

A

FORENSIC REPORT ON THE STOLEN SZECHUAN SAUCE CASE

ANALYZED

Submitted by: KEHINDE OJEWUNMI,

NOAH SHITTA

NAVNEET KAUR

Tools used:

- Autopsy
- Volatility
- FTK manager
- Excel
- Wireshark

1. What's the Operating System of the Server?

To find this we can check in a few places. We've checked in OS information in Autopsy tool

The screenshot shows the Autopsy 4.20.0 interface. The left sidebar contains a tree view of data sources, file views, data artifacts, analysis results, and other tools. The main panel is titled 'Operating System Information' and displays a table with one result. The table has columns for Source Name, S, C, O, Name, Domain, and Program Name. The single row shows '20200918_0347_CDrive.E01' as the source, with values for S, C, and O being empty, Name as 'CITADEL-DC01', Domain as 'C137.local', and Program Name as 'Windows Server 2012 R2 Standard Evaluation'. There is also a 'Save Table as CSV' button. At the bottom, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. A progress bar at the bottom indicates 'Analyzing files from 20200918_0347_CDrive.E01' at 1% completion, with '(7 more...)' and a count of 6.

2. What's the Operating System of the Desktop?

Windows 10 Enterprise Evaluation

Type	Value
Name	DESKTOP-SDN1RPT
Domain	C137.local
Program Name	Windows 10 Enterprise Evaluation
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00329-20000-00001-AA089
Owner	Admin
Source File Path	/img_20200918_0417_DESKTOP-SDN1RPT.E01
Artifact ID	-9223372036854774702

3. What was the local time of the Server?

This can be found in registry explorer and web history folder in Autopsy showing EDT i.e. (UTC-04:00)

Source Name	URL	Date Accessed	Process
WebCacheV01.dat	res://C:/Windows/system32/mmcndmgr.dll/views.htm	2020-09-18 22:32:18 EDT	Micro
WebCacheV01.dat	file:///C:/FileShare/Secret/PortalGunPlans.txt	2020-09-19 03:32:02 EDT	Micro
WebCacheV01.dat	file:///C:/FileShare/Secret/Szechuan%20Sauce.txt	2020-09-19 03:32:21 EDT	Micro
WebCacheV01.dat	file:///C:/FileShare/Secret/SECRET_beth.txt	2020-09-19 03:32:13 EDT	Micro
WebCacheV01.dat	res://iesetup.dll/HardAdmin.htm	2020-09-19 03:23:01 EDT	Micro
WebCacheV01.dat	http://194.61.24.102/	2020-09-19 03:23:41 EDT	Micro
WebCacheV01.dat	http://194.61.24.102/favicon.ico	2020-09-19 03:23:41 EDT	Micro
WebCacheV01.dat	file:///C:/FileShare/Secret/Beth_Secret.txt	2020-09-19 03:35:07 EDT	Micro
WebCacheV01.dat	res://C:/Windows/system32/mmcndmgr.dll/views.htm	2020-09-18 22:32:18 EDT	Micro
WebCacheV01.dat	file:///C:/FileShare/Secret/PortalGunPlans.txt	2020-09-19 03:32:02 EDT	Micro
WebCacheV01.dat	file:///C:/FileShare/Secret/Szechuan%20Sauce.txt	2020-09-19 03:32:21 EDT	Micro

Registry Explorer v1.6.0.0

File Tools Options Bookmarks (26/0) View Help

Registry hives (1) Available bookmarks (26/0)

Enter text to search... Find

Key name	# values	# subkeys	Last write timestamp
Timezoneinforma...	10	0	2020-09-17 17:56:13
Ubp...	8	0	2013-08-22 15:40:04
usb	0	1	2020-09-17 17:56:13
usbflags	0	2	2020-09-17 17:56:13
usbstor	0	5	2020-09-17 17:56:13
VAN	0	3	2013-08-22 15:40:04
Video	0	4	2020-09-17 17:56:13
Wdf	0	4	2020-09-17 17:56:13
WDI	0	3	2013-08-22 15:40:04
Windows	10	0	2020-09-18 23:10:53
Winlogon	0	1	2020-09-17 17:56:13
WMI	0	3	2020-09-17 17:56:13
WorkplaceJoin	1	0	2020-09-17 17:56:13
WPN	0	0	2020-09-17 17:56:13
Enum	34	16	2020-09-19 03:21:47
Hardware Profiles	0	3	2020-09-19 01:22:34
Policies	0	0	2020-09-17 18:05:45
Services	0	454	2020-09-19 03:56:56
ControlSet002	0	5	2013-08-22 14:48:22
DriverDatabase	3	4	2020-09-17 17:56:13
HardwareConfig	2	1	2020-09-19 01:22:34
MountedDevices	5	0	2020-09-17 17:56:13
RNG	2	0	2020-09-19 01:22:35
Select	4	0	2020-09-17 17:56:13
Setup	12	8	2020-09-17 17:59:24
WPA	0	18	2020-09-17 17:59:54
Associated deleted records	0	0	
Unassociated deleted records	0	0	

Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Val...	Is D...	Data
DaylightBias	RegDword	4294967236			
DaylightName	RegSz	@tzres.dll,-211	00...		
StandardStart	RegBinary	00-00-08-00-01-00-02...	00...		
StandardBias	RegDword	0			
StandardName	RegSz	@tzres.dll,-212	00...		
Bias	RegDword	480			
DaylightStart	RegBinary	00-00-03-00-02-00-02...	F0...		
TimeZoneKeyName	RegSz	Pacific Standard Time			
DynamicDaylightTimeDisabled	RegDword	0			
ActiveTimeBias	RegDword	420			

Type viewer Binary viewer

Value name DaylightBias

Value type RegDword

Value 4294967236

Raw value C4-FF-FF-FF

4. Was there a breach?

Yes, The recipe was stolen and some files were deleted

Coreupdate.exe file was found in wireshark

Time	Source	s port	Destination	d port	Protocol	Length	Info
2020-09-18 22:23:41.731918	10.42.85.10	62408	194.61.24.102	80	HTTP		302 GET / HTTP/1.1
2020-09-18 22:23:41.797123	10.42.85.10	62407	194.61.24.102	80	HTTP		255 GET /favicon.ico HTTP/1.1
2020-09-18 22:24:06.939239	10.42.85.10	62410	194.61.24.102	80	HTTP		291 GET /coreupdater.exe HTTP/1.1
2020-09-18 22:39:26.939207	10.42.85.115	50840	194.61.24.102	80	HTTP		428 GET / HTTP/1.1
2020-09-18 22:39:58.410684	10.42.85.115	50864	194.61.24.102	80	HTTP		352 GET /coreupdater.exe HTTP/1.1

```
> Frame 238565: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface 0
> Ethernet II, Src: VMware_e1:84:e6 (00:0c:29:e1:84:e6), Dst: VMware_95:cd:21 (00:0c:29:95:cd:21)
> Internet Protocol Version 4, Src: 10.42.85.10, Dst: 194.61.24.102
> Transmission Control Protocol, Src Port: 62410, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
> Hypertext Transfer Protocol
> GET /coreupdater.exe HTTP/1.1\r\n
Accept: */*\r\n
Referer: http://194.61.24.102/\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Host: 194.61.24.102\r\n
Connection: Keep-Alive\r\n
\r\n
[Full request URI: http://194.61.24.102/coreupdater.exe]
[HTTP request 1/1]
[Response in frame: 238574]
```

(p.src == 194.61.24.102) or (p.dst == 194.61.24.102) && (http.request)

Time	Source	s port	Destination	d port	Protocol	Length	Info
2020-09-18 22:23:41.731918	10.42.85.10	62408	194.61.24.102	80	HTTP		302 GET / HTTP/1.1
2020-09-18 22:23:41.797123	10.42.85.10	62407	194.61.24.102	80	HTTP		255 GET /favicon.ico HTTP/1.1
2020-09-18 22:24:06.939239	10.42.85.10	62410	194.61.24.102	80	HTTP		291 GET /coreupdater.exe HTTP/1.1
2020-09-18 22:39:26.939207	10.42.85.115	50840	194.61.24.102	80	HTTP		428 GET / HTTP/1.1
2020-09-18 22:39:58.410684	10.42.85.115	50864	194.61.24.102	80	HTTP		352 GET /coreupdater.exe HTTP/1.1

```

< GET /coreupdater.exe HTTP/1.1\r\n
> [Expert Info (Chat/Sequence): GET /coreupdater.exe HTTP/1.1\r\n]
  Request Method: GET
  Request URI: /coreupdater.exe
  Request Version: HTTP/1.1
  Accept: */*\r\n
  Referer: http://194.61.24.102/\r\n
  Accept-Encoding: gzip, deflate\r\n
  User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
  Host: 194.61.24.102\r\n
0080  0d 0a 41 63 63 65 70 74  2d 45 6e 63 6f 64 69 6e  ..Accept -Encoding
0090  67 3a 20 67 7a 69 70 2c  20 64 65 66 6c 61 74 65  g: gzip, deflate
00a0  0d 0a 55 73 65 72 2d 41  67 65 6e 74 3a 20 4d 6f  -User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
00b0  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f  ws NT 6.3; WOW64
00c0  77 73 20 4e 54 20 36 2e  33 3b 20 57 4f 57 36 34  ; Trident/7.0; rv:11.0
00d0  3b 20 54 72 69 64 65 6e  74 2f 37 2e 30 3b 20 72  like Gecko
00e0  76 3a 31 31 2e 30 29 20  6c 69 6b 65 20 47 65 63  v:11.0
00f0  6b 6f 0d 0a 48 6f 73 74  3a 20 31 39 34 2e 36 31  ko Host : 194.61
0100  2e 32 34 2e 31 30 32 0d  0a 43 6f 6e 6e 65 63 74  .24.102. Connect
0110  69 6f 6e 3a 20 4b 65 65  70 2d 41 6c 69 76 65 0d  ion: Kee p-Alive.

```

HTTP Accept Encoding (http.accept_encoding), 32 bytes

Packets: 411797 - Displayed: 5 (0.0%)

3:27 PM

Wireshark - Export - HTTP object list

Packet	Hostname	Content Type	Size	Filename
19418	vignette.wikipedia.net	image/jpeg	61 kB	latest?cb=20170112143444
19445	ocsp.comodoca.com	application/ocsp-response	471 bytes	MFEwTz8NMEsw5TAJ6gUrDgMCggUABBRttU9uFqgVGHhJwZyWCNxMvR5ngQUoBEKIZ6W8Qfs4q8p74Kf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%3D
236791	194.61.24.102	text/html	228 bytes	\
236809	194.61.24.102	text/html	195 bytes	favicon.ico
238574	194.61.24.102	application/x-msdos-program	7168 bytes	coreupdater.exe
327366	194.61.24.102	text/html	228 bytes	\
339465	194.61.24.102	application/x-msdos-program	7168 bytes	coreupdater.exe

5. What was the initial entry vector (how did they get in)?

RDP Bruteforce , we can see in multiple time attacker trying to access the server,

Time	Source	s port	Destination	d port	Protocol	Length	Info
2020-09-18 22:24:06.968782	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.968815	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [PSH,
2020-09-18 22:24:06.968848	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [ACK]
2020-09-18 22:24:06.968871	204.79.197.200	443	10.42.85.10	62396	TLSv1.2	83	Application Data
2020-09-18 22:24:06.968893	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.968932	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969260	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [ACK]
2020-09-18 22:24:06.969287	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [PSH,
2020-09-18 22:24:06.969305	204.79.197.200	443	10.42.85.10	62396	TLSv1.2	1315	Application Data
2020-09-18 22:24:06.969401	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969426	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969615	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [ACK]
2020-09-18 22:24:06.969643	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [ACK]
2020-09-18 22:24:06.969660	204.79.197.200	443	10.42.85.10	62396	TLSv1.2	1315	Application Data
2020-09-18 22:24:06.969680	204.79.197.200	443	10.42.85.10	62396	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969696	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969720	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969757	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [PSH,
2020-09-18 22:24:06.969779	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969818	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.969997	204.79.197.200	443	10.42.85.10	62396	TLSv1.2	1315	Application Data
2020-09-18 22:24:06.970077	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]
2020-09-18 22:24:06.970172	204.79.197.200	443	10.42.85.10	62396	TCP	1514	443 → 62396 [ACK]
2020-09-18 22:24:06.970203	204.79.197.200	443	10.42.85.10	62396	TLSv1.2	1335	Application Data
2020-09-18 22:24:06.970254	10.42.85.10	62396	204.79.197.200	443	TCP	60	62396 → 443 [ACK]

6. Was malware used? If so what was it? If there was malware answer the following:
- What process was malicious? C:\Windows\System32\coreupdater.exe
 - Identify the IP Address that delivered the payload.

10.45.85.10 to 194.61.24.102(server)

Time	Source	s port	Destination	d port	Protocol	Length	Info
2020-09-18 22:24:06.915818	284.79.197.200	443	10.42.85.10	62396	TCP	54	443 → 62396 [ACK]
2020-09-18 22:24:06.933825	194.61.24.102	40238	10.42.85.10	3389	TLSv1.2	151	Application Data
2020-09-18 22:24:06.938844	10.42.85.10	62410	194.61.24.102	80	TCP	66	62410 → 80 [SYN,
2020-09-18 22:24:06.938893	10.42.85.10	62409	194.61.24.102	80	TCP	66	62409 → 80 [SYN,
2020-09-18 22:24:06.939039	194.61.24.102	80	10.42.85.10	62410	TCP	66	80 → 62410 [SYN,
2020-09-18 22:24:06.939062	194.61.24.102	80	10.42.85.10	62409	TCP	66	80 → 62409 [SYN,
2020-09-18 22:24:06.939193	10.42.85.10	62410	194.61.24.102	80	TCP	60	62410 → 80 [ACK]
2020-09-18 22:24:06.939223	10.42.85.10	62409	194.61.24.102	80	TCP	60	62409 → 80 [ACK]
2020-09-18 22:24:06.939239	10.42.85.10	62410	194.61.24.102	80	HTTP	291	GET /coreupdater.

> Frame 238559: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: VMware_e1:84:e6 (00:0c:29:e1:84:e6), Dst: VMware_95:cd:21 (00:0c:29:95:cd:21)
> Internet Protocol Version 4, Src: 10.42.85.10, Dst: 194.61.24.102
Transmission Control Protocol, Src Port: 62410, Dst Port: 80, Seq: 0, Len: 0
Source Port: 62410
Destination Port: 80
[Stream index: 30453]
[TCP Segment Len: 0]
Sequence number: 0 (relative sequence number)
[Next sequence number: 0 (relative sequence number)]
Acknowledgment number: 0

```

0000  00 0c 29 95 cd 21 00 0c 29 e1 84 e6 08 00 45 02  ..)!.. ).... E.
0010  00 34 5e 50 40 00 80 06 62 9a 0a 2a 55 0a c2 3d  .4^P@... b.*U...
0020  18 66 f3 ca 00 50 67 70 65 96 00 00 00 80 c2  .f... Pgp .....
0030  ff ff 73 57 00 00 02 04 05 b4 01 03 03 08 01 01  .sW.... ...
0040  04 02

```


The screenshot shows a web interface for a security tool. At the top, it displays the IP address 194.61.24.102 with a note that 3 security vendors flagged it as malicious. Below this, it shows the IP's location as 194.61.24.102 (194.61.24.0/22) and AS 38994 (ERA LLC). A flag indicates it's from Russia (RU). The interface includes tabs for DETECTION, DETAILS, RELATIONS, and COMMUNITY. Under DETECTION, several sources are listed with their findings: CRDF (Malicious), Ipsum (Malicious), Abusix (Clean), ADMINUSLabs (Clean), AlienVault (Clean), GreenSnow (Malicious), 0xSl_F33d (Clean), Acronis (Static ML) (Clean), AICC (MONITORAPP) (Clean), and alphaMountain.ai (Clean).

c. What IP Address is the malware calling to?

204.79.197.200

The screenshot shows a Wireshark capture window titled "case001.pcap" with a filter applied to "ip.addr eq 10.42.85.10". The packet list shows several TCP connections between 10.42.85.10 and 194.61.24.102. A specific GET request is highlighted in blue, showing the URL "/coreupdater". The details and bytes panes provide more information about the selected packet.

d. Where is this malware on disk?

C:\Windows\system32\ extract from autorun

4/14/2010 3:06

PM,"HKLM\System\CurrentControlSet\Services","coreupdater",enabled,"Services",System-wide,"coreupdater:

"","","c:\windows\system32\coreupdater.exe","","C:\Windows\System32\coreupdater.exe",
EED41B4500E473F97C50C7385EF5E374,FD153C66386CA93EC9993D66A84D6F0D
129A3A5C,C3E46C6242056ACE3217A5314CFF2063BE8E9799,88763E60ED00AFD
A80A61647782B597542D9667D2B9A35FB2623967E302FA28E,10F3B92002BB98467
334161CF85D0B1730851F9256F83C27DB125E9A0C1CFDA6,B4C6FFF030479AA3B
12625BE67BF4914

autodesk_cadkey_401 - Microsoft Excel [Product Activation Failed]	
File Home Insert Page Layout Formulas Data Review View	
A24	4/14/2019 3:06 PM,"HKLM\System\CurrentControlSet\Services","coreupdater",enabled,"Services","System-wide",coreupdater:
7	3/1/2014 10:32 PM,"HKLM\Software\Classes\Shell\Open\Command\Default","C:\Program Files\Internet Explorer\explorer.exe",enabled,"Hijacks","System-wide","Internet Explorer","[Verified] Microsoft Corporation","Microsoft Corporation","c:\v
8	9/18/2020 9:39 PM,"HKLM\System\CurrentControlSet\Services_,"Services","System-wide",
8	8/22/2013 1:27 AM,"HKLM\System\CurrentControlSet\Services_,"Services","System-wide",
8	8/22/2013 1:27 AM,"HKLM\System\CurrentControlSet\Services_,"Services","System-wide",
10	8/22/2014 5:02 AM,"HKLM\System\CurrentControlSet\Services_,"AeLookupSvc",enabled,"Services","System-wide","Application Experience: Processes application compatibility cache requests for applications as they are launched","[Verified] Microsoft Windows"
11	8/22/2013 2:53 AM,"HKLM\System\CurrentControlSet\Services_,"ALG",enabled,"Services","System-wide","Application Layer Gateway Service: Provides support for 3rd party protocol plug-ins for Internet Connection Sharing","[Verified] Microsoft Windows","\v
12	8/22/2013 4:01 AM,"HKLM\System\CurrentControlSet\Services_,"AppDsvc",enabled,"Services","System-wide","Application Identity: Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.",\v
13	2/22/2014 5:06 AM,"HKLM\System\CurrentControlSet\Services_,"AppInfo",enabled,"Services","System-wide","Application Information: Facilitates the running of interactive applications with additional administrative privileges.
14	8/22/2013 4:18 AM,"HKLM\System\CurrentControlSet\Services_,"AppMgmt",enabled,"Services","System-wide","Application Management: Processes installation, removal, and enumeration requests for software deployed through Group Policy. If the service is
15	12/10/2013 12:35 AM,"HKLM\System\CurrentControlSet\Services_,"AppReadiness",enabled,"Services","System-wide","App Readiness: Gets apps ready for use the first time a user signs in to this PC and when adding new apps.","[Verified] Microsoft Windows",
16	2/22/2014 1:32 AM,"HKLM\System\CurrentControlSet\Services_,"AppXvc",enabled,"Services","System-wide","AppX Deployment Service (AppXVC): Provides infrastructure support for deploying Store applications. This service is started on demand and if disabled, it will prevent Store applications from launching.",
17	2/22/2014 2:23 AM,"HKLM\System\CurrentControlSet\Services_,"AudioEndpointBuilder",enabled,"Services","System-wide","Windows Audio Endpoint Builder: Manages audio devices for the Windows Audio service. If this service is stopped, audio devices and effects will not function properly. If this service is disabled, audio devices and effects will not function properly. If thi
18	2/22/2014 2:05 AM,"HKLM\System\CurrentControlSet\Services_,"Audiosrv",enabled,"Services","System-wide","Windows Audio Manager: Manages audio for Windows-based programs. If this service is stopped, audio devices and effects will not function properly. If thi
19	10/12/2013 2:48 PM,"HKLM\System\CurrentControlSet\Services_,"BFE",enabled,"Services","System-wide","Base Filtering Engine: The Base Filtering Engine (BFE) is a service that manages firewall and Internet Protocol (IPsec) policies and implements them in the background. If the service is disabled, then any applications that run in the background will not be able to use IPsec.
20	8/22/2013 3:19 AM,"HKLM\System\CurrentControlSet\Services_,"BITS",enabled,"Services","System-wide","Background Intelligent Transfer Service: Transfers files in the background using idle network bandwidth.
21	2/22/2014 2:25 AM,"HKLM\System\CurrentControlSet\Services_,"BrokerInfrastructure",enabled,"Services","System-wide","Background Tasks Infrastructure Service: Windows infrastructure service that controls which background tasks can run on the system.",
22	8/22/2013 4:05 AM,"HKLM\System\CurrentControlSet\Services_,"CertPropSvc",enabled,"Services","System-wide","Certificate Propagation: Copies user certificates and root certificates from smart cards into the current user's certificate store, detects when a certificate changes, and updates other certificates in the store.",
23	8/22/2013 2:54 AM,"HKLM\System\CurrentControlSet\Services_,"COMSysApp",enabled,"Services","System-wide","COM+ System Application: Manages the configuration and tracking of Component Object Model (COM+) based components. If the service is stopped, COM+ based applications will not work.",
24	4/14/2010 3:06 PM,"HKLM\System\CurrentControlSet\Services_,"CoreUpdater_,"c:\windows\system32\coreupdater.exe","C:\Windows\System32\coreupdater.exe",EED41B4500E4739F7C50C7385E5E37,
25	8/22/2013 3:01 AM,"HKLM\System\CurrentControlSet\Services_,"CryptSvc",enabled,"Services","System-wide","Cryptographic Services: Provides three management services: Catalog Database Service, which confirms the signatures of Windows files and allows

```
c:\DesktopAmcache.txt - Notepad
File Edit Format View Help

c:\program files\windowsapps\microsoft.heifimageextension_1.0.22742.0_x64_8wekyb3d8bbwe\codecpacks.heif.exe LastWrite: 2020-09-19 01:32:03Z
Hash: b0cd612ef49b1ec2a4125bc8c183ac5f47ea030

c:\program files\windowsapps\microsoft.vp9videextensions_1.0.22681.0_x64_8wekyb3d8bbwe\codecpacks.vp9.exe LastWrite: 2020-09-19 01:32:09Z
Hash: 906b67339d15be5f776014f1d5bd7a35eca6e4ec

c:\program files\windowsapps\microsoft.webpimageextension_1.0.22753.0_x64_8wekyb3d8bbwe\codecpacks.webp.exe LastWrite: 2020-09-19 01:32:10Z
Hash: 8637d99fa3bc034b37a1870d456445f117f36215

c:\windows\system32\compatelrunner.exe LastWrite: 2020-09-18 04:58:06Z
Hash: 992aaab7a56c5447a2d5209d3135e1f9494a97d5

c:\program files\common files\vmware\drivers\vss\comreg.exe LastWrite: 2020-09-19 01:32:13Z
Hash: 0d564796c79e87ccb49af7b8b0a9369363ff2c8c

c:\windows\system32\coreupdater.exe LastWrite: 2020-09-19 03:40:45Z
Hash: fd153c66386ca93ec9993d66a84d6f0d129a3a5d
```

Parse with Reg ripper

Σ 10f3b92002bb9846733416cf85d0b1730851f9256f83c27db125e9a0c1cfda6

55 security vendors flagged this file as malicious

10f3b92002bb9846733416cf85d0b1730851f9256f83c27db125e9a0c1cfda6 coreupdater.exe 700 KB Size 2021-09-22 16:09:18 UTC 1month ago EXE

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Acronis (Static ML)	Suspicious		Ad-Aware	Trojan.Metasploit.A
AhnLab-V3	Trojan.Win64.RL_Shelma.R298109		Alibaba	Trojan.Win64/Shelma.a548c020
ALYac	Trojan.Metasploit.A		Anti-AVL	Trojan.Generic.ASBL.C673
SecureAge APEX	Malicious		Avast	Win64-MetasploitEncod-A [Tr]
AVG	Win64-MetasploitEncod-A [Tr]		Avira (no cloud)	TR/Crypt.XPACK.Gen?
BitDefender	Trojan.Metasploit.A		CAT-QuickHeal	HackTool.Metasploit.S9212471
Comodo	Malware@#3k99ps66sbl		CrowdStrike Falcon	WinMalicious_confidence_100% (W)
Cylance	Unsafe		Cynet	Malicious (score: 100)
Cyren	W64/Shelma.A		DrWeb	BackDoor.Shell.244
Elastic	Malicious (high Confidence)		Emsisoft	Trojan.Metasploit.A (B)
eScan	Trojan.Metasploit.A		ESET-NOD32	A Variant Of Win64/Rozena.M
FireEye	Generic.mg.eadfb4500e4739f		Fortinet	W64/Rozena.CIJfr
GData	Trojan.Metasploit.A		Gridinsoft	Trojan.Win64.ShellCode.sds1

Result from virustotal.com

- e. When did it first appear?

18 sept 2020 @22.24.06.939239

The screenshot shows a NetworkMiner capture window. At the top, a table lists network traffic with columns for Time, Source, Destination, Port, Protocol, Length, and Info. Several entries are highlighted in green, indicating they are related to the current analysis. Below the table, a detailed view of a selected GET request to 'coreUpdater.exe' is shown. The request details include the method (GET), URI (/coreUpdater.exe), version (HTTP/1.1), headers (Accept: */*, Accept-Encoding: gzip, deflate, User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko, Host: 194.61.24.102), and the raw hex and ASCII payloads. The ASCII payload shows the file's content.

f. Did someone move it?

Its moved from download folder to C:/windows/system32/administration folder

g. What were the capabilities of this malware?

Deleting and moving files from one folder to another, deleted some files moved to recycle bin

The screenshot shows the Autopsy 4.20.0 forensic analysis interface. On the left, a tree view displays various file types and artifacts found on the system. The main pane shows a table of deleted files from the Recycle Bin, with one entry selected: '\$RU2L112.txt' from 'C:\FileShare\Secret\SECRET_beth.txt'. Below the table, a detailed view of this artifact shows its path ('C:\FileShare\Secret\SECRET_beth.txt'), time deleted ('2020-09-18 23:34:27 EDT'), and other metadata. The bottom status bar indicates the analysis is 59% complete.

- h. Is this malware easily obtained? Yes

Using Autopsy tool by checking web history and autoruns, we can easily find out it.

The screenshot shows the Szechuan - Autopsy 4.2.0 interface. The top menu bar includes Case, View, Tools, Window, Help, and several icons for adding data sources, images/videos, communications, geolocation, timeline, and keyword lists. A search bar at the top right contains "Keyword Search".

The left sidebar displays a tree view of the analysis session:

- Data Sources
 - 20200918_0347_CD**rive.E01**
 - 20200918_0347_CD**rive**
- File Views
 - File Types
 - Deleted Files
 - File System (3154)
 - All (3154)
- MB File Size
- Data Artifacts
 - Installed Programs (58)
 - Operating System Information
 - Recent Documents (30)
 - Recycle Bin (2)
 - Shell Bags (50)
 - USB Device Attached (12)
 - Web Bookmarks (2)
 - Web Cookies (2)
 - Web History (16) **(selected)**
- Analysis Results
 - Encryption Suspected (1)
 - Extension Mismatch Detect
 - Keyword Hits (16) **(selected)**
- OS Accounts
- Tags
- Reports

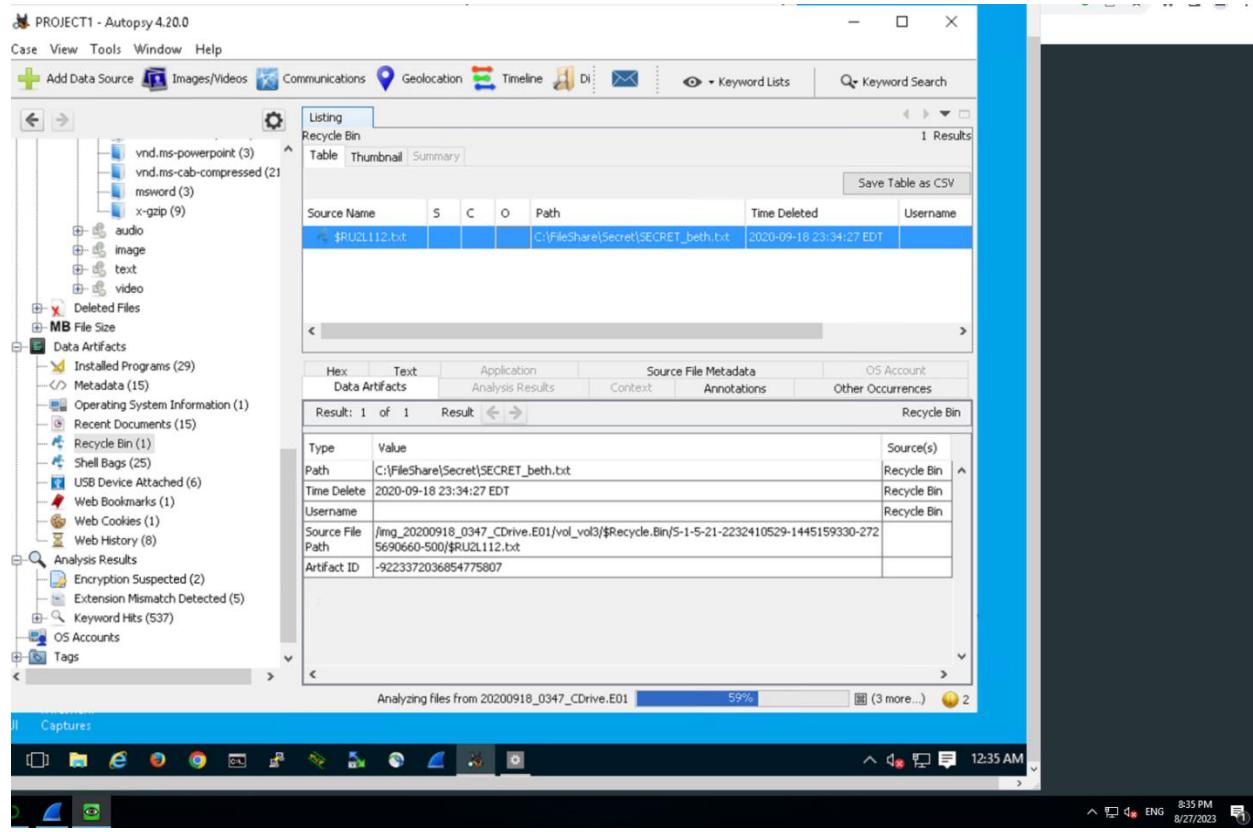
The main pane shows a "Listing" view for "Web History". It includes tabs for Table, Thumbnail, and Summary, with "Table" selected. A "Save Table as CSV" button is in the top right. The results table has columns: Source Name, S, C, O, URL, Date Accessed, and Proc. The table lists 16 entries, all of which are "WebCacheV01.dat" files. The URLs correspond to various local files and network shares, such as http://194.61.24.102/, file:///C:/FileShare/Secret/PortalGunPlans.txt, and file:///C:/FileShare/Secret/Szechuan%20Sauce.txt.

At the bottom, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The "Text" tab is selected. Below the tabs are buttons for Strings, Indexed Text, and Translation. The footer shows "Page: 1 of 1" and "Script: Latin - Basic". The status bar at the bottom indicates "Analyzing files from 20200918_0347_CD**rive.E01**" and "2% (7 more...)".

- i. Was this malware installed with persistence on any machine? Yes

When: 4/14/2010 @ 3:06pmEDT

Where: **HKLM/system/currentcontrolset/services**



Hash integrity has been checked using virus total tool

For memory.zip

Basic properties ⓘ

MD5	64a4e2cb47138084a5c2878066b2d7b1
SHA-1	e8dd11314a2501dc0ad98901a321350d9cd111c2
SHA-256	86658d85d8254e8d30dcc4f50d9c2a8b550a101d2e78a6d932316849e37ad80
Vhash	0b3e31f3da0a40321716410a2ab4616f
SSDEEP	12582912:H8xocBlyVnRyMhq6vKFU9HW9JlkwtZ0zC:HG7BlmRvP2U9aPc
TLSH	T1D5493381F412B50DDFEA6675EEC27A5EEA0C0C1F49575C64EF71314820EAEE0BF1264A
File type	ZIP compressed zip
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	535.42 MB (561424278 bytes)

For autoruns.zip

Basic properties ⓘ

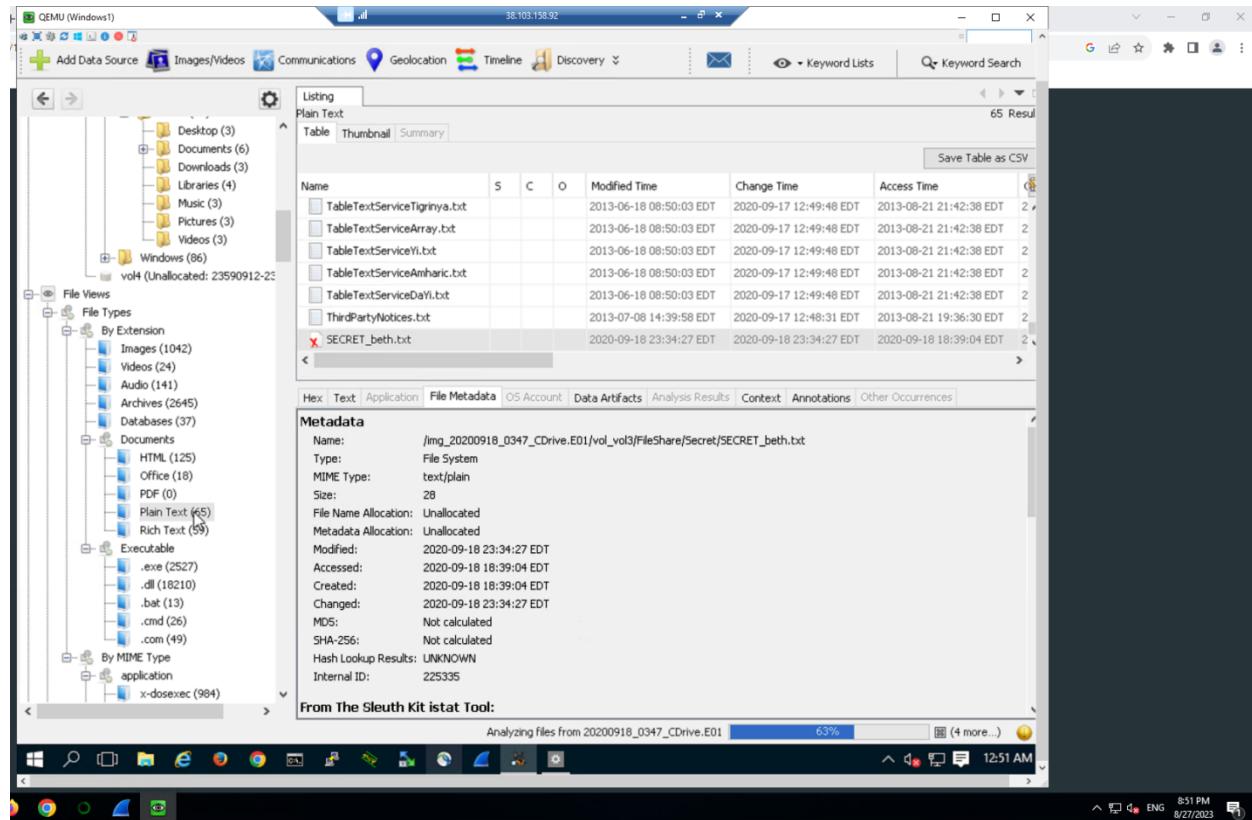
MD5	964eeaf0009d08cc101de4a83a4e5d23
SHA-1	257c2ab4f1916ae9b5ed8e9c8486e48a39042c97
SHA-256	b1db1979b290cf5c954c1965c5e7834259bb8e3e88327d7f6d68b20e4c7cd5b9
Vhash	152d458dfec368b9f3912809dcee648d
SSDEEP	393216:q4RZZL+SDy9T51Ho1wVXf6lckb3tdCO4KJeQ8akMIXI3dAfg16E:jRZrMywZ03TC7k/vJXInd
TLSH	T168D62268F471B965F488C27646B02CF5C7AC6D70C3BA2AC61F30715BAA97A0D4F79870
File type	ZIP compressed zip
Magic	Zip archive data, at least v2.0 to extract
TrID	ZIP compressed archive (80%) PrintFox/Pagefox bitmap (640x800) (20%)
File size	12.91 MB (13540216 bytes)

Partitioning of disk

The screenshot shows the EnCase Forensic software interface. On the left, the 'Data Sources' tree view shows a mounted disk image named '20200918_0347_CDdrive.E01'. The tree displays various partitions and their contents, including 'vol1' (Unallocated), 'vol2' (NTFS / exFAT), 'vol3' (NTFS / exFAT), and 'vol4' (Unallocated). The main pane displays a table titled 'Listing' for the 'Table' tab, showing the following data:

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-718847)	2	2048	716800	NTFS / exFAT (0x07)	Allocated
vol3 (NTFS / exFAT (0x07): 718848-23590911)	3	718848	22872064	NTFS / exFAT (0x07)	Allocated
vol4 (Unallocated: 23590912-23592999)	4	23590912	2048	Unallocated	Unallocated

At the bottom of the interface, a status bar indicates 'Analyzing files from 20200918_0347_CDdrive.E01' and shows the progress bar is at 62% completion.



7. What malicious IP Addresses were involved? 194.61.24.102 and 203.78.103.109

Time	Source	port	Destination	d port	Protocol	Length	Info
2020-09-18 22:23:41.731918	10.42.85.10	62408	194.61.24.102	80	HTTP	302	GET / HTTP/1.1
2020-09-18 22:23:41.797123	10.42.85.10	62407	194.61.24.102	80	HTTP	255	GET /favicon.ico HTTP/1.1
2020-09-18 22:24:06.939239	10.42.85.10	62410	194.61.24.102	80	HTTP	291	GET /coreupdater.exe
2020-09-18 22:39:26.939207	10.42.85.115	50840	194.61.24.102	80	HTTP	428	GET / HTTP/1.1
2020-09-18 22:39:58.410684	10.42.85.115	50864	194.61.24.102	80	HTTP	352	GET /coreupdater.exe

GET /coreupdater.exe HTTP/1.1\r\n
 [Expert Info (Chat/Sequence): GET /coreupdater.exe HTTP/1.1\r\n]
 Request Method: GET
 Request URI: /coreupdater.exe
 Request Version: HTTP/1.1
 Accept: */*\r\n
 Referer: http://194.61.24.102/\r\n
 Accept-Encoding: gzip, deflate\r\n
 User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
 Host: 194.61.24.102\r\n

```
0080 0d 0a 41 63 63 65 70 74 2d 45 6e 63 6f 64 69 6e  .Accept -Encoding
0090 67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 61 74 65  g: gzip, deflate
00a0 0d 0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 4d 6f  ..User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64)
00b0 7a 69 6c 6e 61 2f 35 2e 30 20 28 57 69 6e 64 6f  zilla/5.0 (Windows NT 6.3; WOW64)
00c0 77 73 20 4e 54 20 36 2e 33 3b 20 57 4f 57 36 34  ws NT 6.3; WOW64
00d0 3b 20 54 72 69 64 65 66 74 2f 37 2e 30 3b 20 72 ; Trident/7.0; rv:11.0
00e0 76 3a 31 31 2e 30 29 20 6c 69 6b 65 20 47 65 63 v:11.0) like Gecko
00f0 6b 6f 0d 0a 48 6f 73 74 3a 20 31 39 34 2e 36 31 ko..Host : 194.61
0100 2e 32 34 2f 31 30 32 0d 0a 43 6f 6e 65 63 74 .24.102. -Connect
0110 69 6f 6e 3a 20 4b 65 65 70 2d 41 6c 69 76 65 0d ion: Kee-Alive.
```

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.2.4	203.78.103.109	TCP	66	49690 → 443 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM
2	0.000098	203.78.103.109	192.168.2.4	TCP	66	443 → 49690 [SYN, ACK] Seq=1 Win=64240 Len=0 MSS=1460 SACK_PERM
3	0.000193	192.168.2.4	203.78.103.109	TCP	60	49690 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0



- a. Were any IP Addresses from known adversary infrastructure?

Yes. 194.61.24.102 At the time this lab was released, it was being tracked as a hostile IP address, specifically being tracked as being involved in RDP Brute Force attacks.

However, we were unable to locate any information that reflected hostile statuses at the time that we completed this assignment. It has since been reported as not being involved. Checking virus total.

- b. Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?

No, we could not locate any proof that this adversarial infrastructure was present during any simultaneous attacks. The IP address delivering the CoreUpdater.exe file was 194.61.24.102 and the malware was calling back to an IP in Thailand 203.78.103.109.

8. Did the attacker access any other systems?

Tools Used: TCPDump

- a. How?

The Desktop machine, Desktop-SDN1RPT, was accessed by the attacker using RDP. The attacker Brute Forced the password for the Administrator account on the DC. Once inside the DC they opened a second RDP session from within the Domain Controller to the Desktop machine re-using the same credentials. We can see this using the following tcpdump of the pcap file.

```
sansforensics@siftworkstation: ~/Downloads/Case_001
$ tcpdump -ntttr case001.pcap 'tcp port 3389 and (src net 10.42.85.0/24 and dst net 10.42.85.0/24)' -c15
reading from file case001.pcap, link-type EN10MB (Ethernet)
2020-09-19 02:35:55.285340 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [SEW], seq 3934789806, win 8192, options [mss 1460,nop,wscale 8,nop,nop,sackOK], length 0
2020-09-19 02:35:55.285340 IP 10.42.85.10.62514 > 10.42.85.10.62514: Flags [S.], seq 3456387165, ack 3934789807, win 64000, options [mss 1460,nop,wscale 0,nop,nop,sackOK], length 0
2020-09-19 02:35:55.285680 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [.], ack 1, win 256, length 0
2020-09-19 02:35:55.285950 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [P.], seq 1, ack 1, win 256, length 19
2020-09-19 02:35:55.286000 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [P.], seq 1, ack 20, win 64000, length 19
2020-09-19 02:35:55.286040 IP 10.42.85.115.3389 > 10.42.85.10.62514: Flags [.], ack 1, seq 1, win 256, length 0
2020-09-19 02:35:55.364696 IP 10.42.85.115.3389 > 10.42.85.10.62514: Flags [P.], seq 1, ack 20, win 63981, length 19
2020-09-19 02:35:55.417848 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [.], ack 20, win 256, length 0
2020-09-19 02:36:23.466171 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [P.], seq 20:200, ack 20, win 256, length 180
2020-09-19 02:36:23.466891 IP 10.42.85.115.3389 > 10.42.85.10.62514: Flags [P.], seq 20:884, ack 200, win 63801, length 864
2020-09-19 02:36:23.467377 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [P.], seq 290:519, ack 884, win 253, length 319
2020-09-19 02:36:23.471064 IP 10.42.85.115.3389 > 10.42.85.10.62514: Flags [P.], seq 884:935, ack 518, win 63483, length 51
2020-09-19 02:36:23.476018 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [P.], seq 518:796, ack 935, win 252, length 188
2020-09-19 02:36:23.477273 IP 10.42.85.115.3389 > 10.42.85.10.62514: Flags [P.], seq 935:2156, ack 706, win 63295, length 1221
2020-09-19 02:36:23.482075 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [.], seq 706:2166, ack 2156, win 256, length 1460
2020-09-19 02:36:23.482079 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [P.], seq 2166:2307, ack 2156, win 256, length 141
```

- b. When?

Tools Used: Autopsy

The compromised Domain Administrator account initiated a connection to the

Desktop-SDN1RPT machine from Domain Controller, CITADEL-DC01, at 02:35:55 UTC on 19 September 2020 according to the PCAP, or 03:35:54 on 19 September 2020 according to the Super Timeline when left uncorrected. In reality, it was at 02:35:54 UTC.

The malware was then downloaded at 03:23 on 19 Sept. This info was found in the web cache in the server disk image using Autopsy.

File	Path	Size	Content	Timestamp	Analyzer	IP Address	User	Event ID
WebCacheV01.dat		1	http://194.61.24.102/favicon.ico	2020-09-19 03:23:41 PDT	Microsoft Edge Analyzer	194.61.24.102	Administrator	20200918_0347_CDrive
WebCacheV01.dat		res://iesetup.dll!/hardAdmin.htm		2020-09-19 03:23:01 PDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive
WebCacheV01.dat		1	https://login.live.com/oauth20_authorize.srf?client_id=00000000480728...	2020-09-19 03:16:26 PDT	Microsoft Edge Analyzer	live.com	Admin	20200918_0417_DESKTOP
WebCacheV01.dat		1	https://login.live.com/oauth20_desktop.srf?lc=1033	2020-09-19 03:16:25 PDT	Microsoft Edge Analyzer	live.com	Admin	20200918_0417_DESKTOP
WebCacheV01.dat		0	https://www.reddit.com/?count=25&after=t3_iv2tpq	2020-09-18 23:08:34 PDT	Microsoft Edge Analyzer	reddit.com	mortysmith	20200918_0417_DESKTOP
WebCacheV01.dat		0	https://www.reddit.com/?count=25&after=t3_iv2tpq	2020-09-18 23:08:33 PDT	Microsoft Edge Analyzer	reddit.com	mortysmith	20200918_0417_DESKTOP
WebCacheV01.dat		0	https://zh.wikipedia.org/wiki/Wikipedia:%E5%85%B3%E4%BA%8E	2020-09-18 23:08:26 PDT	Microsoft Edge Analyzer	wikipedia.org	mortysmith	20200918_0417_DESKTOP
WebCacheV01.dat		0	https://donate.wikimedia.org/	2020-09-18 23:08:24 PDT	Microsoft Edge Analyzer	wikimedia.org	mortysmith	20200918_0417_DESKTOP
WebCacheV01.dat		0	https://donate.wikimedia.org/w/index.php?title=Special:LandingPage&co...	2020-09-18 23:08:24 PDT	Microsoft Edge Analyzer	wikimedia.org	mortysmith	20200918_0417_DESKTOP
WebCacheV01.dat		0	https://www.w3.org/2002/07/owl/imports.ttl	2020-09-18 23:08:24 PDT	Microsoft Edge Analyzer	w3.org	mortysmith	20200918_0417_DESKTOP

Hex Text Application Source File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 7 of 8 Result ← → Web History

Visit Details

Username: Administrator
Date Accessed: 2020-09-19 03:23:41 PDT
Domain: 194.61.24.102
URL: http://194.61.24.102/favicon.ico
Program Name: Microsoft Edge Analyzer

c. Did the attacker steal or access any data?

Yes, the attacker was able to access several sensitive files on the system, both on the server and the desktop. Beth_Secret.txt, Szechuan%20Sauce.txt, SECRET_beth.txt, PortalGunPlans.txt from the Server. This was logged in the web cache. From the desktop, Thoughts.txt, loot.zip, PLans.txt, and My%20Social%20Security.... were extracted.

WebCacheV01.dat		file:///C:/FileShare/Secret/Beth_Secret.txt	2020-09-19 03:35:07 PDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		file:///C:/FileShare/Secret/Szechuan%20sauce.txt	2020-09-19 03:32:21 PDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		file:///C:/FileShare/Secret/SECRET_beth.txt	2020-09-19 03:32:13 PDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		file:///C:/FileShare/Secret/PortalGunPlans.txt	2020-09-19 03:32:02 PDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01

When?

Loot.zip was downloaded at around 03:46 along with other files as shown in the screenshot below. This was from the DESKTOP.

WebCacheV01.dat	file:///C:/Users/mortysmith/Desktop/Thoughts.txt	2020-09-19 03:47:39 PDT	Microsoft Edge Analyzer		Administrator	20200918_0417_DESKTOP-SDNIRPT.E01
WebCacheV01.dat	file:///C:/Users/mortysmith/Documents/loot.zip	2020-09-19 03:46:18 PDT	Microsoft Edge Analyzer		Administrator	20200918_0417_DESKTOP-SDNIRPT.E01
WebCacheV01.dat	file:///C:/Users/mortysmith/Documents/Plans.txt	2020-09-19 03:45:39 PDT	Microsoft Edge Analyzer		Administrator	20200918_0417_DESKTOP-SDNIRPT.E01
WebCacheV01.dat	file:///C:/Users/mortysmith/Documents/My%20Social%20Security....	2020-09-19 03:45:34 PDT	Microsoft Edge Analyzer		Administrator	20200918_0417_DESKTOP-SDNIRPT.E01

9. What was the network layout of the victim network?

The network layout you provided is a small local area network (LAN) with a subnet of 10.42.85.0/24. This means the network can accommodate up to 256 IP addresses (from 10.42.85.0 to 10.42.85.255), where the first three octets (10.42.85) represent the network address, and the last octet can be assigned to individual devices.

In this network, there are two hosts:

Domain Controller (DC): Its IP address is 10.42.85.10. The Domain Controller is a server responsible for managing user authentication and granting access to network resources in a Windows domain environment.

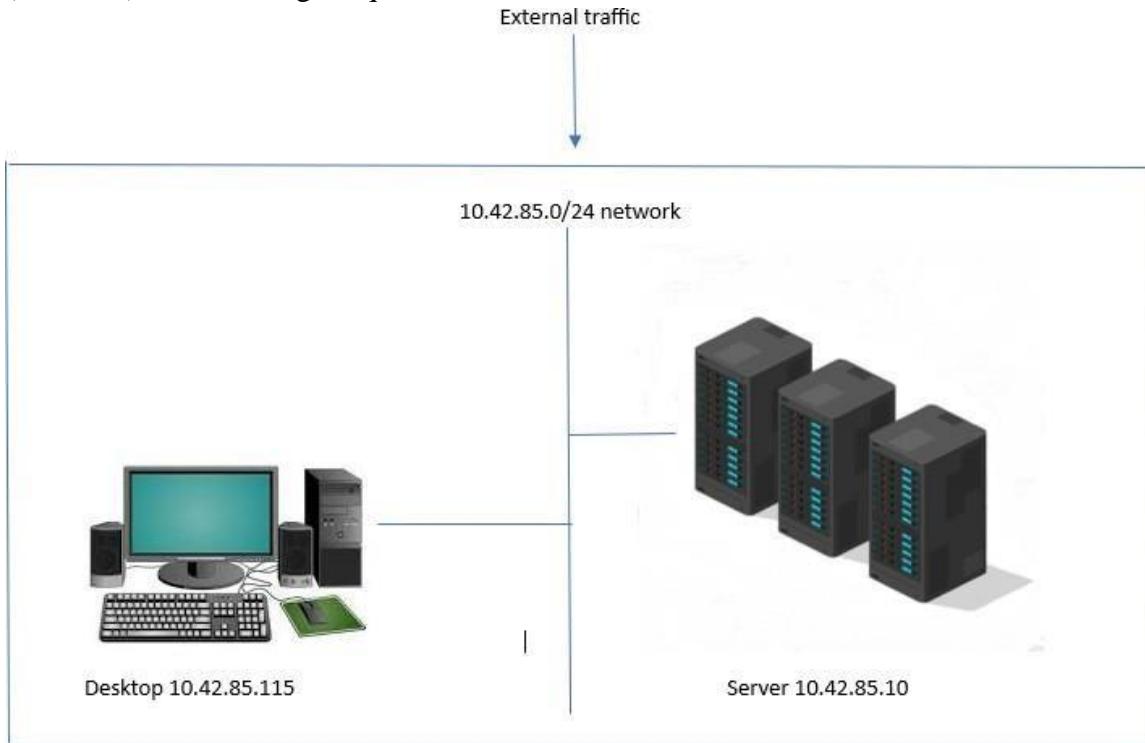
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dx)	Flags(Meta)	Known	Location
PP				2013-09-22 09:29:29 EDT	2020-09-17 13:57:13 EDT	2013-08-22 09:29:29 EDT	2013-08-22 09:29:29 EDT	164	Allocated	Allocated	Unknown	Img_2020
netlogon.drb	1			2020-09-18 21:29:42 EDT	2020-09-10 21:29:22 EDT	2020-09-17 13:57:54 EDT	2020-09-17 13:57:54 EDT	6288	Allocated	Allocated	Unknown	Img_2020
netlogon.dns	1			2020-09-18 21:29:42 EDT	2020-09-10 21:29:22 EDT	2020-09-17 13:57:54 EDT	2020-09-17 13:57:54 EDT	2193	Allocated	Allocated	Unknown	Img_2020
SAM	1			2020-09-18 01:02:29 EDT	2020-09-17 13:56:13 EDT	2020-09-18 10:53:53 EDT	2020-09-18 10:53:53 EDT	262144	Allocated	Allocated	Unknown	Img_2020
SAMLOG1	1			2013-09-22 09:25:49 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	12288	Allocated	Allocated	Unknown	Img_2020
SAMLOG2	1			2020-09-18 19:10:53 EDT	2020-09-17 13:56:13 EDT	2013-09-18 10:53:53 EDT	2013-08-22 09:25:30 EDT	16394	Allocated	Allocated	Unknown	Img_2020
SECURITY	0			2013-09-22 09:25:30 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	0	Allocated	Allocated	Unknown	Img_2020
SECURITY_LOG	1			2013-09-22 09:25:30 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	8192	Allocated	Allocated	Unknown	Img_2020
SECURITY_LOG2	1			2013-09-22 09:25:30 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	8192	Allocated	Allocated	Unknown	Img_2020
SOFTWARE	1			2020-09-18 19:10:53 EDT	2020-09-17 13:56:13 EDT	2020-09-18 10:53:53 EDT	2013-09-22 09:25:30 EDT	4597620	Allocated	Allocated	Unknown	Img_2020
SOFTWARE_LOG	0			2013-09-22 09:25:30 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	0	Allocated	Allocated	Unknown	Img_2020
SOFTWARE_LOG1	1			2013-09-22 09:25:30 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	807136	Allocated	Allocated	Unknown	Img_2020
SOFTWARE_LOG2	1			2013-09-22 09:25:30 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	4014080	Allocated	Allocated	Unknown	Img_2020
SYSTEM	1			2020-09-18 19:10:53 EDT	2020-09-17 13:56:13 EDT	2020-09-18 10:53:53 EDT	2013-08-22 09:25:30 EDT	1289504	Allocated	Allocated	Unknown	Img_2020
SYSTEM.LOG	0			2013-09-22 09:25:30 EDT	2020-09-17 13:56:13 EDT	2013-08-22 09:25:30 EDT	2013-08-22 09:25:30 EDT	0	Allocated	Allocated	Unknown	Img_2020

User/Desktop: Its IP address is 10.42.85.115. This is a typical user's desktop computer or workstation that connects to the network to access shared resources and services provided by the Domain Controller.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dx)	Flags(Meta)	Known	Location
ELAM(5:3b:9eac:3lc:k4-11ea-a811-000d3ae%92b),TMCcenter00	3			2020-09-16 01:41:57 EDT	2020-09-10 01:41:57 EDT	2020-09-19 01:41:57 EDT	2020-09-18 01:41:56 EDT	524298	Allocated	Allocated	Unknown	Img_2020
netlogon.fl	1			2020-09-19 01:08:15 EDT	2020-09-19 01:08:15 EDT	2020-09-19 01:08:15 EDT	2020-09-18 17:42:16 EDT	112	Allocated	Allocated	Unknown	Img_2020
SAM	1			2020-09-18 21:09:37 EDT	2020-09-18 02:37:30 EDT	2020-09-19 01:38:37 EDT	2019-12-07 04:03:44 EDT	69536	Allocated	Allocated	Unknown	Img_2020
SAMLOG1	1			2019-12-07 04:03:44 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	69536	Allocated	Allocated	Unknown	Img_2020
SAMLOG2	1			2019-12-07 04:03:44 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	49152	Allocated	Allocated	Unknown	Img_2020
SECURITY	1			2020-09-18 21:08:37 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	32768	Allocated	Allocated	Unknown	Img_2020
SECURITY_LOG	1			2019-12-07 04:03:44 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	32768	Allocated	Allocated	Unknown	Img_2020
SOFTWARE	1			2020-09-18 21:08:37 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	6861728	Allocated	Allocated	Unknown	Img_2020
SOFTWARE_LOG	1			2019-12-07 04:03:44 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	117948	Allocated	Allocated	Unknown	Img_2020
SYSTEM	1			2019-12-07 04:03:44 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	959260	Allocated	Allocated	Unknown	Img_2020
SYSTEM.LOG1	1			2019-12-07 04:03:44 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	316792	Allocated	Allocated	Unknown	Img_2020
SYSTEM.LOG2	1			2019-12-07 04:03:44 EDT	2020-09-18 02:37:30 EDT	2019-12-07 04:03:44 EDT	2019-12-07 04:03:44 EDT	3148900	Allocated	Allocated	Unknown	Img_2020
COMPONENTS.LOG	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	Unknown	Img_2020
DRIVERS.LOG	0			0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0	Unallocated	Unallocated	Unknown	Img_2020

Both devices are within the same subnet (10.42.85.0/24), which means they can communicate directly with each other without the need for routing. The subnet mask (also

indicated by /24) ensures that all devices in the network share the same first three octets (10.42.85) while having unique values in the last octet.



References

<https://www.virustotal.com/gui/home/upload>

Autopsy User Documentation 4.0 <https://sleuthkit.org/autopsy/docs/user-docs/4.0/>

Comprehensive Guide on FTK Imager; Raj Chandel (November 6, 2020)

<https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/>

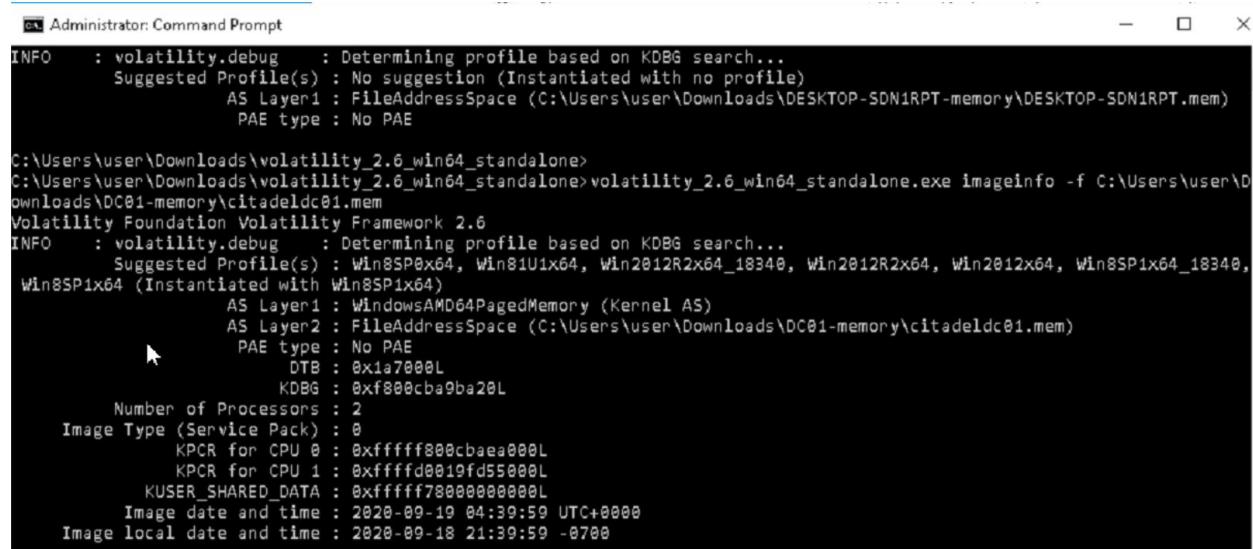
Volatility cheat sheet

https://downloads.volatilityfoundation.org/releases/2.4/CheatSheet_v2.4.pdf

Registry Explorer User Guide; Eric R. Zimmerman (May 19, 2017)

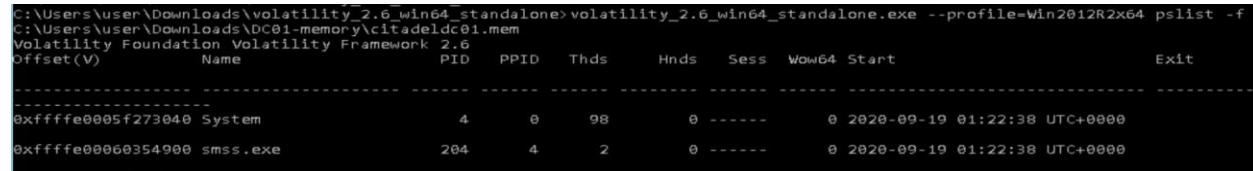
<https://www.oit.va.gov/Services/TRM/files/RegistryExplorerManual.pdf>

Appendix



```
Administrator: Command Prompt
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : No suggestion (Instantiated with no profile)
                        AS Layer1 : FileAddressSpace (C:\Users\user\Downloads\DESKTOP-SDN1RPT-memory\DESKTOP-SDN1RPT.mem)
                        PAE type : No PAE

C:\Users\user\Downloads\volatility_2.6_win64_standalone>
C:\Users\user\Downloads\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe imageinfo -f C:\Users\user\Downloads\DC01-memory\citadeldc01.mem
Volatility Foundation Volatility Framework 2.6
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win8SP0x64, Win8U1x64, Win2012R2x64_18340, Win2012R2x64, Win2012x64, Win8SP1x64_18340,
          Win8SP1x64 (Instantiated with Win8SP1x64)
                        AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
                        AS Layer2 : FileAddressSpace (C:\Users\user\Downloads\DC01-memory\citadeldc01.mem)
                        PAE type : No PAE
                        DTB : 0x1a7000L
                        KDBG : 0xf800cba9ba20L
          Number of Processors : 2
          Image Type (Service Pack) : 0
                        KPCR for CPU 0 : 0xfffff800cbaea000L
                        KPCR for CPU 1 : 0xfffffd0019fd5000L
                        KUSER_SHARED_DATA : 0xfffff78000000000L
          Image date and time : 2020-09-19 04:39:59 UTC+0000
          Image local date and time : 2020-09-18 21:39:59 -0700
```



```
C:\Users\user\Downloads\volatility_2.6_win64_standalone>volatility_2.6_win64_standalone.exe --profile=Win2012R2x64 pslist -f
C:\Users\user\Downloads\DC01-memory\citadeldc01.mem
Volatility Foundation Volatility Framework 2.6
offset(V)      Name          PID  PPID  Thds  Hnds  Sess  Wow64 Start           Exit
-----
0xfffffe0005f273040 System        4     0    98     0 ----- 0 2020-09-19 01:22:38 UTC+0000
0xfffffe00060354900 smss.exe     204    4     2     0 ----- 0 2020-09-19 01:22:38 UTC+0000
```

0xfffffe00061a30900	vmtoolsd.exe	1600	452	9	0	0	0	2020-09-19 01:22:57 UTC+0000
0xfffffe00061a9a800	wlms.exe	1644	452	2	0	0	0	2020-09-19 01:22:57 UTC+0000
0xfffffe00061a9b2c0	dfssvc.exe	1660	452	11	0	0	0	2020-09-19 01:22:57 UTC+0000
0xfffffe0006291b7c0	svchost.exe	1956	452	30	0	0	0	2020-09-19 01:23:20 UTC+0000
0xfffffe000629b3080	vds.exe	796	452	11	0	0	0	2020-09-19 01:23:20 UTC+0000
0xfffffe000629926c0	svchost.exe	1236	452	8	0	0	0	2020-09-19 01:23:21 UTC+0000
0xfffffe000629de900	WmiPrvSE.exe	2056	640	11	0	0	0	2020-09-19 01:23:21 UTC+0000
0xfffffe00062a26900	dlhost.exe	2216	452	10	0	0	0	2020-09-19 01:23:21 UTC+0000
0xfffffe00062a2a900	msdtc.exe	2460	452	9	0	0	0	2020-09-19 01:23:21 UTC+0000
0xfffffe000631cb900	spoolsv.exe	3724	452	13	0	0	0	2020-09-19 03:29:40 UTC+0000
0xfffffe00062fe7700	coreupdater.ex	3644	2244	0	-----	2	0	2020-09-19 03:56:37 UTC+0000
03:56:52 UTC+0000								2020-09-19
0xfffffe00062f04900	taskhostex.exe	3796	848	7	0	1	0	2020-09-19 04:36:03 UTC+0000
0xfffffe00063171900	explorer.exe	3472	3960	39	0	1	0	2020-09-19 04:36:03 UTC+0000
0xfffffe00060ce2080	ServerManager.	400	1904	10	0	1	0	2020-09-19 04:36:03 UTC+0000
0xfffffe00063299280	vm3dservice.ex	3260	3472	1	0	1	0	2020-09-19 04:36:14 UTC+0000
0xfffffe00062ede1c0	vmtoolsd.exe	2608	3472	8	0	1	0	2020-09-19 04:36:14 UTC+0000
0xfffffe00063021900	FTK Imager.exe	2840	3472	9	0	1	0	2020-09-19 04:37:04 UTC+0000
0xfffffe0006313f900	WMIADAP.exe	3056	848	5	0	0	0	2020-09-19 04:37:42 UTC+0000

Checking processes that are running

```
Administrator: Command Prompt
0x1631b5e8      UDPv4    0.0.0.0:0
2020-09-19 01:22:57 UTC+0000
0x1631bcf0      UDPv4    0.0.0.0:0
2020-09-19 01:22:57 UTC+0000
0x163427b0      UDPv4    0.0.0.0:0
2020-09-19 01:22:57 UTC+0000
0x16342ec0      UDPv4    0.0.0.0:0
2020-09-19 01:22:57 UTC+0000
0x1644d2e0      UDPv4    0.0.0.0:0
2020-09-19 01:22:57 UTC+0000
Interrupted
^C
C:\Users\user\Downloads\volatility_2.6_win64_standalone>
C:\Users\user\Downloads\volatility_2.6_win64_standalone>
C:\Users\user\Downloads\volatility_2.6_win64_standalone>
C:\Users\user\Downloads\volatility_2.6_win64_standalone>
C:\Users\user\Downloads\volatility_2.6_win64_standalone> volatility_2.6_win64_standalone.exe --profile=Win2012R2x64 netstat -an -f C:\Users\user\Downloads\DC01-memory\citadeldc01.mem > output.csv
Volatility Foundation Volatility Framework 2.6
```

Check for processes that are performing network activities

File	Edit	Format	View	Help	Offset(P)	Proto	Local Address	Foreign Address	State	Pid	Owner
Created					0x1600730	UDPV4	0.0.0.0:0	*:*		1368	dns.exe
					0x1600730	UDPV6	:::0	*:*		1368	dns.exe
					0x1600ec0	UDPV4	0.0.0.0:0	*:*		1368	dns.exe
					0x1600ec0	UDPV6	:::0	*:*		1368	dns.exe
					0x60182590	TCPv4	10.42.85.10:62613	203.78.103.109:443	ESTABLISHED	3644	coreupdater.exe
					0x601cda00	TCPv6	fe80::2dcf:e660:be73:d220:135	fe80::2dcf:e660:be73:d220:62779	CLOSED	684	svchost.exe

Result for processes that are performing network activities

```
C:\Users\user\Downloads\volatility_2.6_win64_standalone>
C:\Users\user\Downloads\volatility_2.6_win64_standalone> volatility_2.6_win64_standalone.exe
--profile=Win2012R2x64 malfind -f C:\Users\user\Downloads\DC01-memory\citadeldc01.mem > malfind.txt
```

Checking for hidden or injected code/DLLs in user mode memory