69d00580:userinit.exe	4756	732	0	-----	2018-08-01	19:20:57	UTC+0000
.. 0xffffc20c69cfe580:explorer.exe	4824	4756	125	0	2018-08-01	19:20:58	UTC+0000
... 0xffffc20c6ddad580:svchost.exe	8560	4824	10	0	2018-08-01	20:13:10	UTC+0000
... 0xffffc20c6e495080:cmd.exe	8868	4824	0	-----	2018-08-01	19:40:14	UTC+0000

Answer: explorer.exe

Task 4:

What is the MAC address of this machine's default gateway?

I tried several ways with netstat, netscan, I tried to use printkey on several keys like "Microsoft\Windows NT\CurrentVersion\NetworkList" and "System\CurrentControlSet\Services\Tcpip\Parameters\Interfaces" but didn't find nothing so I used the hint which says to use: "Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged"

```
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 hivexcan | grep -i tcp
Volatility Foundation Volatility Framework 2.6.1
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 printkey -K "Microsoft\Windows NT\CurrentVersion\NetworkList"
Legend: (S) = Stable (V) = Volatile
-----
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: NetworkList (S)
Last updated: 2018-08-01 18:50:26 UTC+0000
Subkeys:
(S) DefaultMediacost
(S) NewNetworks
(S) Rta
(S) Permissions
(S) Profiles
(S) Signatures
Values:
REG_SZ : (S) 192.228.79.201
REG_DWORD FirstNetwork : (S) 0
REG_DWORD HostNameIpAddr : (S) 2001:478:40:53
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 printkey -K "Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable (V) = Volatile
-----
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: Unmanaged (S)
Last updated: 2018-08-01 18:50:26 UTC+0000
Subkeys:
(S) 01010300F000F00000000000F000F0E3E937A40DC0BA3142602986CB7ED508B43802FEEDECFD06E7141DC1D150
Values:
remnux@remnux:~/volatility$ python2 vol.py -f '/home/remnux/memdump.mem' --profile=Win10x64_17134 printkey -K "Microsoft\Windows NT\CurrentVersion\NetworkList\Signatures\Unmanaged\01010300F000F00000000000F000F0E3E937A40DC0BA3142602986CB7ED508B43802FEEDECFD06E7141DC1D150"
Volatility Foundation Volatility Framework 2.6.1
Legend: (S) = Stable (V) = Volatile
-----
Registry: \SystemRoot\System32\Config\SOFTWARE
Key name: 01010300F000F00000000000F000F0E3E937A40DC0BA3142602986CB7ED508B43802FEEDECFD06E7141DC1D150 (S)
Last updated: 2018-08-01 18:50:26 UTC+0000
Subkeys:
Values:
REG_SZ ProfileGuid : (S) {590800F-8FBC-4067-9ED8-237BD3DA8F3}
REG_SZ Description : (S) Network
REG_DWORD Source : (S) 0
REG_SZ DnsSuffix : (S) localdomain
REG_SZ FirstNetwork : (S) Network
REG_BINARY DefaultGatewayMac : (S) .PV...
00000000 00 50 5a 7e db 07
remnux@remnux:~/volatility$
```

Then I saw a Subkey with a long name so I used printkey again on the Subkey and found the MAC

Answer: 00:50:56:fed8:07

Task 5:

What is the name of the file that is hidden in the alternative data stream?

I didn't know what exactly alternative data stream is so I just learned about it as much I could understand and I used the hint to parse the MFT and grepped for "ads name" and then there will be \$DATA with some string

```
remnux@remnux:~/volatility$ cat mft.txt | grep -i ads
$DATA ADS Name: $Bad
2018-08-01 19:38:23 UTC+0000 2018-08-01 19:38:23 UTC+0000 2018-08-01 22:45:49 UTC+0000 2018-08-01 22:45:49 UTC+0000 shared\IMEP001V.EXE
2018-08-01 22:45:49 UTC+0000 2018-08-01 22:45:49 UTC+0000 2018-08-01 22:45:49 UTC+0000 2018-08-01 22:45:49 UTC+0000 IMEP001V.EXE
2018-08-01 22:45:01 UTC+0000 2018-08-01 22:45:01 UTC+0000 2018-08-01 22:45:01 UTC+0000 2018-08-01 22:45:01 UTC+0000 ANCS00-1.1 \W\wads.dll
2018-08-01 22:45:01 UTC+0000 2018-08-01 22:45:01 UTC+0000 2018-08-01 22:45:01 UTC+0000 2018-08-01 22:45:01 UTC+0000 Windows\System32\wads.dll
2018-04-12 09:15:02 UTC+0000 2018-04-12 09:15:02 UTC+0000 2018-08-01 22:45:16 UTC+0000 2018-04-12 09:15:02 UTC+0000 Windows\System32\en-US\wadsldpc.dll.mui
2018-04-12 09:15:02 UTC+0000 2018-04-12 09:15:02 UTC+0000 2018-08-01 22:45:16 UTC+0000 2018-04-12 09:15:02 UTC+0000 wadsldpc.dll.mui
2018-08-01 22:45:16 UTC+0000 2018-08-01 22:45:16 UTC+0000 2018-08-01 22:45:16 UTC+0000 2018-08-01 22:45:16 UTC+0000 WD1761-1.1 \E\wadsldpc.dll.mui
2018-08-01 22:45:16 UTC+0000 2018-08-01 22:45:16 UTC+0000 2018-08-01 22:45:16 UTC+0000 2018-08-01 22:45:16 UTC+0000 wadsldpc.dll.mui
remnux@remnux:~/volatility$ cat mft.txt | grep -i ads
$DATA ADS Name: $Max
2018-08-01 19:38:23 UTC+0000 2018-08-01 19:38:23 UTC+0000 2018-08-01 19:38:23 UTC+0000 2018-08-01 19:38:23 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\User\Default\DOMStore\B0HQF50B\ADS\PUB~1.XML
2018-08-01 19:38:23 UTC+0000 2018-08-01 19:38:23 UTC+0000 2018-08-01 19:38:23 UTC+0000 2018-08-01 19:38:23 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\User\Default\DOMStore\B0HQF50B\ads.pubnatic[1].xml
2018-08-01 19:41:08 UTC+0000 2018-08-01 19:41:08 UTC+0000 2018-08-01 19:41:08 UTC+0000 2018-08-01 19:41:08 UTC+0000 Program Files\W7D089-1\MID308-1.0 \X\images\About\ads.CoreBackgroundImage.jpg
2018-08-01 19:41:08 UTC+0000 2018-08-01 19:41:08 UTC+0000 2018-08-01 19:41:08 UTC+0000 2018-08-01 19:41:08 UTC+0000 Program Files\W7D089-1\MID308-1.0 \X\images\About\ads.GenericBackgroundImage.jpg
2018-08-01 22:44:22 UTC+0000 2018-08-01 22:44:22 UTC+0000 2018-08-01 22:44:22 UTC+0000 2018-08-01 22:44:22 UTC+0000 ProgramData\Microsoft\Windows\Start Menu\Places\04 - Downlo\ads.lnk
2018-08-01 22:44:22 UTC+0000 2018-08-01 22:44:22 UTC+0000 2018-08-01 22:44:22 UTC+0000 2018-08-01 22:44:22 UTC+0000 Windows\WinSxS\amd64_microsoft-windows-explorer-shortcuts_31bf3856ad364e35_10.0.17134.1_none_9d38764d7a16749b\04 - Downloads\ads.lnk
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 Windows\WinSxS\amd64_microsoft-windows-a...terface-ldapc-layer_31bf3856ad364e35_10.0.17134.1_none_44b30090cfa7bf66\wadsldpc.dll
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 Windows\System32\wadsldpc.dll
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 Windows\System32\wadsint.dll
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 wadsint.dll
2018-08-01 22:44:00 UTC+0000 2018-08-01 22:44:00 UTC+0000 2018-08-01 22:44:00 UTC+0000 2018-08-01 22:44:00 UTC+0000 Users\Default\Downlo\ads
2018-08-01 22:44:02 UTC+0000 2018-08-01 22:44:02 UTC+0000 2018-08-01 22:44:02 UTC+0000 2018-08-01 22:44:02 UTC+0000 Windows\WinSxS\amd64_microsoft-windows-lis-ads\compatibility_31bf3856ad364e35_10.0.17134.1_none_cd1bbd614a8e3a9
2018-01-18 00:16:10 UTC+0000 2018-01-18 00:16:10 UTC+0000 2018-01-18 00:16:10 UTC+0000 2018-01-18 00:16:10 UTC+0000 Windows\DIGITA~1\en-US\wads\hattrdfs.dll
2018-08-01 19:31:07 UTC+0000 2018-08-01 19:31:07 UTC+0000 2018-08-01 19:31:07 UTC+0000 2018-08-01 19:31:07 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\User\Default\DOMStore\X06A1075\google\ads.g.doubleclick[1].xml
2018-08-01 19:40:07 UTC+0000 2018-08-01 19:40:07 UTC+0000 2018-08-01 19:40:07 UTC+0000 2018-08-01 19:40:07 UTC+0000 Downlo\ads
2018-08-01 19:33:56 UTC+0000 2018-08-01 19:33:56 UTC+0000 2018-08-01 19:33:56 UTC+0000 2018-08-01 19:33:56 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\Cache\W9AFBYED\pub\ads-1.25
2018-08-01 19:33:56 UTC+0000 2018-08-01 19:33:56 UTC+0000 2018-08-01 19:33:56 UTC+0000 2018-08-01 19:33:56 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\Cache\W9AFBYED\pub\ads_inpl_236[1].js
2018-08-01 19:14:28 UTC+0000 2018-08-01 19:14:28 UTC+0000 2018-08-01 19:14:28 UTC+0000 2018-08-01 19:14:28 UTC+0000 Ads
2018-08-01 19:14:28 UTC+0000 2018-08-01 19:14:28 UTC+0000 2018-08-01 19:14:28 UTC+0000 2018-08-01 19:14:28 UTC+0000 Ads\Control
2018-08-01 21:48:06 UTC+0000 2018-08-01 21:48:06 UTC+0000 2018-08-01 21:48:06 UTC+0000 2018-08-01 21:48:06 UTC+0000 Windows\System32\Tasks\MICROS~1\Windows\Speech\Headset\E-1
2018-08-01 21:48:06 UTC+0000 2018-08-01 21:48:06 UTC+0000 2018-08-01 21:48:06 UTC+0000 2018-08-01 21:48:06 UTC+0000 Windows\System32\Tasks\MICROS~1\Windows\Speech\Headset\ButtonPress
$DATA ADS Name: Zone.Identifier
2018-08-01 19:37:45 UTC+0000 2018-08-01 19:37:45 UTC+0000 2018-08-01 19:37:45 UTC+0000 2018-08-01 19:37:45 UTC+0000 Users\CTF\AppData\Local\Packages\MicrosoftEdge_8wekyb3d8bbwe\AC\#1001\MICROS~1\Cache\W9AFBYED\amzn_ads[1].js
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 wadsreset.dll
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 Windows\System32\wadsinext.dll
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 Windows\WinSxS\amd64_microsoft-windows-a...rface-ldap-provider_31bf3856ad364e35_10.0.17134.1_none_01ae08bae413f06d\wadsldp.dll
2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 2018-08-01 22:44:46 UTC+0000 Windows\System32\wadsldp.dll
2018-08-01 19:03:01 UTC+0000 2018-08-01 19:03:01 UTC+0000 2018-08-01 19:03:01 UTC+0000 2018-08-01 19:03:01 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\OneDrive\18.111.0663.0000\api-ms-win-core-processthreads-l1-1-1.dll
2018-08-01 18:51:06 UTC+0000 2018-08-01 18:51:06 UTC+0000 2018-08-01 18:51:06 UTC+0000 2018-08-01 18:51:06 UTC+0000 Users\CTF\Downlo\ads
2018-08-01 22:44:00 UTC+0000 2018-08-01 22:44:00 UTC+0000 2018-08-01 22:44:00 UTC+0000 2018-08-01 22:44:00 UTC+0000 Users\Public\Downlo\ads
2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 VADSHMA-1.DLL
2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 Vads\shared\voiceagents.dll
2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 2018-08-01 19:06:43 UTC+0000 Windows\SystemApps\MICROS~1\COR\Wad\shared\VoiceAgents.dll
2018-08-01 18:50:25 UTC+0000 2018-08-01 18:50:25 UTC+0000 2018-08-01 18:50:25 UTC+0000 2018-08-01 18:50:25 UTC+0000 ProgramData\Microsoft\Windows\DEVICE~2\dmrccache\downlo\ads
$DATA ADS Name: yes.txt
remnux@remnux:~/volatility$ cat mft.txt | grep -i "ads name"
grep: name: No such file or directory
remnux@remnux:~/volatility$ cat mft.txt | grep -i "ads name"
$DATA ADS Name: $Bad
$DATA ADS Name: $Max
$DATA ADS Name: Zone.Identifier
$DATA ADS Name: yes.txt
remnux@remnux:~/volatility$
```

Answer: yes.txt

Task 6:

What is the full path of the browser cache created when the user visited "www.13cubed.com"?

I used the hint which says to grep for the domain in the MFT file

```
remnux@remnux:~/volatility$ cat mft.txt | grep -i "13cubed"
2018-08-01 19:29:27 UTC+0000 2018-08-01 19:29:27 UTC+0000 2018-08-01 19:29:27 UTC+0000 2018-08-01 19:29:27 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\Cache\AHF2COV9\13cubed[1].htm
2018-08-01 19:37:05 UTC+0000 2018-08-01 19:37:05 UTC+0000 2018-08-01 19:37:05 UTC+0000 2018-08-01 19:37:05 UTC+0000 Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\Cache\10DBNKYD\13cubed[1].png
```

Answer: Users\CTF\AppData\Local\Packages\MICROS~1\MIC\AC\#1001\MICROS~1\Cache\AHF2COV9\13cubed[1].htm