CS4419 Digital Forensics Final Report

Noah Clements

3585596

6/22/2021

1.vmem

1.

1.1. The image appears to be WinXPSP2x86

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/volatility/1.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 18:24:00 UTC+0000
     Image local date and time : 2010-08-15 14:24:00 -0400
```

1.2. Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EeL017aPOy5Ainzhl0jjd7oBZvFfuVHDorx9khbQvutA3g?e=DgRrpD

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem handles -t File
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EfAKtYqmuHxFndN8ypPb19UBaoTbZPqa1O5R7-cpDNlUFA?e=NoXiwO

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem filescan > 1_filescan.txt
Volatility Foundation Volatility Framework 2.6
```

1.3.

I was able to confidently crack the admin password, with the other 3 needing some more work. The guest password likely suggests that it is using a different algorithm. SUPPORT was unable to be cracked.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:4e857c004024e53cd538de64dedac36b:842b4013c45a3b8fec76ca54e5910581:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8f57385a61425fc7874c3268aa249ea1:::
kali@kali:~/Desktop/volatility$
```

Administrator:password
Guest: $HEX[0005170001c084]
HelpAssistant: eg#4JzYDUc56qz
SUPPORT_388945a0: ?

1.4. No encryption keys were found with findaes for aeskeyfind

```
kali@kali:~/Desktop/volatility$ ./findaes 1.vmem
Searching 1.vmem
```

Found some RSA keys with rsakeyfind: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/Ea5a337ZWFlJv6rKFysIxe4Bsc_fW-BE9ygiHBRgQqse_g?e=gAbsNW

```
kali@kali:~/Desktop/volatility$ ./rsakeyfind 1.vmem > 1_rsakeys.txt
```

1.5. Nothing standing out for config files

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem filescan | grep cfg
Volatility Foundation Volatility Framework 2.6
0×000000000115cad8      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\icfgnt5.dll
0×0000000002e47710      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\inetcfg.dll
0×0000000004868d48      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\netcfgx.dll
0×0000000004a963b8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\hnetcfg.dll
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem filescan | grep conf
Volatility Foundation Volatility Framework 2.6
0×00000000003f3f08      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\ipconf.tsp
0×000000000106be80      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY.LOG
0×00000000010d5f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0×000000000112cb18      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM.LOG
0×0000000001160218      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0×0000000001160430      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0×0000000001187620      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default.LOG
0×000000000438b100      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software
0×00000000043d6e60      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0×000000000486b028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default
0×0000000004a96c08      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0×0000000005c5ceb8      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0×0000000005ce64b0      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0×0000000005ce7a90      1      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0×0000000006629028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software.LOG
0×0000000006779028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system.LOG
0×000000000687f028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system
```

1.6. Nothing particularly suspicious, other than explorer.exe being the parent process of IEXPLORER.EXE

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0×810b1660:System                                      4      0     58    183 1970-01-01 00:00:00 UTC+0000
. 0×ff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0×ff1ec978:winlogon.exe                            632    544     20    518 2010-08-11 06:06:23 UTC+0000
... 0×ff255020:lsass.exe                              688    632     19    344 2010-08-11 06:06:24 UTC+0000
... 0×ff247020:services.exe                           676    632     16    269 2010-08-11 06:06:24 UTC+0000
.... 0×ff1b8b28:vmtoolsd.exe                         1668    676      5    221 2010-08-11 06:06:35 UTC+0000
..... 0×ff125020:cmd.exe                             1136   1668      0 ------ 2010-08-15 18:24:00 UTC+0000
.... 0×80ff88d8:svchost.exe                           856    676     17    199 2010-08-11 06:06:24 UTC+0000
.... 0×ff1d7da0:spoolsv.exe                          1432    676     13    135 2010-08-11 06:06:26 UTC+0000
.... 0×80fbf910:svchost.exe                          1028    676     71   1341 2010-08-11 06:06:24 UTC+0000
..... 0×80f94588:wuauclt.exe                          468   1028      4    134 2010-08-11 06:09:37 UTC+0000
..... 0×ff364310:wscntfy.exe                          888   1028      1     27 2010-08-11 06:06:49 UTC+0000
.... 0×ff217560:svchost.exe                           936    676     10    272 2010-08-11 06:06:24 UTC+0000
.... 0×ff143b28:TPAutoConnSvc.e                      1968    676      5    100 2010-08-11 06:06:39 UTC+0000
..... 0×ff38b5f8:TPAutoConnect.e                     1084   1968      1     61 2010-08-11 06:06:52 UTC+0000
.... 0×ff22d558:svchost.exe                          1088    676      5     80 2010-08-11 06:06:25 UTC+0000
.... 0×ff218230:vmacthlp.exe                          844    676      1     24 2010-08-11 06:06:24 UTC+0000
.... 0×ff25a7e0:alg.exe                               216    676      6    105 2010-08-11 06:06:39 UTC+0000
.... 0×ff203b80:svchost.exe                          1148    676     14    208 2010-08-11 06:06:26 UTC+0000
.... 0×ff1fdc88:VMUpgradeHelper                      1788    676      4    100 2010-08-11 06:06:38 UTC+0000
... 0×80fdc368:logon.scr                              124    632      1     15 2010-08-15 18:21:28 UTC+0000
.. 0×ff1ecda0:csrss.exe                               608    544     10    369 2010-08-11 06:06:23 UTC+0000
 0×ff3865d0:explorer.exe                             1724   1708     12    341 2010-08-11 06:09:29 UTC+0000
. 0×ff3667e8:VMwareTray.exe                           432   1724      1     49 2010-08-11 06:09:31 UTC+0000
. 0×ff374980:VMwareUser.exe                           452   1724      6    189 2010-08-11 06:09:32 UTC+0000
. 0×ff3ad1a8:IEXPLORE.EXE                            2044   1724     10    366 2010-08-15 18:11:17 UTC+0000
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ------ ------- -------- --------
0x06499b80 svchost.exe            1148 True   True   True     True   True   True    True
0x04b5a980 VMwareUser.exe          452 True   True   True     True   True   True    True
0x010f7588 wuauclt.exe             468 True   True   True     True   True   True    True
0x0211ab28 TPAutoConnSvc.e        1968 True   True   True     True   True   True    True
0x04c2b310 wscntfy.exe             888 True   True   True     True   True   True    True
0x061ef558 svchost.exe            1088 True   True   True     True   True   True    True
0x06015020 services.exe            676 True   True   True     True   True   True    True
0x0485d1a8 IEXPLORE.EXE           2044 True   True   True     True   True   True    True
0x06384230 vmacthlp.exe            844 True   True   True     True   True   True    True
0x0655fc88 VMUpgradeHelper        1788 True   True   True     True   True   True    True
0x06945da0 spoolsv.exe            1432 True   True   True     True   True   True    True
0x05f027e0 alg.exe                 216 True   True   True     True   True   True    True
0x05f47020 lsass.exe               688 True   True   True     True   True   True    True
0x04a065d0 explorer.exe           1724 True   True   True     True   True   True    True
0x066f0978 winlogon.exe            632 True   True   True     True   True   True    True
0x0115b8d8 svchost.exe             856 True   True   True     True   True   True    True
0x063c5560 svchost.exe             936 True   True   True     True   True   True    True
0x01122910 svchost.exe            1028 True   True   True     True   True   True    True
0x0113f368 logon.scr               124 True   True   True     True   True   True    True
0x069d5b28 vmtoolsd.exe           1668 True   True   True     True   True   True    True
0x04be97e8 VMwareTray.exe          432 True   True   True     True   True   True    True
0x049c15f8 TPAutoConnect.e        1084 True   True   True     True   True   True    True
0x02e47020 cmd.exe                1136 True   True   False    True   False  False   False    2010-08-15 18:24:00 UTC+0000
0x066f0da0 csrss.exe               608 True   True   True     True   False  True    True
0x05471020 smss.exe                544 True   True   True     True   False  False   False
0x01214660 System                    4 True   True   True     True   False  False   False
0x066f1c08 logonui.exe            1168 False  True   False    False  False  False   False    2010-08-11 06:09:35 UTC+0000
```

logonui.exe appears to be hidden from all other scans

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem dlllist
```

dlllist link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/ETJAiS6yqPpFmeOEb1PQDjYBjYp9hN96mVu3OtyTQIy4ww?e=vGCl2K

handles -t Process shows something odd with iexplorer and cmd.exe, something to look into:

```
0x80f94588    1028      0x160c    0x1f0fff Process          wuauclt.exe(468)
0xff22d558    1088       0x120    0x1f07fb Process          svchost.exe(1088)
0xff1d7da0    1432       0x124    0x1f0fff Process          spoolsv.exe(1432)
0xff125020    1668       0x378    0x1f0fff Process          cmd.exe(1136)
0xff38b5f8    1968       0x194    0x1f0fff Process          TPAutoConnect.e(1084)
0xff3ad1a8    2044       0x4d8    0x1f0fff Process          IEXPLORE.EXE(2044)
kali@kali:~/Desktop/volatility$
```

Envars shows that the computer hostname is BILLY-DB5B96DD3, and is an admin.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem envars
Volatility Foundation Volatility Framework 2.6
Pid      Process            Block      Variable                       Value
-------- ---------------- ---------- ------------------------------ ----------
     608 csrss.exe          0x00100000 ComSpec                        C:\WINDOWS\system32\cmd.exe
     608 csrss.exe          0x00100000 FP_NO_HOST_CHECK               NO
     608 csrss.exe          0x00100000 NUMBER_OF_PROCESSORS           1
     608 csrss.exe          0x00100000 OS                             Windows_NT
     608 csrss.exe          0x00100000 Path                           C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
     608 csrss.exe          0x00100000 PATHEXT                        .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
     608 csrss.exe          0x00100000 PROCESSOR_ARCHITECTURE         x86
     608 csrss.exe          0x00100000 PROCESSOR_IDENTIFIER           x86 Family 6 Model 23 Stepping 10, GenuineIntel
     608 csrss.exe          0x00100000 PROCESSOR_LEVEL                6
     608 csrss.exe          0x00100000 PROCESSOR_REVISION             170a
     608 csrss.exe          0x00100000 SystemDrive                    C:
     608 csrss.exe          0x00100000 SystemRoot                     C:\WINDOWS
     608 csrss.exe          0x00100000 TEMP                           C:\WINDOWS\TEMP
     608 csrss.exe          0x00100000 TMP                            C:\WINDOWS\TEMP
     608 csrss.exe          0x00100000 windir                         C:\WINDOWS
     632 winlogon.exe       0x00010000 ALLUSERSPROFILE                C:\Documents and Settings\All Users
     632 winlogon.exe       0x00010000 APPDATA                        C:\Documents and Settings\Administrator\Application Data
     632 winlogon.exe       0x00010000 CommonProgramFiles             C:\Program Files\Common Files
     632 winlogon.exe       0x00010000 COMPUTERNAME                   BILLY-DB5B96DD3
     632 winlogon.exe       0x00010000 ComSpec                        C:\WINDOWS\system32\cmd.exe
     632 winlogon.exe       0x00010000 FP_NO_HOST_CHECK               NO
     632 winlogon.exe       0x00010000 LOGONSERVER                    \\BILLY-DB5B96DD3
```

Envars also shows a weird variable for IEXPLORER.EXE

```
2044 IEXPLORE.EXE  0x00010000 ALLUSERSPROFILE          C:\Documents and Settings\All Users
2044 IEXPLORE.EXE  0x00010000 APPDATA                 C:\Documents and Settings\Administrator\Applica
2044 IEXPLORE.EXE  0x00010000 CLIENTNAME              Console
2044 IEXPLORE.EXE  0x00010000 CommonProgramFiles      C:\Program Files\Common Files
2044 IEXPLORE.EXE  0x00010000 COMPUTERNAME            BILLY-DB5B96DD3
2044 IEXPLORE.EXE  0x00010000 ComSpec                 C:\WINDOWS\system32\cmd.exe
2044 IEXPLORE.EXE  0x00010000 FP_NO_HOST_CHECK        NO
2044 IEXPLORE.EXE  0x00010000 GIEVMXDVLMISML          EWONSYG
2044 IEXPLORE.EXE  0x00010000 HOMEDRIVE               C:
2044 IEXPLORE.EXE  0x00010000 HOMEPATH                \Documents and Settings\Administrator
2044 IEXPLORE.EXE  0x00010000 LOGONSERVER             \\BILLY-DB5B96DD3
2044 IEXPLORE.EXE  0x00010000 NUMBER_OF_PROCESSORS    1
2044 IEXPLORE.EXE  0x00010000 OS                      Windows_NT
2044 IEXPLORE.EXE  0x00010000 Path                    C:\Program Files\Internet Explorer;;C:\WINDOWS\
2044 IEXPLORE.EXE  0x00010000 PATHEXT                 .COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WS
2044 IEXPLORE.EXE  0x00010000 PROCESSOR_ARCHITECTURE  x86
2044 IEXPLORE.EXE  0x00010000 PROCESSOR_IDENTIFIER    x86 Family 6 Model 23 Stepping 10, GenuineIntel
```

1.7.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EVaXyw50PtZPs66Jgh1rS6UBEVA_5_q4okVID_xUwZnFCQ?e=T2pdwV

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem apihooks > 1_apihooks.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/Eb12DYOCJyRJowC2EeePL0kB5N_5zpzMAIFXsbcVYSD9Gw?e=g0pcrf

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem malfind > 1_malfind.txt
Volatility Foundation Volatility Framework 2.6
```

Malfind shows that explorer.exe and IEXPLORER.EXE appear to have code injected into them:

```
Process: explorer.exe Pid: 1724 Address: 0x1b20000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01b20000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01b20010  00 00 b2 01 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01b20020  10 00 b2 01 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x01b20030  20 00 b2 01 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x01b20000 0000              ADD [EAX], AL
0x01b20002 0000              ADD [EAX], AL
0x01b20004 0000              ADD [EAX], AL
0x01b20006 0000              ADD [EAX], AL
0x01b20008 0000              ADD [EAX], AL
0x01b2000a 0000              ADD [EAX], AL
0x01b2000c 0000              ADD [EAX], AL
0x01b2000e 0000              ADD [EAX], AL
0x01b20010 0000              ADD [EAX], AL
0x01b20012 b201              MOV DL, 0x1
```

It appears that the PE header was deliberately zero'd out in an effort to wipe traces.

```
Process: IEXPLORE.EXE Pid: 2044 Address: 0x7ff80000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 45, PrivateMemory: 1, Protection: 6

0x7ff80000  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x7ff80010  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x7ff80020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x7ff80030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................

0x7ff80000 0000            ADD [EAX], AL
0x7ff80002 0000            ADD [EAX], AL
0x7ff80004 0000            ADD [EAX], AL
0x7ff80006 0000            ADD [EAX], AL
0x7ff80008 0000            ADD [EAX], AL
0x7ff8000a 0000            ADD [EAX], AL
0x7ff8000c 0000            ADD [EAX], AL
```

Therefore, I brought the address into volshell

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem volshell -p 2044
Volatility Foundation Volatility Framework 2.6
Current context: IEXPLORE.EXE @ 0xff3ad1a8, pid=2044, ppid=1724 DTB=0x6cc0320
Welcome to volshell! Current memory image is:
file:///home/kali/Desktop/volatility/1.vmem
To get help, type 'hh()'
>>> dis(0x7ff80000)
>>> dis(0x7ff81000)
0x7ff81000 81ec20010000                    SUB ESP, 0x120
0x7ff81006 53                              PUSH EBX
0x7ff81007 8b9c2430010000                  MOV EBX, [ESP+0x130]
0x7ff8100e 8bc3                            MOV EAX, EBX
0x7ff81010 2404                            AND AL, 0x4
0x7ff81012 55                              PUSH EBP
0x7ff81013 f6d8                            NEG AL
0x7ff81015 56                              PUSH ESI
0x7ff81016 57                              PUSH EDI
0x7ff81017 8bbc2434010000                  MOV EDI, [ESP+0x134]
0x7ff8101e 6805010000                      PUSH DWORD 0x105
0x7ff81023 8d4c242c                        LEA ECX, [ESP+0x2c]
0x7ff81027 51                              PUSH ECX
0x7ff81028 1bc0                            SBB EAX, EAX
0x7ff8102a 25270c0000                      AND EAX, 0xc27
0x7ff8102f 33f6                            XOR ESI, ESI
0x7ff81031 8bef                            MOV EBP, EDI
0x7ff81033 89442418                        MOV [ESP+0x18], EAX
0x7ff81037 8974241c                        MOV [ESP+0x1c], ESI
0x7ff8103b ff15b0e1f97f                    CALL DWORD [0x7ff9e1b0]
0x7ff81041 3d05010000                      CMP EAX, 0x105
```

The main page showed nothing, but after using the second page instead we discover code execution in IEXPLORER.EXE

Used vaddump to dump IEXPLORER.EXE address

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem vaddump -b 0x7ff80000 -D dump
Volatility Foundation Volatility Framework 2.6
Pid        Process              Start      End        Result
---------- -------------------- ---------- ---------- ------

      1028 svchost.exe          0x7ff80000 0x7ff80fff dump/svchost.exe.1122910.0x7ff80000-0x7ff80fff.dmp
      2044 IEXPLORE.EXE         0x7ff80000 0x7ffadfff dump/IEXPLORE.EXE.485d1a8.0x7ff80000-0x7ffadfff.dmp
kali@kali:~/Desktop/volatility$
```

Using strings.exe against the dump revealed some secrets of how IEXPLORER.EXE infects.

```
PeekMessageA
ole32.dll
kernel32.dll
advapi32.dll
user32.dll
Progman
Internet Explorer_Server
cleanup
appinit_dlls
rundll32.exe
winlogon.exe

*.nhs.net/*
*.nhs.uk/*
*.hilton.*
*.yahoo.*
*.google.*
checkbox
password
text
submit
hidden
AccessibleObjectFromWindow
oleacc.dll
Assertion has failed in .\src\iexplore.cpp(%d)
Reference count of %s is nonzero (%d)
F'D,3
%D,3
```

Likely searching for browsers on the host

```
*\explorer.exe
*\intern*\iexplore.exe
*\firefox.exe
*\opera.exe
*\skype.exe
AFCORE
COM2PLUS_MessageWindowClass
#wnd
```

Registry Keys to ensure persistence

```
Unregistering object %s
SOFTWARE\Microsoft\Windows NT\CurrentVersion
SOFTWARE\Microsoft\Windows\CurrentVersion
RegisteredOrganization
\???*.dll
*32.dll
Software\Classes\CLSID\InprocServer32
ThreadingModel
Apartment
Software\Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers
SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce
Software\Microsoft\Windows NT\CurrentVersion\Windows
AppInit_DLLs
rundll32.exe ,init
#rundll
Allocated new DLL path %s (pid: %d)
Registry key cannot be opened (%w)
```

Possible C2 Communication

```
Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1)
+OhuS
domainpathSet-Cookie:
Location:
http://
PACKET
TRANSMIT
%s←%a
Ownership of the mutex object has not been released. Session context for %s cannot be removed
RELAY
HTTPP
Request of %a for %s has been failed
http://CONNECT Host: Connection: close
Proxy-Connection: close
HTTP/1.0 503 Connection failed
HTTP/1.0 200 Connection established
SOCKS
EXEC
File specified for %s cannot be validated
```

And a maliciously crafted DLL (more specifically, D**i**L)

```
&]|v
C:\WINDOWS\system32\comsbap.dIl
SetEvent
CreateThread
```

Performed a filescan on the malicious DLL to find offset

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem filescan | grep comsbap
Volatility Foundation Volatility Framework 2.6
0x0000000005c5aee0      1      0 R--r-- \Device\HarddiskVolume1\WINDOWS\system32\comsbap.dat
0x0000000005ce4be0      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\comsbap.dIl
0x0000000005ce4c78      1      0 R--r-- \Device\HarddiskVolume1\WINDOWS\system32\comsbap.dIl
kali@kali:~/Desktop/volatility$
```

Unloaded modules in case anything was deliberately destroyed

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem unloadedmodules
Volatility Foundation Volatility Framework 2.6
Name                 StartAddress  EndAddress    Time
-------------------- ------------  ------------  ----
Sfloppy.SYS          0x00fc178000  0xfc17b000    2010-08-11 06:06:17
Cdaudio.SYS          0x00fc7b3000  0xfc7b8000    2010-08-11 06:06:17
vmdebug.sys          0x00fc66b000  0xfc674000    2010-08-11 06:06:47
splitter.sys         0x00fc9cd000  0xfc9cf000    2010-08-11 06:07:39
aec.sys              0x00f3124000  0xf3147000    2010-08-11 06:07:44
swmidi.sys           0x00f377d000  0xf378b000    2010-08-11 06:07:44
DMusic.sys           0x00f323c000  0xf3249000    2010-08-11 06:07:44
kmixer.sys           0x00f30fa000  0xf3124000    2010-08-11 06:07:44
drmkaud.sys          0x00fcab8000  0xfcab9000    2010-08-11 06:07:44
kmixer.sys           0x00f2fe0000  0xf300a000    2010-08-15 18:10:26
kmixer.sys           0x00f2ecb000  0xf2ef5000    2010-08-15 18:13:34
```

1.8.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EdMW_gfCSzdJiUPRmREUn9IB_d9OELXIQudFXCajbUEHOA?e=Luxr0d

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem modules > 1_modules.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EWTQY1WbyV9MtvUqrHHgdPMBmQLxsMhTC_LMDQOrPPsGBw?e=Evesms

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem driverscan > 1_drivers.txt
Volatility Foundation Volatility Framework 2.6
```

Handles Mutant scan shows possibility of Doc.Downloader.Generic-6327950-1 malware: https://blog.talosintelligence.com/2017/06/threat-roundup-0602-0609.html

```
0x80ef7a38   2044      0x134   0x100000 Mutant          _!MSFTHISTORY!_
0x80fe35c8   2044      0x13c   0x100000 Mutant          c:!documents and settings!administrator!local settings!temporary internet files!content.i
e5!
0x80fcdef8   2044      0x144   0x100000 Mutant          c:!documents and settings!administrator!cookies!
0xff248eb0   2044      0x14c   0x100000 Mutant          c:!documents and settings!administrator!local settings!history!history.ie5!
0xff2071d0   2044      0x16c   0x100000 Mutant          WininetStartupMutex
0xff122770   2044      0x174   0x100000 Mutant          WininetConnectionMutex
0x80f77380   2044      0x178   0x1f0001 Mutant
0x80f0cb60   2044      0x17c   0x100000 Mutant          WininetProxyRegistryMutex
0xff3864f8   2044      0x194   0x120001 Mutant          ShimCacheMutex
0xff282140   2044      0x1a4   0x1f0001 Mutant
0x80f79ea8   2044      0x1b0   0x1f0001 Mutant
0x80f79e68   2044      0x1c4   0x1f0001 Mutant
0xff2995a0   2044      0x1d0   0x1f0001 Mutant
0x80efefe0   2044      0x1d8   0x1f0001 Mutant
0xff1f6380   2044      0x20c   0x1f0001 Mutant          GETBKODKOTAE
0x80efefa0   2044      0x214   0x1f0001 Mutant
0x80ff3308   2044      0x270   0x1f0001 Mutant
0xff1e68b0   2044      0x28c   0x100000 Mutant          RasPbFile
0xff29e8e0   2044      0x4a4   0x1f0001 Mutant          CTF.LBES.MutexDefaultS-1-5-21-1614895754-436374069-839522115-500
0xff157ed0   2044      0x4a8   0x1f0001 Mutant          CTF.Compart.MutexDefaultS-1-5-21-1614895754-436374069-839522115-500
0xff29fc98   2044      0x4ac   0x1f0001 Mutant          CTF.Asm.MutexDefaultS-1-5-21-1614895754-436374069-839522115-500
0x80fb0c88   2044      0x4b0   0x1f0001 Mutant          CTF.Layouts.MutexDefaultS-1-5-21-1614895754-436374069-839522115-500
0x80f58a00   2044      0x4b4   0x1f0001 Mutant          CTF.TMD.MutexDefaultS-1-5-21-1614895754-436374069-839522115-500
0xff237298   2044      0x4f4   0x1f0001 Mutant          oleacc-msaa-loaded
0xff26c440   2044      0x5e0   0x1f0001 Mutant
0xff220a40   2044      0x5e8   0x1f0001 Mutant
0xff39cab0   2044      0x5f0   0x1f0001 Mutant
0x80fa9b30   2044      0x5f8   0x1f0001 Mutant
0xff284f08   2044      0x600   0x1f0001 Mutant          MidiMapper_modLongMessage_RefCnt
0xff25dfe0   2044      0x604   0x1f0001 Mutant          MidiMapper_Configure
0xff36e568   2044      0x6f8   0x1f0001 Mutant          c:!documents and settings!administrator!local settings!history!history.ie5!mshist01201008
1520100816!
0xff1257c8   2044      0x6fc   0x1f0001 Mutant          _!SHMSFTHISTORY!_
kali@kali:~/Desktop/volatility$
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EV4Av4-Z4KFDq3Ut7BfnMyYBb2QcuLc-kLlD35BxeT0m8w?e=NRVY1f

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem thrdscan > 2_thrdscan.txt
Volatility Foundation Volatility Framework 2.6
```

1.9. No suspicious outgoing traffic noticed. Appears to be Microsoft and AT&T traffic.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---

kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x00eda590 172.16.176.143:1058       65.54.81.209:80           2044
0x01079e70 172.16.176.143:1082       209.234.234.16:80         2044
0x0107c888 172.16.176.143:1059       4.23.40.126:80            2044
0x0108fcd8 172.16.176.143:1072       65.55.15.124:80           2044
0x010fa448 172.16.176.143:1065       65.55.253.21:80           2044
0x02214988 172.16.176.143:1092       65.54.81.14:80            2044
0x026c68a8 172.16.176.143:1074       65.55.15.243:80           2044
0x02ae4bb0 172.16.176.143:1073       65.55.15.123:80           2044
0x048b25f0 172.16.176.143:1085       65.55.149.119:80          2044
0x04a045f8 172.16.176.143:1057       65.54.81.49:80            2044
0x04a04e70 172.16.176.143:1095       69.43.160.145:80          2044
0x04a4a4a0 172.16.176.143:1084       12.120.180.24:80          2044
0x04be2558 172.16.176.143:1079       65.54.81.22:80            2044
0x05536e70 172.16.176.143:1090       65.54.81.14:80            2044
0x05802340 172.16.176.143:1062       65.55.18.18:80            2044
0x05c9e200 172.16.176.143:1067       65.54.81.14:80            2044
0x05deea30 172.16.176.143:1068       65.54.81.14:80            2044
0x06015ab0 172.16.176.143:1053       207.46.170.10:80          2044
0x0605f208 172.16.176.143:1086       202.89.231.60:80          2044
0x06125538 172.16.176.143:1083       65.54.81.79:80            2044
0x0623a438 172.16.176.143:1066       96.6.41.210:80            2044
0x06450720 172.16.176.143:1077       65.55.149.121:80          2044
0x064509f0 172.16.176.143:1063       64.4.18.73:80             2044
0x06497a68 172.16.176.143:1075       65.55.15.124:80           2044
0x067bd218 172.16.176.143:1070       65.54.81.209:80           2044
0x07c17be0 172.16.176.143:1060       65.55.239.161:80          2044
```

Odd port activity from IEXPLORER.EXE however (port 1052)

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x80fd1008        4      0     47 GRE             0.0.0.0         2010-08-11 06:08:00 UTC+0000
0xff158c00     2044   1052     17 UDP             127.0.0.1       2010-08-15 18:11:19 UTC+0000
0xff258008      688    500     17 UDP             0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff2984a0     1088   1078     17 UDP             0.0.0.0         2010-08-15 18:11:23 UTC+0000
0xff367008        4    445      6 TCP             0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x80ffc128      936    135      6 TCP             0.0.0.0         2010-08-11 06:06:24 UTC+0000
0xff225b70      688      0    255 Reserved        0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff254008     1028    123     17 UDP             127.0.0.1       2010-08-15 18:24:00 UTC+0000
0x80fce930     1088   1025     17 UDP             0.0.0.0         2010-08-11 06:06:38 UTC+0000
```

1.10.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1c49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xe1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ae580 0x01bbd580 [no name]
0xe101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008978 0x01824978 [no name]
0xe1e158c0 0x009728c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1da4008 0x00f6e008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
```

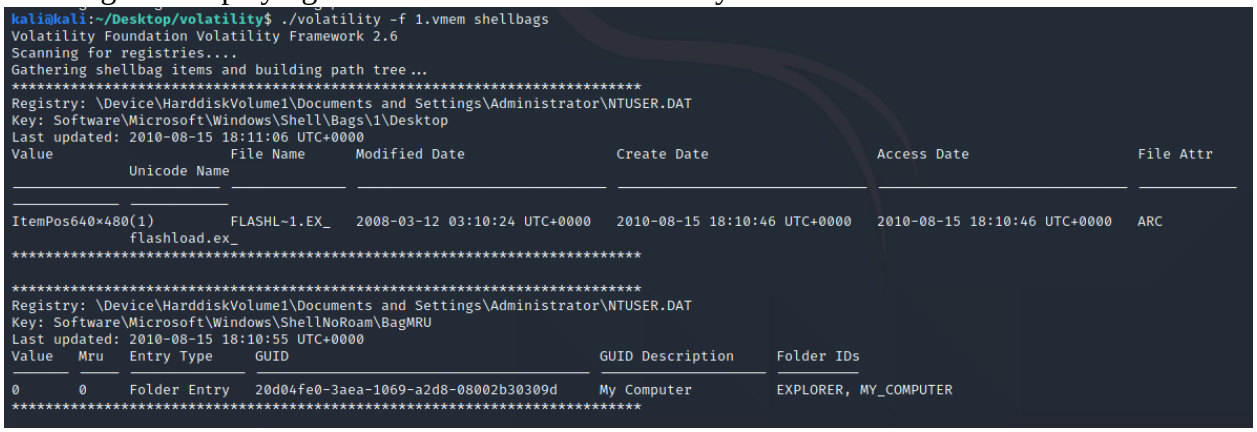
I found a RDP Private Key using lsadump:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem lsadump
Volatility Foundation Volatility Framework 2.6
L$RTMTIMEBOMB_1320153D-8DA3-4e8e-B27B-0D888223A588
0x00000000  80 c9 63 7f 03 67 cb 01                           ..c..g..

_SC_LmHosts

L${6B3E6424-AF3E-4bff-ACB6-DA535F0DDC0A}
0x00000000  2b d1 5d 56 5e 8e c0 7e 20 0e ec 40 cc 20 b9 f6   +.]V^..~ ..@. ..
0x00000010  60 8d ef aa be 4e 6d 27 aa b6 f0 11 9d a8 73 67   `....Nm'......sg
0x00000020  fe 28 ef de 99 f7 bb 02 5c df 31 77 ab a7 a3 85   .(......\.1w....
0x00000030  a7 13 aa 93 0f ff 83 3b                           .......;

_SC_RpcSs

SAC
0x00000000  02 00 00 00                                       ....

G${ED8F4747-E13D-47bc-856B-5CEFE1A81A7F}
0x00000000  09 79 8f 1b 4e 69 72 41 9f 27 2d 63 ec 18 ce 62   .y..NirA.'-c...b

L$HYDRAENCKEY_28ada6da-d622-11d1-9cb9-00c04fb16e75
0x00000000  52 53 41 32 48 00 00 00 00 02 00 00 3f 00 00 00   RSA2H.......?...
```

Odd userassist activity with flashload:

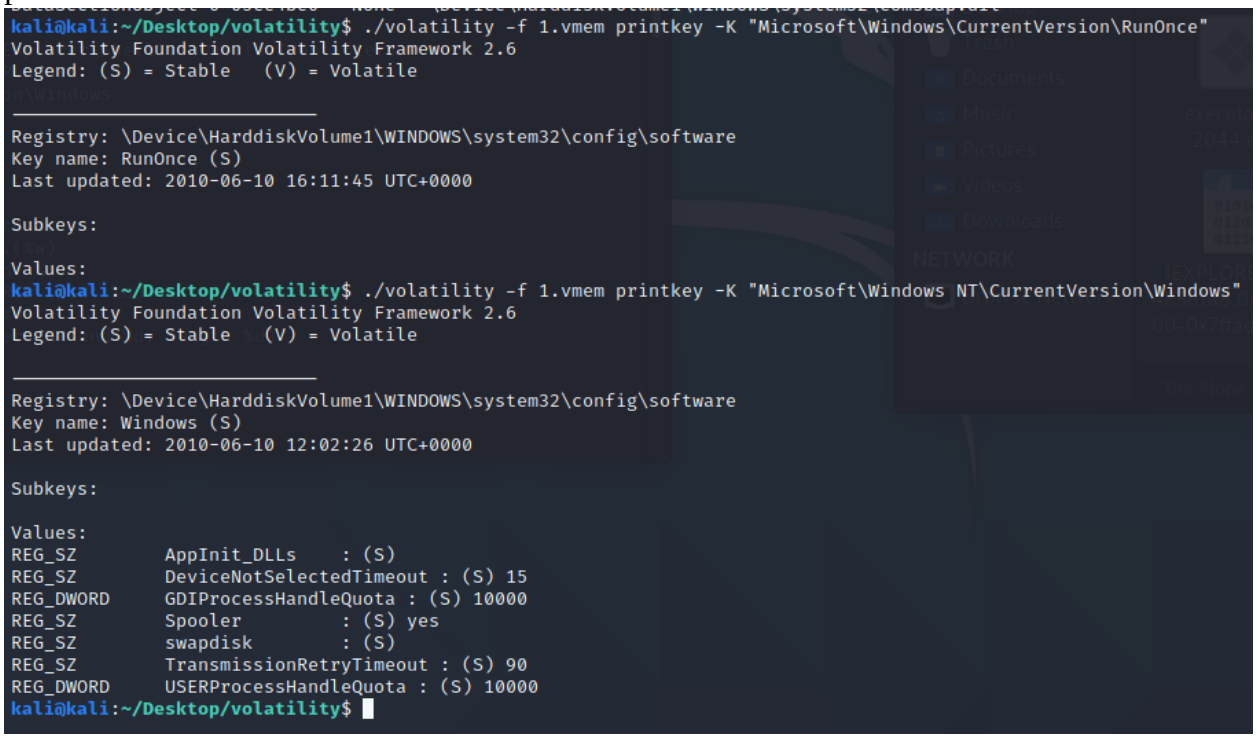
```
REG_BINARY    UEME_RUNPATH:C:\Documents and Settings\Administrator\Desktop\flashload.exe :
ID:             2
Count:          1
Last updated:   2010-08-15 18:11:13 UTC+0000
Raw Data:
0x00000000  02 00 00 00 06 00 00 00 b0 12 f5 3e a5 3c cb 01   ...........>.<..

REG_BINARY    UEME_RUNPATH:C:\Program Files\Internet Explorer\iexplore.exe :
ID:             2
Count:          1
Last updated:   2010-08-15 18:11:17 UTC+0000
Raw Data:
0x00000000  02 00 00 00 06 00 00 00 f0 46 a1 41 a5 3c cb 01   .........F.A.<..
```

Shellbag also displaying some odd flashload.exe activity:



```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem shellbags
Volatility Foundation Volatility Framework 2.6
Scanning for registries....
Gathering shellbag items and building path tree...
**************************************************************************
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key: Software\Microsoft\Windows\Shell\Bags\1\Desktop
Last updated: 2010-08-15 18:11:06 UTC+0000
Value                File Name      Modified Date                Create Date                  Access Date                  File Attr
             Unicode Name
-------------------- -------------- ---------------------------- ---------------------------- ---------------------------- ----------
-------------------- --------------
ItemPos640×480(1)        FLASHL~1.EX_   2008-03-12 03:10:24 UTC+0000   2010-08-15 18:10:46 UTC+0000   2010-08-15 18:10:46 UTC+0000   ARC
             flashload.ex_
**************************************************************************

**************************************************************************
Registry: \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
Key: Software\Microsoft\Windows\ShellNoRoam\BagMRU
Last updated: 2010-08-15 18:10:55 UTC+0000
Value   Mru   Entry Type     GUID                                 GUID Description     Folder IDs
-------- ----  -------------- ------------------------------------ -------------------- ----------
0       0     Folder Entry   20d04fe0-3aea-1069-a2d8-08002b30309d     My Computer          EXPLORER, MY_COMPUTER
**************************************************************************
```

For more *registry* information, I used the registry keys found from strings.exe against the dump:
you can see that AppInit_DLLs (from the dump strings) is a value, which confirms persistence with the malware.



```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem printkey -K "Microsoft\Windows\CurrentVersion\RunOnce"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: RunOnce (S)
Last updated: 2010-06-10 16:11:45 UTC+0000

Subkeys:

Values:
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\Windows"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Windows (S)
Last updated: 2010-06-10 12:02:26 UTC+0000

Subkeys:

Values:
REG_SZ        AppInit_DLLs    : (S)
REG_SZ        DeviceNotSelectedTimeout : (S) 15
REG_DWORD     GDIProcessHandleQuota : (S) 10000
REG_SZ        Spooler         : (S) yes
REG_SZ        swapdisk        : (S)
REG_SZ        TransmissionRetryTimeout : (S) 90
REG_DWORD     USERProcessHandleQuota : (S) 10000
kali@kali:~/Desktop/volatility$
```

comsbap is a persistent malicious DLL

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem printkey -K "Microsoft\Windows\CurrentVersion\Explorer\ShellIconOverlayIdentifiers"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------
Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: ShellIconOverlayIdentifiers (S)
Last updated: 2010-08-15 18:11:14 UTC+0000

Subkeys:
  (S) comsbap
  (S) Offline Files

Values:
kali@kali:~/Desktop/volatility$
```

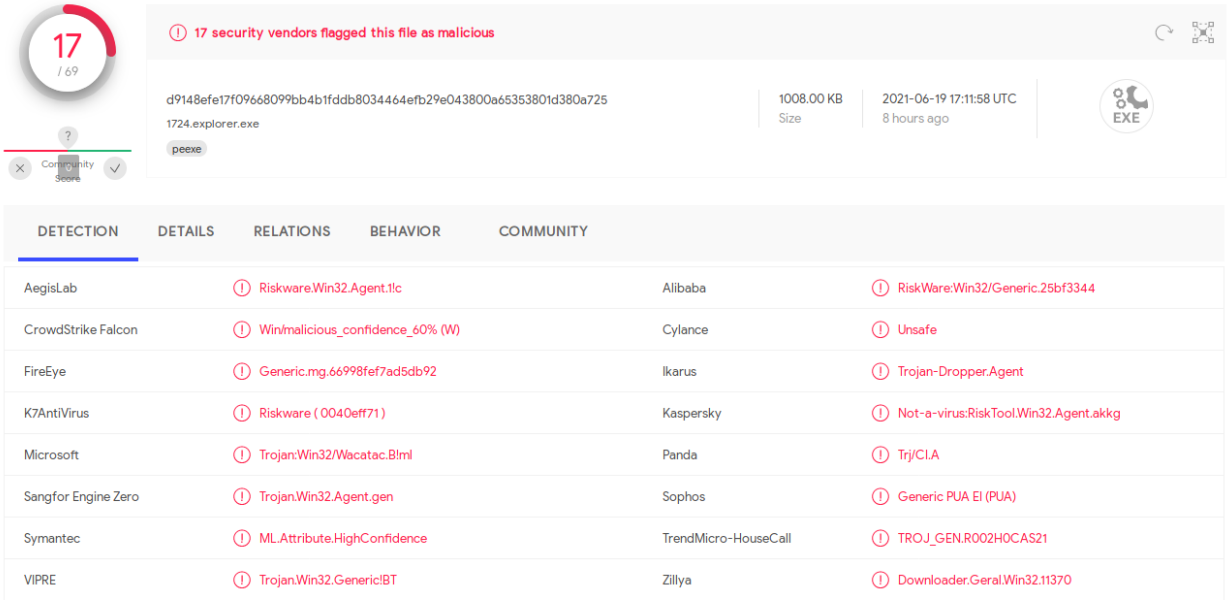
2. The malicious functions found were explorer.exe (PID 1724):

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem procdump -p 1724 -D dump
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0xff3865d0 0x01000000 explorer.exe         OK: executable.1724.exe
kali@kali:~/Desktop/volatility$
```

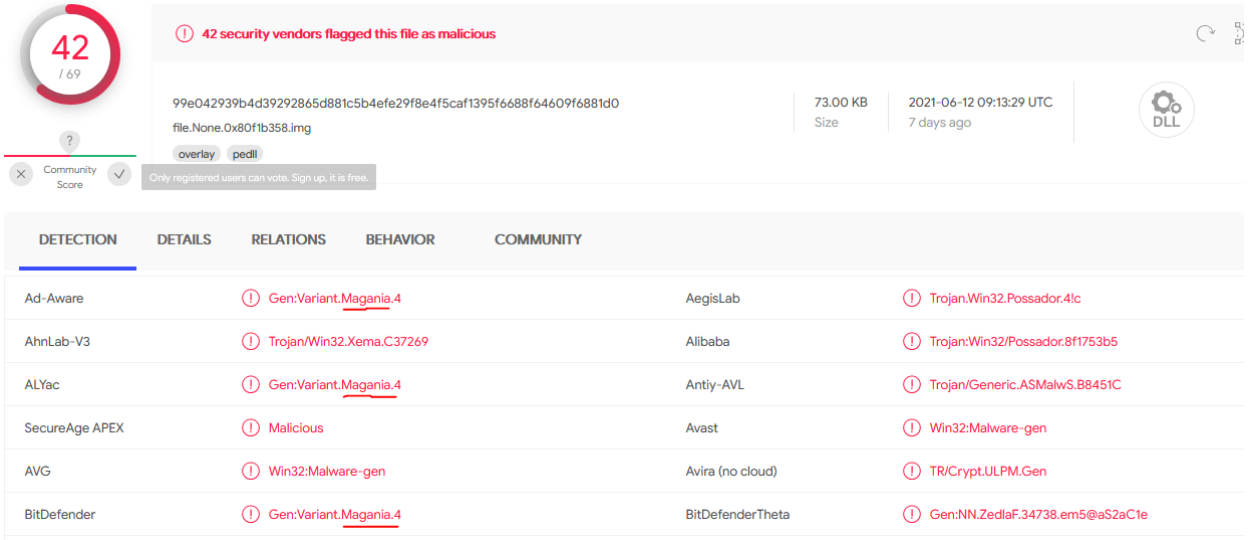
and comsbap.dll

```
kali@kali:~/Desktop/volatility$ ./volatility -f 1.vmem dumpfiles -Q 0x0000000005c5aee0 -D dump
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x05c5aee0   None   \Device\HarddiskVolume1\WINDOWS\system32\comsbap.dat
kali@kali:~/Desktop/volatility$
```

3. Thanks to the malicious .exe found, the malware family appears to be called Magania.



and comsbap.dll, which gave a 42/69 score in Virustotal:



4. Upon further research, I believe this malware belongs to Coreflood. Coreflood is a password stealing trojan that injects code into the “explorer.exe” process. The infecting process usually happens upon the user browsing malicious websites or downloading infected executables. It will then communicate to the C2 server via HTTP. It modifies specific registries to ensure that the malware is persistent and runs every time Windows starts up. This Russian-made trojan in 2010 infected government agencies, police departments, airports, banks, universities, hospitals, and other businesses. The FBI was given authorization to delete the Coreflood trojan from infected computers and seize almost 30 domains used for the C2 communication, which reduced the botnet size by 90% in the US. The main goal of this malware was to harvest passwords, emails, usernames, banking credentials, and any other sensitive information.

2.vmem

1.

1.1. Image appears to be WinXPSP2x86

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/volatility/2.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 19:11:21 UTC+0000
     Image local date and time : 2010-08-15 15:11:21 -0400
```

1.2. Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/ETdyGxKcf79Ei4AJ9kD2FVoB5EKNAsz743v2YD8k8xfMTA?e=JyhTS1

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem handles -t File
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EUlagOzo3yhNmt4qLLepdeEBpE5WndPN96Zue2kSsHH7hQ?e=kEgVUl

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem filescan > 2_filescan.txt
Volatility Foundation Volatility Framework 2.6
```

1.3. Same hashes as 1.vmem, cracked password above.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:4e857c004024e53cd538de64dedac36b:842b4013c45a3b8fec76ca54e5910581:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8f57385a61425fc7874c3268aa249ea1:::
```

Found odd lsadump with RDP related activity:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem lsadump
Volatility Foundation Volatility Framework 2.6
L$RTMTIMEBOMB_1320153D-8DA3-4e8e-B27B-0D888223A588
0x00000000  80 c9 63 7f 03 67 cb 01                              ..c..g..

_SC_LmHosts

_SC_upnphost

20ed87e2-3b82-4114-81f9-5e219ed4c481-SALEMHELPACCOUNT

_SC_RpcSs

0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantAccount
0x00000000  65 00 67 00 23 00 34 00 4a 00 7a 00 59 00 44 00    e.g.#.4.J.z.Y.D.
```

I also found the same RDP encryption key as 1.vmem

1.4. Could not find any encryption keys with findaes or aeskeyfind

```
kali@kali:~/Desktop/volatility$ ./findaes 2.vmem
Searching 2.vmem
```

found some RSA keys with rsakeyfind: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EQudDsfsAsxOvi0gct2dWbQBIN50FntBCwcP4VEeQYCzmQ?e=XNRjEK

```
kali@kali:~/Desktop/volatility$ ./rsakeyfind 2.vmem > 2_rsakeys.txt
```

1.5. Nothing suspicious, same as 1.vmem

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem filescan | grep cfg
Volatility Foundation Volatility Framework 2.6
0x0000000001065768      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\inetcfg.dll
0x0000000001069828      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\icfgnt5.dll
0x0000000004868d48      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\netcfgx.dll
0x0000000004a963b8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\hnetcfg.dll
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem filescan | grep conf
Volatility Foundation Volatility Framework 2.6
0x00000000003f3f08      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\ipconf.tsp
0x000000000106be80      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY.LOG
0x00000000010d5f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x000000000112cb18      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM.LOG
0x0000000001160218      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x0000000001160430      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x0000000001187620      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default.LOG
0x000000000438b100      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software
0x00000000043d6e60      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0x000000000486b028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default
0x0000000004a96c08      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0x0000000005c5ceb8      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x0000000005ce64b0      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x0000000005ce7a90      1      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x0000000006629028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software.LOG
0x0000000006779028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system.LOG
0x000000000687f028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system
kali@kali:~/Desktop/volatility$
```

1.6. Processes that stick out are lanmanwrk.exe, and the logonui.exe that was hidden.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                      4      0     57    182 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                            632    544     18    511 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                              688    632     19    344 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                           676    632     16    269 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                         1668    676      5    221 2010-08-11 06:06:35 UTC+0000
..... 0xff1f9b08:cmd.exe                              460   1668      0 ------ 2010-08-15 19:11:21 UTC+0000
.... 0x80ff88d8:svchost.exe                           856    676     17    199 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                          1432    676     12    134 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                          1028    676     75   1373 2010-08-11 06:06:24 UTC+0000
..... 0x80f94588:wuauclt.exe                          468   1028      4    135 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                          888   1028      1     27 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                           936    676     11    274 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                      1968    676      5    100 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                     1084   1968      1     61 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                          1088    676      6     86 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                          844    676      1     24 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                               216    676      6    105 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                          1148    676     14    209 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                      1788    676      4    100 2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                               608    544     10    378 2010-08-11 06:06:23 UTC+0000
 0xff3825f8:lanmanwrk.exe                            1180   1060      2     75 2010-08-15 19:09:12 UTC+0000
 0xff3865d0:explorer.exe                             1724   1708     13    326 2010-08-11 06:09:29 UTC+0000
. 0xff3667e8:VMwareTray.exe                           432   1724      1     49 2010-08-11 06:09:31 UTC+0000
. 0xff38a410:IEXPLORE.EXE                            1340   1724     12    346 2010-08-15 19:09:26 UTC+0000
. 0xff374980:VMwareUser.exe                           452   1724      8    206 2010-08-11 06:09:32 UTC+0000
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x06499b80 svchost.exe            1148 True   True   True     True   True  True    True
0x04b5a980 VMwareUser.exe          452 True   True   True     True   True  True    True
0x010f7588 wuauclt.exe             468 True   True   True     True   True  True    True
0x04c2b310 wscntfy.exe             888 True   True   True     True   True  True    True
0x061ef558 svchost.exe            1088 True   True   True     True   True  True    True
0x06015020 services.exe            676 True   True   True     True   True  True    True
0x069d5b28 vmtoolsd.exe           1668 True   True   True     True   True  True    True
0x01122910 svchost.exe            1028 True   True   True     True   True  True    True
0x06384230 vmacthlp.exe            844 True   True   True     True   True  True    True
0x0655fc88 VMUpgradeHelper        1788 True   True   True     True   True  True    True
0x06945da0 spoolsv.exe            1432 True   True   True     True   True  True    True
0x05f027e0 alg.exe                 216 True   True   True     True   True  True    True
0x049c15f8 TPAutoConnect.e        1084 True   True   True     True   True  True    True
0x05f47020 lsass.exe               688 True   True   True     True   True  True    True
0x04a065d0 explorer.exe           1724 True   True   True     True   True  True    True
0x066f0978 winlogon.exe            632 True   True   True     True   True  True    True
0x0115b8d8 svchost.exe             856 True   True   True     True   True  True    True
0x063c5560 svchost.exe             936 True   True   True     True   True  True    True
0x049c2410 IEXPLORE.EXE           1340 True   True   True     True   True  True    True
0x04be97e8 VMwareTray.exe          432 True   True   True     True   True  True    True
0x0211ab28 TPAutoConnSvc.e        1968 True   True   True     True   True  True    True
0x04a4b5f8 lanmanwrk.exe          1180 True   True   True     True   True  True    True
0x05471020 smss.exe                544 True   True   True     True   False False   False
0x065a3b08 cmd.exe                 460 True   True   False    True   False False   False    2010-08-15 19:11:21 UTC+0000
0x066f0da0 csrss.exe               608 True   True   True     True   False True    True
0x01214660 System                    4 True   True   True     True   False False   False
0x066f1c08 logonui.exe            1168 False  True   False    False  False False   False    2010-08-11 06:09:35 UTC+0000
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EaTMcAw_GaBGhx4d_mqbDVkBEy2yRfV5sxYrx7p1vqWnQA?e=D5JLYl

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem dlllist
```

I noticed in a “privs” search that it was very similar to 1.vmem, but had lanmanwrk.exe and IEXPLORER.EXE was a different PID (2044 in 1.vmem)

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem privs --silent
Volatility Foundation Volatility Framework 2.6
Pid      Process          Value  Privilege                       Attributes               Description
-------- ---------------- -----  ------------------------------- ------------------------ -----------
     632 winlogon.exe         8  SeSecurityPrivilege             Present,Enabled          Manage auditing and security log
     632 winlogon.exe        10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
     632 winlogon.exe        25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
     688 lsass.exe            2  SeCreateTokenPrivilege          Present,Enabled          Create a token object
     688 lsass.exe           10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
     688 lsass.exe           25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
    1028 svchost.exe          2  SeCreateTokenPrivilege          Present,Enabled          Create a token object
    1028 svchost.exe          9  SeTakeOwnershipPrivilege        Present,Enabled          Take ownership of files/objects
    1028 svchost.exe          3  SeAssignPrimaryTokenPrivilege   Present,Enabled          Replace a process-level token
    1028 svchost.exe          5  SeIncreaseQuotaPrivilege        Present,Enabled          Increase quotas
    1028 svchost.exe          8  SeSecurityPrivilege             Present,Enabled          Manage auditing and security log
    1028 svchost.exe         22  SeSystemEnvironmentPrivilege    Present,Enabled          Edit firmware environment values
    1028 svchost.exe         17  SeBackupPrivilege               Present,Enabled          Backup files and directories
    1028 svchost.exe         18  SeRestorePrivilege              Present,Enabled          Restore files and directories
    1028 svchost.exe         19  SeShutdownPrivilege             Present,Enabled          Shut down the system
    1028 svchost.exe         10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
    1028 svchost.exe         12  SeSystemtimePrivilege           Present,Enabled          Change the system time
    1028 svchost.exe         25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
    1028 svchost.exe         28  SeManageVolumePrivilege         Present,Enabled          Manage the files on a volume
    1432 spoolsv.exe         10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
    1432 spoolsv.exe         25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
    1788 VMUpgradeHelper     10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
    1788 VMUpgradeHelper     25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
    1724 explorer.exe        10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
    1724 explorer.exe        25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
     432 VMwareTray.exe      10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
     432 VMwareTray.exe      25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
     452 VMwareUser.exe      10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
     452 VMwareUser.exe      25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
    1180 lanmanwrk.exe       10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
    1180 lanmanwrk.exe       25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
    1340 IEXPLORE.EXE        10  SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
    1340 IEXPLORE.EXE        25  SeUndockPrivilege               Present,Enabled          Remove computer from docking station
kali@kali:~/Desktop/volatility$
```

1.7.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EdUegp1rE4VGl7JRmdSdvmQBHEXFEGCQOxdyGr17iogeNg?e=TIsaPe

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem apihooks > 2_apihooks.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EWo4pOwhVk5DnUIVy4GQ5yMBLt93Ap_pm7-Am6lMoWXmxg?e=Jb7IMY

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem malfind > 2_malfind.txt
Volatility Foundation Volatility Framework 2.6
```

1.8.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/Ec59wAUJD91PkpvNuFvfjDEBVllerWr7_IRrU9oeL5j1Gw?e=8JcQJ2

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem modules > 2_modules.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EdhKiozhHPhIsphLoAtydLoBD2d5e1u9vfErBQjmTJ87hQ?e=rDiKSE

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem driverscan > 2_drivers.txt
Volatility Foundation Volatility Framework 2.6
```

I found a suspicious driver related to lanmanwrk.exe, and a suspicious Temp file in filescan

```
0x0000000006452638      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Wir
0x0000000006452ea0      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\lanmandrv.sys
0x00000000064535b8      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\WinSxS\x86_Microsoft.Wir
0x0000000006453a10      1      1 R--rw- \Device\HarddiskVolume1\WINDOWS\system32
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem handles -t File | grep Temp
Volatility Foundation Volatility Framework 2.6
0xff1dc200   1148      0x164   0x12019f File           \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings
E5\index.dat
0x80f062e0   1668      0x2ac   0x13019f File           \Device\HarddiskVolume1\WINDOWS\Temp\Perflib_Perfdata_684.dat
0x80f2b900   1724      0x504   0x12019f File           \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Setting
IE5\index.dat
0xff39aad0    452      0x254   0x12019f File           \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Setting
IE5\index.dat
0x80ffab70   1340      0x138   0x12019f File           \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Setting
IE5\index.dat
0xff236028   1340      0x6a8   0x120089 File           \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Setting
IE5\0H2PKTU1\Sync[1].html
0xff212848   1340      0x6c0   0x120089 File           \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Setting
IE5\EBWBQT8J\Include[1].html
kali@kali:~/Desktop/volatility$
```

Suspicious objects were seen in a Mutant scan

```
0xff21e0e0    856      0x1ec   0x1f0001 Mutant
0xff22f0e0    856      0x1f8   0x1f0001 Mutant
0xff2232e8    856      0x200   0x1f0001 Mutant
0xff2741f0    856      0x218   0x1f0001 Mutant          746bbf3569adEncrypt
0xff15a2c0    856      0x238   0x1f0001 Mutant
0x80fca0e0    856      0x288   0x1f0001 Mutant
0xff257148   1028       0x24   0x1f0001 Mutant          SHIMLIB_LOG_MUTEX
0xff21d960   1028      0x2b8   0x1f0001 Mutant
0xff209bc8   1028      0x2bc   0x1f0001 Mutant
```

```
0×ff272440   1724      0×2b0    0×1f0001 Mutant
0×ff272258   1724      0×2b8    0×1f0001 Mutant
0×ff277dd0   1724      0×2f0    0×1f0001 Mutant          _SHuassist.mtx
0×80f74de8   1724      0×384    0×1f0001 Mutant
0×ff372608   1724      0×394    0×1f0001 Mutant
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/Ef4NEaR3789NvvO3JiwQT_MB0a9sx0uL6I1_ps0oTaB7Tw?e=Da2mW3

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem thrdscan > 2_thrdscan.txt
Volatility Foundation Volatility Framework 2.6
```

Unloaded modules were relatively same as 1.vmem

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem unloadedmodules
Volatility Foundation Volatility Framework 2.6
Name                 StartAddress EndAddress Time
-------------------- ------------ ---------- ----
Sfloppy.SYS          0×00fc178000 0×fc17b000 2010-08-11 06:06:17
Cdaudio.SYS          0×00fc7b3000 0×fc7b8000 2010-08-11 06:06:17
vmdebug.sys          0×00fc66b000 0×fc674000 2010-08-11 06:06:47
splitter.sys         0×00fc9cd000 0×fc9cf000 2010-08-11 06:07:39
aec.sys              0×00f3124000 0×f3147000 2010-08-11 06:07:44
swmidi.sys           0×00f377d000 0×f378b000 2010-08-11 06:07:44
DMusic.sys           0×00f323c000 0×f3249000 2010-08-11 06:07:44
kmixer.sys           0×00f30fa000 0×f3124000 2010-08-11 06:07:44
drmkaud.sys          0×00fcab8000 0×fcab9000 2010-08-11 06:07:44
kmixer.sys           0×00f2fe0000 0×f300a000 2010-08-15 19:03:58
```

1.9. Benign connections

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0×01069670 172.16.176.143:1082      65.54.81.184:80           1340
0×01156b50 172.16.176.143:1083      65.54.81.186:80           1340
0×01163460 172.16.176.143:1079      12.120.180.24:80          1340
0×02214988 172.16.176.143:1052      207.46.170.123:80         1340
0×0485e2f0 172.16.176.143:1096      65.54.81.173:80           1340
0×049c1b58 172.16.176.143:1077      65.55.15.123:80           1340
0×049c2cf0 172.16.176.143:1067      65.54.81.173:80           1340
0×04a045f8 172.16.176.143:1069      96.6.41.211:80            1340
0×04c2d670 172.16.176.143:1084      65.55.239.161:80          1340
0×057c1e70 172.16.176.143:1068      65.54.81.173:80           1340
0×05802340 172.16.176.143:1085      65.55.239.161:80          1340
0×05c16d40 172.16.176.143:1078      65.55.15.125:80           1340
0×05ca0ce0 172.16.176.143:1076      65.54.81.201:80           1340
0×05e39cf8 172.16.176.143:1066      66.235.139.54:80          1340
0×05e7e7f8 172.16.176.143:1094      65.54.81.173:80           1340
0×06015ab0 172.16.176.143:1053      207.46.140.21:80          1340
```

Some odd ports coming out of svchost.exe (PID 1088): 1025,1060, and 1080
Odd ports coming out of svchost.exe (PID 936): 135
Odd ports coming out of IEXPLORER.EXE (PID 1340): 1051, 1076, 1072, 1079, 1900, 1075, 1065, 1066, 1073, 52,

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ---------- --------------- -------------------
0x80fd1008        4      0     47 GRE            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0xff258008      688    500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff367008        4    445      6 TCP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x80ffc128      936    135      6 TCP            0.0.0.0         2010-08-11 06:06:24 UTC+0000
0xff153a20     1028    123     17 UDP            127.0.0.1       2010-08-15 19:11:21 UTC+0000
0xff225b70      688      0    255 Reserved       0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x80fce930     1088   1025     17 UDP            0.0.0.0         2010-08-11 06:06:38 UTC+0000
0xff126730     1088   1060     17 UDP            0.0.0.0         2010-08-15 19:09:30 UTC+0000
0xff127d28      216   1026      6 TCP            127.0.0.1       2010-08-11 06:06:39 UTC+0000
0x80f71158     1088   1080     17 UDP            0.0.0.0         2010-08-15 19:09:33 UTC+0000
0xff39eac0     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:11:21 UTC+0000
0xff3ae2f8     1340   1051     17 UDP            127.0.0.1       2010-08-15 19:09:28 UTC+0000
0xff1b8250      688   4500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff382e98        4   1033      6 TCP            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x80fbdc40        4    445     17 UDP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem sockscan
Volatility Foundation Volatility Framework 2.6
Offset(P)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ---------- --------------- -------------------
0x007c0a20     1028    123     17 UDP            127.0.0.1       2010-08-15 19:11:21 UTC+0000
0x010caa00     1340   1069      6 TCP            0.0.0.0         2010-08-15 19:09:31 UTC+0000
0x010d4158     1088   1080     17 UDP            0.0.0.0         2010-08-15 19:09:33 UTC+0000
0x010d7e98     1340   1076      6 TCP            0.0.0.0         2010-08-15 19:09:32 UTC+0000
0x010f7400     1340   1072      6 TCP            0.0.0.0         2010-08-15 19:09:31 UTC+0000
0x01120c40        4    445     17 UDP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x01131930     1088   1025     17 UDP            0.0.0.0         2010-08-11 06:06:38 UTC+0000
0x01134008        4      0     47 GRE            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x0115f128      936    135      6 TCP            0.0.0.0         2010-08-11 06:06:24 UTC+0000
0x02d6e730     1088   1060     17 UDP            0.0.0.0         2010-08-15 19:09:30 UTC+0000
0x02daad28      216   1026      6 TCP            127.0.0.1       2010-08-11 06:06:39 UTC+0000
0x0438ee40     1340   1079      6 TCP            0.0.0.0         2010-08-15 19:09:33 UTC+0000
0x0445c2f8     1340   1051     17 UDP            127.0.0.1       2010-08-15 19:09:28 UTC+0000
0x04863458     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:02:55 UTC+0000
0x04864e98     1340   1075      6 TCP            0.0.0.0         2010-08-15 19:09:32 UTC+0000
0x04866888     1148   1900     17 UDP            172.16.176.143  2010-08-15 19:02:55 UTC+0000
0x0486cac0     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:11:21 UTC+0000
0x04a4be98        4   1033      6 TCP            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x04be7008        4    445      6 TCP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x05c5a3c0     1340   1066      6 TCP            0.0.0.0         2010-08-15 19:09:31 UTC+0000
0x05c5b660     1340   1065      6 TCP            0.0.0.0         2010-08-15 19:09:31 UTC+0000
0x05dee200        4    137     17 UDP            172.16.176.143  2010-08-15 19:02:55 UTC+0000
0x05e33d68     1028    123     17 UDP            127.0.0.1       2010-08-15 19:02:55 UTC+0000
0x05f44008      688    500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x05f48008        4    138     17 UDP            172.16.176.143  2010-08-15 19:02:55 UTC+0000
0x06237b70      688      0    255 Reserved       0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x06384e98        4    138     17 UDP            172.16.176.143  2010-08-11 06:06:28 UTC+0000
0x0644e980     1340   1073      6 TCP            0.0.0.0         2010-08-15 19:09:32 UTC+0000
0x06450a18     1340     52      0 HOPOPT         0.0.0.0         2010-08-15 19:09:34 UTC+0000
0x06450c98        4    139      6 TCP            172.16.176.143  2010-08-15 19:02:55 UTC+0000
0x069d5250      688   4500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
```

1.10.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1c49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xe1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ae580 0x01bbd580 [no name]
0xe101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008978 0x01824978 [no name]
0xe1e158c0 0x009728c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1da4008 0x00f6e008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
```

printkey for Run shows that lanmanwrk.exe was added as a key, proving that the malware is persistent even after rebooting:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem printkey -K "Microsoft\Windows\CurrentVersion\Run"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Run (S)
Last updated: 2010-08-15 19:09:19 UTC+0000

Subkeys:

Values:
REG_SZ        VMware Tools    : (S) "C:\Program Files\VMware\VMware Tools\VMwareTray.exe"
REG_SZ        VMware User Process : (S) "C:\Program Files\VMware\VMware Tools\VMwareUser.exe"
REG_SZ        lanmanwrk.exe   : (S) C:\WINDOWS\System32\lanmanwrk.exe
kali@kali:~/Desktop/volatility$
```

Suspicious Userassist activity with sophialite.exe, this indicates that the user initiated the infection with this executable:

```
REG_BINARY    UEME_RUNPATH:C:\Documents and Settings\Administrator\Desktop\sophialite.exe :
ID:             2
Count:          1
Last updated:   2010-08-15 19:09:10 UTC+0000
Raw Data:
0x00000000  02 00 00 00 06 00 00 00 60 be 64 57 ad 3c cb 01   ........`.dW.<..
```

Shimcache activity:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem shimcache
Volatility Foundation Volatility Framework 2.6
Last Modified                  Last Update                    Path
------------------------------ ------------------------------ ----
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:11:19 UTC+0000   \??\C:\WINDOWS\system32\oobe\msoobe.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:11:39 UTC+0000   \??\C:\WINDOWS\system32\oobe\oobebaln.exe
2006-02-28 12:00:00 UTC+0000   2010-08-11 06:04:52 UTC+0000   \??\C:\WINDOWS\system32\wscntfy.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:20:28 UTC+0000   \??\C:\WINDOWS\System32\cscui.dll
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:12:09 UTC+0000   \??\C:\Program Files\Outlook Express\setup50.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:12:08 UTC+0000   \??\C:\WINDOWS\inf\unregmp2.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:20:29 UTC+0000   \??\C:\WINDOWS\system32\NETSHELL.dll
2010-02-09 21:04:30 UTC+0000   2010-06-10 16:12:37 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\unzip.exe
2010-02-09 20:57:14 UTC+0000   2010-06-10 16:20:33 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
2010-02-09 20:57:14 UTC+0000   2010-06-10 16:12:49 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\TPVCGateway.exe
2010-02-09 21:00:20 UTC+0000   2010-06-10 16:20:18 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmacthlp.exe
2010-02-09 21:00:00 UTC+0000   2010-06-10 16:20:30 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmwareuser.exe
2010-02-09 21:00:10 UTC+0000   2010-06-10 16:20:30 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmwaretray.exe
2010-02-09 21:00:14 UTC+0000   2010-06-10 16:20:29 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:20:31 UTC+0000   \??\C:\WINDOWS\system32\shdocvw.dll
2010-02-09 20:59:20 UTC+0000   2010-06-10 16:20:32 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat
2010-02-09 21:00:16 UTC+0000   2010-06-10 16:20:32 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\VMUpgradeHelper.exe
2010-02-09 20:57:14 UTC+0000   2010-06-10 16:20:36 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
2010-06-10 16:12:49 UTC+0000   2010-08-11 06:03:17 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\resume-vm-default.bat
2010-02-09 21:00:24 UTC+0000   2010-08-11 06:03:18 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\VMip.exe
```

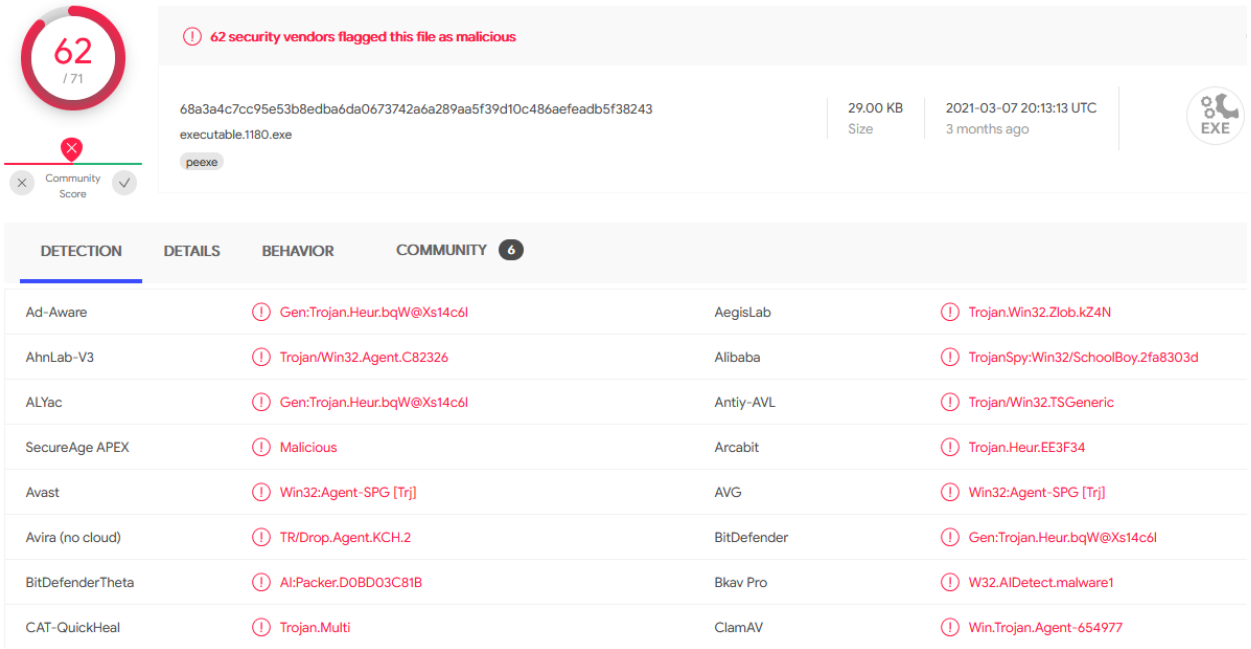
2. Dumped lanmanwrk.exe (PID 1180) after initial findings:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem procdump -p 1180 -D .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0xff3825f8 0x00400000 lanmanwrk.exe        OK: executable.1180.exe
```

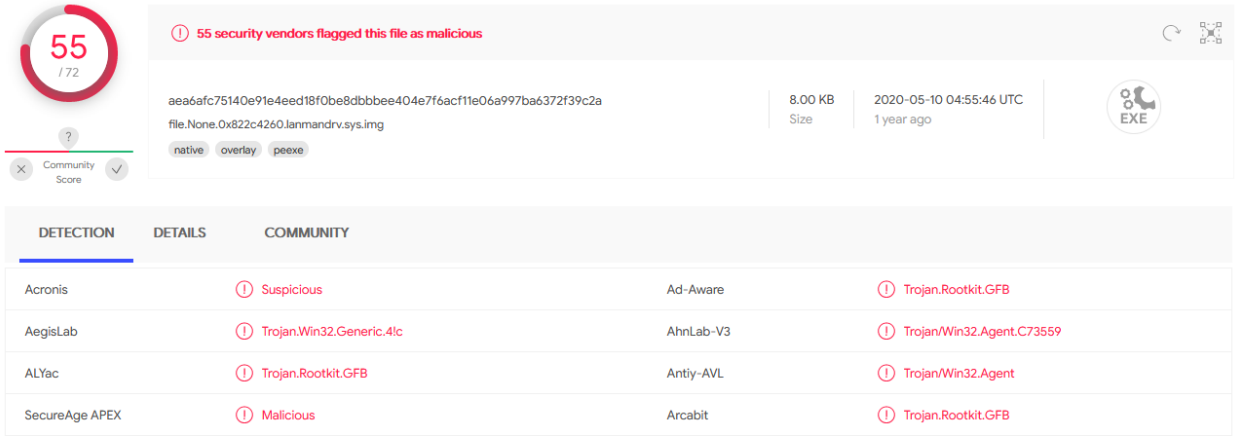
Also dropped lanmandrv.sys after finding it in filescan:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem dumpfiles -Q 0x000000006452ea0 -D dump
Volatility Foundation Volatility Framework 2.6
ImageSectionObject 0x06452ea0   None   \Device\HarddiskVolume1\WINDOWS\system32\lanmandrv.sys
DataSectionObject 0x06452ea0   None   \Device\HarddiskVolume1\WINDOWS\system32\lanmandrv.sys
kali@kali:~/Desktop/volatility$
```

3. Lanmanwrk.exe:



lanmandrv.sys:



4. This malware family belongs to Laqma, which is a trojan that installs a kernel-mode rootkit driver and communicates with a C2 server. The rootkit driver is labelled as “lanmandrv.sys”, which is used to hide the malware’s process and files from the user. It then copies itself as “lanmanwrk.exe”. The trojan can communicate info about the host to the C2 server, while also being able to be controlled remotely which can lead to more malicious processes being executed. It also inputs it’s .exe file into the Run registry to ensure persistence every time the host boots up. The goal of this malware appears to be similar to 1.vmem, where it is a credential harvester and backdoor into the system. Any passwords, emails, bank creds, usernames, or more will be harvested and sent back to the C2 server.

3.mem

1.

1.1. Image appears to be Win10x64_10586, however as you'll see in the following commands, sometimes Win2016x64_14393 had to be used.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win10x64_10586, Win10x64_14393, Win10x64, Win2016x64_14393
                     AS Layer1 : Win10AMD64PagedMemory (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/volatility/3.mem)
                      PAE type : No PAE
                           DTB : 0x1aa000L
                          KDBG : 0xf80294b73500L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0xfffff80294bc5000L
             KUSER_SHARED_DATA : 0xfffff78000000000L
           Image date and time : 2018-05-17 06:13:07 UTC+0000
     Image local date and time : 2018-05-17 01:13:07 -0500
```

1.2. Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EWBiJ5dXrelCt2E5meX7RSEBI9fHXjjp8qrfjWdNaAqeoQ?e=l6Xwbe

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 handles -t File > 3_files.txt
```

Filescan link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EclSziY67ltIrVJ1UQUMllMBzuIXeozTsNYQ1KSHi4jevg?e=ogzrmR

1.3. I was unable to read hashes from the registry using all possible profiles

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 hashdump
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Unable to read hashes from registry
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_14393 hashdump
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Unable to read hashes from registry
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64 hashdump
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Unable to read hashes from registry
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 hashdump
Volatility Foundation Volatility Framework 2.6
ERROR   : volatility.debug    : Unable to read hashes from registry
kali@kali:~/Desktop/volatility$
```

1.4. I found lots of encryption keys using findaes:

```
kali@kali:~/Desktop/volatility$ ./findaes 3.mem
Searching 3.mem
Found AES-128 key schedule at offset 0×1ce8740:
fa 09 71 1a b5 cf cc 44 3c 66 d9 8a ea c4 de ca
Found AES-256 key schedule at offset 0×1efb71c:
8b 44 b7 60 17 a8 6c db aa a9 f7 6c 3c 57 7b 8d 9e 81 cc 2c ea 91 e0 a4 7a 40 6d ee 83 e9 66 86
Found AES-256 key schedule at offset 0×1efb9ac:
03 6b b5 ec 46 0d 03 4b 69 f0 9d e4 db 80 66 0e 15 e5 e0 a8 71 73 2c c0 15 69 36 6f cd 6f de 62
Found AES-128 key schedule at offset 0×3422e10:
9c 33 06 3e 71 0c 8c 91 9b fa a4 b3 8b 27 87 1c
Found AES-256 key schedule at offset 0×3d3ebb0:
4b 7d 7c 07 7a 0c 4a ea f0 0e d5 fc 86 3c 9a 5e a3 fd df c6 67 60 ee 1a 1f d5 eb 53 23 e2 b0 f7
Found AES-128 key schedule at offset 0×5ba6e08:
4f de 9e 66 17 a9 8e 05 02 24 e1 58 4b 86 88 6d
Found AES-128 key schedule at offset 0×5e812f0:
70 2d 0f a6 92 8d 00 ad 21 50 ca d6 66 5e 91 5c
Found AES-128 key schedule at offset 0×5e81cf0:
70 2d 0f a6 92 8d 00 ad 21 50 ca d6 66 5e 91 5c
Found AES-256 key schedule at offset 0×5eaa100:
64 fb 99 75 96 14 69 ef d1 37 92 25 7b c0 d5 50 c1 4b b4 ba 39 54 62 0b da 4d d8 6d b4 89 27 2b
Found AES-128 key schedule at offset 0×6b59e08:
4f de 9e 66 17 a9 8e 05 02 24 e1 58 4b 86 88 6d
Found AES-256 key schedule at offset 0×73bbaf0:
12 69 fd 50 36 13 ea 82 20 97 e6 01 9e 67 1e 27 36 50 0e eb b4 6b 98 b6 87 3d 1b f5 5f 7f 7e a9
Found AES-256 key schedule at offset 0×8f0c7d8:
d2 ad 56 c1 e4 3d d4 09 6c a7 ad 02 77 d2 14 da c4 ee 0f a5 03 f4 05 53 9d 1f 9e 56 bd 00 30 6c
Found AES-256 key schedule at offset 0×a76714c:
d2 ad 56 c1 e4 3d d4 09 6c a7 ad 02 77 d2 14 da c4 ee 0f a5 03 f4 05 53 9d 1f 9e 56 bd 00 30 6c
Found AES-128 key schedule at offset 0×cb40c20:
8d f2 16 47 58 90 bb 88 88 6f 05 98 81 59 dc ad
Found AES-128 key schedule at offset 0×cb83970:
f1 4c 47 b7 02 d9 bc fe 4e 15 71 4e b3 20 92 e5
Found AES-128 key schedule at offset 0×d206c20:
8d f2 16 47 58 90 bb 88 88 6f 05 98 81 59 dc ad
Found AES-128 key schedule at offset 0×d380b80:
19 84 e5 87 88 28 0f 75 68 9e c8 1c 07 7b 73 17
Found AES-128 key schedule at offset 0×e64f6d0:
```

We can find the 512 bit encryption key by finding two 256 bit keys that are consecutive in memory.

```
kali@kali:~/Desktop/volatility$ ./findaes 3.mem
Searching 3.mem
Found AES-128 key schedule at offset 0×1ce8740:
fa 09 71 1a b5 cf cc 44 3c 66 d9 8a ea c4 de ca
Found AES-256 key schedule at offset 0×1efb71c:
8b 44 b7 60 17 a8 6c db aa a9 f7 6c 3c 57 7b 8d 9e 81 cc 2c ea 91 e0 a4 7a 40 6d ee 83 e9 66 86
Found AES-256 key schedule at offset 0×1efb9ac:
03 6b b5 ec 46 0d 03 4b 69 f0 9d e4 db 80 66 0e 15 e5 e0 a8 71 73 2c c0 15 69 36 6f cd 6f de 62
Found AES-128 key schedule at offset 0×3422e10:
9c 33 06 3e 71 0c 8c 91 9b fa a4 b3 8b 27 87 1c
Found AES-256 key schedule at offset 0×3d3ebb0:
```

Since Intel x86–64 uses little-endian scheme, we combine the keys in reverse order.

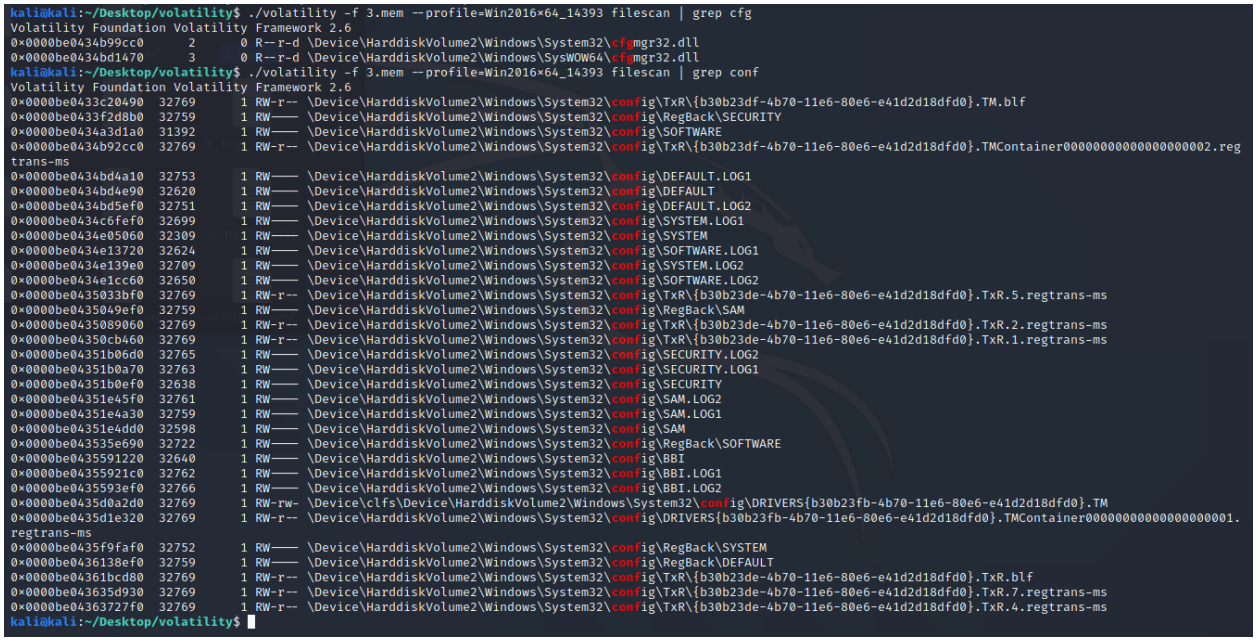
Encryption key: 03 6b b5 ec 46 0d 03 4b 69 f0 9d e4 db 80 66 0e 15 e5 e0 a8 71 73 2c c0 15 69 36 6f cd 6f de 62 8b 44 b7 60 17 a8 6c db aa a9 f7 6c 3c 57 7b 8d 9e 81 cc 2c ea 91 e0 a4 7a 40 6d ee 83 e9 66 86

Found RSA keys:

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/ERyRSg7FQVFCmGK-48cS6zABG15HArS1lvtJqvvQiIVptA?e=Ze1n4e

```
kali@kali:~/Desktop/volatility$ ./rsakeyfind 3.mem > 3_rsakeys.txt
```

1.5.



```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 filescan | grep cfg
Volatility Foundation Volatility Framework 2.6
0x0000be0434b99cc0      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\cfgmgr32.dll
0x0000be0434bd1470      3      0 R--r-d \Device\HarddiskVolume2\Windows\SysWOW64\cfgmgr32.dll
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 filescan | grep conf
Volatility Foundation Volatility Framework 2.6
0x0000be0433c20490  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23df-4b70-11e6-80e6-e41d2d18dfd0}.TM.blf
0x0000be0433f2d8b0  32759      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\RegBack\SECURITY
0x0000be0434a3d1a0  31392      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SOFTWARE
0x0000be0434b92cc0  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23df-4b70-11e6-80e6-e41d2d18dfd0}.TMContainer00000000000000000002.reg
trans-ms
0x0000be0434bd4a10  32753      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\DEFAULT.LOG1
0x0000be0434bd4e90  32620      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\DEFAULT
0x0000be0434bd5ef0  32751      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\DEFAULT.LOG2
0x0000be0434c6fef0  32699      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SYSTEM.LOG1
0x0000be0434e05060  32309      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SYSTEM
0x0000be0434e13720  32624      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SOFTWARE.LOG1
0x0000be0434e139e0  32709      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SYSTEM.LOG2
0x0000be0434e1cc60  32650      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SOFTWARE.LOG2
0x0000be0435033bf0  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23de-4b70-11e6-80e6-e41d2d18dfd0}.TxR.5.regtrans-ms
0x0000be0435049ef0  32759      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\RegBack\SAM
0x0000be0435089060  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23de-4b70-11e6-80e6-e41d2d18dfd0}.TxR.2.regtrans-ms
0x0000be04350cb460  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23de-4b70-11e6-80e6-e41d2d18dfd0}.TxR.1.regtrans-ms
0x0000be04351b06d0  32765      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SECURITY.LOG2
0x0000be04351b0a70  32763      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SECURITY.LOG1
0x0000be04351b0ef0  32638      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SECURITY
0x0000be04351e45f0  32761      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SAM.LOG2
0x0000be04351e4a30  32759      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SAM.LOG1
0x0000be04351e4dd0  32598      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\SAM
0x0000be043535e690  32722      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\RegBack\SOFTWARE
0x0000be0435591220  32640      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\BBI
0x0000be04355921c0  32762      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\BBI.LOG1
0x0000be0435593ef0  32766      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\BBI.LOG2
0x0000be0435d0a2d0  32769      1 RW-rw- \Device\clfs\Device\HarddiskVolume2\Windows\System32\config\DRIVERS{b30b23fb-4b70-11e6-80e6-e41d2d18dfd0}.TM
0x0000be0435d1e320  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\DRIVERS{b30b23fb-4b70-11e6-80e6-e41d2d18dfd0}.TMContainer00000000000000000001.
regtrans-ms
0x0000be0435f9faf0  32752      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\RegBack\SYSTEM
0x0000be0436138ef0  32759      1 RW---- \Device\HarddiskVolume2\Windows\System32\config\RegBack\DEFAULT
0x0000be04361bcd80  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23de-4b70-11e6-80e6-e41d2d18dfd0}.TxR.blf
0x0000be043635d930  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23de-4b70-11e6-80e6-e41d2d18dfd0}.TxR.7.regtrans-ms
0x0000be04363727f0  32769      1 RW-r-- \Device\HarddiskVolume2\Windows\System32\config\TxR\{b30b23de-4b70-11e6-80e6-e41d2d18dfd0}.TxR.4.regtrans-ms
kali@kali:~/Desktop/volatility$
```

1.6.

Parent PID for chrome.exe, notepad.exe, and FTK Imager.exe is explorer.exe
Also two smss.exe's, one is child of the first.
Multiple svchost.exe's all with the same parent PID (764), suggests something possibly suspicious

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xffffbe0434fbb080:wininit.exe                       668    576      1      0 2018-05-17 05:27:19 UTC+0000
. 0xffffbe043518d800:lsass.exe                        772    668     11      0 2018-05-17 05:27:19 UTC+0000
. 0xffffbe0435198080:services.exe                     764    668      5      0 2018-05-17 05:27:19 UTC+0000
.. 0xffffbe04355a6800:svchost.exe                     648    764     20      0 2018-05-17 05:27:20 UTC+0000
.. 0xffffbe0433af7800:vmacthlp.exe                   1176    764      1      0 2018-05-17 05:27:20 UTC+0000
.. 0xffffbe0435206800:svchost.exe                    1824    764      7      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe0435a2b800:dllhost.exe                    2596    764     10      0 2018-05-17 05:27:23 UTC+0000
.. 0xffffbe0435b67080:svchost.exe                    2716    764      9      0 2018-05-17 05:27:30 UTC+0000
.. 0xffffbe0435209800:ossec-agent.ex                 1836    764      6      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe04352175c0:vmtoolsd.exe                   1864    764      9      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe04355ba800:svchost.exe                     820    764     13      0 2018-05-17 05:27:20 UTC+0000
.. 0xffffbe043523d800:wlms.exe                       1908    764      4      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe04352a3800:SearchIndexer.                 1988    764     16      0 2018-05-17 05:27:21 UTC+0000
... 0xffffbe0436390500:SearchFilterHo                 288   1988      8      0 2018-05-17 06:12:11 UTC+0000
... 0xffffbe043680a280:SearchProtocol                2936   1988     10      0 2018-05-17 06:12:11 UTC+0000
.. 0xffffbe043545c800:svchost.exe                    1348    764      9      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe0435914800:svchost.exe                    1788    764     12      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe04359cb080:TPAutoConnSvc.                 2444    764      7      0 2018-05-17 05:27:23 UTC+0000
... 0xffffbe0435363080:TPAutoConnect.                3476   2444      4      0 2018-05-17 05:27:33 UTC+0000
.... 0xffffbe04355d7700:conhost.exe                  3484   3476      1      0 2018-05-17 05:27:33 UTC+0000
.. 0xffffbe04351f1800:svchost.exe                     844    764     20      0 2018-05-17 05:27:20 UTC+0000
... 0xffffbe0435e93800:SearchUI.exe                  3904    844     32      0 2018-05-17 05:27:35 UTC+0000
... 0xffffbe0435e6d800:ShellExperienc                3836    844     31      0 2018-05-17 05:27:34 UTC+0000
... 0xffffbe0433f12800:dllhost.exe                   1928    844      5      0 2018-05-17 05:35:01 UTC+0000
... 0xffffbe04359f0800:WmiPrvSE.exe                  2536    844     11      0 2018-05-17 05:27:23 UTC+0000
... 0xffffbe0435d71440:RuntimeBroker.                3260    844     18      0 2018-05-17 05:27:33 UTC+0000
.. 0xffffbe0433b273c0:svchost.exe                    1232    764     54      0 2018-05-17 05:27:21 UTC+0000
... 0xffffbe0435b42080:taskhostw.exe                 3324   1232     15      0 2018-05-17 05:27:33 UTC+0000
... 0xffffbe0435d82800:sihost.exe                    3292   1232     13      0 2018-05-17 05:27:33 UTC+0000
... 0xffffbe0433ea4800:taskhostw.exe                 4184   1232      5      0 2018-05-17 05:30:23 UTC+0000
.. 0xffffbe04358df800:spoolsv.exe                    1748    764     15      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe0435234800:svchost.exe                    1888    764     10      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe04359c2800:MsMpEng.exe                    4688    764      5      0 2018-05-17 05:30:30 UTC+0000
.. 0xffffbe0433b36800:svchost.exe                    1252    764     23      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe043550b400:svchost.exe                     880    764     13      0 2018-05-17 05:27:20 UTC+0000
.. 0xffffbe0435d80800:svchost.exe                    3304    764      7      0 2018-05-17 05:27:33 UTC+0000
.. 0xffffbe0433af0080:svchost.exe                    1140    764     24      0 2018-05-17 05:27:20 UTC+0000
.. 0xffffbe0435a9a800:msdtc.exe                      2804    764      9      0 2018-05-17 05:27:24 UTC+0000
.. 0xffffbe04354f7800:svchost.exe                    1656    764      4      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe0435223800:VGAuthService.                 1876    764      2      0 2018-05-17 05:27:21 UTC+0000
.. 0xffffbe04355c4800:svchost.exe                     892    764     20      0 2018-05-17 05:27:20 UTC+0000
 0xffffbe0434bce080:csrss.exe                         584    576     10      0 2018-05-17 05:27:19 UTC+0000
 0xffffbe0433a3c040:System                              4      0     99      0 2018-05-17 05:27:17 UTC+0000
. 0xffffbe0433dcb800:smss.exe                         496      4      2      0 2018-05-17 05:27:17 UTC+0000
.. 0xffffbe0434f26080:smss.exe                        644    496      0 ------ 2018-05-17 05:27:19 UTC+0000
... 0xffffbe0434fa2080:csrss.exe                      652    644     11      0 2018-05-17 05:27:19 UTC+0000
... 0xffffbe0434fb7080:winlogon.exe                   704    644      2      0 2018-05-17 05:27:19 UTC+0000
.... 0xffffbe0434453080:fontdrvhost.ex                5044    704      5      0 2018-05-17 05:28:44 UTC+0000
.... 0xffffbe043555c080:dwm.exe                       988    704     11      0 2018-05-17 05:27:20 UTC+0000
.... 0xffffbe0435dda800:userinit.exe                 3564    704      0 ------ 2018-05-17 05:27:33 UTC+0000
..... 0xffffbe0435de4480:explorer.exe                3588   3564     84      0 2018-05-17 05:27:34 UTC+0000
...... 0xffffbe0435057800:notepad.exe                 196   3588      3      0 2018-05-17 05:56:53 UTC+0000
...... 0xffffbe0435f5d080:iexplore.exe               1412   3588     16      0 2018-05-17 05:36:35 UTC+0000
....... 0xffffbe043621c800:iexplore.exe              4484   1412     39      0 2018-05-17 05:41:21 UTC+0000
....... 0xffffbe0435f80080:iexplore.exe              2272   1412     32      0 2018-05-17 05:36:36 UTC+0000
...... 0xffffbe043432f080:chrome.exe                  192   3588      0 ------ 2018-05-17 06:03:00 UTC+0000
...... 0xffffbe0435fa6800:vmtoolsd.exe                996   3588      7      0 2018-05-17 05:27:46 UTC+0000
...... 0xffffbe043619a080:FTK Imager.exe             4244   3588     20      0 2018-05-17 06:12:30 UTC+0000
...... 0xffffbe0436398800:notepad.exe                2868   3588      3      0 2018-05-17 05:55:24 UTC+0000
```

psxview doesn't really show anything suspicious, no hidden files

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)          Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
------------------ -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x000000000defc800 smss.exe                496 True   True   False    False  False False   False
0x0000000003f16800 vmacthlp.exe           1176 True   True   False    False  False True    False
0x00000000151f4080 chrome.exe              192 True   True   False    False  False True    False
0x00000000074a9800 svchost.exe            1824 True   True   False    False  False True    False
0x0000000002fd5080 services.exe            764 True   True   False    False  False True    False
0x0000000016fea800 WmiPrvSE.exe           2536 True   True   False    False  False True    False
0x00000000010d5080 wininit.exe             668 True   True   False    False  False True    False
0x000000000e7d6080 svchost.exe            2716 True   True   False    False  False True    False
0x00000000002ab800 svchost.exe            3304 True   True   False    False  False True    False
0x00000000081d7080 csrss.exe               584 True   True   False    False  False True    False
0x0000000018c0c800 svchost.exe            1656 True   True   False    False  False True    False
0x0000000015068800 taskhostw.exe          4184 True   True   False    False  False True    False
0x000000001793a800 notepad.exe             196 True   True   False    False  False True    False
0x000000000f5c6800 SearchIndexer.         1988 True   True   False    False  False True    False
0x000000000e6ab800 SearchUI.exe           3904 True   True   False    False  False True    False
0x000000000f9e6800 wlms.exe               1908 True   True   False    False  False True    False
0x000000000cc4e080 FTK Imager.exe         4244 True   True   False    False  False True    False
0x0000000016de0800 svchost.exe            1788 True   True   False    False  False True    False
0x000000001d0fc080 fontdrvhost.ex         5044 True   True   False    False  False True    False
0x00000000129183c0 svchost.exe            1232 True   True   False    False  False True    False
0x000000000f831800 svchost.exe             820 True   True   False    False  False True    False
0x00000000120a4400 svchost.exe             880 True   True   False    False  False True    False
0x000000001422a440 RuntimeBroker.         3260 True   True   False    False  False True    False
0x000000000e6d2800 lsass.exe               772 True   True   False    False  False True    False
0x000000000e98e480 explorer.exe           3588 True   True   False    False  False True    False
0x0000000001822080 TPAutoConnect.         3476 True   True   False    False  False True    False
0x00000000138bc800 MsMpEng.exe            4688 True   True   False    False  False True    False
0x0000000013a40800 sihost.exe             3292 True   True   False    False  False True    False
0x0000000010adf080 taskhostw.exe          3324 True   True   False    False  False True    False
0x000000000cb20080 iexplore.exe           2272 True   True   False    False  False True    False
0x0000000019b215c0 vmtoolsd.exe           1864 True   True   False    False  False True    False
0x000000000f8c2080 winlogon.exe            704 True   True   False    False  False True    False
0x0000000015232700 conhost.exe            3484 True   True   False    False  False True    False
0x0000000000224040 System                    4 True   True   False    False  False False   False
0x0000000000879800 notepad.exe            2868 True   True   False    False  False True    False
0x000000001c6a1800 svchost.exe             844 True   True   False    False  False True    False
0x0000000010ca5080 TPAutoConnSvc.         2444 True   True   False    False  False True    False
0x000000001a6da800 ossec-agent.ex         1836 True   True   False    False  False True    False
0x0000000013adb800 vmtoolsd.exe            996 True   True   False    False  False True    False
0x000000000aa3c800 svchost.exe             648 True   True   False    False  False True    False
0x00000000036a8080 smss.exe                644 True   True   False    False  False True    False
0x000000001541d800 svchost.exe            1252 True   True   False    False  False True    False
0x00000000146d2800 ShellExperienc         3836 True   True   False    False  False True    False
0x000000000bd29080 iexplore.exe           1412 True   True   False    False  False True    False
0x000000001243e800 svchost.exe             892 True   True   False    False  False True    False
0x0000000005aff800 VGAuthService.         1876 True   True   False    False  False True    False
0x000000000b200800 svchost.exe            1348 True   True   False    False  False True    False
0x0000000016192800 userinit.exe           3564 True   True   False    False  False True    False
0x0000000005d61800 spoolsv.exe            1748 True   True   False    False  False True    False
0x0000000003420500 SearchFilterHo          288 True   True   False    False  False True    False
0x0000000012482800 msdtc.exe              2804 True   True   False    False  False True    False
0x0000000000e2e080 svchost.exe            1140 True   True   False    False  False True    False
0x0000000001fc3800 dllhost.exe            1928 True   True   False    False  False True    False
0x000000000d945800 iexplore.exe           4484 True   True   False    False  False True    False
0x000000000b17d280 SearchProtocol         2936 True   True   False    False  False True    False
0x00000000113e6800 svchost.exe            1888 True   True   False    False  False True    False
0x00000000110b2080 csrss.exe               652 True   True   False    False  False True    False
0x00000000163e7800 dllhost.exe            2596 True   True   False    False  False True    False
0x0000000013a93080 dwm.exe                 988 True   True   False    False  False True    False
0x00000000163df9ee .                    42 ... 0 False  True   False    False  False False   False
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EcOKKD3RCjRAjN5YBvPtUc8B_xvm9wDO5gOaZYrLb1552w?e=JxaIrN

```
kali@kali:~/Desktop/volatility$ ./volatility -f 2.vmem --profile=Win10x64_10586 dllist
```

Privs showing a lot of manually added privileges to MsMpEng.exe, which is Windows Defender.
This may have been done in an effort to circumvent or disable anti-virus detection.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 privs --silent
Volatility Foundation Volatility Framework 2.6
Pid      Process          Value  Privilege                       Attributes               Description
-------- ---------------- -----  ------------------------------- ------------------------ -----------
     772 lsass.exe            2 SeCreateTokenPrivilege          Present,Enabled          Create a token object
     988 dwm.exe             33 SeIncreaseWorkingSetPrivilege   Present,Enabled          Allocate more memory for user application
s
     648 svchost.exe         21 SeAuditPrivilege                Present,Enabled          Generate security audits
    1252 svchost.exe         21 SeAuditPrivilege                Present,Enabled          Generate security audits
    1656 svchost.exe         21 SeAuditPrivilege                Present,Enabled          Generate security audits
    4688 MsMpEng.exe          3 SeAssignPrimaryTokenPrivilege   Present,Enabled          Replace a process-level token
    4688 MsMpEng.exe          5 SeIncreaseQuotaPrivilege        Present,Enabled          Increase quotas
    4688 MsMpEng.exe          8 SeSecurityPrivilege             Present,Enabled          Manage auditing and security log
    4688 MsMpEng.exe          9 SeTakeOwnershipPrivilege        Present,Enabled          Take ownership of files/objects
    4688 MsMpEng.exe         10 SeLoadDriverPrivilege           Present,Enabled          Load and unload device drivers
    4688 MsMpEng.exe         17 SeBackupPrivilege               Present,Enabled          Backup files and directories
    4688 MsMpEng.exe         18 SeRestorePrivilege              Present,Enabled          Restore files and directories
    4688 MsMpEng.exe         19 SeShutdownPrivilege             Present,Enabled          Shut down the system
    4688 MsMpEng.exe         22 SeSystemEnvironmentPrivilege    Present,Enabled          Edit firmware environment values
```

1.7. Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EUQRpNU6PkZLqoFdx-SbfM8B-QBNjyPN2_DwKTjpOxiDLQ?e=PB1P8F

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 apihooks > 3_apihooks.txt
Volatility Foundation Volatility Framework 2.6
```

Malfind found nothing.

1.8. Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EUyhC43BNi5NqnjOp5muOCsBxt8RaUHI5KEJYR8DyTA1bQ?e=B09tzr

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 modules > 3_modules.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EVO5GSOlCOBEmi5PHH_cozIBTYpPjkRnGUIpg3Je401x4Q?e=PBWe8F

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 driverscan > 3_drivers.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/ESBCsYdaoTdErDJRIcGo92kBHVzpzmDoTvuM1nFa3pFkJA?e=0Wg7vn

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 thrdscan > 3_thrdscan.txt
Volatility Foundation Volatility Framework 2.6
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 unloadedmodules
Volatility Foundation Volatility Framework 2.6
Name                 StartAddress       EndAddress         Time
-------------------- ------------------ ------------------ ----
sacdrv.sys           0xfffff80e3e6d0000 0xfffff80e3e6ec000 2018-05-17 05:27:13
hwpolicy.sys         0xfffff80e3f3d0000 0xfffff80e3f3df000 2018-05-17 05:27:17
WdBoot.sys           0xfffff80e3e650000 0xfffff80e3e65f000 2018-05-17 05:27:17
dam.sys              0xfffff80e3f610000 0xfffff80e3f624000 2018-05-17 05:27:17
dump_LSI_SAS.sys     0xfffff80e3f4f0000 0xfffff80e3f50f000 2018-05-17 05:27:17
dump_storport.sys    0xfffff80e3f4c0000 0xfffff80e3f4cf000 2018-05-17 05:27:17
WdFilter.sys         0xfffff80e3ecf0000 0xfffff80e3ed40000 2018-05-17 05:30:26
```

Some very suspicious activity in Mutantscan:

```
0×0000be0436086b70        2        1      1 0×0000000000000000          .NET Data Provider for Oracle_Perf_Library_Lock_PID_748
0×0000be0436086c30        2        1      1 0×0000000000000000          .NET CLR Networking 4.0.0.0_Perf_Library_Lock_PID_748
0×0000be0436086cf0        2        1      1 0×0000000000000000          .NET CLR Networking_Perf_Library_Lock_PID_748
0×0000be0436086e30    32189        1      1 0×0000000000000000
0×0000be0436087080    32490        1      1 0×0000000000000000          PerfOS_Perf_Library_Lock_PID_748
0×0000be0436087470        1        1      1 0×0000000000000000
0×0000be04360876c0        2        1      1 0×0000000000000000          WSearchIdxPi_Perf_Library_Lock_PID_748
0×0000be0436087780        3        2      1 0×0000000000000000          WmiApRpl_Perf_Library_Lock_PID_748
0×0000be0436087840        2        1      1 0×0000000000000000          Windows Workflow Foundation 4.0.0.0_Perf_Library_Lock_PID_748
0×0000be0436087900        2        1      1 0×0000000000000000          usbhub_Perf_Library_Lock_PID_748
0×0000be04360879c0        2        1      1 0×0000000000000000          UGTHRSVC_Perf_Library_Lock_PID_748
0×0000be0436087a80        2        1      1 0×0000000000000000          UGatherer_Perf_Library_Lock_PID_748
0×0000be0436087b40        2        1      1 0×0000000000000000
0×0000be0436087c00        2        1      1 0×0000000000000000          Tcpip_Perf_Library_Lock_PID_748
0×0000be0436087cc0        2        1      1 0×0000000000000000
0×0000be0436087d80        2        1      1 0×0000000000000000          Spooler_Perf_Library_Lock_PID_748
0×0000be0436087e40        2        1      1 0×0000000000000000          SMSvcHost 4.0.0.0_Perf_Library_Lock_PID_748
0×0000be0436087f00        2        1      1 0×0000000000000000          RemoteAccess_Perf_Library_Lock_PID_748
0×0000be0436087fc0        2        1      1 0×0000000000000000          PerfProc_Perf_Library_Lock_PID_748
0×0000be04360c54a0    32768        1      1 0×0000000000000000          SM0:1232:232:WilStaging_01
0×0000be04360d3080    32768        1      1 0×0000000000000000          SM0:1140:232:WilStaging_01
0×0000be04360d74a0    32762        1      1 0×0000000000000000
0×0000be04360dd8b0   655337       20      1 0×0000000000000000          {5312EE61-79E3-4A24-BFE1-132B85B23C3A}
0×0000be04360f7fc0    32675        4      1 0×0000000000000000          SmartScreen_AppRepSettings_Mutex
0×0000be04360ffa90    32768        1      1 0×0000000000000000          SM0:996:232:WilStaging_01
0×0000be04361119a0    32758        1      1 0×0000000000000000          SM0:1232:120:WilError_01
0×0000be0436115200    32768        1      1 0×0000000000000000          SM0:3304:120:WilError_01
0×0000be0436132900        1        1      1 0×0000000000000000
0×0000be04361c4960    32764        1      1 0×0000000000000000          https://www.bing.com/
0×0000be04361cd080    32768        1      1 0×0000000000000000          ZonesLockedCacheCounterMutex
0×0000be0436207580    32768        1      1 0×0000000000000000
0×0000be043629ea90        2        1      1 0×0000000000000000          SmartScreen_ClientId_Mutex
0×0000be04362cb660    32768        1      1 0×0000000000000000
0×0000be0436338d50    32768        1      1 0×0000000000000000          SM0:4244:128:WilStaging_01
0×0000be0436339e30    32756        1      1 0×0000000000000000          http://www.getcreditcardnumbers.com/
0×0000be043636f910    32768        1      1 0×0000000000000000          SM0:1888:120:WilError_01
0×0000be043638c470    32768        1      1 0×0000000000000000          SM0:2272:64:WilError_01
0×0000be04363c9080    32760        1      1 0×0000000000000000          https://platform.twitter.com/
0×0000be0436704280    32652        1      1 0×0000000000000000          https://www.youtube.com/
0×0000be0436709160        1        1      1 0×0000000000000000
0×0000be04367dafc0    32768        1      1 0×0000000000000000          SM0:3260:120:WilError_01
0×0000be0436a3cd90    32768        1      1 0×0000000000000000          !IECompat!Mutex
kali@kali:~/Desktop/volatility$
```

The malware either may have originated from mail.com, or possibly setup as backdoor for exfiltrating data:

```
0×0000be043506d430        2        1      1 0×0000000000000000          CommunicationManager_Mutex
0×0000be0435083490    32704        1      1 0×0000000000000000          https://www.mail.com/
0×0000be0435091cd0    32768        1      1 0×0000000000000000          SM0:2936:120:WilError_01
0×0000be0435097fc0        1        1      1 0×0000000000000000
0×0000be04350d5fc0    32756        1      1 0×0000000000000000          https://home.navigator-lxa.mail.com/
0×0000be04350d8830    32768        1      1 0×0000000000000000          SM0:3836:232:WilStaging_01
0×0000be04350f0ee0        1        1      1 0×0000000000000000
0×0000be04350fd2a0    32768        1      1 0×0000000000000000
0×0000be0435117800    65535        2      1 0×0000000000000000          http://marketing.accessdata.com/
```

Some suspicious temp files:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016×64_14393 filescan | grep Temp
Volatility Foundation Volatility Framework 2.6
0×0000be0435075080  32532      1 RWDrwd \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\~DF764BC9F6876AD011.TMP
0×0000be0435101c40     16      0 R--r-d \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\ad_driver.sys
0×0000be043524a080  32731      1 -W-rw- \Device\HarddiskVolume2\Windows\Temp\vmware-vmsvc.log
0×0000be0435b28910  32335      1 RWDrwd \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\~DFEA0AEBE1B7B7CB70.TMP
0×0000be0435ea4380  32737      1 -W-rw- \Device\HarddiskVolume2\Windows\Temp\vmware-vmusr.log
0×0000be0435f18330  32783      1 RW-r-- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Packages\Microsoft.Window
eCache_100_0_Header.bin
0×0000be0435f1abb0  32780      1 RW-r-- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Packages\Microsoft.Window
eCache_100_0_Data.bin
0×0000be0435fdba80      2      0 R--r-d \Device\HarddiskVolume2\Windows\System32\TempSignedLicenseExchangeTask.dll
0×0000be043603e670  32720      1 RWDrwd \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\~DF09CED4AC3BF216BB.TMP
0×0000be043607d080  32638      1 RWDrwd \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\~DF945CA8E38C5B3AC4.TMP
0×0000be0436297ef0  32673      1 RWDrwd \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\~DFFB35C9CB7B6808E8.TMP
0×0000be04363df9a0  32679      1 RWDrwd \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\~DFF665B608F85A5AF8.TMP
0×0000be043680f9a0  32679      1 RWDrwd \Device\HarddiskVolume2\Users\ADMINI~1\AppData\Local\Temp\~DF615539DE5797ADB9.TMP
kali@kali:~/Desktop/volatility$
```

Suspicious .dll downloaded with ms-update:

```
0xffffbe0436230900   3588            0x1a68          0x100020 File            \Device\HarddiskVolume2\Windows\WinSxS\amd64_microsoft.windows.c..-control
0xffffbe04367f2ef0   3588            0x1aa0          0x120089 File            \Device\HarddiskVolume2\Windows\WinSxS\amd64_microsoft.windows.c..
-controls.resources_6595b64144ccf1df_6.0.14393.953_en-us_58206768f32c3a58\comctl32.dll.mui
0xffffbe0435141c00   3588            0x1ab0          0x120089 File            \Device\HarddiskVolume2\Windows\System32\en-US\shdocvw.dll.mui
```

Some Automatic Crash Recovery files:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 filescan | grep Active
Volatility Foundation Volatility Framework 2.6
0x0000be0435509d60  30350      1 RW---- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\RecoveryStore.{42FD8A34-5
994-11E8-A39A-000C290358B4}.dat
0x0000be04360c3960  32138      1 RW---- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{59DD9FEE-5996-11E8-A39A-
000C290358B4}.dat
0x0000be0436195080  31399      1 RW---- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{42C6D1ED-5998-11E8-A39A-
000C290358B4}.dat
0x0000be0436289ef0  32038      1 RW---- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{0662B324-5998-11E8-A39A-
000C290358B4}.dat
0x0000be043680e1b0  32183      1 RW---- \Device\HarddiskVolume2\Users\Administrator\AppData\Local\Microsoft\Internet Explorer\Recovery\High\Active\{679DB71D-5996-11E8-A39A-
000C290358B4}.dat
kali@kali:~/Desktop/volatility$
```

Odd temp file downloaded in handles -t File:

```
0xffffbe043511d7f0   1232            0x1b70          0x100020 File            \Device\HarddiskVolume2
0xffffbe0433cb8460   1232            0x1c44          0x120089 File            \Device\HarddiskVolume2
0xffffbe04352bea00   1232            0x1ce4          0x120196 File            \Device\HarddiskVolume2\Windows\SoftwareDistribution\Download\085532b3fce6344007c2396ae209e3e4\BIT2E60.tmp
0xffffbe0435eb2770   1232            0x1ee0          0x120089 File            \Device\DeviceApi\CMNotify
0xffffbe0435ea3450   1232            0x1ff4          0x120089 File            \Device\DeviceApi\CMNotify
```

Analyzed mftparser activity, lots of odd and suspicious activity:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win2016x64_14393 mftparser > 3_mftparser.txt
Volatility Foundation Volatility Framework 2.6
kali@kali:~/Desktop/volatility$
```

Package modification:

```
$STANDARD_INFORMATION
Creation                       Modified                       MFT Altered                    Access Date                    Type
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----

2017-12-26 18:00:51 UTC+0000 2017-03-04 06:32:56 UTC+0000   2018-04-21 19:23:51 UTC+0000   2017-12-26 18:00:51 UTC+0000   Archive

**************************************************************************
**************************************************************************
MFT entry found at offset 0x163b400
Attribute: In Use & File
Record Number: 112365
Link count: 0


$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----------

2018-04-21 18:48:48 UTC+0000 2018-03-23 03:25:03 UTC+0000   2018-04-21 18:48:55 UTC+0000   2018-04-21 18:48:48 UTC+0000   Windows\WinSxS\Catalogs\68aa51558d96f6f29a60ef2c9fe78732e30a337879a

$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----------

2018-04-21 18:48:48 UTC+0000 2018-03-23 03:25:03 UTC+0000   2018-04-21 18:48:55 UTC+0000   2018-04-21 18:48:48 UTC+0000   Package_134_for_KB4093137~31bf3856ad364e35~amd64~~10.0.1.6.cat

$DATA
```

sendmail.dll modified:

```
$STANDARD_INFORMATION
Creation                       Modified                       MFT Altered                    Access Date                    Type
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----

2017-12-26 18:00:51 UTC+0000 2017-06-21 06:59:41 UTC+0000   2018-04-14 19:45:32 UTC+0000   2017-12-26 18:00:51 UTC+0000   Archive

$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----------

2017-12-26 18:00:51 UTC+0000 2017-06-21 06:59:41 UTC+0000   2017-12-26 18:11:40 UTC+0000   2017-12-26 18:00:51 UTC+0000   Windows\System32\sendmail.dll

$FILE_NAME
Creation                       Modified                       MFT Altered                    Access Date                    Name/Path
------------------------------ ------------------------------ ------------------------------ ------------------------------ ----------

2017-12-26 18:00:51 UTC+0000 2017-06-21 06:59:41 UTC+0000   2017-12-26 18:11:19 UTC+0000   2017-12-26 18:00:51 UTC+0000   sendmail.dll
```

Odd desktop.ini modification activity, includes shell32.exe:

```
*******************************************************************************
*******************************************************************************
MFT entry found at offset 0×bd6000
Attribute: In Use & File
Record Number: 21352
Link count: 1


$STANDARD_INFORMATION
Creation                      Modified                      MFT Altered                   Access Date                   Type
----------------------------- ----------------------------- ----------------------------- ----------------------------- ----

2016-07-16 13:18:49 UTC+0000 2016-07-16 13:18:49 UTC+0000   2017-12-20 19:34:05 UTC+0000   2016-07-16 13:18:49 UTC+0000   Archive

$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path
----------------------------- ----------------------------- ----------------------------- ----------------------------- ----------

2017-12-20 19:34:05 UTC+0000 2017-12-20 19:34:05 UTC+0000   2017-12-20 19:34:05 UTC+0000   2017-12-20 19:34:05 UTC+0000   desktop.ini

$DATA
0000000000: ff fe 0d 00 0a 00 5b 00 2e 00 53 00 68 00 65 00   ......[ … S.h.e.
0000000010: 6c 00 6c 00 43 00 6c 00 61 00 73 00 73 00 49 00   l.l.C.l.a.s.s.I.
0000000020: 6e 00 66 00 6f 00 5d 00 0d 00 0a 00 4c 00 6f 00   n.f.o.].....L.o.
0000000030: 63 00 61 00 6c 00 69 00 7a 00 65 00 64 00 52 00   c.a.l.i.z.e.d.R.
0000000040: 65 00 73 00 6f 00 75 00 72 00 63 00 65 00 4e 00   e.s.o.u.r.c.e.N.
0000000050: 61 00 6d 00 65 00 3d 00 40 00 25 00 53 00 79 00   a.m.e•=.@.%.S.y.
0000000060: 73 00 74 00 65 00 6d 00 52 00 6f 00 6f 00 74 00   s.t.e.m.R.o.o.t.
0000000070: 25 00 5c 00 73 00 79 00 73 00 74 00 65 00 6d 00   %.\.s.y.s.t.e.m.
0000000080: 33 00 32 00 5c 00 73 00 68 00 65 00 6c 00 6c 00   3.2.\.s.h.e.l.l.
0000000090: 33 00 32 00 2e 00 64 00 6c 00 6c 00 2c 00 2d 00   3.2 … d.l.l.,•–.
00000000a0: 32 00 31 00 37 00 38 00 31 00 0d 00 0a 00         2.1.7.8.1.....
```

```
$STANDARD_INFORMATION
Creation                      Modified                      MFT Altered                   Access Date                   Type
----------------------------- ----------------------------- ----------------------------- ----------------------------- ----

2016-07-16 13:23:24 UTC+0000 2016-07-16 13:21:29 UTC+0000   2017-12-20 19:34:05 UTC+0000   2016-07-16 13:21:29 UTC+0000   Hidden & System & Archive

$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path
----------------------------- ----------------------------- ----------------------------- ----------------------------- ----------

2017-12-20 19:34:05 UTC+0000 2017-12-20 19:34:05 UTC+0000   2017-12-20 19:34:05 UTC+0000   2017-12-20 19:34:05 UTC+0000   PROGRA~1\desktop.ini

$DATA
0000000000: ff fe 0d 00 0a 00 5b 00 2e 00 53 00 68 00 65 00   ......[ … S.h.e.
0000000010: 6c 00 6c 00 43 00 6c 00 61 00 73 00 73 00 49 00   l.l.C.l.a.s.s.I.
0000000020: 6e 00 66 00 6f 00 5d 00 0d 00 0a 00 4c 00 6f 00   n.f.o.].....L.o.
0000000030: 63 00 61 00 6c 00 69 00 7a 00 65 00 64 00 52 00   c.a.l.i.z.e.d.R.
0000000040: 65 00 73 00 6f 00 75 00 72 00 63 00 65 00 4e 00   e.s.o.u.r.c.e.N.
0000000050: 61 00 6d 00 65 00 3d 00 40 00 25 00 53 00 79 00   a.m.e•=.@.%.S.y.
0000000060: 73 00 74 00 65 00 6d 00 52 00 6f 00 6f 00 74 00   s.t.e.m.R.o.o.t.
0000000070: 25 00 5c 00 73 00 79 00 73 00 74 00 65 00 6d 00   %.\.s.y.s.t.e.m.
0000000080: 33 00 32 00 5c 00 73 00 68 00 65 00 6c 00 6c 00   3.2.\.s.h.e.l.l.
0000000090: 33 00 32 00 2e 00 64 00 6c 00 6c 00 2c 00 2d 00   3.2 … d.l.l.,•–.
00000000a0: 32 00 31 00 37 00 38 00 31 00 0d 00 0a 00         2.1.7.8.1.....
```

Why is powershell.exe inside a desktop.ini?

```
$STANDARD_INFORMATION
Creation                      Modified                      MFT Altered                   Access Date                   Type
----------------------------- ----------------------------- ----------------------------- ----------------------------- ----

2017-12-20 19:41:21 UTC+0000 2016-07-16 13:21:38 UTC+0000   2017-12-20 19:41:21 UTC+0000   2017-12-20 19:41:21 UTC+0000   Hidden & System & Archive

$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path
----------------------------- ----------------------------- ----------------------------- ----------------------------- ----------

2017-12-20 19:41:21 UTC+0000 2016-07-16 13:21:38 UTC+0000   2017-12-20 19:34:55 UTC+0000   2017-12-20 19:41:21 UTC+0000   desktop.ini

$DATA
0000000000: 0d 0a 5b 4c 6f 63 61 6c 69 7a 65 64 46 69 6c 65   ..[LocalizedFile
0000000010: 4e 61 6d 65 73 5d 0d 0a 57 69 6e 64 6f 77 73 20   Names]..Windows.
0000000020: 50 6f 77 65 72 53 68 65 6c 6c 20 49 53 45 20 28   PowerShell.ISE.(
0000000030: 78 38 36 29 2e 6c 6e 6b 3d 40 25 53 79 73 74 65   x86).lnk=@%Syste
0000000040: 6d 52 6f 6f 74 25 5c 73 79 73 74 65 6d 33 32 5c   mRoot%\system32\
0000000050: 57 69 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c   WindowsPowerShel
0000000060: 6c 5c 76 31 2e 30 5c 70 6f 77 65 72 73 68 65 6c   l\v1.0\powershel
0000000070: 6c 2e 65 78 65 2c 2d 31 30 32 0d 0a 57 69 6e 64   l.exe,-102..Wind
0000000080: 6f 77 73 20 50 6f 77 65 72 53 68 65 6c 6c 20 49   ows.PowerShell.I
0000000090: 53 45 2e 6c 6e 6b 3d 40 25 53 79 73 74 65 6d 52   SE.lnk=@%SystemR
00000000a0: 6f 6f 74 25 5c 73 79 73 74 65 6d 33 32 5c 57 69   oot%\system32\Wi
00000000b0: 6e 64 6f 77 73 50 6f 77 65 72 53 68 65 6c 6c 5c   ndowsPowerShell\
00000000c0: 76 31 2e 30 5c 70 6f 77 65 72 73 68 65 6c 6c 2e   v1.0\powershell.
00000000d0: 65 78 65 2c 2d 31 30 31 0d 0a                     exe,-101..

*******************************************************************************
*******************************************************************************
```

More shell32.exe activity

```
$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path
----------------------------- ----------------------------- ----------------------------- ----------------------------- ---------

2017-12-20 19:41:21 UTC+0000 2016-07-16 13:18:56 UTC+0000  2017-12-20 19:34:05 UTC+0000  2017-12-20 19:41:21 UTC+0000  Run.lnk

$OBJECT_ID
Object ID: f7f59dfe-e7e8-e711-a394-000c290358b4
Birth Volume ID: 80000000-b801-0000-0000-180000000400
Birth Object ID: 99010000-1800-0000-4c00-000001140200
Birth Domain ID: 00000000-c000-0000-0000-0046c5010000

$DATA
0000000000: 4c 00 00 00 01 14 02 00 00 00 00 00 c0 00 00 00   L...............
0000000010: 00 00 00 46 c5 01 00 00 00 00 00 00 00 00 00 00    ...F............
0000000020: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0000000030: 00 00 00 00 00 00 00 00 e7 ff ff ff 01 00 00 00   ................
0000000040: 00 00 00 00 00 00 00 00 00 00 00 00 16 00 14 00   ................
0000000050: 1f 80 f3 a1 59 25 d7 21 d4 11 bd af 00 c0 4f 60   ....Y%.!......O`
0000000060: b9 f0 00 00 1c 00 40 00 25 00 77 00 69 00 6e 00   ......@.%.w.i.n.
0000000070: 64 00 69 00 72 00 25 00 5c 00 65 00 78 00 70 00   d.i.r.%.\.e.x.p.
0000000080: 6c 00 6f 00 72 00 65 00 72 00 2e 00 65 00 78 00   l.o.r.e.r...e.x.
0000000090: 65 00 2c 00 2d 00 37 00 30 00 30 00 33 00 1d 00   e.,.-.7.0.0.3...
00000000a0: 25 00 77 00 69 00 6e 00 64 00 69 00 72 00 25 00   %.w.i.n.d.i.r.%.
00000000b0: 5c 00 73 00 79 00 73 00 74 00 65 00 6d 00 33 00   \.s.y.s.t.e.m.3.
00000000c0: 32 00 5c 00 73 00 68 00 65 00 6c 00 6c 00 33 00   2.\.s.h.e.l.l.3.
00000000d0: 32 00 2e 00 64 00 6c 00 6c 00 bb 00 00 00 09 00   2...d.l.l.......
00000000e0: 00 a0 2d 00 00 00 31 53 50 53 e2 8a 58 46 bc 4c   ..-...1SPS..XF.L
00000000f0: 38 43 bb fc 13 93 26 98 6d ce 11 00 00 00 00 00   8C....&.m.......
0000000100: 00 00 00 13 00 00 00 00 00 00 00 00 00 00 00 82   ................
0000000110: 00 00 00 31 53 50 53 55 28 4c 9f 79 9f 39 4b a8    ...1SPSU(L.y.9K.
0000000120: d0 e1 d4 2d e1 d5 f3 55 00 00 00 05 00 00 00 00   ...-...U........
0000000130: 1f 00 00 00 22 00 00 00 4d 00 69 00 63 00 72 00   ....".M.i.c.r.
0000000140: 6f 00 73 00 6f 00 66 00 74 00 2e 00 57 00 69 00   o.s.o.f.t...W.i.
0000000150: 6e 00 64 00 6f 00 77 00 73 00 2e 00 53 00 68 00   n.d.o.w.s...S.h.
0000000160: 65 00 6c 00 6c 00 2e 00 52 00 75 00 6e 00 44 00   e.l.l...R.u.n.D.
0000000170: 69 00 61 00 6c 00 6f 00 67 00 00 00 11 00 00 00   i.a.l.o.g.......
0000000180: 12 00 00 00 00 13 00 00 00 01 00 00 00 00 00 00   ................
0000000190: 00 00 00 00 00 00 00 00 00 00                     ..........
```

Wireshark download:

```
$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path
----------------------------- ----------------------------- ----------------------------- ----------------------------- ---------

2017-12-26 18:09:30 UTC+0000 2017-12-26 18:09:57 UTC+0000  2017-12-26 18:09:57 UTC+0000  2017-12-26 18:09:30 UTC+0000  Users\ADMINI~1\DOWNLO~1\Wireshark-win64-2.4.3.exe

$DATA


$OBJECT_ID
Object ID: 40000000-0000-0000-0050-730300000000
Birth Volume ID: 984d7303-0000-0000-984d-730300000000
Birth Object ID: 31014707-1221-070d-7031-101d940c3120
Birth Domain ID: 1d680431-4839-f122-3141-6cc0cd314531

**************************************************************************
**************************************************************************
MFT entry found at offset 0x41fa000
Attribute: In Use & File
Record Number: 111524
Link count: 2
```

Weird dll file names

```
$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path
----------------------------- ----------------------------- ----------------------------- ----------------------------- ---------

2017-12-26 18:02:00 UTC+0000 2017-09-07 04:55:57 UTC+0000  2018-04-14 19:45:30 UTC+0000  2017-12-26 18:02:00 UTC+0000  $$DeleteMe.localspl.dll.01d3d9a6473dbe0d.0029

$DATA
```

```
$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path
----------------------------- ----------------------------- ----------------------------- ----------------------------- ---------

2016-07-16 13:19:58 UTC+0000 2016-07-16 13:19:58 UTC+0000  2017-12-20 19:35:07 UTC+0000  2016-07-16 13:19:58 UTC+0000  $$DeleteMe.MSWB7.dll.01d37ec369cda953.005c

$DATA
```

More IE Recovery .dat files

```
$STANDARD_INFORMATION
Creation                  Modified                  MFT Altered               Access Date               Type
------------------------  ------------------------  ------------------------  ------------------------  ----
2018-05-17 05:36:35 UTC+0000 2018-05-17 06:12:57 UTC+0000   2018-05-17 06:12:57 UTC+0000   2018-05-17 05:36:35 UTC+0000   Archive

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2018-05-17 05:36:35 UTC+0000 2018-05-17 05:36:35 UTC+0000   2018-05-17 05:36:35 UTC+0000   2018-05-17 05:36:35 UTC+0000   High\Active\RECOVE~1.DAT

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2018-05-17 05:36:35 UTC+0000 2018-05-17 05:36:35 UTC+0000   2018-05-17 05:36:35 UTC+0000   2018-05-17 05:36:35 UTC+0000   High\Active\RecoveryStore.{42FD8A34-5994-11E8-A39A-000C290358B4}.dat
```

Odd modification name change

```
$STANDARD_INFORMATION
Creation                  Modified                  MFT Altered               Access Date               Type
------------------------  ------------------------  ------------------------  ------------------------  ----
2017-12-20 21:06:05 UTC+0000 2017-12-20 21:06:05 UTC+0000   2017-12-20 21:06:05 UTC+0000   2017-12-20 21:06:05 UTC+0000   Archive

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2017-12-20 21:06:05 UTC+0000 2017-12-20 21:06:05 UTC+0000   2017-12-20 21:06:05 UTC+0000   2017-12-20 21:06:05 UTC+0000   Users\ADMINI~1\AppData\Local\MICROS~1\Windows\Caches\CVERSI~2.DB

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2017-12-20 21:06:05 UTC+0000 2017-12-20 21:06:05 UTC+0000   2017-12-20 21:06:05 UTC+0000   2017-12-20 21:06:05 UTC+0000   Users\ADMINI~1\AppData\Local\MICROS~1\Windows\Caches\cversions.1.db

$DATA
```

This may likely be the source for malware download:

```
$STANDARD_INFORMATION
Creation                  Modified                  MFT Altered               Access Date               Type
------------------------  ------------------------  ------------------------  ------------------------  ----
2017-12-20 19:41:23 UTC+0000 2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   Hidden & System & Reparse Point & Content not indexed

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2017-12-20 19:41:23 UTC+0000 2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   Users\ADMINI~1\AppData\Local\MICROS~1\Windows\INETCA~1\Content.IE5

**********************************************************************
**********************************************************************
MFT entry found at offset 0xacca800
Attribute: In Use & Directory
Record Number: 105102
Link count: 1
```

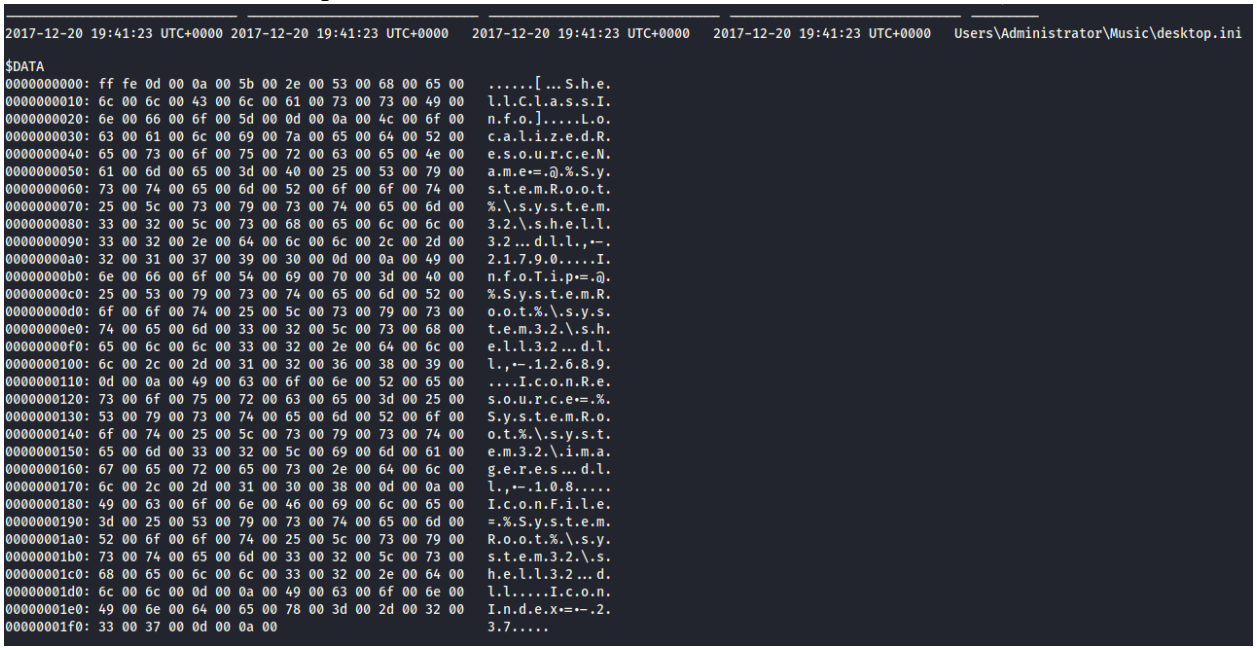
Odd Windows Media Playback modification

```
**********************************************************************
**********************************************************************
MFT entry found at offset 0xde40c00
Attribute: In Use & File
Record Number: 104755
Link count: 0


$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2018-04-14 19:29:49 UTC+0000 2018-03-22 03:08:31 UTC+0000   2018-04-14 19:44:53 UTC+0000   2018-04-14 19:29:49 UTC+0000   Windows.Media.Playback.BackgroundMediaPlayer.dll

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2018-04-14 19:29:49 UTC+0000 2018-03-22 03:08:31 UTC+0000   2018-04-14 19:45:31 UTC+0000   2018-04-14 19:29:49 UTC+0000   Windows\SysWOW64\Windows.Media.Playback.BackgroundMediaPlayer.dll
```

Odd HTML file

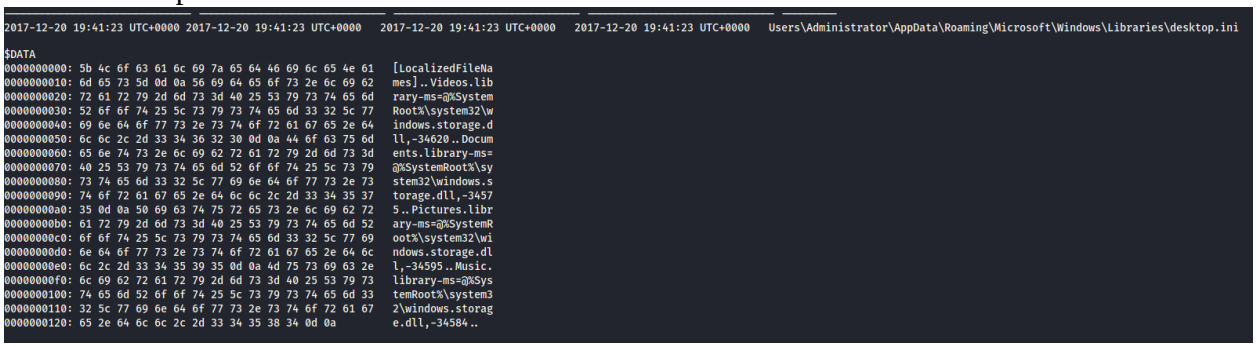
```
$STANDARD_INFORMATION
Creation                  Modified                  MFT Altered               Access Date               Type
------------------------  ------------------------  ------------------------  ------------------------  ----
2018-05-17 06:03:26 UTC+0000 2018-05-17 06:03:26 UTC+0000   2018-05-17 06:03:26 UTC+0000   2018-05-17 06:03:26 UTC+0000   Archive & Content not indexed

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2018-05-17 06:03:26 UTC+0000 2018-05-17 06:03:26 UTC+0000   2018-05-17 06:03:26 UTC+0000   2018-05-17 06:03:26 UTC+0000   PRODUC~1.HTM

$FILE_NAME
Creation                  Modified                  MFT Altered               Access Date               Name/Path
------------------------  ------------------------  ------------------------  ------------------------  ---------
2018-05-17 06:03:26 UTC+0000 2018-05-17 06:03:26 UTC+0000   2018-05-17 06:03:26 UTC+0000   2018-05-17 06:03:26 UTC+0000   product-download[1].htm

$DATA
```

Desktop.ini in Music folder? Was also found in Documents, Searches, Downloads. Favorites, Public/Desktop folder



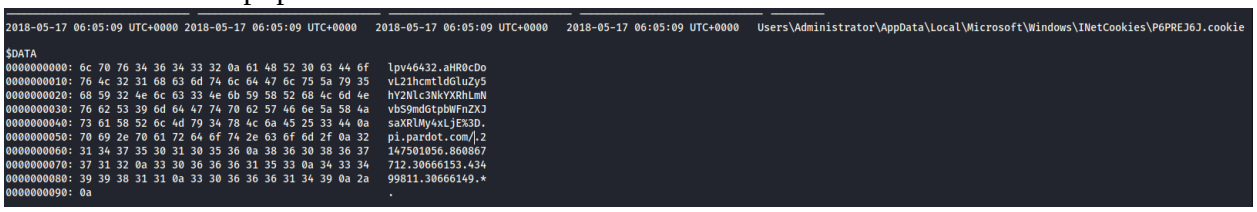
```
2017-12-20 19:41:23 UTC+0000 2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   Users\Administrator\Music\desktop.ini

$DATA
0000000000: ff fe 0d 00 0a 00 5b 00 2e 00 53 00 68 00 65 00   ......[ … S.h.e.
0000000010: 6c 00 6c 00 43 00 6c 00 61 00 73 00 73 00 49 00   l.l.C.l.a.s.s.I.
0000000020: 6e 00 66 00 6f 00 5d 00 0d 00 0a 00 4c 00 6f 00   n.f.o.].....L.o.
0000000030: 63 00 61 00 6c 00 69 00 7a 00 65 00 64 00 52 00   c.a.l.i.z.e.d.R.
0000000040: 65 00 73 00 6f 00 75 00 72 00 63 00 65 00 4e 00   e.s.o.u.r.c.e.N.
0000000050: 61 00 6d 00 65 00 3d 00 40 00 25 00 53 00 79 00   a.m.e•=.@.%.S.y.
0000000060: 73 00 74 00 65 00 6d 00 52 00 6f 00 6f 00 74 00   s.t.e.m.R.o.o.t.
0000000070: 25 00 5c 00 73 00 79 00 73 00 74 00 65 00 6d 00   %.\.s.y.s.t.e.m.
0000000080: 33 00 32 00 5c 00 73 00 68 00 65 00 6c 00 6c 00   3.2.\.s.h.e.l.l.
0000000090: 33 00 32 00 2e 00 64 00 6c 00 6c 00 2c 00 2d 00   3.2 … d.l.l.,•–.
00000000a0: 32 00 31 00 37 00 39 00 30 00 0d 00 0a 00 49 00   2.1.7.9.0.....I.
00000000b0: 6e 00 66 00 6f 00 54 00 69 00 70 00 3d 00 40 00   n.f.o.T.i.p•=.@.
00000000c0: 25 00 53 00 79 00 73 00 74 00 65 00 6d 00 52 00   %.S.y.s.t.e.m.R.
00000000d0: 6f 00 6f 00 74 00 25 00 5c 00 73 00 79 00 73 00   o.o.t.%.\.s.y.s.
00000000e0: 74 00 65 00 6d 00 33 00 32 00 5c 00 73 00 68 00   t.e.m.3.2.\.s.h.
00000000f0: 65 00 6c 00 6c 00 33 00 32 00 2e 00 64 00 6c 00   e.l.l.3.2 … d.l.
0000000100: 6c 00 2c 00 2d 00 31 00 32 00 36 00 38 00 39 00   l.,•–.1.2.6.8.9.
0000000110: 0d 00 0a 00 49 00 63 00 6f 00 6e 00 52 00 65 00   ....I.c.o.n.R.e.
0000000120: 73 00 6f 00 75 00 72 00 63 00 65 00 3d 00 25 00   s.o.u.r.c.e•=.%.
0000000130: 53 00 79 00 73 00 74 00 65 00 6d 00 52 00 6f 00   S.y.s.t.e.m.R.o.
0000000140: 6f 00 74 00 25 00 5c 00 73 00 79 00 73 00 74 00   o.t.%.\.s.y.s.t.
0000000150: 65 00 6d 00 33 00 32 00 5c 00 69 00 6d 00 61 00   e.m.3.2.\.i.m.a.
0000000160: 67 00 65 00 72 00 65 00 73 00 2e 00 64 00 6c 00   g.e.r.e.s … d.l.
0000000170: 6c 00 2c 00 2d 00 31 00 30 00 38 00 0d 00 0a 00   l.,•–.1.0.8.....
0000000180: 49 00 63 00 6f 00 6e 00 46 00 69 00 6c 00 65 00   I.c.o.n.F.i.l.e.
0000000190: 3d 00 25 00 53 00 79 00 73 00 74 00 65 00 6d 00   =.%.S.y.s.t.e.m.
00000001a0: 52 00 6f 00 6f 00 74 00 25 00 5c 00 73 00 79 00   R.o.o.t.%.\.s.y.
00000001b0: 73 00 74 00 65 00 6d 00 33 00 32 00 5c 00 73 00   s.t.e.m.3.2.\.s.
00000001c0: 68 00 65 00 6c 00 6c 00 33 00 32 00 2e 00 64 00   h.e.l.l.3.2 … d.
00000001d0: 6c 00 6c 00 0d 00 0a 00 49 00 63 00 6f 00 6e 00   l.l.....I.c.o.n.
00000001e0: 49 00 6e 00 64 00 65 00 78 00 3d 00 2d 00 32 00   I.n.d.e.x•=•–.2.
00000001f0: 33 00 37 00 0d 00 0a 00                           3.7.....
```

Weird desktop.ini



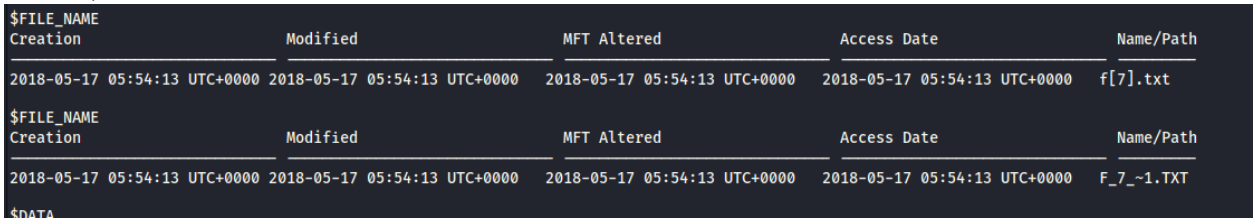
```
2017-12-20 19:41:23 UTC+0000 2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   2017-12-20 19:41:23 UTC+0000   Users\Administrator\AppData\Roaming\Microsoft\Windows\Libraries\desktop.ini

$DATA
0000000000: 5b 4c 6f 63 61 6c 69 7a 65 64 46 69 6c 65 4e 61   [LocalizedFileNa
0000000010: 6d 65 73 5d 0d 0a 56 69 64 65 6f 73 2e 6c 69 62   mes]..Videos.lib
0000000020: 72 61 72 79 2d 6d 73 3d 40 25 53 79 73 74 65 6d   rary-ms=@%System
0000000030: 52 6f 6f 74 25 5c 73 79 73 74 65 6d 33 32 5c 77   Root%\system32\w
0000000040: 69 6e 64 6f 77 73 2e 73 74 6f 72 61 67 65 2e 64   indows.storage.d
0000000050: 6c 6c 2c 2d 33 34 36 32 30 0d 0a 44 6f 63 75 6d   ll,-34620..Docum
0000000060: 65 6e 74 73 2e 6c 69 62 72 61 72 79 2d 6d 73 3d   ents.library-ms=
0000000070: 40 25 53 79 73 74 65 6d 52 6f 6f 74 25 5c 73 79   @%SystemRoot%\sy
0000000080: 73 74 65 6d 33 32 5c 77 69 6e 64 6f 77 73 2e 73   stem32\windows.s
0000000090: 74 6f 72 61 67 65 2e 64 6c 6c 2c 2d 33 34 35 37   torage.dll,-3457
00000000a0: 35 0d 0a 50 69 63 74 75 72 65 73 2e 6c 69 62 72   5..Pictures.libr
00000000b0: 61 72 79 2d 6d 73 3d 40 25 53 79 73 74 65 6d 52   ary-ms=@%SystemR
00000000c0: 6f 6f 74 25 5c 73 79 73 74 65 6d 33 32 5c 77 69   oot%\system32\wi
00000000d0: 6e 64 6f 77 73 2e 73 74 6f 72 61 67 65 2e 64 6c   ndows.storage.dl
00000000e0: 6c 2c 2d 33 34 35 39 35 0d 0a 4d 75 73 69 63 2e   l,-34595..Music.
00000000f0: 6c 69 62 72 61 72 79 2d 6d 73 3d 40 25 53 79 73   library-ms=@%Sys
0000000100: 74 65 6d 52 6f 6f 74 25 5c 73 79 73 74 65 6d 33   temRoot%\system3
0000000110: 32 5c 77 69 6e 64 6f 77 73 2e 73 74 6f 72 61 67   2\windows.storag
0000000120: 65 2e 64 6c 6c 2c 2d 33 34 35 38 34 0d 0a         e.dll,-34584..
```

weird cookie with pi.pardot.com in file



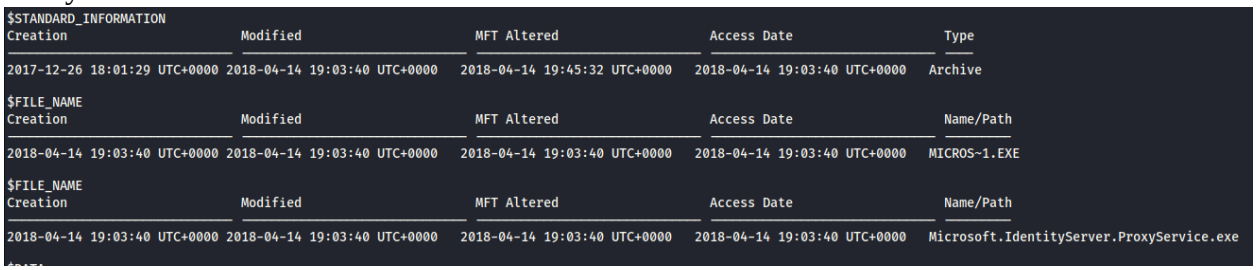
```
2018-05-17 06:05:09 UTC+0000 2018-05-17 06:05:09 UTC+0000   2018-05-17 06:05:09 UTC+0000   2018-05-17 06:05:09 UTC+0000   Users\Administrator\AppData\Local\Microsoft\Windows\INetCookies\P6PREJ6J.cookie

$DATA
0000000000: 6c 70 76 34 36 34 33 32 0a 61 48 52 30 63 44 6f   lpv46432.aHR0cDo
0000000010: 76 4c 32 31 68 63 6d 74 6c 64 47 6c 75 5a 79 35   vL21hcmtldGluZy5
0000000020: 68 59 32 4e 6c 63 33 4e 6b 59 58 52 68 4c 6d 4e   hY2Nlc3NkYXRhLmN
0000000030: 76 62 53 39 6d 64 47 74 70 62 57 46 6e 5a 58 4a   vbS9mdGtpbWFnZXJ
0000000040: 73 61 58 52 5a 4d 79 34 78 4c 6a 45 25 33 44 0a   saXRlMy4xLjE%3D.
0000000050: 70 69 2e 70 61 72 64 6f 74 2e 63 6f 6d 2f 0a 32   pi.pardot.com/.2
0000000060: 31 34 37 35 30 31 30 35 36 0a 38 36 30 38 36 37   147501056.860867
0000000070: 37 31 32 0a 33 30 36 36 36 31 35 33 0a 34 33 34   712.30666153.434
0000000080: 39 39 38 31 31 0a 33 30 36 36 36 31 34 39 0a 2a   99811.30666149.*
0000000090: 0a                                                .
```

f.txt means that the browser protected the user from a malicious exploit (https://stackoverflow.com/questions/28535603/google-chrome-forcing-download-of-f-txt-file)



```
$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path

2018-05-17 05:54:13 UTC+0000 2018-05-17 05:54:13 UTC+0000   2018-05-17 05:54:13 UTC+0000   2018-05-17 05:54:13 UTC+0000   f[7].txt

$FILE_NAME
Creation                      Modified                      MFT Altered                   Access Date                   Name/Path

2018-05-17 05:54:13 UTC+0000 2018-05-17 05:54:13 UTC+0000   2018-05-17 05:54:13 UTC+0000   2018-05-17 05:54:13 UTC+0000   F_7_~1.TXT

$DATA
```

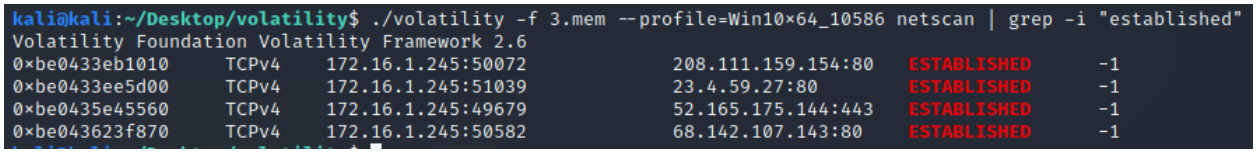
Proxy Service modified



```
$STANDARD_INFORMATION
Creation                 Modified                 MFT Altered              Access Date              Type
-----------------------  -----------------------  -----------------------  -----------------------  -------
2017-12-26 18:01:29 UTC+0000 2018-04-14 19:03:40 UTC+0000   2018-04-14 19:45:32 UTC+0000   2018-04-14 19:03:40 UTC+0000   Archive

$FILE_NAME
Creation                 Modified                 MFT Altered              Access Date              Name/Path
-----------------------  -----------------------  -----------------------  -----------------------  ----------
2018-04-14 19:03:40 UTC+0000 2018-04-14 19:03:40 UTC+0000   2018-04-14 19:03:40 UTC+0000   2018-04-14 19:03:40 UTC+0000   MICROS~1.EXE

$FILE_NAME
Creation                 Modified                 MFT Altered              Access Date              Name/Path
-----------------------  -----------------------  -----------------------  -----------------------  ----------
2018-04-14 19:03:40 UTC+0000 2018-04-14 19:03:40 UTC+0000   2018-04-14 19:03:40 UTC+0000   2018-04-14 19:03:40 UTC+0000   Microsoft.IdentityServer.ProxyService.exe
```

All this Master File Table activity suggests something malicious is going on behind the scenes, likely “fileless” malware.

1.9. Connections, connscan, sockets were unavailable to use as the image was not supported. Instead I used netscan and queried on the established connections. No suspicious connections were viewed.

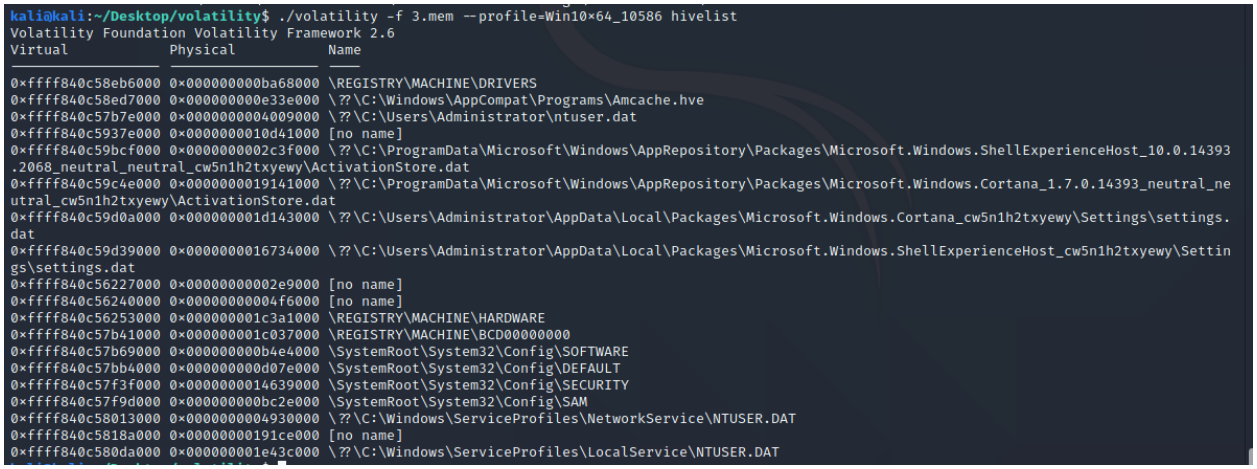


```
kali@kali:~/Desktop/volatility$ ./volatility -f 3.mem --profile=Win10x64_10586 netscan | grep -i "established"
Volatility Foundation Volatility Framework 2.6
0xbe0433eb1010     TCPv4    172.16.1.245:50072             208.111.159.154:80   ESTABLISHED      -1
0xbe0433ee5d00     TCPv4    172.16.1.245:51039             23.4.59.27:80        ESTABLISHED      -1
0xbe0435e45560     TCPv4    172.16.1.245:49679             52.165.175.144:443   ESTABLISHED      -1
0xbe043623f870     TCPv4    172.16.1.245:50582             68.142.107.143:80    ESTABLISHED      -1
```

I used a yarascan with custom rule “http” and found some suspicious UPNP activity

```
Owner: Process svchost.exe Pid 2716
0x7fff7a3618bb  68 74 74 70 3a 2f 2f 25 73 2f 75 70 6e 70 2f 65   http://%s/upnp/e
0x7fff7a3618cb  76 65 6e 74 69 6e 67 2f 25 73 3e 0d 0a 54 69 6d   venting/%s>..Tim
0x7fff7a3618db  65 6f 75 74 3a 20 53 65 63 6f 6e 64 2d 25 64 0d   eout:.Second-%d.
0x7fff7a3618eb  0a 0d 0a 00 00 53 49 44 3a 20 25 73 0d 0a 00 00   .....SID:.%s....
0x7fff7a3618fb  00 00 00 00 00 53 49 44 3a 20 25 73 0d 0a 54 69   .....SID:.%s..Ti
0x7fff7a36190b  6d 65 6f 75 74 3a 20 53 65 63 6f 6e 64 2d 25 64   meout:.Second-%d
0x7fff7a36191b  0d 0a 00 00 00 75 75 69 64 3a 00 00 00 75 70 6e   .....uuid:...upn
0x7fff7a36192b  70 3a 72 6f 6f 74 64 65 76 69 63 65 00 75 72 6e   p:rootdevice.urn
0x7fff7a36193b  3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f 72   :schemas-upnp-or
0x7fff7a36194b  67 3a 73 65 72 76 69 63 65 3a 00 00 00 75 72 6e   g:service:...urn
0x7fff7a36195b  3a 73 63 68 65 6d 61 73 2d 75 70 6e 70 2d 6f 72   :schemas-upnp-or
0x7fff7a36196b  67 3a 64 65 76 69 63 65 3a 00 00 00 00 64 e0 47   g:device:....d.G
0x7fff7a36197b  bc f5 6d 43 32 ac 32 3b 5f 4f fe b8 92 51 00 00   ..mC2.2;_O...Q..
0x7fff7a36198b  00 00 00 00 00 f0 1b aa 79 1f 40 ed 3a f0 0a 1c   ........y.@.:...
0x7fff7a36199b  c2 e2 95 65 8d 68 74 74 70 3a 2f 2f 00 75 6e 6b   ...e.http://.unk
0x7fff7a3619ab  6e 6f 77 6e 00 4d 2d 50 4f 53 54 00 00 cc 20 ce   nown.M-POST.....
Rule: r1
Owner: Process svchost.exe Pid 2716
0x7fff7a3619a0  68 74 74 70 3a 2f 2f 00 75 6e 6b 6e 6f 77 6e 00   http://.unknown.
0x7fff7a3619b0  4d 2d 50 4f 53 54 00 00 cc 20 ce 8f ad 1a 11 38   M-POST.........8
0x7fff7a3619c0  3e 8d d8 17 2f ed 69 f3 01 00 00 00 00 00 00 00   >.../.i.........
0x7fff7a3619d0  68 00 74 00 74 00 70 00 3a 00 2f 00 2f 00 2a 00   h.t.t.p.:././.*.
0x7fff7a3619e0  3a 00 25 00 64 00 25 00 53 00 00 00 00 00 00 00   :.%.d.%.S.......
0x7fff7a3619f0  0d 32 4e 8d 70 0c c0 3e 8d 2a 0f b3 c3 ed b3 1b   .2N.p..>.*......
0x7fff7a361a00  68 00 74 00 74 00 70 00 61 00 70 00 69 00 2e 00   h.t.t.p.a.p.i...
0x7fff7a361a10  64 00 6c 00 6c 00 00 00 48 74 74 70 49 6e 69 74   d.l.l...HttpInit
0x7fff7a361a20  69 61 6c 69 7a 65 00 00 48 74 74 70 43 72 65 61   ialize..HttpCrea
0x7fff7a361a30  74 65 48 74 74 70 48 61 6e 64 6c 65 00 00 00 00   teHttpHandle....
0x7fff7a361a40  48 74 74 70 41 64 64 55 72 6c 00 00 00 00 00 00   HttpAddUrl......
0x7fff7a361a50  48 74 74 70 54 65 72 6d 69 6e 61 74 65 00 00 00   HttpTerminate...
0x7fff7a361a60  48 74 74 70 52 65 6d 6f 76 65 55 72 6c 00 00 00   HttpRemoveUrl...
0x7fff7a361a70  48 74 74 70 52 65 63 65 69 76 65 52 65 71 75 65   HttpReceiveReque
0x7fff7a361a80  73 74 45 6e 74 69 74 79 42 6f 64 79 00 00 00 00   stEntityBody....
0x7fff7a361a90  48 74 74 70 53 65 6e 64 48 74 74 70 52 65 73 70   HttpSendHttpResp
Rule: r1
```

1.10.



Was unable to find any suspicious registry keys after doing 20 or so queries.

2. No suspicious or malicious PID were viewed. This is likely a file-less malware. I was unable to dump a lot of suspicious files labelled above, likely due to the fact that they were wiped. Many processes (svshost) weren't able to be dumped due to paging errors.
3. No virustotal results due to above.
4. I believe this malware is a part of the ShadowThreat APT as explained here: https://medium.com/@rmrf.tech/new-cyberthreat-replaces-operating-system-with-a-fake-part-1-96ba253fafc3. This was discovered after looking into the Mutants in Mutantscan, and after a couple days of analyzing this incredibly advanced malware and memory dump I believe this is the malware family.

   The first clue is in the second phase of ShadowThreat where they mention UPnP, which I discovered in a yarascan.

   The third phase explains Windows Defender being injected with code, which we noticed in the "privs" command where MsMgEng.exe had a lot of manually added privileges. This article and the one below goes on to explain the added privilege of uploading drivers, malicious code injection, stopping telemetry sending and updating signatures for Windows Defender.

   They also mentioned uploading obfuscated code via Powershell and executing in RAM for file-less malware, which we got a hint of in the suspicious desktop.ini's planted around the machine's folder.

   The article also mentions escalating privilege using ms-update. A lot of amd64_microsoft files were noticed in the filescan, so that may be another clue.

   An odd .dll (comctl32.dll) appeared in a amd64 windows update file, which is discussed about being downloaded in the article below.

In this following article (https://medium.com/@rmrf.tech/revealing-some-details-about-shadowthreat-initial-intrusion-3269eaa1c935), it discusses using spear phishing techniques and downloading compressed data to a specific location *(C:\Users\user\AppData\Local\Microsoft\Windows\Temporary Internet Files\Content.IE5)*. This location was discovered in the mftparser analysis.

Continuing with the mftparser analysis, Automatic Crash Recovery files were created just like the article explained *(C:\Users\user\AppData\Local\Microsoft\InternetExplorer\Recovery\High\Active\RecoveryStore.{<GUID>}.dat)*.
It also notes that the desktop.ini files were read, which I discovered a lot of anomalous desktop.ini activity in mftparser.

Seven Temp files were created and discovered in filescan with identical format as the article. *(C:\Users\user\AppData\Local\Temp\~<name>.TMP)*

With the UPnP activity previously mentioned, the APT delivers updates for UPnP components, one of them being Windows Media Player. This was noticed in the mftparser activity where a WMP .DLL file was modified. Many other anomalies mentioned were noticed in my lengthy analysis.

In conclusion, this is incredibly advanced malware. I believe this is anti-forensics and file-less malware. After analysis on the memory dump and reading articles on it, the malware appears to replace the operating system completing by disabling Windows security/Defender features and applying fake updates. They get complete full access to the host to gather information, use as a bot, apply ransomware, or possibly control/destroy SCADA systems.

4.vmem

1.

1.1. Image appears to be WinXPS2x86

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/volatility/4.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 17:43:45 UTC+0000
     Image local date and time : 2010-08-15 13:43:45 -0400
```

1.2. Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/Edb5qgSEDydKoPMuWMXLlTcBnuFJr-spDAzS4IqtO2Jgzg?e=YYDne1

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem handles -t File > 4_files.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EdSbaNsyYSpLnG5IegGjKysBDM7vojB1ULhfM0FELTQo7w?e=LQWEZ3

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem filescan > 4_filescan.txt
Volatility Foundation Volatility Framework 2.6
```

1.3. Same hashes as 1.vmem

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:4e857c004024e53cd538de64dedac36b:842b4013c45a3b8fec76ca54e5910581:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8f57385a61425fc7874c3268aa249ea1:::
```

Same RDP encryption key and activity with lsadump

```
0083343a-f925-4ed7-b1d6-d95d17a0b57b-RemoteDesktopHelpAssistantSID
0x00000000  01 05 00 00 00 00 00 05 15 00 00 00 8a 5a 41 60   .............ZA`
0x00000010  35 8a 02 1a 43 17 0a 32 e8 03 00 00              5...C..2....

kali@kali:~/Desktop/volatility$
```

1.4. None found with findaes and aeskeyfinder

```
kali@kali:~/Desktop/volatility$ ./findaes 4.vmem
Searching 4.vmem
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EWvEokNicn9Onh5RBlhVnrIBLYJlcQdqhS870emk5VJTmA?e=5xxcq8

```
kali@kali:~/Desktop/volatility$ ./rsakeyfind 4.vmem > 4_rsakeys.txt
```

1.5.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem filescan | grep cfg
Volatility Foundation Volatility Framework 2.6
0x0000000004868d48      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\netcfgx.dll
0x0000000004a963b8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\hnetcfg.dll
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem filescan | grep conf
Volatility Foundation Volatility Framework 2.6
0x00000000003f3f08      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\ipconf.tsp
0x000000000106be80      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY.LOG
0x00000000010d5f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x000000000112cb18      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM.LOG
0x0000000001160218      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x0000000001160430      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x0000000001187620      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default.LOG
0x000000000438b100      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software
0x00000000043d6e60      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0x000000000486b028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default
0x0000000004a96c08      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0x0000000005c5ceb8      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x0000000005ce64b0      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x0000000005ce7a90      1      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x0000000006629028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software.LOG
0x0000000006779028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system.LOG
0x000000000687f028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system
kali@kali:~/Desktop/volatility$
```

1.6. Nothing in particular pops out in the processes, other than aelas.exe. I've never seen that process before.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                      4      0     58    190 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                            632    544     19    513 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                              688    632     21    349 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                           676    632     16    269 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                         1668    676      5    221 2010-08-11 06:06:35 UTC+0000
..... 0x80f167b8:cmd.exe                             1368   1668      0 ------ 2010-08-15 17:43:45 UTC+0000
.... 0x80ff88d8:svchost.exe                           856    676     18    203 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                          1432    676     13    135 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                          1028    676     88   1426 2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0:wuauclt.exe                         1732   1028      7    178 2010-08-11 06:07:44 UTC+0000
..... 0x80f94588:wuauclt.exe                          468   1028      7    139 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                          888   1028      4     32 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                           936    676     11    268 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                      1968    676      5    100 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                     1084   1968      4     66 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                          1088    676      6     80 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                          844    676      1     24 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                               216    676      7    108 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                          1148    676     15    212 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                      1788    676      5    102 2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                               608    544     11    434 2010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                             1724   1708     18    414 2010-08-11 06:09:29 UTC+0000
. 0xff22f3d0:aelas.exe                               1984   1724     19    139 2010-08-15 17:43:26 UTC+0000
. 0xff374980:VMwareUser.exe                           452   1724     11    208 2010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe                           432   1724      4     53 2010-08-11 06:09:31 UTC+0000
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x06499b80 svchost.exe            1148 True   True   True     True   True  True    True
0x04b5a980 VMwareUser.exe          452 True   True   True     True   True  True    True
0x010f7588 wuauclt.exe             468 True   True   True     True   True  True    True
0x04c2b310 wscntfy.exe             888 True   True   True     True   True  True    True
0x061ef558 svchost.exe            1088 True   True   True     True   True  True    True
0x04a065d0 explorer.exe           1724 True   True   True     True   True  True    True
0x06945da0 spoolsv.exe            1432 True   True   True     True   True  True    True
0x06015020 services.exe            676 True   True   True     True   True  True    True
0x069d5b28 vmtoolsd.exe           1668 True   True   True     True   True  True    True
0x06384230 vmacthlp.exe            844 True   True   True     True   True  True    True
0x0655fc88 VMUpgradeHelper        1788 True   True   True     True   True  True    True
0x010c3da0 wuauclt.exe            1732 True   True   True     True   True  True    True
0x05f027e0 alg.exe                 216 True   True   True     True   True  True    True
0x05f47020 lsass.exe               688 True   True   True     True   True  True    True
0x061ad3d0 aelas.exe              1984 True   True   True     True   True  True    True
0x066f0978 winlogon.exe            632 True   True   True     True   True  True    True
0x0115b8d8 svchost.exe             856 True   True   True     True   True  True    True
0x063c5560 svchost.exe             936 True   True   True     True   True  True    True
0x01122910 svchost.exe            1028 True   True   True     True   True  True    True
0x04be97e8 VMwareTray.exe          432 True   True   True     True   True  True    True
0x0211ab28 TPAutoConnSvc.e        1968 True   True   True     True   True  True    True
0x049c15f8 TPAutoConnect.e        1084 True   True   True     True   True  True    True
0x05471020 smss.exe                544 True   True   True     True   False False   False
0x066f0da0 csrss.exe               608 True   True   True     True   False True    True
0x010797b8 cmd.exe                1368 True   True   False    True   False False   False    2010-08-15 17:43:45 UTC+0000
0x01214660 System                    4 True   True   True     True   False False   False
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EdoVGPSjqupKv13A57DZEW0BvYlAvGQt20NzrLvLqbSTTA?e=jp6ge3

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem dlllist
```

Noticed the same odd executable in the handles Process search: aelas.exe

```
0xff203b80    688      0x480      0x478 Process          svchost.exe(1148)
0x80fbf910    688      0x4c8      0x478 Process          svchost.exe(1028)
0x80fbf910    688      0x520      0x478 Process          svchost.exe(1028)
0xff143b28    688      0x524      0x478 Process          TPAutoConnSvc.e(1968)
0xff22f3d0    688      0x534      0x478 Process          aelas.exe(1984)
0xff1b8b28    688      0x568      0x478 Process          vmtoolsd.exe(1668)
0x80fbf910    688      0x580      0x478 Process          svchost.exe(1028)
0xff217560    856      0x14c   0x1f0fff Process          svchost.exe(936)
0xff1ecda0    856      0x298   0x1f0fff Process          csrss.exe(608)
0xff1ec978    856      0x29c   0x1f0fff Process          winlogon.exe(632)
0xff1ec978   1028      0x120      0x478 Process          winlogon.exe(632)
0xff1ec978   1028      0x128      0x478 Process          winlogon.exe(632)
0xff1ec978   1028      0x12c   0x100000 Process          winlogon.exe(632)
0xff1ec978   1028      0x15c      0x47a Process          winlogon.exe(632)
0xff22f3d0   1028      0x344      0x478 Process          aelas.exe(1984)
0x80fbf910   1028      0x360   0x1f0fff Process          svchost.exe(1028)
0xff374980   1028      0x784      0x478 Process          VMwareUser.exe(452)
0xff1b8b28   1028      0x8f8      0x478 Process          vmtoolsd.exe(1668)
0xff3667e8   1028      0xa10      0x478 Process          VMwareTray.exe(432)
0xff38b5f8   1028      0xd04      0x478 Process          TPAutoConnect.e(1084)
0x80fbf910   1028      0xd10       0x68 Process          svchost.exe(1028)
0xff3865d0   1028      0xf80      0x478 Process          explorer.exe(1724)
0xff255020   1028     0x11b8   0x100000 Process          lsass.exe(688)
```

After doing a getsids search, I discovered it has quite elevated privileges:

```
aelas.exe (1984): S-1-5-21-1614895754-436374069-839522115-500 (Administrator)
aelas.exe (1984): S-1-5-21-1614895754-436374069-839522115-513 (Domain Users)
aelas.exe (1984): S-1-1-0 (Everyone)
aelas.exe (1984): S-1-5-32-544 (Administrators)
aelas.exe (1984): S-1-5-32-545 (Users)
aelas.exe (1984): S-1-5-4 (Interactive)
aelas.exe (1984): S-1-5-11 (Authenticated Users)
aelas.exe (1984): S-1-5-5-0-59917 (Logon Session)
aelas.exe (1984): S-1-2-0 (Local (Users with the ability to log in locally))
cmd.exe (1368): S-1-5-18 (Local System)
cmd.exe (1368): S-1-5-32-544 (Administrators)
cmd.exe (1368): S-1-1-0 (Everyone)
cmd.exe (1368): S-1-5-11 (Authenticated Users)
```

Notice odd aelas.exe and wuauclt.exe activity in privs:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem privs --silent
Volatility Foundation Volatility Framework 2.6
Pid      Process          Value  Privilege                       Attributes          Description
-------- ---------------- -----  ------------------------------- ------------------- -----------
     632 winlogon.exe         8  SeSecurityPrivilege             Present,Enabled     Manage auditing and security log
     632 winlogon.exe        10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
     632 winlogon.exe        25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
     688 lsass.exe            2  SeCreateTokenPrivilege          Present,Enabled     Create a token object
     688 lsass.exe           10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
     688 lsass.exe           25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
    1028 svchost.exe          2  SeCreateTokenPrivilege          Present,Enabled     Create a token object
    1028 svchost.exe          9  SeTakeOwnershipPrivilege        Present,Enabled     Take ownership of files/objects
    1028 svchost.exe          3  SeAssignPrimaryTokenPrivilege   Present,Enabled     Replace a process-level token
    1028 svchost.exe          5  SeIncreaseQuotaPrivilege        Present,Enabled     Increase quotas
    1028 svchost.exe          8  SeSecurityPrivilege             Present,Enabled     Manage auditing and security log
    1028 svchost.exe         22  SeSystemEnvironmentPrivilege    Present,Enabled     Edit firmware environment values
    1028 svchost.exe         17  SeBackupPrivilege               Present,Enabled     Backup files and directories
    1028 svchost.exe         18  SeRestorePrivilege              Present,Enabled     Restore files and directories
    1028 svchost.exe         19  SeShutdownPrivilege             Present,Enabled     Shut down the system
    1028 svchost.exe         10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
    1028 svchost.exe         12  SeSystemtimePrivilege           Present,Enabled     Change the system time
    1028 svchost.exe         25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
    1028 svchost.exe         28  SeManageVolumePrivilege         Present,Enabled     Manage the files on a volume
    1432 spoolsv.exe         10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
    1432 spoolsv.exe         25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
    1788 VMUpgradeHelper     10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
    1788 VMUpgradeHelper     25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
    1732 wuauclt.exe          2  SeCreateTokenPrivilege          Present,Enabled     Create a token object
    1732 wuauclt.exe          9  SeTakeOwnershipPrivilege        Present,Enabled     Take ownership of files/objects
    1732 wuauclt.exe          3  SeAssignPrimaryTokenPrivilege   Present,Enabled     Replace a process-level token
    1732 wuauclt.exe          5  SeIncreaseQuotaPrivilege        Present,Enabled     Increase quotas
    1732 wuauclt.exe          8  SeSecurityPrivilege             Present,Enabled     Manage auditing and security log
    1732 wuauclt.exe         22  SeSystemEnvironmentPrivilege    Present,Enabled     Edit firmware environment values
    1732 wuauclt.exe         17  SeBackupPrivilege               Present,Enabled     Backup files and directories
    1732 wuauclt.exe         18  SeRestorePrivilege              Present,Enabled     Restore files and directories
    1732 wuauclt.exe         19  SeShutdownPrivilege             Present,Enabled     Shut down the system
    1732 wuauclt.exe         10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
    1732 wuauclt.exe         12  SeSystemtimePrivilege           Present,Enabled     Change the system time
    1732 wuauclt.exe         25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
    1732 wuauclt.exe         28  SeManageVolumePrivilege         Present,Enabled     Manage the files on a volume
    1724 explorer.exe        10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
    1724 explorer.exe        25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
     432 VMwareTray.exe      10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
     432 VMwareTray.exe      25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
     452 VMwareUser.exe      10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
     452 VMwareUser.exe      25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
    1984 aelas.exe           10  SeLoadDriverPrivilege           Present,Enabled     Load and unload device drivers
    1984 aelas.exe           25  SeUndockPrivilege               Present,Enabled     Remove computer from docking station
```

1.7.

Nothing was observed with apihooks

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EdIFnH9swnpPlRPXpqfKWYkBdopf5v7o73fftqSQBhqKlw?e=ziCmY1

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem malfind > 4_malfind.txt
Volatility Foundation Volatility Framework 2.6
```

Upon first look, explorer.exe, wuauclt.exe and aelas.exe may have code injected into them

```
Process: wscntfy.exe Pid: 888 Address: 0x900000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00900000  e8 00 00 00 00 5d 81 ed 05 10 40 00 8d 85 2f 10   .....]....@.../.
0x00900010  40 00 50 6a 00 6a 00 ff 95 27 10 40 00 6a ff ff   @.Pj.j...'.@.j..
0x00900020  95 2b 10 40 00 eb f6 3f eb 80 7c 42 24 80 7c 77   .+.@...?..|B$.|w
0x00900030  73 63 6e 74 66 79 2e 65 78 65 4d 5f 38 38 38 5f   scntfy.exeM_888_


Process: wuauclt.exe Pid: 468 Address: 0x12e0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x012e0000  e8 00 00 00 00 5d 81 ed 05 10 40 00 8d 85 2f 10   .....]....@.../.
0x012e0010  40 00 50 6a 00 6a 00 ff 95 27 10 40 00 6a ff ff   @.Pj.j...'.@.j..
0x012e0020  95 2b 10 40 00 eb f6 3f eb 80 7c 42 24 80 7c 77   .+.@...?..|B$.|w
0x012e0030  75 61 75 63 6c 74 2e 65 78 65 4d 5f 34 36 38 5f   uauclt.exeM_468_


Process: aelas.exe Pid: 1984 Address: 0x1aa0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01aa0000  e8 00 00 00 00 5d 81 ed 05 10 40 00 8d 85 2f 10   .....]....@.../.
0x01aa0010  40 00 50 6a 00 6a 00 ff 95 27 10 40 00 6a ff ff   @.Pj.j...'.@.j..
0x01aa0020  95 2b 10 40 00 eb f6 3f eb 80 7c 42 24 80 7c 61   .+.@...?..|B$.|a
0x01aa0030  65 6c 61 73 2e 65 78 65 4d 5f 31 39 38 34 5f 00   elas.exeM_1984_.
```

1.8.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/ERR4ejTefLVDvcJwK3-a7ngBCer0ndXYu17k4EFcVYUaRw?e=b2Tgbh

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem modules > 4_modules.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/Edb5qgSEDydKoPMuWMXLlTcBnuFJr-spDAzS4IqtO2Jgzg?e=aWQ9yQ

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem driverscan > 4_drivers.txt
Volatility Foundation Volatility Framework 2.6
```

Odd Temp file, which are on all XP machines

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem filescan | grep Temp
Volatility Foundation Volatility Framework 2.6
0x00000000010671a8      1      0 R--rwd \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
0x00000000010692e0      2      1 RWDrw- \Device\HarddiskVolume1\WINDOWS\Temp\Perflib_Perfdata_684.dat
0x00000000010bf260      1      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
0x0000000001118748      1      0 R--rwd \Device\HarddiskVolume1\DOCUME~1\ADMINI~1\LOCALS~1\Temp\unattend.cmd
0x0000000001169640      1      0 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
0x00000000048b1ad0      1      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\index.dat
0x0000000006b40200      1      1 RW-rw- \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Temporary Internet Files\Content.IE5\index.dat
```

Mutantscan had some suspicious Mutant objects:

```
0x0ff3ac548    468        0x70    0x1f0001 Mutant
0x0ff20eeb0    468        0xfc    0x1f0001 Mutant           WindowsUpdateTracingMutex
0x0ff1e5528    468       0x21c    0x1f0001 Mutant           wuauclt.exeM_468_
0x0ff1583c0   1984        0x3c    0x1f0001 Mutant           uxJLpe1m
0x080f783d8   1984        0x88    0x1f0001 Mutant
0x080fb48e8   1984        0x94    0x1f0001 Mutant
0x0ff141900   1984        0x9c    0x1f0001 Mutant
0x0ff396c10   1984       0x114    0x1f0001 Mutant           smss.exeM_544_
0x0ff245518   1984       0x118    0x1f0001 Mutant           csrss.exeM_608_
0x080f97220   1984       0x11c    0x1f0001 Mutant           winlogon.exeM_632_
0x0ff20a0d0   1984       0x120    0x1f0001 Mutant           services.exeM_676_
0x0ff1e7dc0   1984       0x124    0x1f0001 Mutant           lsass.exeM_688_
0x080f18290   1984       0x128    0x1f0001 Mutant           vmacthlp.exeM_844_
0x080fff030   1984       0x12c    0x1f0001 Mutant           svchost.exeM_856_
0x080f664f0   1984       0x130    0x1f0001 Mutant           svchost.exeM_1028_
0x0ff150a28   1984       0x134    0x1f0001 Mutant           spoolsv.exeM_1432_
0x0ff26e1d8   1984       0x138    0x1f0001 Mutant           vmtoolsd.exeM_1668_
0x0ff2862a8   1984       0x13c    0x1f0001 Mutant           vmupgradehelper.exeM_1788_
0x0ff29a250   1984       0x140    0x1f0001 Mutant           tpautoconnsvc.exeM_1968_
0x080fbbb40   1984       0x154    0x1f0001 Mutant           wuauclt.exeM_1732_
0x080f97f10   1984       0x190    0x1f0001 Mutant           aelas.exeM_1984_
0x080f785a0   1984       0x198    0x1f0001 Mutant           Ap1mutx7
0x0ff14b140   1984       0x1c8    0x1f0001 Mutant
0x0ff122b88   1984       0x1d8    0x1f0001 Mutant
kali@kali:~/Desktop/volatility$
```

The two random codes correlate to Sality backdoor (https://securelist.com/a-new-version-of-sality-at-large/29587/).

```
0x140    0x1f0001 Mutant
0x1d8    0x1f0001 Mutant           HGFSMUTEX00000000000242b4
0x1e8    0x1f0001 Mutant
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/ETThqkAGxIxMkUMdJ7YjaH0BxmryhCMgCT4eegnuzweP6g?e=YcGjam

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem thrdscan > 4_thrdscan.txt
Volatility Foundation Volatility Framework 2.6
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem unloadedmodules
Volatility Foundation Volatility Framework 2.6
Name                 StartAddress EndAddress Time
-------------------- ------------ ---------- ----
Sfloppy.SYS          0x00fc178000 0xfc17b000 2010-08-11 06:06:17
Cdaudio.SYS          0x00fc7b3000 0xfc7b8000 2010-08-11 06:06:17
vmdebug.sys          0x00fc66b000 0xfc674000 2010-08-11 06:06:47
splitter.sys         0x00fc9cd000 0xfc9cf000 2010-08-11 06:07:39
aec.sys              0x00f3124000 0xf3147000 2010-08-11 06:07:44
swmidi.sys           0x00f377d000 0xf378b000 2010-08-11 06:07:44
DMusic.sys           0x00f323c000 0xf3249000 2010-08-11 06:07:44
kmixer.sys           0x00f30fa000 0xf3124000 2010-08-11 06:07:44
drmkaud.sys          0x00fcab8000 0xfcab9000 2010-08-11 06:07:44
kmixer.sys           0x00f2fe0000 0xf300a000 2010-08-15 17:39:57
```

1.9. Benign Microsoft connections

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------ ------------------------- ---
0x02214988 172.16.176.143:1034      131.107.115.254:80        1260
0x06015ab0 172.16.176.143:1037      131.107.115.254:443       1260
```

Odd port activity from svchost.exe (PID 936): 135
Odd port activity from svchost.exe (PID 1028): 123, 1055
Odd port activity from svchost.exe (PID 1088): 1025
Odd port activity from aelas.exe (PID 1984): 5565
Odd port activity from svchost.exe (PID 1184): 1900

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x80fd1008        4      0     47 GRE             0.0.0.0         2010-08-11 06:08:00 UTC+0000
0xff258008      688    500     17 UDP             0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff367008        4    445      6 TCP             0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x80ffc128      936    135      6 TCP             0.0.0.0         2010-08-11 06:06:24 UTC+0000
0xff225b70      688      0    255 Reserved        0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff227340     1028    123     17 UDP             127.0.0.1       2010-08-15 17:43:45 UTC+0000
0x80fce930     1088   1025     17 UDP             0.0.0.0         2010-08-11 06:06:38 UTC+0000
0xff36b250     1028   1055      6 TCP             0.0.0.0         2010-08-15 17:43:45 UTC+0000
0xff396c68     1984   5565     17 UDP             0.0.0.0         2010-08-15 17:43:32 UTC+0000
0xff127d28      216   1026      6 TCP             127.0.0.1       2010-08-11 06:06:39 UTC+0000
0xff153a20     1148   1900     17 UDP             127.0.0.1       2010-08-15 17:43:45 UTC+0000
0xff1b8250      688   4500     17 UDP             0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff382e98        4   1033      6 TCP             0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x80fbdc40        4    445     17 UDP             0.0.0.0         2010-08-11 06:06:17 UTC+0000
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem sockscan
Volatility Foundation Volatility Framework 2.6
Offset(P)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ --------------- --------------- -----------
0x007c0a20     1148   1900     17 UDP             127.0.0.1       2010-08-15 17:43:45 UTC+0000
0x01120c40        4    445     17 UDP             0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x01131930     1088   1025     17 UDP             0.0.0.0         2010-08-11 06:06:38 UTC+0000
0x01134008        4      0     47 GRE             0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x011568a8        4    138     17 UDP             172.16.176.143  2010-08-15 17:38:54 UTC+0000
0x0115f128      936    135      6 TCP             0.0.0.0         2010-08-11 06:06:24 UTC+0000
0x02daad28      216   1026      6 TCP             127.0.0.1       2010-08-11 06:06:39 UTC+0000
0x043d4ac8     1148   1900     17 UDP             127.0.0.1       2010-08-15 17:38:54 UTC+0000
0x048636a0        4    137     17 UDP             172.16.176.143  2010-08-15 17:38:54 UTC+0000
0x0486ee98        4    139      6 TCP             172.16.176.143  2010-08-15 17:38:54 UTC+0000
0x048b5c68     1984   5565     17 UDP             0.0.0.0         2010-08-15 17:43:32 UTC+0000
0x04a4be98        4   1033      6 TCP             0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x04be3250     1028   1055      6 TCP             0.0.0.0         2010-08-15 17:43:45 UTC+0000
0x04be3c08     1028   1048      6 TCP             0.0.0.0         2010-08-15 17:38:54 UTC+0000
0x04be7008        4    445      6 TCP             0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x05dee200     1028    123     17 UDP             127.0.0.1       2010-08-15 17:38:54 UTC+0000
0x05f44008      688    500     17 UDP             0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x06124650     1028   1047     17 UDP             127.0.0.1       2010-08-15 17:38:54 UTC+0000
0x06235340     1028    123     17 UDP             127.0.0.1       2010-08-15 17:43:45 UTC+0000
0x06237b70      688      0    255 Reserved        0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x06384e98        4    138     17 UDP             172.16.176.143  2010-08-11 06:06:28 UTC+0000
0x069d5250      688   4500     17 UDP             0.0.0.0         2010-08-11 06:06:35 UTC+0000
```

1.10.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1c49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xe1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ae580 0x01bbd580 [no name]
0xe101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008978 0x01824978 [no name]
0xe1e158c0 0x009728c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1da4008 0x00f6e008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
```

2. Dumped aelas.exe (PID 1984) after suspicious findings:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem procdump -p 1984 -D .
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x8ff22f3d0 0x00400000 aelas.exe            OK: executable.1984.exe
```

Also dumped wuauclt.exe (PID 468) after noticing code injection

```
kali@kali:~/Desktop/volatility$ ./volatility -f 4.vmem procdump -p 468 -D dump
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x80f94588 0x00400000 wuauclt.exe          OK: executable.468.exe
kali@kali:~/Desktop/volatility$
```

3. Virustotal scan confirms hypothesis of Sality worm/trojan from aelas.exe:

60 security vendors flagged this file as malicious

7fac6867e112c8720fb351226af55bb62ccfebe1ea56d6c75271f0a7a3c6c734
1984.aelas.exe
peexe

69.00 KB
Size

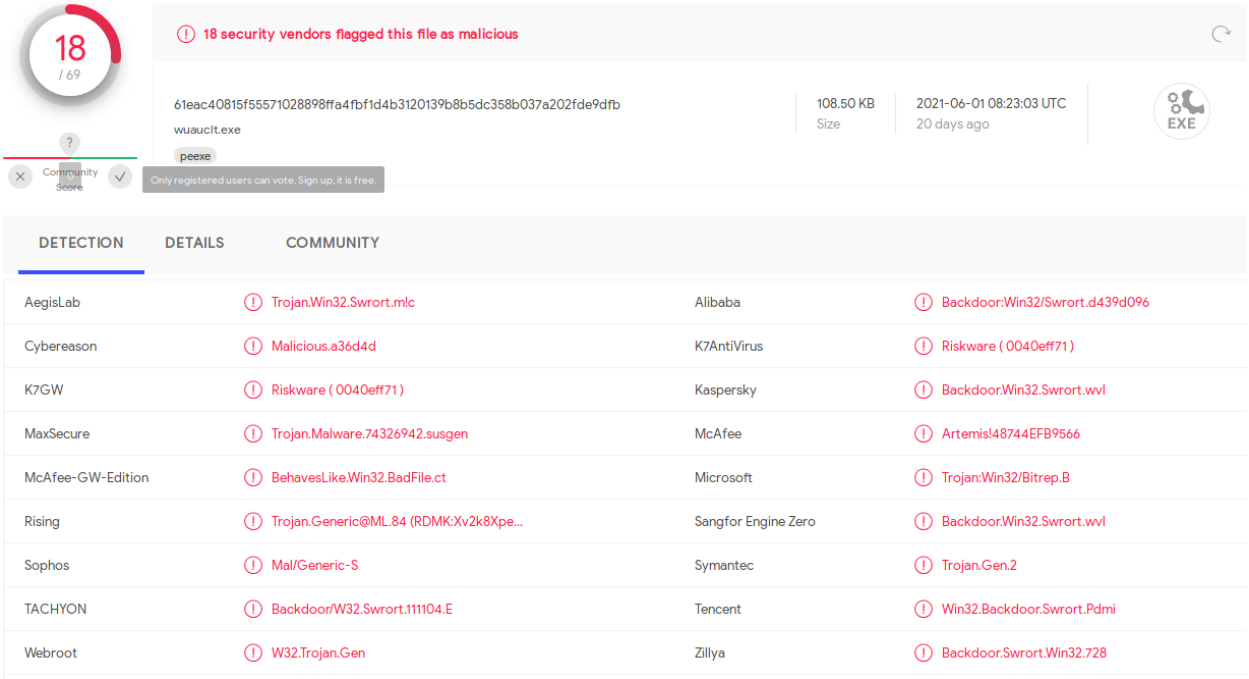
2020-02-02 07:27:08 UTC
1 year ago

EXE

DETECTION | DETAILS | BEHAVIOR | COMMUNITY 12

Acronis	Suspicious	Ad-Aware	Win32.Sality.3
Alibaba	Virus:Win32/Sality.76ab89d2	ALYac	Win32.Sality.3
Antiy-AVL	Virus/Win32.Sality.gen	SecureAge APEX	Malicious
Arcabit	Win32.Sality.3	Avast	Win32:Dh-A [Heur]
AVG	Win32:Dh-A [Heur]	Avira (no cloud)	WORM/Rbot.Gen
Baidu	Win32.Trojan.Sality.p	BitDefender	Win32.Sality.3
BitDefenderTheta	AI:FileInfector.A5ECCBAB0E	Bkav Pro	W32.SalDropv3.Worm

And another malicious executable (PID 468):



4. The malware family belongs to Sality, which is a polymorphic virus that infects executables with extensions .scr or .exe. The malware deletes files with specific extensions and stops security processes to avoid detection. The virus installs a backdoor which allows the remote C2 server to execute any commands it'd like on the host. This version of the Sality family (Sality.ag) appears to install a DLL to filter the internet traffic, while halting any security software at the same time. It also adds the driver to 'SystemCurrentControlSetControlSafeBoot" to ensure persistence and boot even in safe mode.

5.vmem

1.

1.1. Image appears to be WinXPSP2x86

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/kali/Desktop/volatility/5.vmem)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80544ce0L
          Number of Processors : 1
     Image Type (Service Pack) : 2
                KPCR for CPU 0 : 0xffdff000L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2010-08-15 19:17:56 UTC+0000
     Image local date and time : 2010-08-15 15:17:56 -0400
```

1.2. Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EffXpsYj4yRFvgGfERZOVXcBKKvbDnrNNCmDmjhpd2876w?e=bVEL7p

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem handles -t File > 5_files.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/ESO166qL-BhJtLWDbQxrkGcBqNh_-Pit2uS0_Jg5GDCCiA?e=GMlFgq

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem filescan > 5_filescan.txt
Volatility Foundation Volatility Framework 2.6
```

1.3. Same hashes as 1.vmem, also same RDP Key and lsadump activity

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem hashdump
Volatility Foundation Volatility Framework 2.6
Administrator:500:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:4e857c004024e53cd538de64dedac36b:842b4013c45a3b8fec76ca54e5910581:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8f57385a61425fc7874c3268aa249ea1:::
```

1.4.

```
kali@kali:~/Desktop/volatility$ ./findaes 5.vmem
Searching 5.vmem
Found AES-256 key schedule at offset 0xfd91cc:
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f
Found AES-256 key schedule at offset 0x65d76d4:
00 01 02 03 04 05 06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15 16 17 18 19 1a 1b 1c 1d 1e 1f
```

Appears to be a default 256 bit key.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EX1bFfvkY3ZOg0dNzts8BhUBllTfKsGOmtk7YJruywZzsg?e=ToqaeB

```
kali@kali:~/Desktop/volatility$ ./rsakeyfind 5.vmem > 5_rsakeys.txt
```

1.5. A little different than the rest of XP dumps.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem filescan | grep cfg
Volatility Foundation Volatility Framework 2.6
0x0000000004868d48      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\netcfgx.dll
0x000000000004a963b8      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\hnetcfg.dll
0x0000000006495028      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\hnetcfg.dll
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem filescan | grep conf
Volatility Foundation Volatility Framework 2.6
0x0000000003f3f08      1      0 R--r-d \Device\HarddiskVolume1\WINDOWS\system32\ipconf.tsp
0x000000000106be80      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY.LOG
0x0000000010d5f90      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x000000000112cb18      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM.LOG
0x0000000001160218      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x0000000001160430      1      0 R--rwd \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x0000000001187620      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default.LOG
0x000000000438b100      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software
0x00000000043d6e60      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0x000000000486b028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\default
0x0000000004a96c08      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\SECURITY
0x0000000005884258      2      1 RW-rw- \Device\HarddiskVolume1\WINDOWS\system32\config\systemprofile\Local Settings\History\History.IE5\index.dat
0x0000000005c5ceb8      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SysEvent.Evt
0x0000000005ce64b0      2      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\AppEvent.Evt
0x0000000005ce7a90      1      1 RW-r-- \Device\HarddiskVolume1\WINDOWS\system32\config\SecEvent.Evt
0x00000000063c6c88      2      1 RW-rw- \Device\HarddiskVolume1\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5
\index.dat
0x000000000655f028      2      1 RW-rw- \Device\HarddiskVolume1\WINDOWS\system32\config\systemprofile\Cookies\index.dat
0x0000000006629028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\software.LOG
0x0000000006779028      1      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system.LOG
0x000000000687f028      4      1 RW---- \Device\HarddiskVolume1\WINDOWS\system32\config\system
kali@kali:~/Desktop/volatility$
```

1.6. Nothing suspicious popping out other than VMip.exe hidden process

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem pstree
Volatility Foundation Volatility Framework 2.6
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x810b1660:System                                      4      0     58    379 1970-01-01 00:00:00 UTC+0000
. 0xff2ab020:smss.exe                                 544      4      3     21 2010-08-11 06:06:21 UTC+0000
.. 0xff1ec978:winlogon.exe                            632    544     24    536 2010-08-11 06:06:23 UTC+0000
... 0xff255020:lsass.exe                              688    632     21    405 2010-08-11 06:06:24 UTC+0000
... 0xff247020:services.exe                           676    632     16    288 2010-08-11 06:06:24 UTC+0000
.... 0xff1b8b28:vmtoolsd.exe                         1668    676      5    225 2010-08-11 06:06:35 UTC+0000
..... 0xff224020:cmd.exe                              124   1668      0 ------ 2010-08-15 19:17:55 UTC+0000
.... 0x80ff88d8:svchost.exe                           856    676     29    336 2010-08-11 06:06:24 UTC+0000
.... 0xff1d7da0:spoolsv.exe                          1432    676     14    145 2010-08-11 06:06:26 UTC+0000
.... 0x80fbf910:svchost.exe                          1028    676     88   1424 2010-08-11 06:06:24 UTC+0000
..... 0x80f60da0:wuauclt.exe                         1732   1028      7    189 2010-08-11 06:07:44 UTC+0000
..... 0x80f94588:wuauclt.exe                          468   1028      4    142 2010-08-11 06:09:37 UTC+0000
..... 0xff364310:wscntfy.exe                          888   1028      1     40 2010-08-11 06:06:49 UTC+0000
.... 0xff217560:svchost.exe                           936    676     11    288 2010-08-11 06:06:24 UTC+0000
.... 0xff143b28:TPAutoConnSvc.e                      1968    676      5    106 2010-08-11 06:06:39 UTC+0000
..... 0xff38b5f8:TPAutoConnect.e                     1084   1968      1     68 2010-08-11 06:06:52 UTC+0000
.... 0xff22d558:svchost.exe                          1088    676      7     93 2010-08-11 06:06:25 UTC+0000
.... 0xff218230:vmacthlp.exe                          844    676      1     37 2010-08-11 06:06:24 UTC+0000
.... 0xff25a7e0:alg.exe                               216    676      8    120 2010-08-11 06:06:39 UTC+0000
.... 0xff203b80:svchost.exe                          1148    676     15    217 2010-08-11 06:06:26 UTC+0000
.... 0xff1fdc88:VMUpgradeHelper                      1788    676      5    112 2010-08-11 06:06:38 UTC+0000
.. 0xff1ecda0:csrss.exe                               608    544     10    410 2010-08-11 06:06:23 UTC+0000
 0xff3865d0:explorer.exe                             1724   1708     13    326 2010-08-11 06:09:29 UTC+0000
. 0xff374980:VMwareUser.exe                           452   1724      8    207 2010-08-11 06:09:32 UTC+0000
. 0xff3667e8:VMwareTray.exe                           432   1724      1     60 2010-08-11 06:09:31 UTC+0000
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P)  Name                    PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
---------- -------------------- ------ ------ ------ -------- ------ ----- ------- -------- --------
0x06015020 services.exe            676 True   True   True     True   True  True    True
0x063c5560 svchost.exe             936 True   True   True     True   True  True    True
0x06499b80 svchost.exe            1148 True   True   True     True   True  True    True
0x04c2b310 wscntfy.exe             888 True   True   True     True   True  True    True
0x049c15f8 TPAutoConnect.e        1084 True   True   True     True   True  True    True
0x05f027e0 alg.exe                 216 True   True   True     True   True  True    True
0x05f47020 lsass.exe               688 True   True   True     True   True  True    True
0x010f7588 wuauclt.exe             468 True   True   True     True   True  True    True
0x01122910 svchost.exe            1028 True   True   True     True   True  True    True
0x069d5b28 vmtoolsd.exe           1668 True   True   True     True   True  True    True
0x06384230 vmacthlp.exe            844 True   True   True     True   True  True    True
0x0115b8d8 svchost.exe             856 True   True   True     True   True  True    True
0x04b5a980 VMwareUser.exe          452 True   True   True     True   True  True    True
0x010c3da0 wuauclt.exe            1732 True   True   True     True   True  True    True
0x04a065d0 explorer.exe           1724 True   True   True     True   True  True    True
0x04be97e8 VMwareTray.exe          432 True   True   True     True   True  True    True
0x0211ab28 TPAutoConnSvc.e        1968 True   True   True     True   True  True    True
0x06945da0 spoolsv.exe            1432 True   True   True     True   True  True    True
0x066f0978 winlogon.exe            632 True   True   True     True   True  True    True
0x0655fc88 VMUpgradeHelper        1788 True   True   True     True   True  True    True
0x061ef558 svchost.exe            1088 True   True   True     True   True  True    True
0x06238020 cmd.exe                 124 True   True   False    True   False False   False    2010-08-15 19:17:56 UTC+0000
0x066f0da0 csrss.exe               608 True   True   True     True   False True    True
0x05471020 smss.exe                544 True   True   True     True   False False   False
0x01214660 System                    4 True   True   True     True   False False   False
0x069a7328 VMip.exe               1944 False  True   False    False  False False   False    2010-08-15 19:17:56 UTC+0000
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EcEFR0Wt97JPi9X4QyvyfxMBQSBUIaFwBgG7KCTk0bamaw?e=TOM6IA

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem dlllist
```

Notice odd wscntfy.exe privs, and different PID's for wuauclt.exe:

```
  1432 spoolsv.exe          25 SeUndockPrivilege              Present,Enabled         Remove computer from docking station
  1788 VMUpgradeHelper      10 SeLoadDriverPrivilege          Present,Enabled         Load and unload device drivers
  1788 VMUpgradeHelper      25 SeUndockPrivilege              Present,Enabled         Remove computer from docking station
   888 wscntfy.exe          20 SeDebugPrivilege               Present,Enabled         Debug programs
  1084 TPAutoConnect.e      20 SeDebugPrivilege               Present,Enabled         Debug programs
  1732 wuauclt.exe           2 SeCreateTokenPrivilege         Present,Enabled         Create a token object
  1732 wuauclt.exe           9 SeTakeOwnershipPrivilege       Present,Enabled         Take ownership of files/objects
  1732 wuauclt.exe           3 SeAssignPrimaryTokenPrivilege  Present,Enabled         Replace a process-level token
  1732 wuauclt.exe           5 SeIncreaseQuotaPrivilege       Present,Enabled         Increase quotas
  1732 wuauclt.exe           8 SeSecurityPrivilege            Present,Enabled         Manage auditing and security log
  1732 wuauclt.exe          22 SeSystemEnvironmentPrivilege   Present,Enabled         Edit firmware environment values
  1732 wuauclt.exe          17 SeBackupPrivilege              Present,Enabled         Backup files and directories
  1732 wuauclt.exe          18 SeRestorePrivilege             Present,Enabled         Restore files and directories
  1732 wuauclt.exe          19 SeShutdownPrivilege            Present,Enabled         Shut down the system
  1732 wuauclt.exe          10 SeLoadDriverPrivilege          Present,Enabled         Load and unload device drivers
  1732 wuauclt.exe          12 SeSystemtimePrivilege          Present,Enabled         Change the system time
  1732 wuauclt.exe          25 SeUndockPrivilege              Present,Enabled         Remove computer from docking station
  1732 wuauclt.exe          28 SeManageVolumePrivilege        Present,Enabled         Manage the files on a volume
  1724 explorer.exe          8 SeSecurityPrivilege            Present,Enabled         Manage auditing and security log
  1724 explorer.exe         20 SeDebugPrivilege               Present,Enabled         Debug programs
  1724 explorer.exe         10 SeLoadDriverPrivilege          Present,Enabled         Load and unload device drivers
  1724 explorer.exe         25 SeUndockPrivilege              Present,Enabled         Remove computer from docking station
   432 VMwareTray.exe       20 SeDebugPrivilege               Present,Enabled         Debug programs
   432 VMwareTray.exe       10 SeLoadDriverPrivilege          Present,Enabled         Load and unload device drivers
   432 VMwareTray.exe       25 SeUndockPrivilege              Present,Enabled         Remove computer from docking station
   452 VMwareUser.exe       20 SeDebugPrivilege               Present,Enabled         Debug programs
   452 VMwareUser.exe       10 SeLoadDriverPrivilege          Present,Enabled         Load and unload device drivers
   452 VMwareUser.exe       25 SeUndockPrivilege              Present,Enabled         Remove computer from docking station
   468 wuauclt.exe          20 SeDebugPrivilege               Present,Enabled         Debug programs
kali@kali:~/Desktop/volatility$
```

1.7.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EdVWKgjNoylOoC98IrPk_GwBO-T3dcWgYPmgsrxWMyjk2A?e=Xy0QQk

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem apihooks > 5_apihooks.txt
Volatility Foundation Volatility Framework 2.6
```

svchost.exe (PID 856) appears to have hooks with ntdll.dll as the victim:

```
Hook mode: Usermode
Hook type: Inline/Trampoline
Process: 856 (svchost.exe)
Victim module: ntdll.dll (0x7c900000 - 0x7c9b0000)
Function: ntdll.dll!NtCreateThread at 0x7c90d7d2
Hook address: 0xb73b47
Hooking module: <unknown>

Disassembly(0):
0x7c90d7d2 e970632684      JMP 0xb73b47
0x7c90d7d7 ba0003fe7f      MOV EDX, 0x7ffe0300
0x7c90d7dc ff12            CALL DWORD [EDX]
0x7c90d7de c22000          RET 0x20
0x7c90d7e1 90              NOP
0x7c90d7e2 90              NOP
0x7c90d7e3 90              NOP
0x7c90d7e4 90              NOP
0x7c90d7e5 90              NOP
0x7c90d7e6 90              NOP
0x7c90d7e7 b8              DB 0xb8
0x7c90d7e8 36              DB 0x36
0x7c90d7e9 00              DB 0x0

Disassembly(1):
0xb73b47 55              PUSH EBP
0xb73b48 8bec            MOV EBP, ESP
0xb73b4a 83ec18          SUB ESP, 0x18
0xb73b4d 53              PUSH EBX
0xb73b4e 56              PUSH ESI
0xb73b4f 57              PUSH EDI
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EQoLvp61-BNHiWuZr_a3GiUBPvzyS8nJiUO5VOf5MoMhIg?e=YgoSGL

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem malfind > 5_malfind.txt
Volatility Foundation Volatility Framework 2.6
```

svchost.exe (PID 856) appears to have code injected into it

```
Process: svchost.exe Pid: 856 Address: 0x0b70000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 38, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x00b70000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x00b70010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x00b70020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x00b70030  00 00 00 00 00 00 00 00 00 00 00 00 d0 00 00 00   ................

0x00b70000 4d               DEC EBP
0x00b70001 5a               POP EDX
```

1.8.

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EcnKatSHKp5JpHX_3k2VXyMBbz2bFuagjhWbELAIuNudYQ?e=mOwT79

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem modules > 5_modules.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EagrPAhqwUdGrZQsMGHgRWABQN9wyji0RYK5SVbBNxgE9g?e=pB4iYc

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem driverscan > 5_drivers.txt
Volatility Foundation Volatility Framework 2.6
```

Link: https://unbcloud-my.sharepoint.com/:t:/g/personal/nclement_unb_ca/EQByHXyVhyxOoQj0RH_qqMkBngIerWDJqX56oPhM61JRqA?e=vHMblj

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem thrdscan > 5_thrdscan.txt
Volatility Foundation Volatility Framework 2.6
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem unloadedmodules
Volatility Foundation Volatility Framework 2.6
Name                 StartAddress  EndAddress    Time
-------------------- ------------  ------------  ----
Sfloppy.SYS          0x00fc178000  0xfc17b000    2010-08-11 06:06:17
Cdaudio.SYS          0x00fc7b3000  0xfc7b8000    2010-08-11 06:06:17
vmdebug.sys          0x00fc66b000  0xfc674000    2010-08-11 06:06:47
splitter.sys         0x00fc9cd000  0xfc9cf000    2010-08-11 06:07:39
aec.sys              0x00f3124000  0xf3147000    2010-08-11 06:07:44
swmidi.sys           0x00f377d000  0xf378b000    2010-08-11 06:07:44
DMusic.sys           0x00f323c000  0xf3249000    2010-08-11 06:07:44
kmixer.sys           0x00f30fa000  0xf3124000    2010-08-11 06:07:44
drmkaud.sys          0x00fcab8000  0xfcab9000    2010-08-11 06:07:44
kmixer.sys           0x00f2fe0000  0xf300a000    2010-08-15 19:16:47
```

1.9.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem connections
Volatility Foundation Volatility Framework 2.6
Offset(V)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem connscan
Volatility Foundation Volatility Framework 2.6
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x02214988 172.16.176.143:1054       193.104.41.75:80          856
0x06015ab0 0.0.0.0:1056              193.104.41.75:80          856
```

Connections correlate to Zeus malware:

2009/11/27_17:48 -	193.104.41.75/cbd/75.exe	-	zeus v1 trojan	49934
2009/11/27_20:35 -	210.51.166.217/exe/fole1.exe	-	trojan	9929
2009/11/27_22:03 -	213.163.89.254/gyh/sedmoipontoi.exe	-	zeus v1 trojan	49544
2009/11/28_16:09 -	193.104.41.75/kissme/rec.php	-	zeus v1 drop zone	49934
2009/11/28_19:22 -	193.104.27.251/rsf/loadjavad.php	-	trojan Oficla	12604
2009/11/29_13:05 -	193.104.41.75/cbd/75.bro	-	zeus v1 config file	49934

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem sockets
Volatility Foundation Volatility Framework 2.6
Offset(V)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ---------- --------------- -----------
0x80fd1008        4      0     47 GRE            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0xff258008      688    500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff367008        4    445      6 TCP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x80ffc128      936    135      6 TCP            0.0.0.0         2010-08-11 06:06:24 UTC+0000
0xff37cd28     1028   1058      6 TCP            0.0.0.0         2010-08-15 19:17:56 UTC+0000
0xff20c478      856  29220      6 TCP            0.0.0.0         2010-08-15 19:17:27 UTC+0000
0xff225b70      688      0    255 Reserved       0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff254008     1028    123     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0x80fce930     1088   1025     17 UDP            0.0.0.0         2010-08-11 06:06:38 UTC+0000
0xff127d28      216   1026      6 TCP            127.0.0.1       2010-08-11 06:06:39 UTC+0000
0xff206a20     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0xff1b8250      688   4500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0xff382e98        4   1033      6 TCP            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x80fbdc40        4    445     17 UDP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem sockscan
Volatility Foundation Volatility Framework 2.6
Offset(P)       PID   Port  Proto Protocol        Address         Create Time
---------- -------- ------ ------ ---------- --------------- -----------
0x007c0a20     1148   1900     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x01120c40        4    445     17 UDP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x01131930     1088   1025     17 UDP            0.0.0.0         2010-08-11 06:06:38 UTC+0000
0x01134008        4      0     47 GRE            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x011568a8        4    138     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x0115f128      936    135      6 TCP            0.0.0.0         2010-08-11 06:06:24 UTC+0000
0x02daad28      216   1026      6 TCP            127.0.0.1       2010-08-11 06:06:39 UTC+0000
0x04863458        4    139      6 TCP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x04864578     1028     68     17 UDP            172.16.176.143  2010-08-15 19:17:26 UTC+0000
0x04864a08        4    137     17 UDP            172.16.176.143  2010-08-15 19:15:43 UTC+0000
0x04a4be98        4   1033      6 TCP            0.0.0.0         2010-08-11 06:08:00 UTC+0000
0x04a51d28     1028   1058      6 TCP            0.0.0.0         2010-08-15 19:17:56 UTC+0000
0x04be7008        4    445      6 TCP            0.0.0.0         2010-08-11 06:06:17 UTC+0000
0x05dee200     1028    123     17 UDP            127.0.0.1       2010-08-15 19:15:43 UTC+0000
0x05e33d68     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:15:43 UTC+0000
0x05f44008      688    500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x05f48008     1028    123     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0x06236e98     1028     68     17 UDP            172.16.176.143  2010-08-15 19:17:56 UTC+0000
0x06237b70      688      0    255 Reserved       0.0.0.0         2010-08-11 06:06:35 UTC+0000
0x06450478      856  29220      6 TCP            0.0.0.0         2010-08-15 19:17:27 UTC+0000
0x06496a20     1148   1900     17 UDP            127.0.0.1       2010-08-15 19:17:56 UTC+0000
0x069d5250      688   4500     17 UDP            0.0.0.0         2010-08-11 06:06:35 UTC+0000
```

1.10.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem hivelist
Volatility Foundation Volatility Framework 2.6
Virtual    Physical   Name
---------- ---------- ----
0xe1c49008 0x036dc008 \Device\HarddiskVolume1\Documents and Settings\LocalService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1c41b60 0x04010b60 \Device\HarddiskVolume1\Documents and Settings\LocalService\NTUSER.DAT
0xe1a39638 0x021eb638 \Device\HarddiskVolume1\Documents and Settings\NetworkService\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1a33008 0x01f98008 \Device\HarddiskVolume1\Documents and Settings\NetworkService\NTUSER.DAT
0xe153ab60 0x06b7db60 \Device\HarddiskVolume1\WINDOWS\system32\config\software
0xe1542008 0x06c48008 \Device\HarddiskVolume1\WINDOWS\system32\config\default
0xe1537b60 0x06ae4b60 \SystemRoot\System32\Config\SECURITY
0xe1544008 0x06c4b008 \Device\HarddiskVolume1\WINDOWS\system32\config\SAM
0xe13ae580 0x01bbd580 [no name]
0xe101b008 0x01867008 \Device\HarddiskVolume1\WINDOWS\system32\config\system
0xe1008978 0x01824978 [no name]
0xe1e158c0 0x009728c0 \Device\HarddiskVolume1\Documents and Settings\Administrator\Local Settings\Application Data\Microsoft\Windows\UsrClass.dat
0xe1da4008 0x00f6e008 \Device\HarddiskVolume1\Documents and Settings\Administrator\NTUSER.DAT
```

Very suspicious registry key for winlogon. UserInit is to tell the machine what programs should be launched right after logging in. “sdra64.exe” seems to be quite malicious.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem printkey -K "Microsoft\Windows NT\CurrentVersion\Winlogon"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\software
Key name: Winlogon (S)
Last updated: 2010-08-15 19:17:23 UTC+0000

Subkeys:
  (S) GPExtensions
  (S) Notify
  (S) SpecialAccounts
  (V) Credentials

Values:
REG_DWORD     AutoRestartShell : (S) 1
REG_SZ        DefaultDomainName : (S) BILLY-DB5B96DD3
REG_SZ        DefaultUserName : (S) Administrator
REG_SZ        LegalNoticeCaption : (S)
REG_SZ        LegalNoticeText : (S)
REG_SZ        PowerdownAfterShutdown : (S) 0
REG_SZ        ReportBootOk    : (S) 1
REG_SZ        Shell           : (S) Explorer.exe
REG_SZ        ShutdownWithoutLogon : (S) 0
REG_SZ        System          : (S)
REG_SZ        Userinit        : (S) C:\WINDOWS\system32\userinit.exe,C:\WINDOWS\system32\sdra64.exe,
REG_SZ        VmApplet        : (S) rundll32 shell32,Control_RunDLL "sysdm.cpl"
REG_DWORD     SfcQuota        : (S) 4294967295
REG_SZ        allocatecdroms  : (S) 0
REG_SZ        allocatedasd    : (S) 0
REG_SZ        allocatefloppies : (S) 0
REG_SZ        cachedlogonscount : (S) 10
REG_DWORD     forceunlocklogon : (S) 0
REG_DWORD     passwordexpirywarning : (S) 14
REG_SZ        scremoveoption  : (S) 0
REG_DWORD     AllowMultipleTSSessions : (S) 1
REG_EXPAND_SZ UIHost          : (S) logonui.exe
REG_DWORD     LogonType       : (S) 1
REG_SZ        Background      : (S) 0 0 0
REG_SZ        AutoAdminLogon  : (S) 0
REG_SZ        DebugServerCommand : (S) no
REG_DWORD     SFCDisable      : (S) 0
REG_SZ        WinStationsDisabled : (S) 0
REG_DWORD     HibernationPreviouslyEnabled : (S) 1
REG_DWORD     ShowLogonOptions : (S) 0
REG_SZ        AltDefaultUserName : (S) Administrator
REG_SZ        AltDefaultDomainName : (S) BILLY-DB5B96DD3
kali@kali:~/Desktop/volatility$
```

Found the executables with filescan:

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem filescan | grep sdra64
Volatility Foundation Volatility Framework 2.6
0x00000000029d9b40      1      1 R----- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
0x00000000029d9cf0      1      0 -WD--- \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
kali@kali:~/Desktop/volatility$
```

Firewall appears to have been disabled.

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem printkey -K "ControlSet001\Services\SharedAccess\Parameters\FirewallPolicy\StandardProfile"
Volatility Foundation Volatility Framework 2.6
Legend: (S) = Stable   (V) = Volatile

----------------------------

Registry: \Device\HarddiskVolume1\WINDOWS\system32\config\system
Key name: StandardProfile (S)
Last updated: 2010-08-15 19:17:24 UTC+0000

Subkeys:
  (S) AuthorizedApplications

Values:
REG_DWORD     EnableFirewall  : (S) 0
```

Pretty clear what malware family this is now..

```
REG_BINARY    UEME_RUNPATH:C:\Documents and Settings\Administrator\Desktop\ZeuS_binary_5767b2c6d84d87a47d12da03f4f376ad.exe :
ID:             2
Count:          1
Last updated:   2010-08-15 19:17:23 UTC+0000
Raw Data:
0x00000000  02 00 00 00 06 00 00 00 60 35 58 7d ae 3c cb 01   ........`5X}.<..
```

Shimcache:

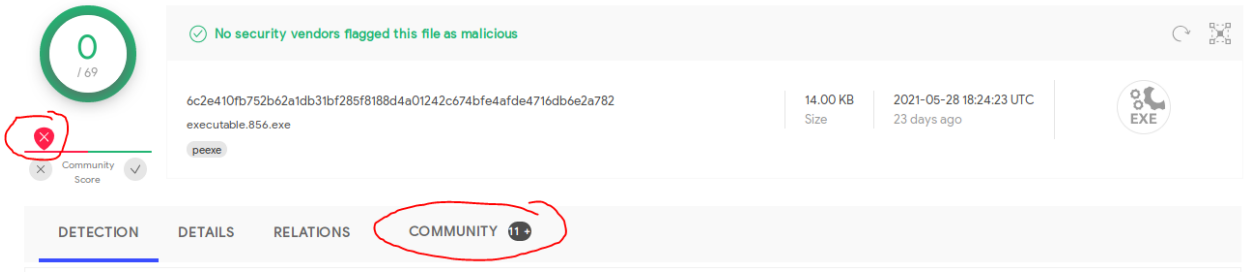
```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem shimcache
Volatility Foundation Volatility Framework 2.6
Last Modified                  Last Update                    Path
------------------------------ ------------------------------ ----
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:11:19 UTC+0000   \??\C:\WINDOWS\system32\oobe\msoobe.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:11:39 UTC+0000   \??\C:\WINDOWS\system32\oobe\oobebaln.exe
2006-02-28 12:00:00 UTC+0000   2010-08-11 06:04:52 UTC+0000   \??\C:\WINDOWS\system32\wscntfy.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:20:28 UTC+0000   \??\C:\WINDOWS\System32\cscui.dll
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:12:09 UTC+0000   \??\C:\Program Files\Outlook Express\setup50.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:12:08 UTC+0000   \??\C:\WINDOWS\inf\unregmp2.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:20:29 UTC+0000   \??\C:\WINDOWS\system32\NETSHELL.dll
2010-02-09 21:04:30 UTC+0000   2010-06-10 16:12:37 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\unzip.exe
2010-02-09 20:57:14 UTC+0000   2010-06-10 16:20:33 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\TPAutoConnSvc.exe
2010-02-09 20:57:14 UTC+0000   2010-06-10 16:12:49 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\TPVCGateway.exe
2010-02-09 21:00:20 UTC+0000   2010-06-10 16:20:18 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmacthlp.exe
2010-02-09 21:00:00 UTC+0000   2010-06-10 16:20:30 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmwareuser.exe
2010-02-09 21:00:10 UTC+0000   2010-06-10 16:20:30 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmwaretray.exe
2010-02-09 21:00:14 UTC+0000   2010-06-10 16:20:29 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\vmtoolsd.exe
2006-02-28 12:00:00 UTC+0000   2010-06-10 16:20:31 UTC+0000   \??\C:\WINDOWS\system32\shdocvw.dll
2010-02-09 20:59:20 UTC+0000   2010-06-10 16:20:32 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\poweron-vm-default.bat
2010-02-09 21:00:16 UTC+0000   2010-06-10 16:20:32 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\VMUpgradeHelper.exe
2010-02-09 20:57:14 UTC+0000   2010-06-10 16:20:36 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\TPAutoConnect.exe
2010-06-10 16:12:49 UTC+0000   2010-08-11 06:03:17 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\resume-vm-default.bat
2010-02-09 21:00:24 UTC+0000   2010-08-11 06:03:18 UTC+0000   \??\C:\Program Files\VMware\VMware Tools\VMip.exe
kali@kali:~/Desktop/volatility$
```

2. Malicious executables was svchost.exe (PID 856), and sdra64.exe

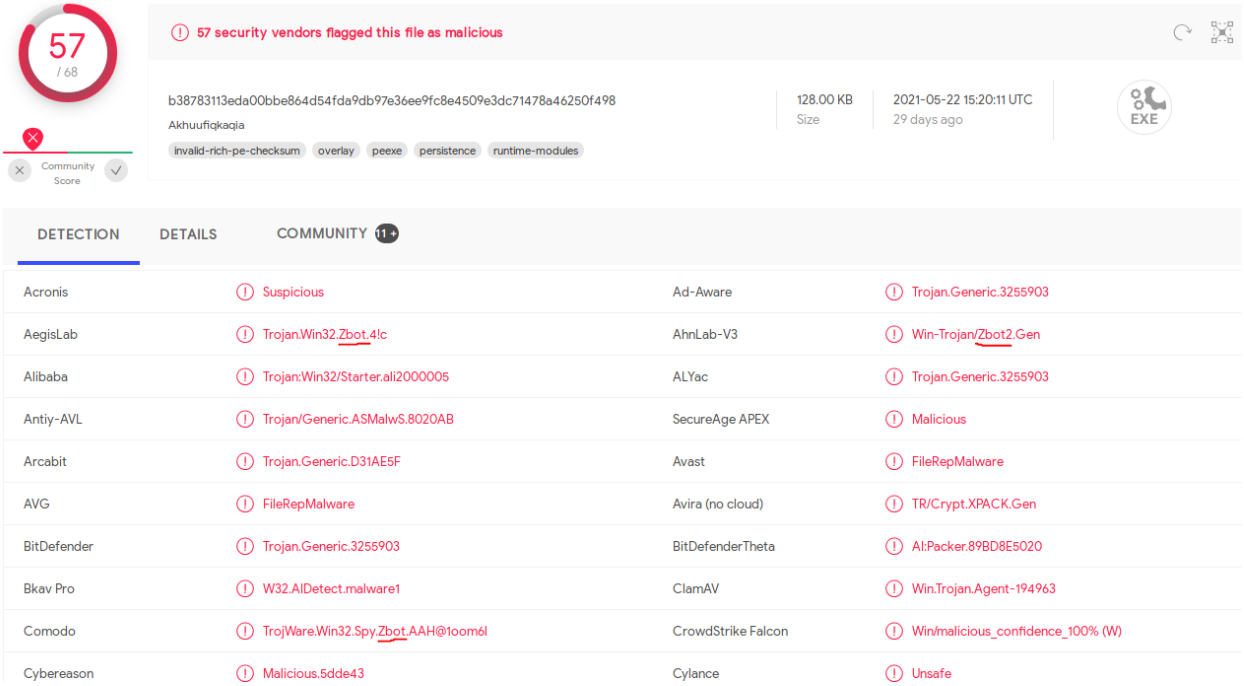
```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem procdump -p 856 -D dump
Volatility Foundation Volatility Framework 2.6
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x80ff88d8 0x01000000 svchost.exe          OK: executable.856.exe
kali@kali:~/Desktop/volatility$
```

```
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem dumpfiles -Q 0x00000000029d9b40 -D dump
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x029d9b40   None   \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
kali@kali:~/Desktop/volatility$ ./volatility -f 5.vmem dumpfiles -Q 0x00000000029d9cf0 -D dump
Volatility Foundation Volatility Framework 2.6
DataSectionObject 0x029d9cf0   None   \Device\HarddiskVolume1\WINDOWS\system32\sdra64.exe
kali@kali:~/Desktop/volatility$
```

3. Svchost.exe came back clean but with a very low community score, which suggests that the malware wasn't detected



sdra64.exe came back as malicious:



Conclusion: sdra64.exe confirms the hypothesis that it is Zeus malware.

4. After analysis of the hashes in Virustotal and of the memory dump, this belong to the Zeus malware family. Zeus was an incredibly successful trojan/botnet around 2010 that infected millions. The main goal of the malware is to install a backdoor and make the host a bot to add to their botnet, which they can control from their C2 server. The other goal is to act as a credential harvester and keylogger, with a focus on stealing banking credentials.