A

FORENSIC REPORT ON THE STOLEN SZECHUAN SAUCE CASE

ANALYZED

Submitted by: KEHINDE OJEWUNMI,

NOAH SHITTA

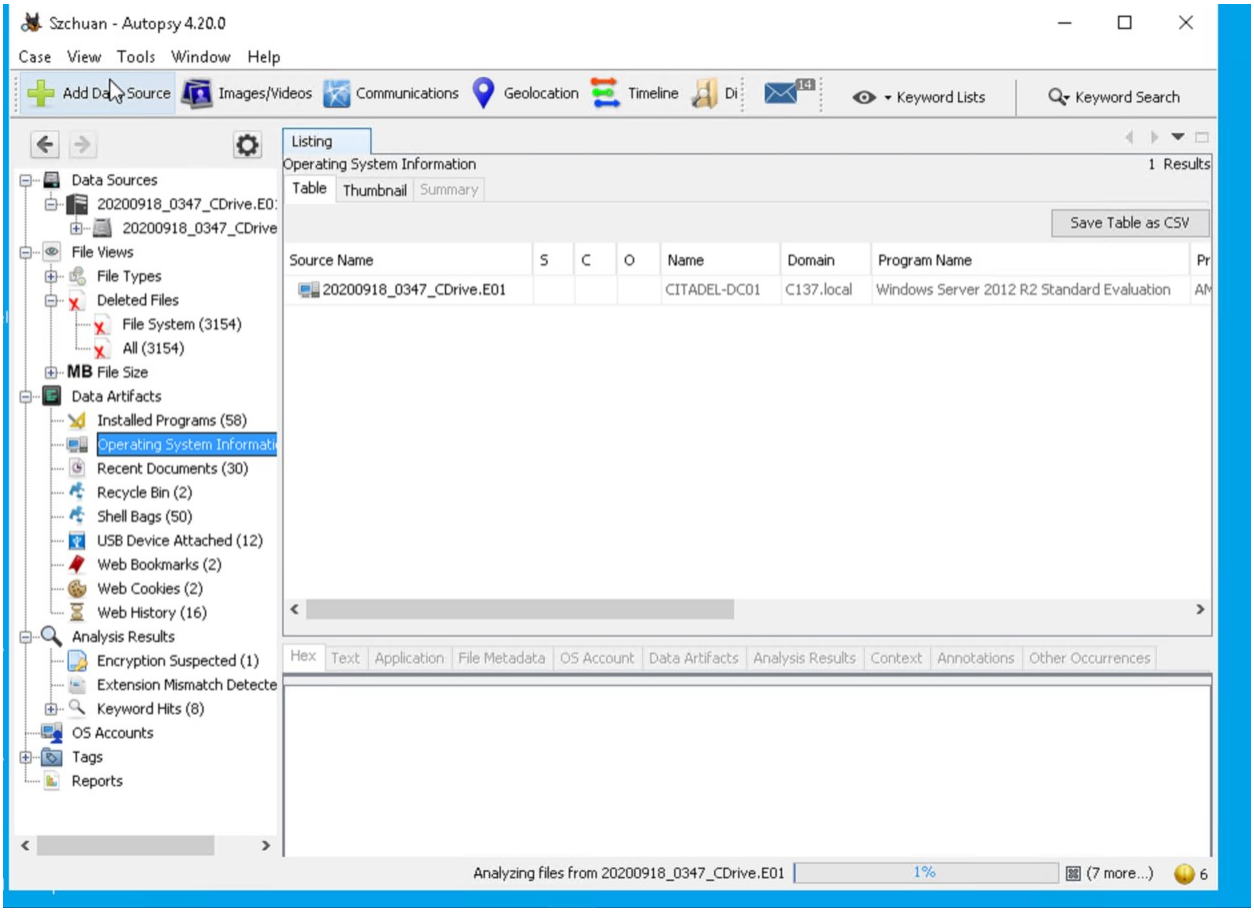
NAVNEET KAUR

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

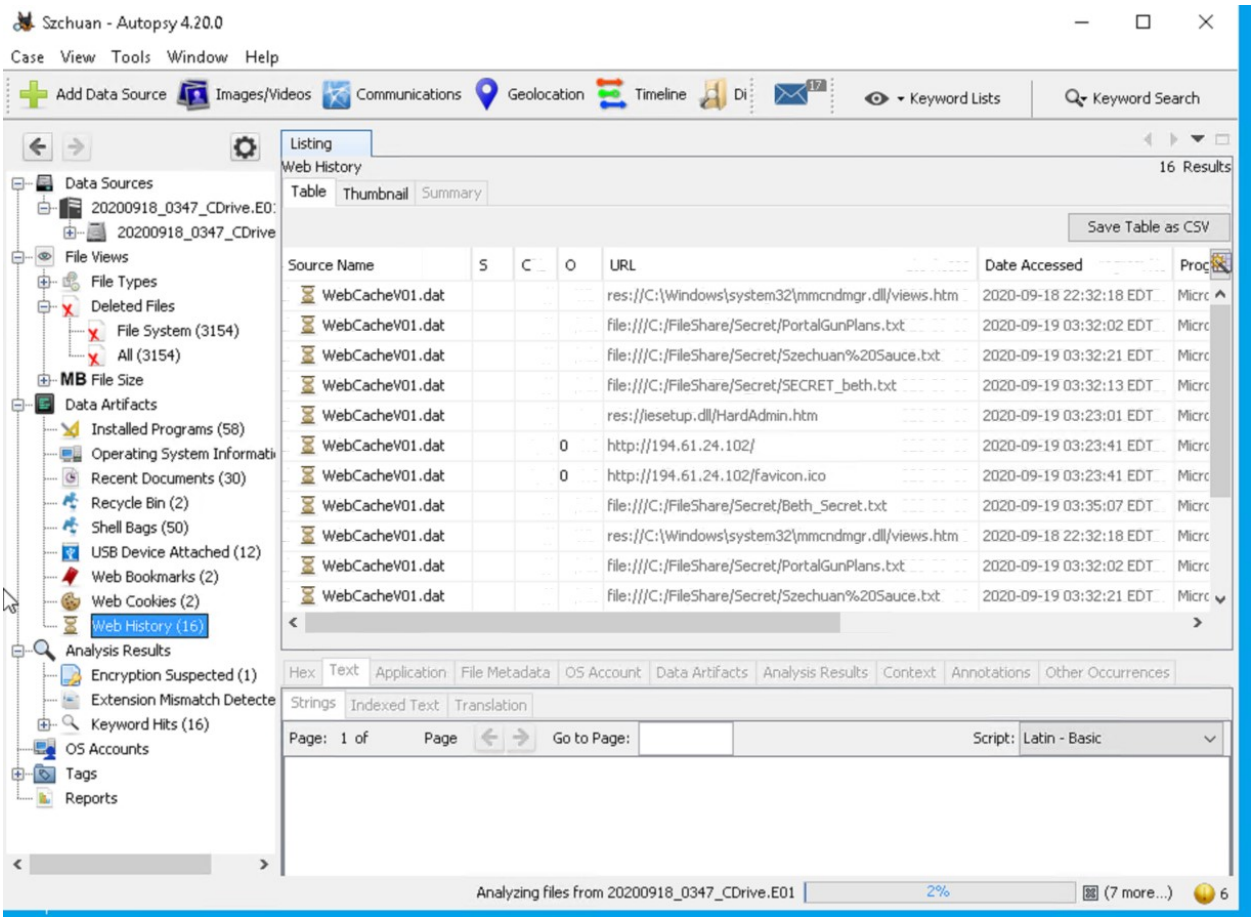


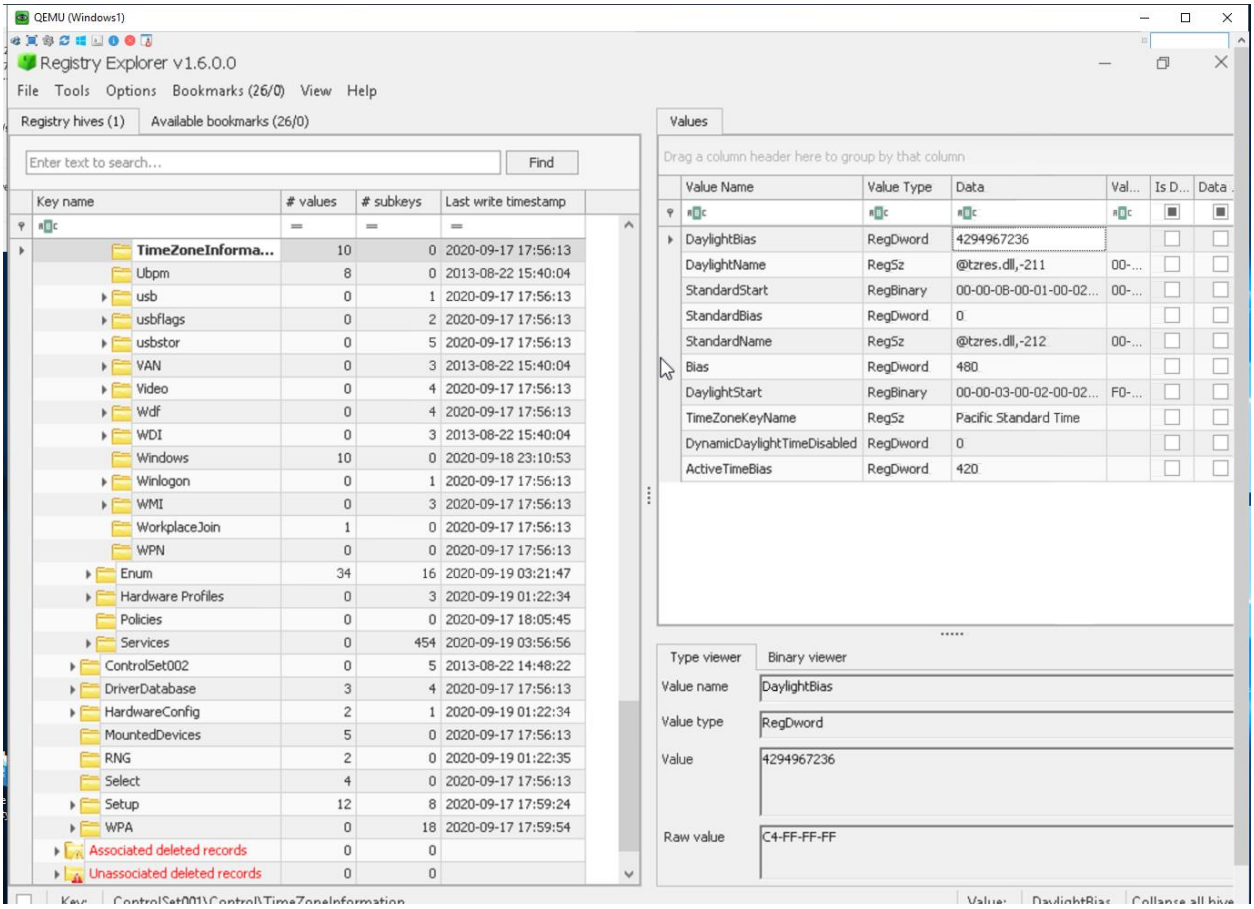
2. What's the Operating System of the Desktop?
   Windows 10 Enterprise Evaluation

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)

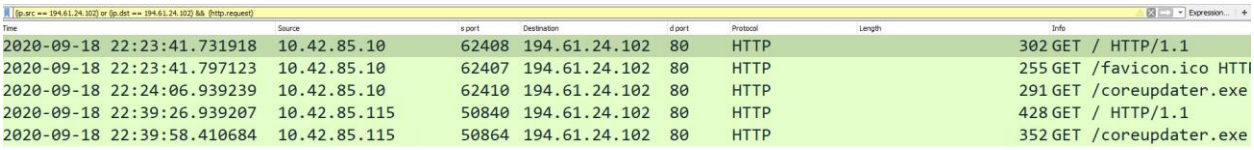




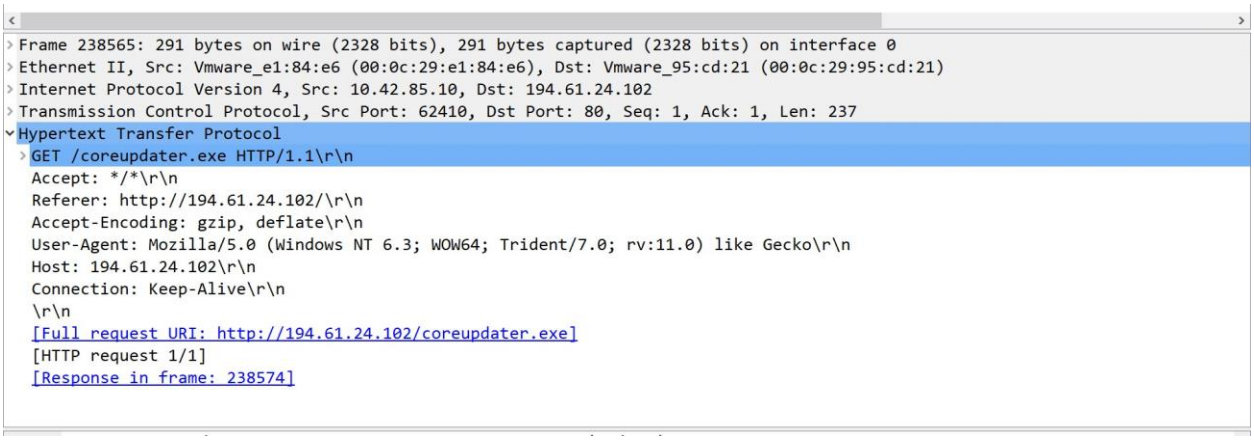
4. Was there a breach?

Yes, The recipe was stolen and some files were deleted

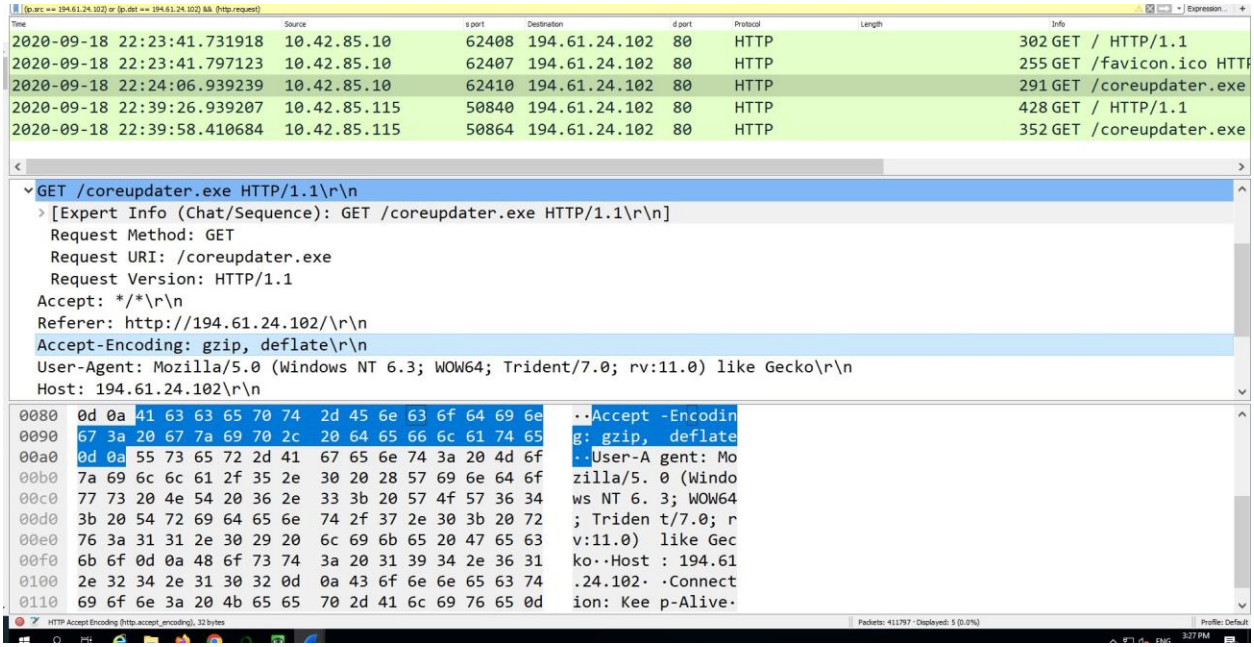
Coreupdate.exe file was found in wireshark



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 HTT
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



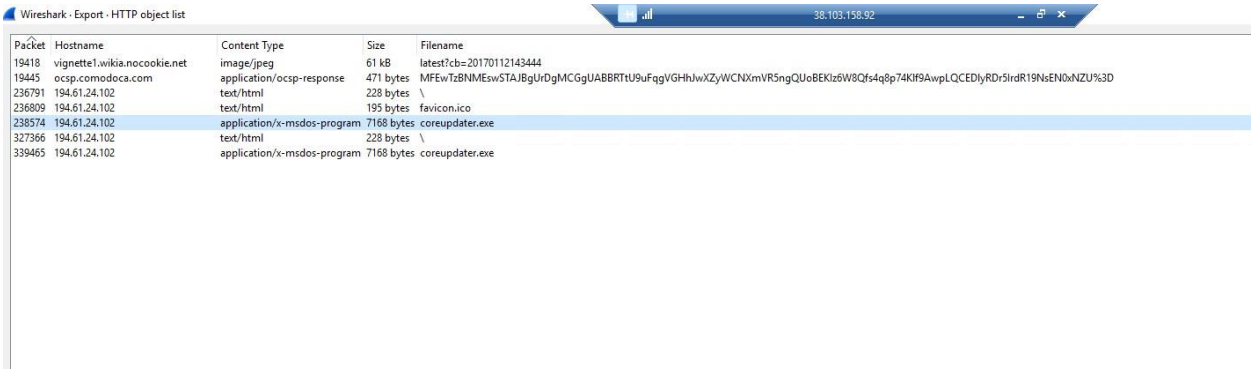
```
> Frame 238565: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface 0
> Ethernet II, Src: Vmware_e1:84:e6 (00:0c:29:e1:84:e6), Dst: Vmware_95:cd:21 (00:0c:29:95:cd:21)
> Internet Protocol Version 4, Src: 10.42.85.10, Dst: 194.61.24.102
> Transmission Control Protocol, Src Port: 62410, Dst Port: 80, Seq: 1, Ack: 1, Len: 237
v 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]
```



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
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 -Encodin
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-A gent: Mo
00b0  7a 69 6c 6c 61 2f 35 2e  30 20 28 57 69 6e 64 6f   zilla/5. 0 (Windo
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 6e  74 2f 37 2e 30 3b 20 72   ; Triden t/7.0; r
00e0  76 3a 31 31 2e 30 29 20  6c 69 6b 65 20 47 65 63   v:11.0)  like Gec
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·
```

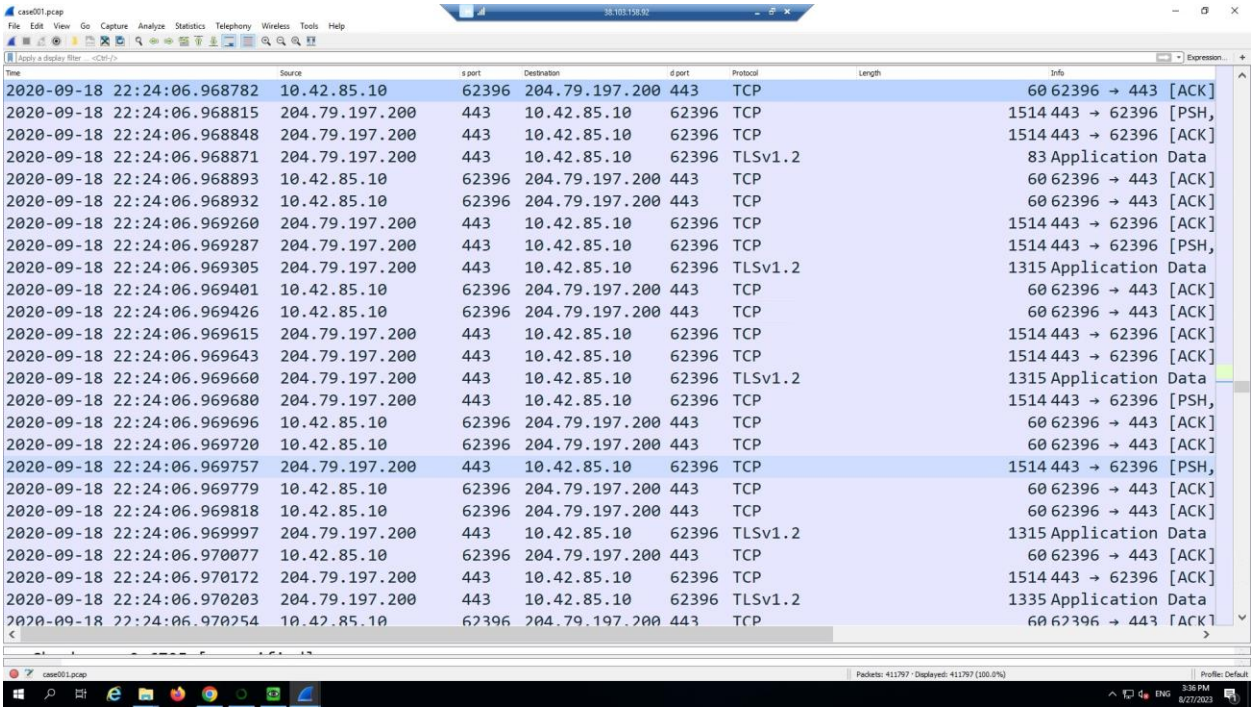


Wireshark · Export · HTTP object list

Packet	Hostname	Content Type	Size	Filename
19418	vignette1.wikia.nocookie.net	image/jpeg	61 kB	latest?cb=20170112143444
19445	ocsp.comodoca.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%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)?

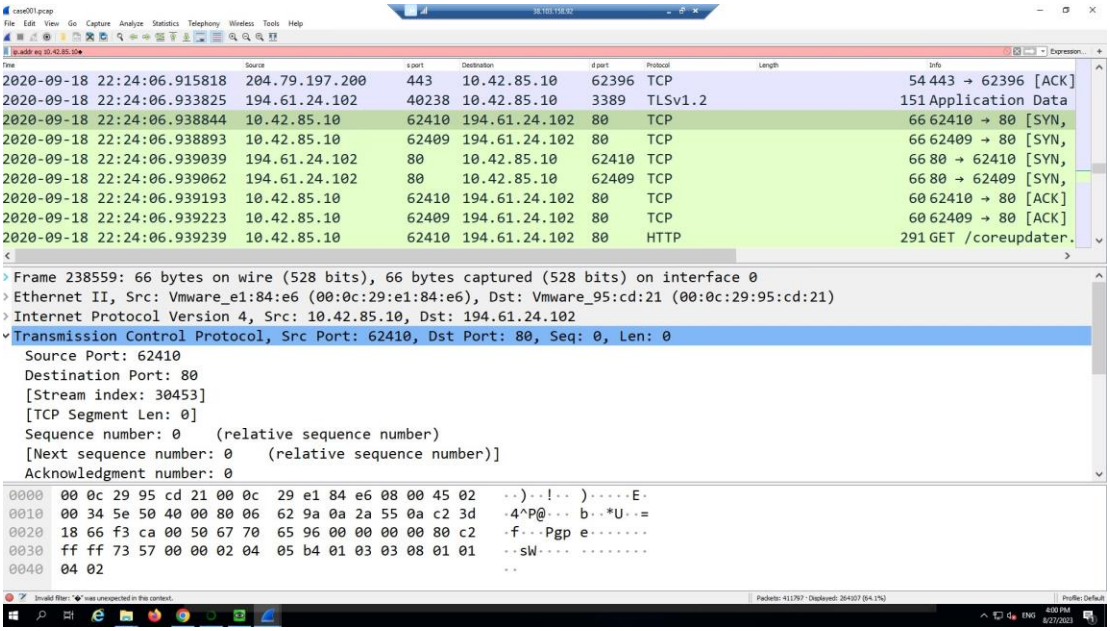
RDP Bruteforce , we can see in multiple time attacker trying to access the server,



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	1514	443 → 62396 [PSH,
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:
   a. What process was malicious? C:\Windows\System32\coreupdater.exe
   b. 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	204.79.197.200	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.

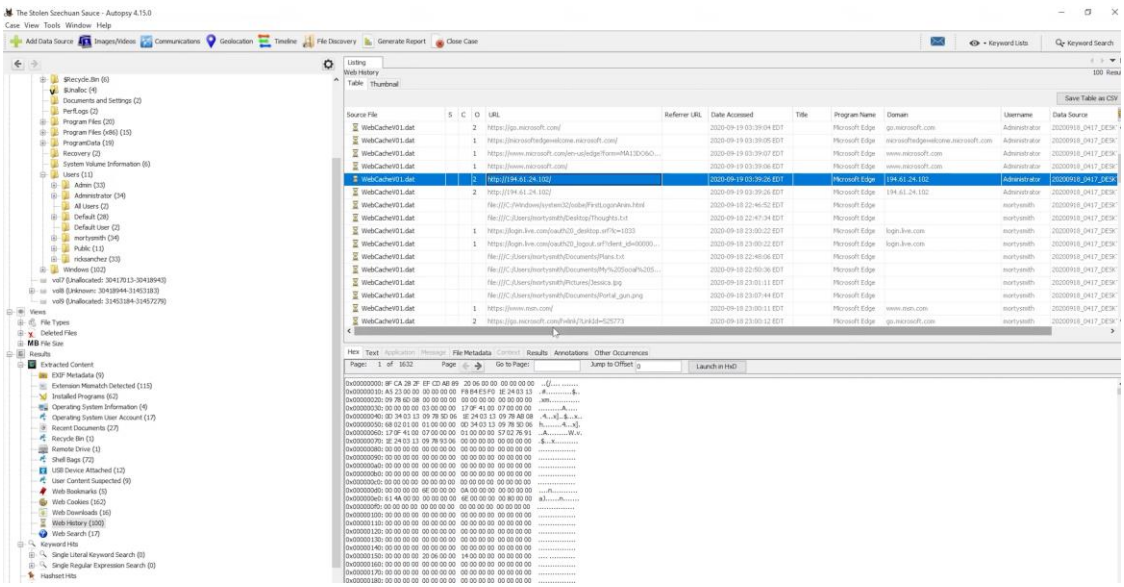
```
> Frame 238559: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface 0
> Ethernet II, Src: Vmware_e1:84:e6 (00:0c:29:e1:84:e6), Dst: Vmware_95:cd:21 (00:0c:29:95:cd:21)
> Internet Protocol Version 4, Src: 10.42.85.10, Dst: 194.61.24.102
v Transmission Control Protocol, Src Port: 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 00 80 c2   ·f···Pgp e·······
0030  ff ff 73 57 00 00 02 04  05 b4 01 03 03 08 01 01   ··sW···· ········
0040  04 02                                             ··
```

Wireshark · Export · HTTP object list

38.103.158.92

Packet	Hostname	Content Type	Size	Filename
19418	vignette1.wikia.nocookie.net	image/jpeg	61 kB	latest?cb=20170112143444
19445	ocsp.comodoca.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDgMCGgUABBRTtU9uFqgVGHhJwXZyWCNXmVR5ngQUoBEKIz6W8Qfs4q8p74Klf9AwpLQCEDlyRDr5IrdR19NsEN0xNZU%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



MAXMIND Products Support Developers Company Blog Contact

GeoIP2 Databases Demo

Show Sidebar

IP Addresses

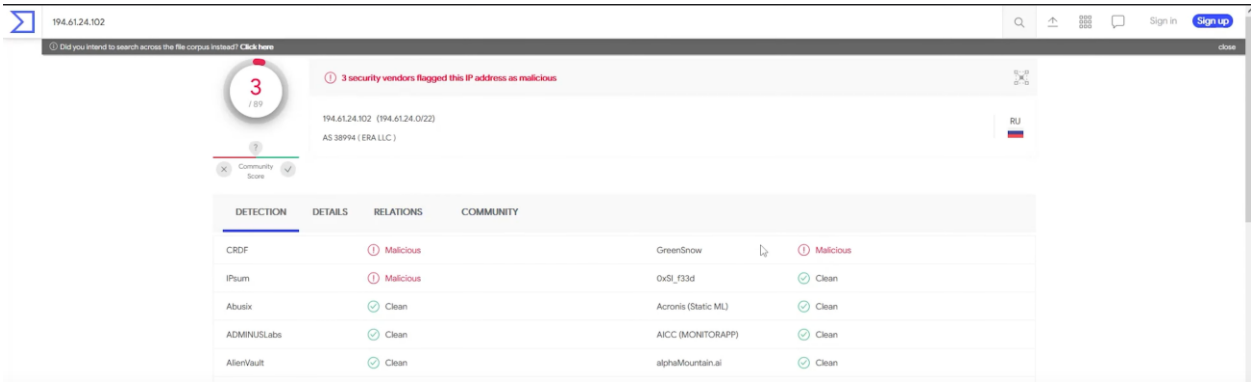
194.61.24.102

Enter up to 25 IP addresses separated by spaces or commas. You can also test your own IP address.

Submit

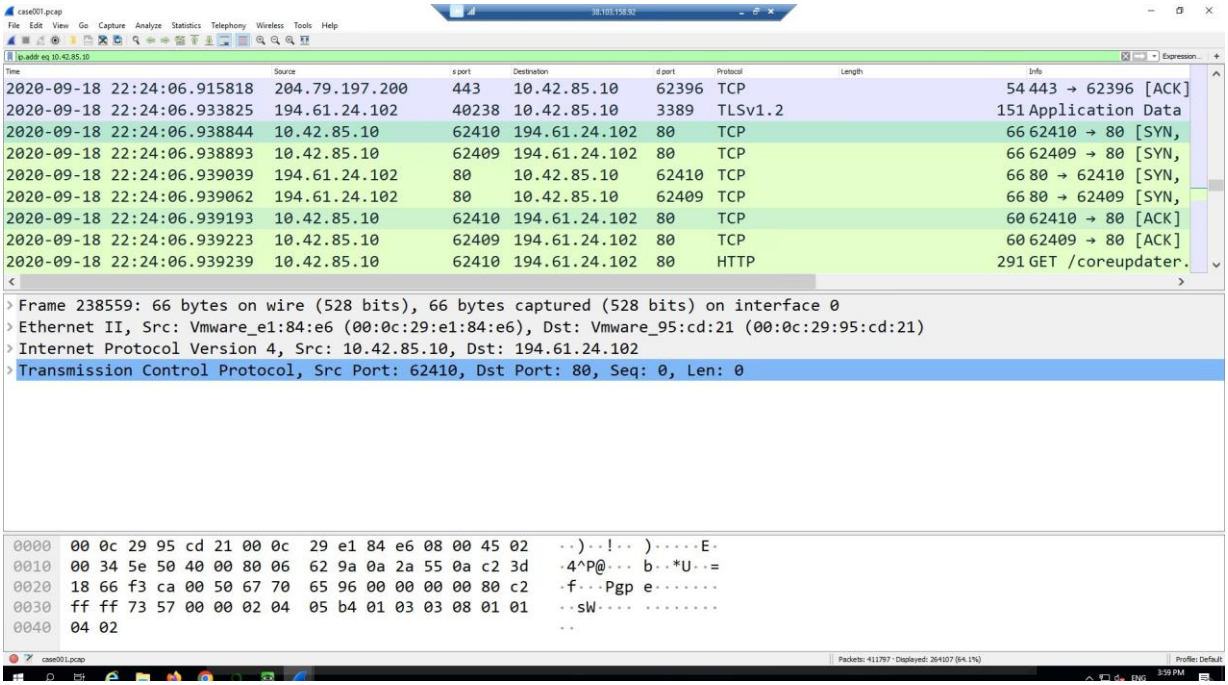
GeoIP2 City Results

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
194.61.24.102	RU	Russia, Europe	194.61.24.0/25		55.7386, 37.6068	1000	ERA LLC	ERA LLC		



c. What IP Address is the malware calling to?

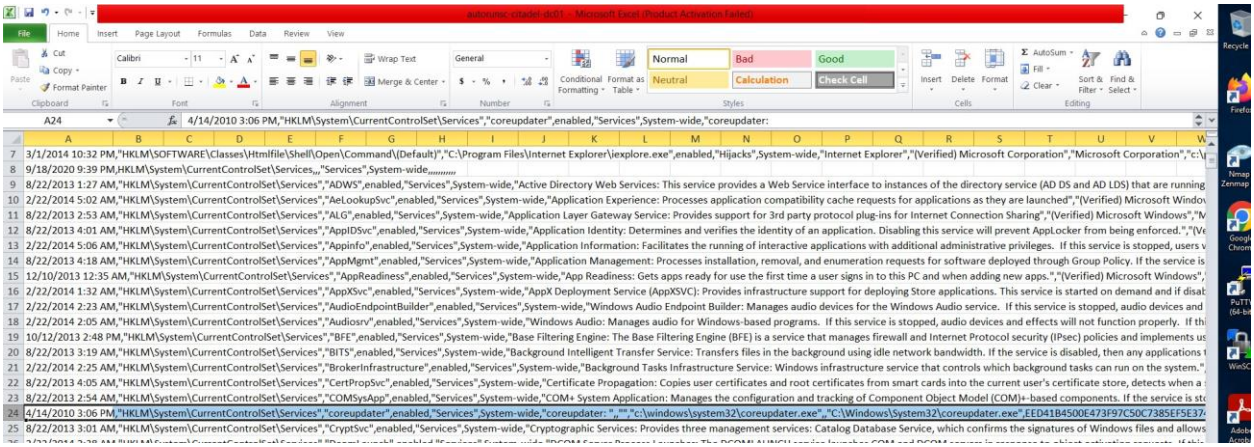
204.79.197.200

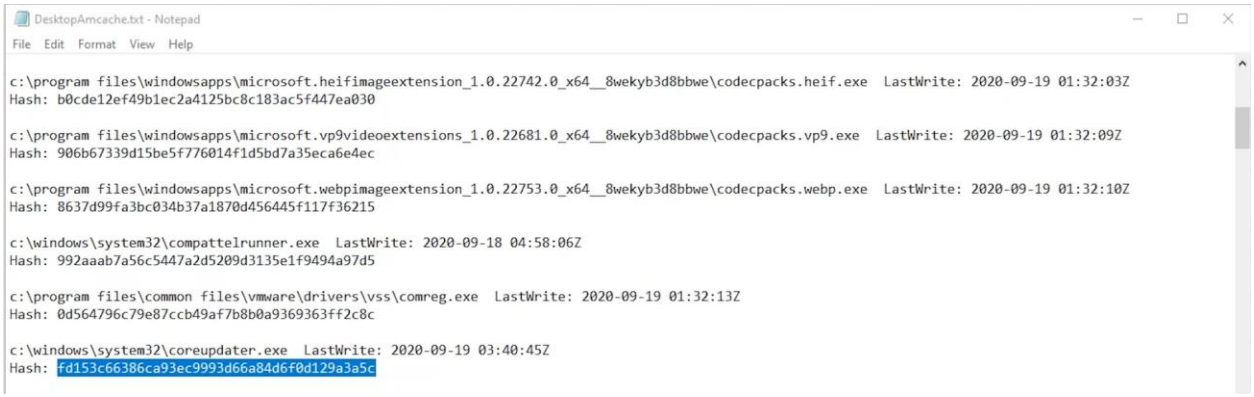


d. Where is this malware on disk?

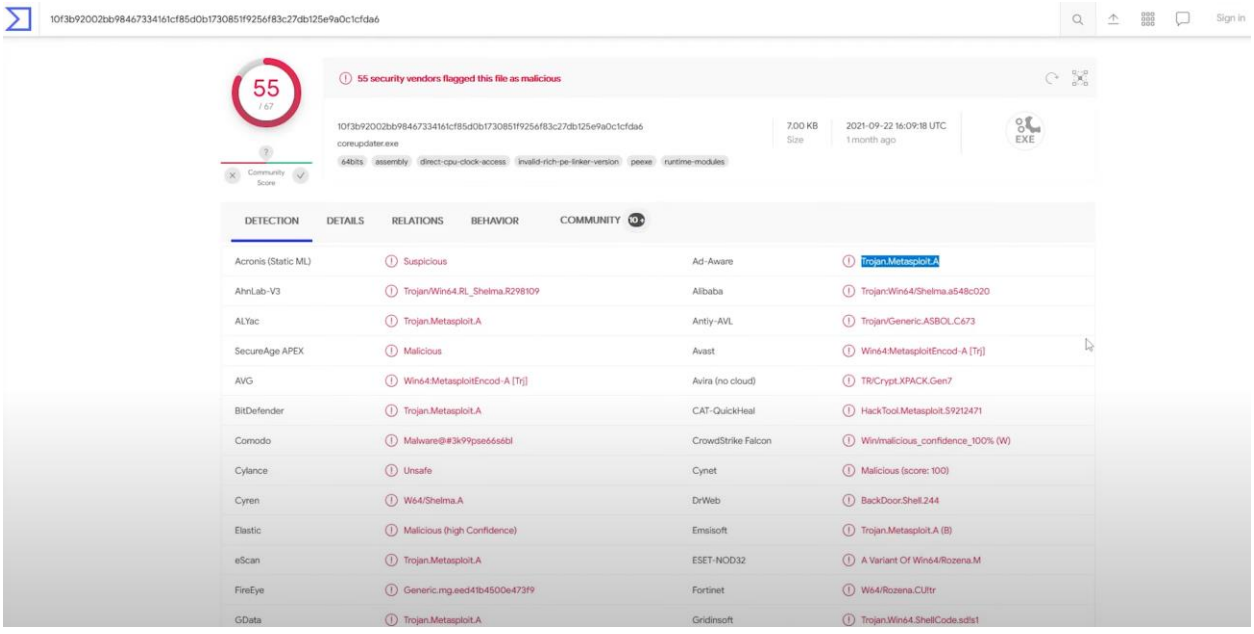
C:\Windows\system32\ extract from autorun

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,FD153C66386CA93EC9993D66A84D6F0D129A3A5C,C3E46C6242056ACE3217A5314CFF2063BE8E9799,88763E60ED00AFDA80A61647782B597542D9667D2B9A35FB2623967E302FA28E,10F3B92002BB98467334161CF85D0B1730851F9256F83C27DB125E9A0C1CFDA6,B4C6FFF030479AA3B12625BE67BF4914





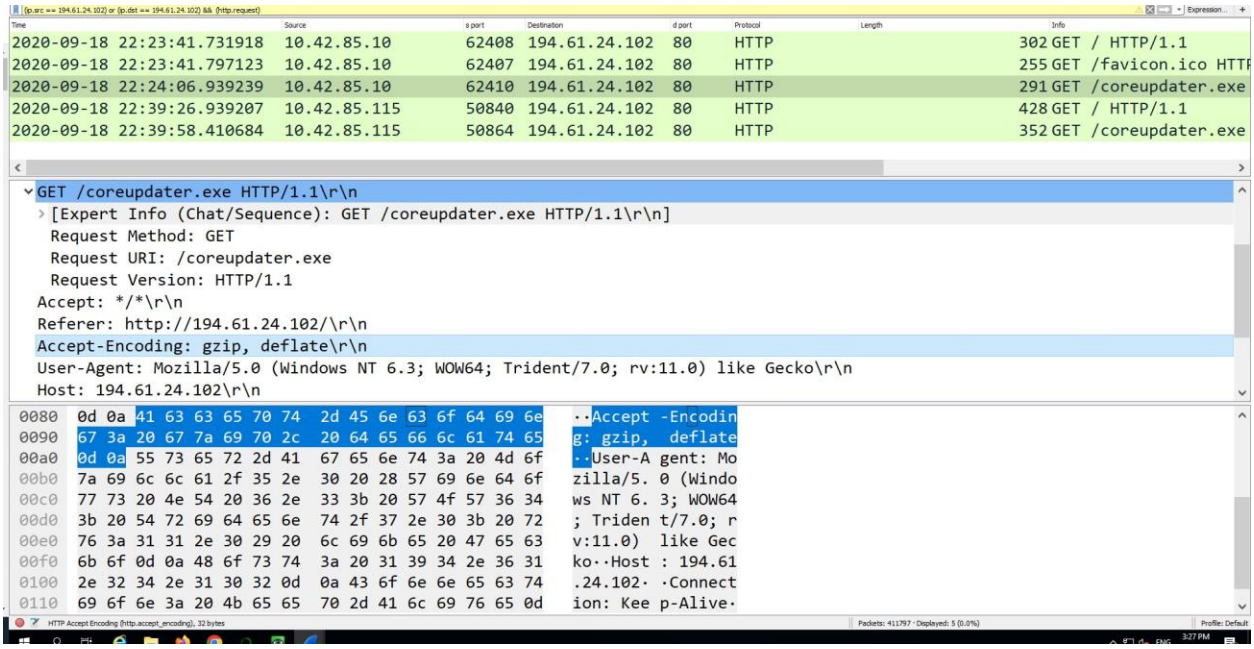
Parse with Reg ripper



Result from virustotal.com

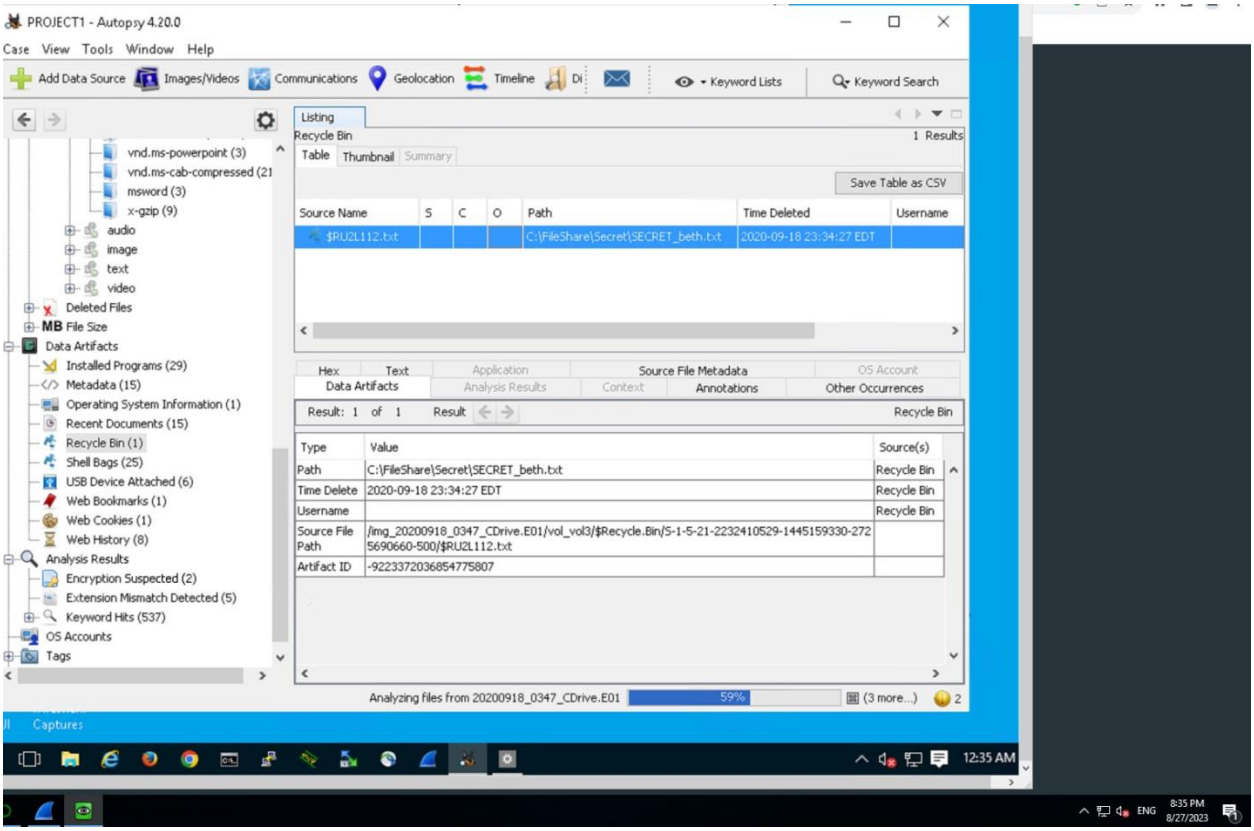
e. When did it first appear?

18 sept 2020 @22.24.06.939239



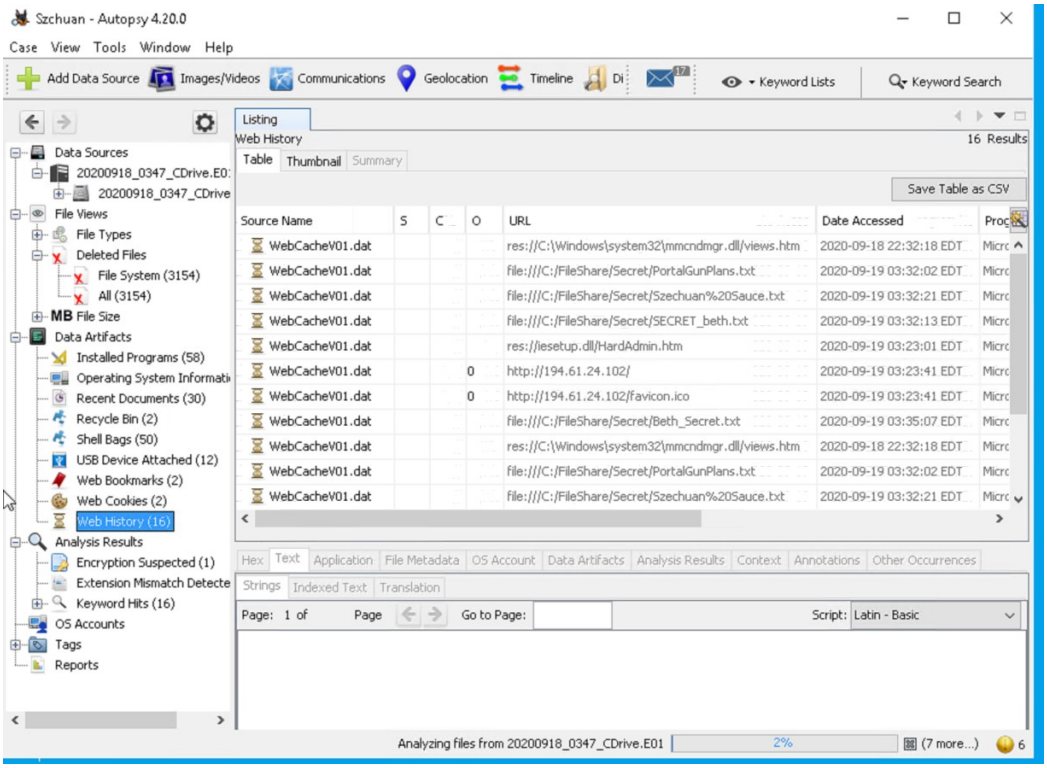
f. Did someone move it?
Its moved from download folder to C:/windows/system32/administration folder

g. What were the capabilities of this malware?
Deleting and moving files from one folder to another, deleted some files moved to recycle bin



h. Is this malware easily obtained? Yes

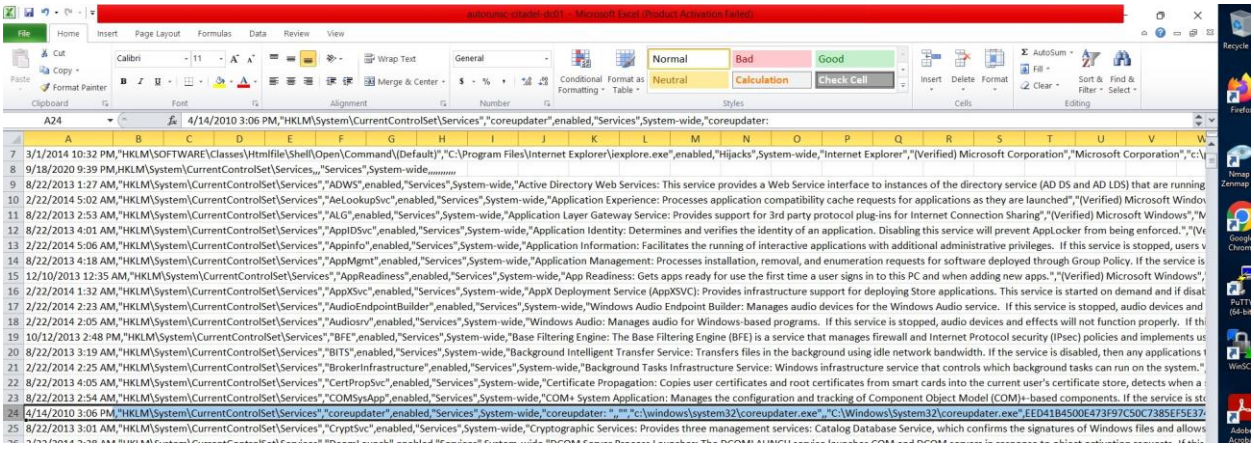
Using Autopsy tool by checking web history and autoruns, we can easily find out it.

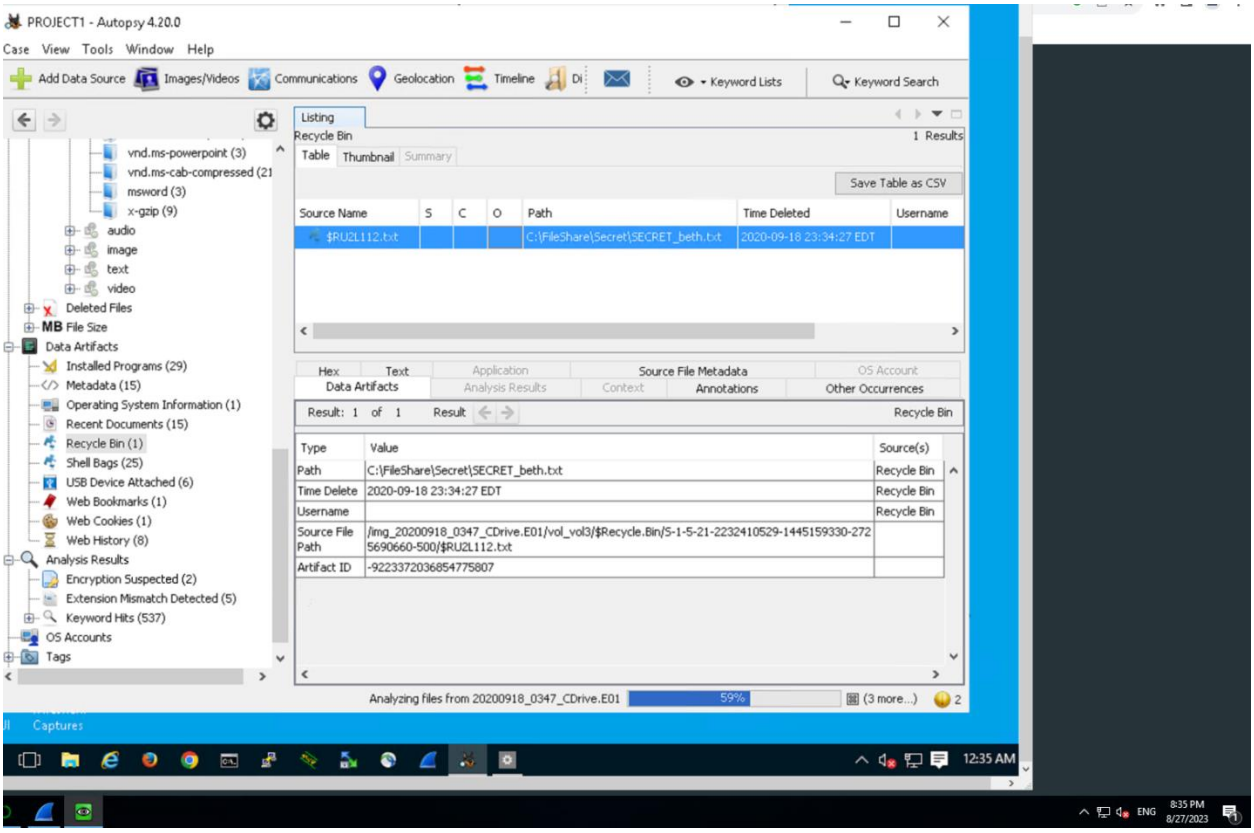


i. Was this malware installed with persistence on any machine? Yes

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 ⓘ

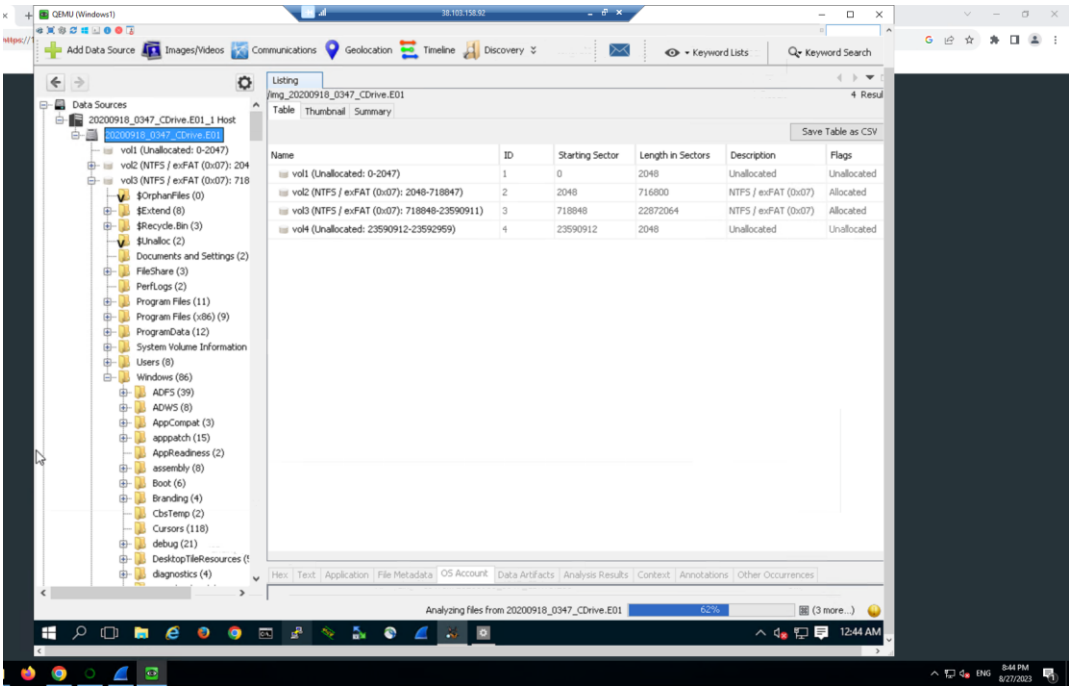
MD5	64a4e2cb47138084a5c2878066b2d7b1
SHA-1	e8dd11314a2501dc0ad98901a321350d9cd111c2
SHA-256	86658d85d8254e8d30dccc4f50d9c2a8b550a101d2e78a6d932316849e37ad80
Vhash	0b3e31f3da0a40321716410a2ab4616f
SSDEEP	12582912:H8xocBlyVnRyMhq6vKFU9HW9JlkwtZ0zC:HG7BlmRvP2U9aPc
TLSH	T1D5493381F412B50DDFEA6675EEC27A5EEA0C0C1F49575C64EF71314820EAEE0BF1264A
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)

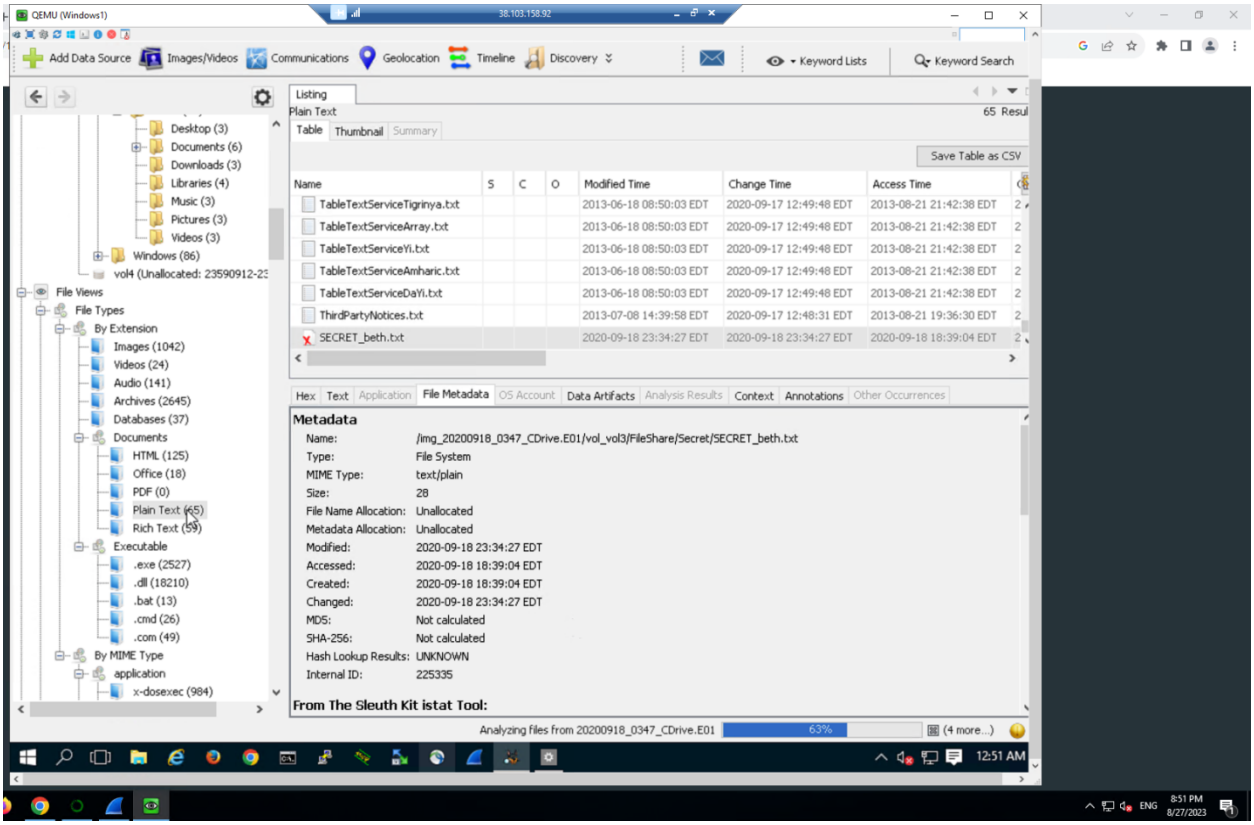
For autoruns.zip

Basic properties ⓘ

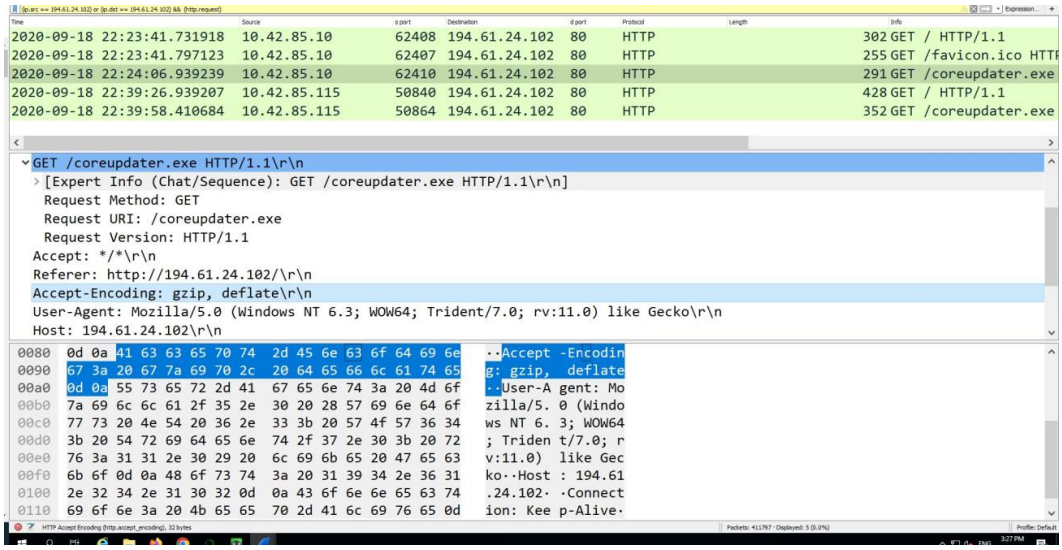
MD5	964eeaf0009d08cc101de4a83a4e5d23
SHA-1	257c2ab4f1916ae9b5ed8e9c8486e48a39042c97
SHA-256	b1db1979b290cf5c954c1965c5e7834259bb8e3e88327d7f6d68b20e4c7cd5b9
Vhash	152d458dfec368b9f3912809dcee648d
SSDEEP	393216:q4RZZL+SDy9T51Ho1wVXf6lckb3tdCO4KJeQ8akMlXI3dAfg16E:jRZrMywZ03TC7k/vJXINd
TLSH	T168D62268F471B965F488C27646B02CF5C7AC6D70C3BA2AC61F30715BAA97A0D4F79870
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)

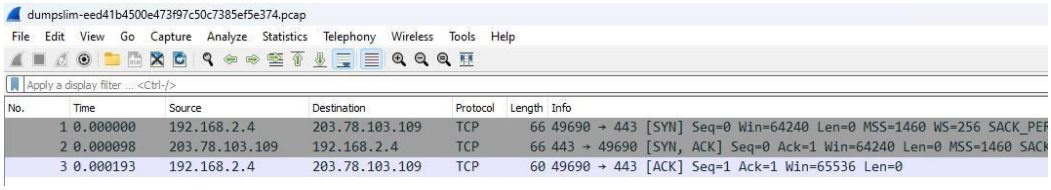
Partitioning of disk

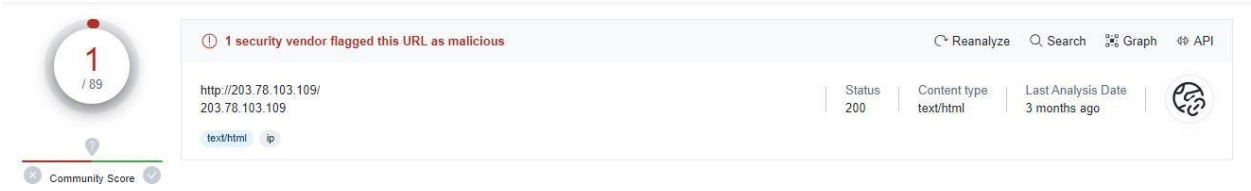




7. What malicious IP Addresses were involved? 194.61.24.102 and 203.78.103.109







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 -nttttr 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 02:35:55.285542 IP 10.42.85.115.3389 > 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 02:35:55.285688 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [.], ack 1, win 256, length 0
2020-09-19 02:35:55.291953 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [P.], seq 1:20, ack 1, win 256, length 19
2020-09-19 02:35:55.347240 IP 10.42.85.115.3389 > 10.42.85.10.62514: Flags [.], ack 20, win 63981, length 0
2020-09-19 02:35:55.364696 IP 10.42.85.115.3389 > 10.42.85.10.62514: Flags [P.], seq 1:20, 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 200:518, ack 884, win 253, length 318
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 518:706, 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
```

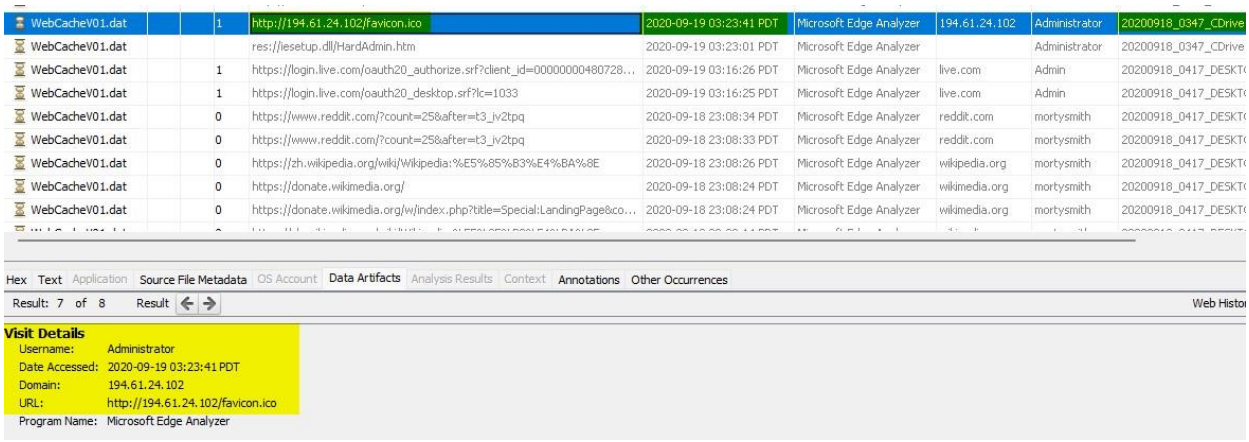
b. When?

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.

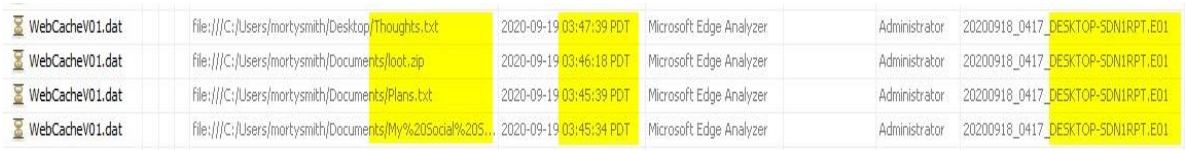


c. Did the attacker steal or access any data?

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.

When?

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

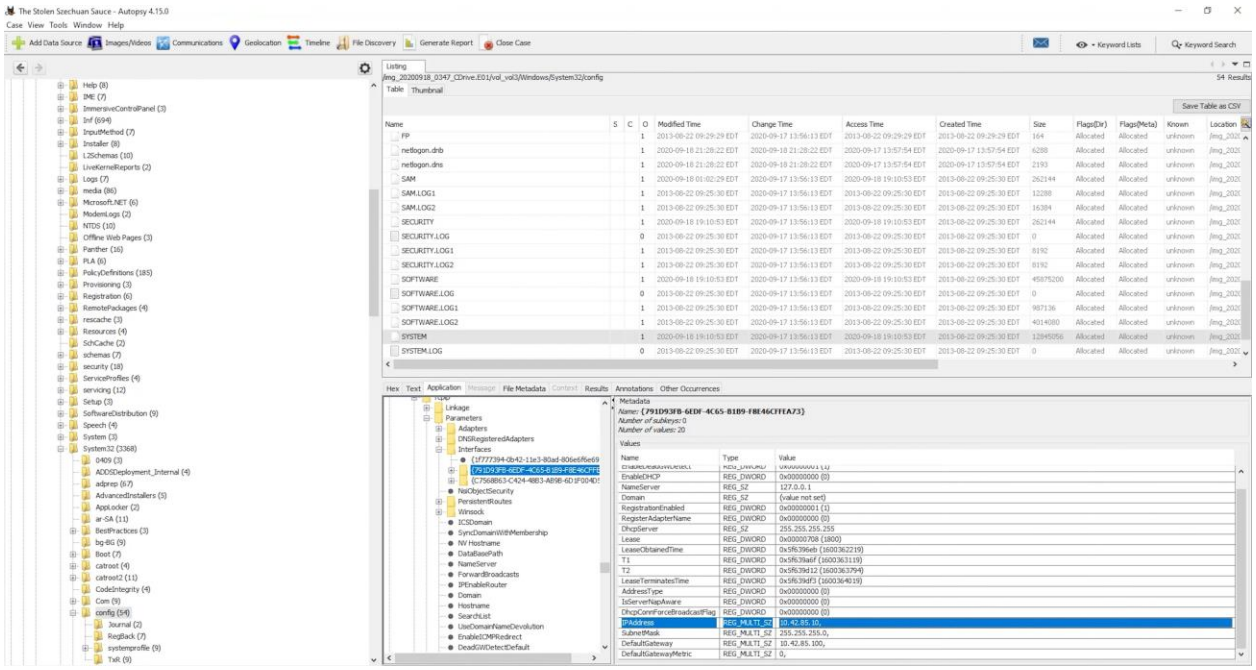


9. What was the network layout of the victim network?

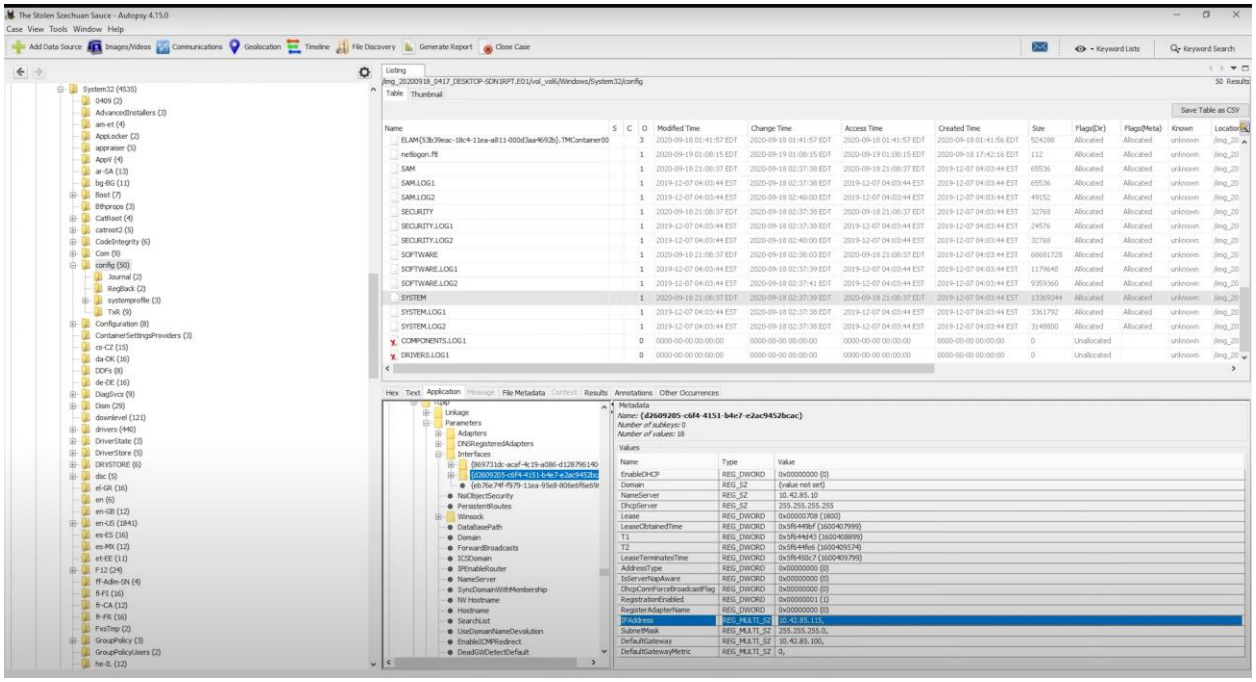
The network layout you provided is a small local area network (LAN) with a subnet of 10.42.85.0/24. This means the network can accommodate up to 256 IP addresses (from 10.42.85.0 to 10.42.85.255), where the first three octets (10.42.85) represent the network address, and the last octet can be assigned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

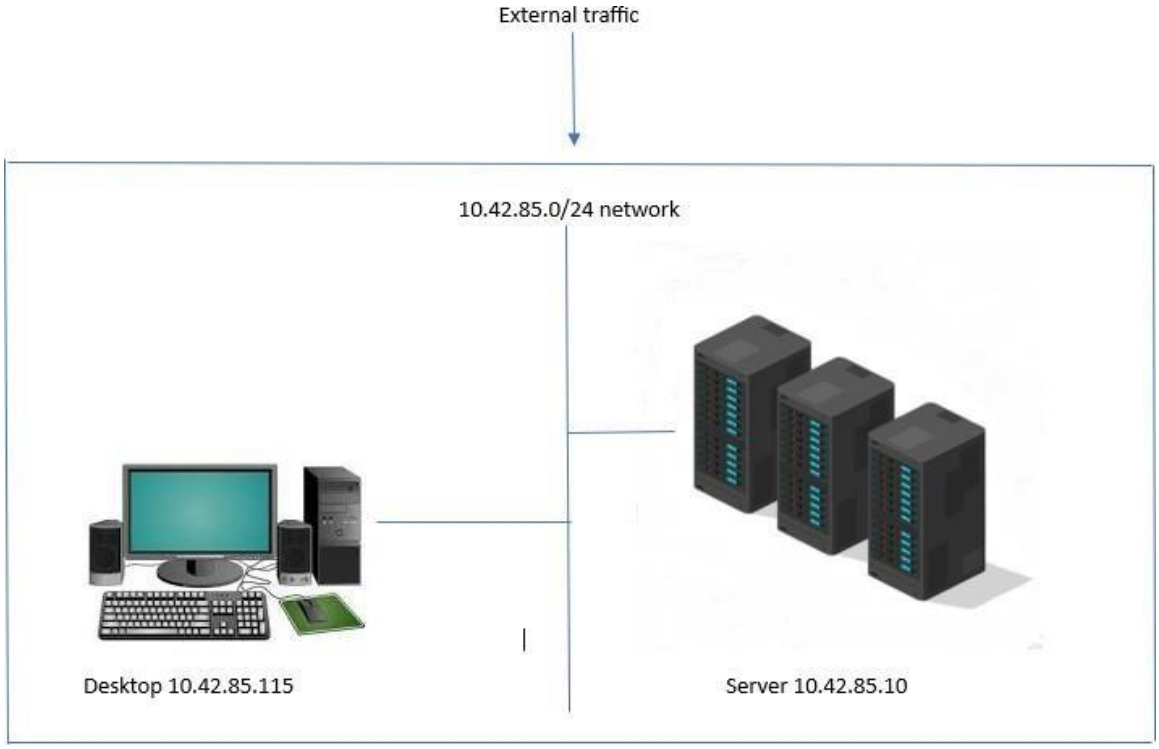


User/Desktop: Its IP address is 10.42.85.115. This is a typical user's desktop computer or workstation that connects to the network to access shared resources and services provided by the Domain Controller.



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

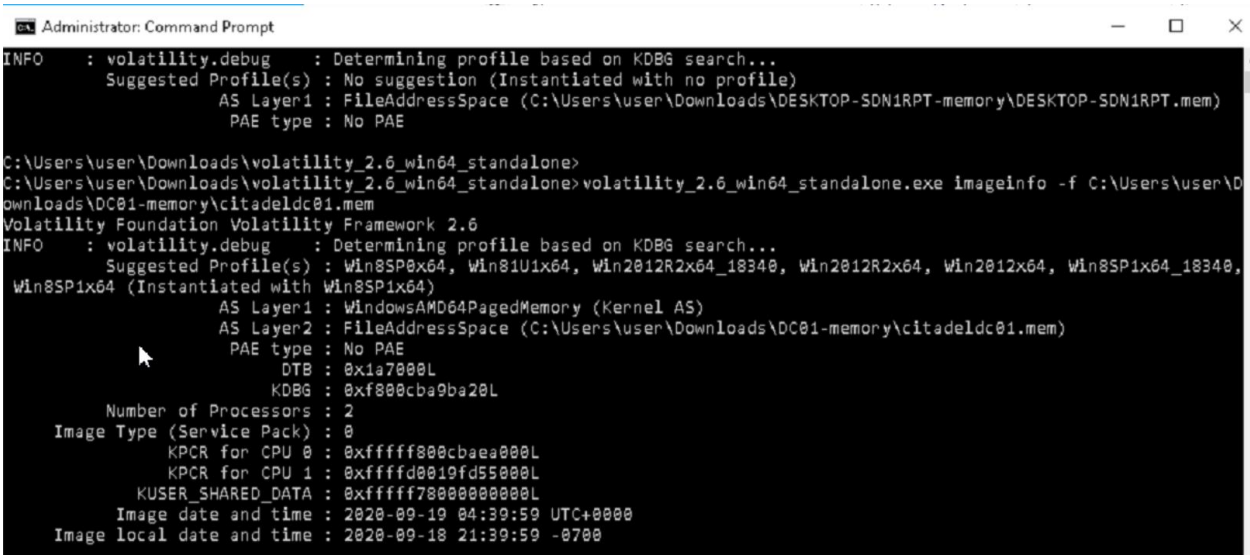
Autopsy User Documentation 4.0 https://sleuthkit.org/autopsy/docs/user-docs/4.0/

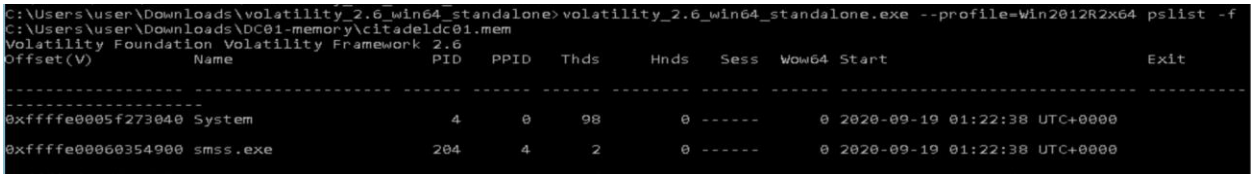
Comprehensive Guide on FTK Imager; Raj Chandel (November 6, 2020)
https://www.hackingarticles.in/comprehensive-guide-on-ftk-imager/

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





```
0xffffe00061a30900 vmtoolsd.exe          1600    452      9        0      0      0 2020-09-19 01:22:57 UTC+0000
0xffffe00061a9a800 wlms.exe              1644    452      2        0      0      0 2020-09-19 01:22:57 UTC+0000
0xffffe00061a9b2c0 dfssvc.exe            1660    452     11        0      0      0 2020-09-19 01:22:57 UTC+0000
0xffffe0006291b7c0 svchost.exe           1956    452     30        0      0      0 2020-09-19 01:23:20 UTC+0000
0xffffe000629b3080 vds.exe                796    452     11        0      0      0 2020-09-19 01:23:20 UTC+0000
0xffffe000629926c0 svchost.exe           1236    452      8        0      0      0 2020-09-19 01:23:21 UTC+0000
0xffffe000629de900 WmiPrvSE.exe          2056    640     11        0      0      0 2020-09-19 01:23:21 UTC+0000
0xffffe00062a26900 dllhost.exe           2216    452     10        0      0      0 2020-09-19 01:23:21 UTC+0000
0xffffe00062a2a900 msdtc.exe             2460    452      9        0      0      0 2020-09-19 01:23:21 UTC+0000
0xffffe000631cb900 spoolsv.exe           3724    452     13        0      0      0 2020-09-19 03:29:40 UTC+0000
0xffffe00062fe7700 coreupdater.ex        3644   2244      0 --------      2      0 2020-09-19 03:56:37 UTC+0000   2020-09-19
 03:56:52 UTC+0000
0xffffe00062f04900 taskhostex.exe        3796    848      7        0      1      0 2020-09-19 04:36:03 UTC+0000
0xffffe00063171900 explorer.exe          3472   3960     39        0      1      0 2020-09-19 04:36:03 UTC+0000
0xffffe00060ce2080 ServerManager.         400   1904     10        0      1      0 2020-09-19 04:36:03 UTC+0000
0xffffe00063299280 vm3dservice.ex        3260   3472      1        0      1      0 2020-09-19 04:36:14 UTC+0000
0xffffe00062ede1c0 vmtoolsd.exe          2608   3472      8        0      1      0 2020-09-19 04:36:14 UTC+0000
0xffffe00063021900 FTK Imager.exe        2840   3472      9        0      1      0 2020-09-19 04:37:04 UTC+0000
0xffffe0006313f900 WMIADAP.exe           3056    848      5        0      0      0 2020-09-19 04:37:42 UTC+0000
```

Checking processes that are running

```
Administrator: Command Prompt
0x1631b5e0          UDPv4    0.0.0.0:0                      *:*                                    1368      dns.exe
 2020-09-19 01:22:57 UTC+0000
0x1631bcf0          UDPv4    0.0.0.0:0                      *:*                                    1368      dns.exe
 2020-09-19 01:22:57 UTC+0000
0x163427b0          UDPv4    0.0.0.0:0                      *:*                                    1368      dns.exe
 2020-09-19 01:22:57 UTC+0000
0x16342ec0          UDPv4    0.0.0.0:0                      *:*                                    1368      dns.exe
 2020-09-19 01:22:57 UTC+0000
0x164ad2e0          UDPv4    0.0.0.0:0                      *:*                                    1368      dns.exe
 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 netsc
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

```
output.csv - Notepad
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
2020-09-19 01:22:57 UTC+0000
0x1600730          UDPv6    :::0                           *:*                                   1368      dns.exe
2020-09-19 01:22:57 UTC+0000
0x1600ec0          UDPv4    0.0.0.0:0                      *:*                                   1368      dns.exe
2020-09-19 01:22:57 UTC+0000
0x1600ec0          UDPv6    :::0                           *:*                                   1368      dns.exe
```

```
output.csv - Notepad
File  Edit  Format  View  Help
0x601fae50         TCPv6    :::62475                       :::0                  LISTENING       3724      spoolsv.exe
0x5ffe1d10         TCPv6    fe80::2dcf:e660:be73:d220:49155 fe80::2dcf:e660:be73:d220:62777 CLOSED          460
lsass.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 > ma
lfind.txt
```

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