Forensics Report and Documentation

CASE 001 – THE STOLEN SZECHUAN SAUCE

- Jasraj Johal

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

***Tools Used*: Autopsy**

Windows Server 2012 R2
The Operating System of the server was found using Autopsy software on the artifact - E01-DC01 system disk image, supplied on the project page.

Type	Value
Name	CITADEL-DC01
Domain	C137.local
Program Name	Windows Server 2012 R2 Standard Evaluation
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP

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

***Tools Used*: Autopsy**

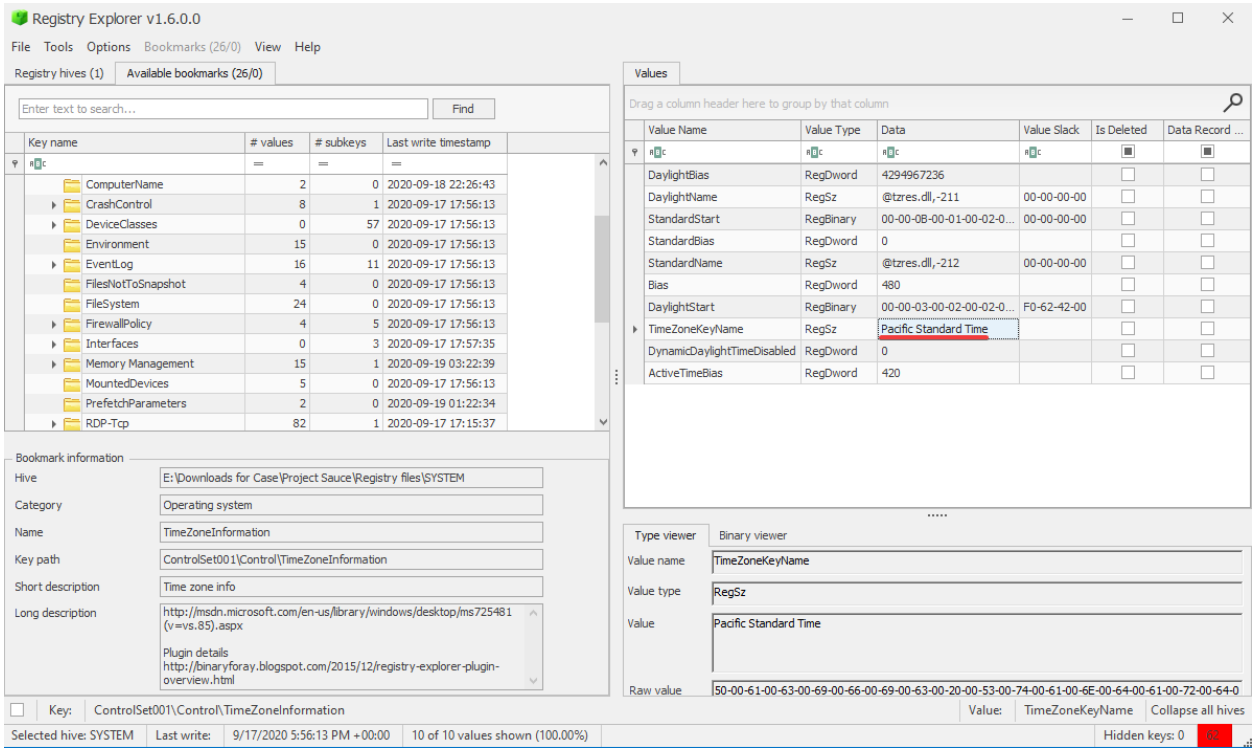
Windows 10 Enterprise Evaluation
The desktop's Operating System was discovered using Autopsy software on the artifact - DESKTOP-E01 system disk image.

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?

***Tools Used*: Registry Explorer**

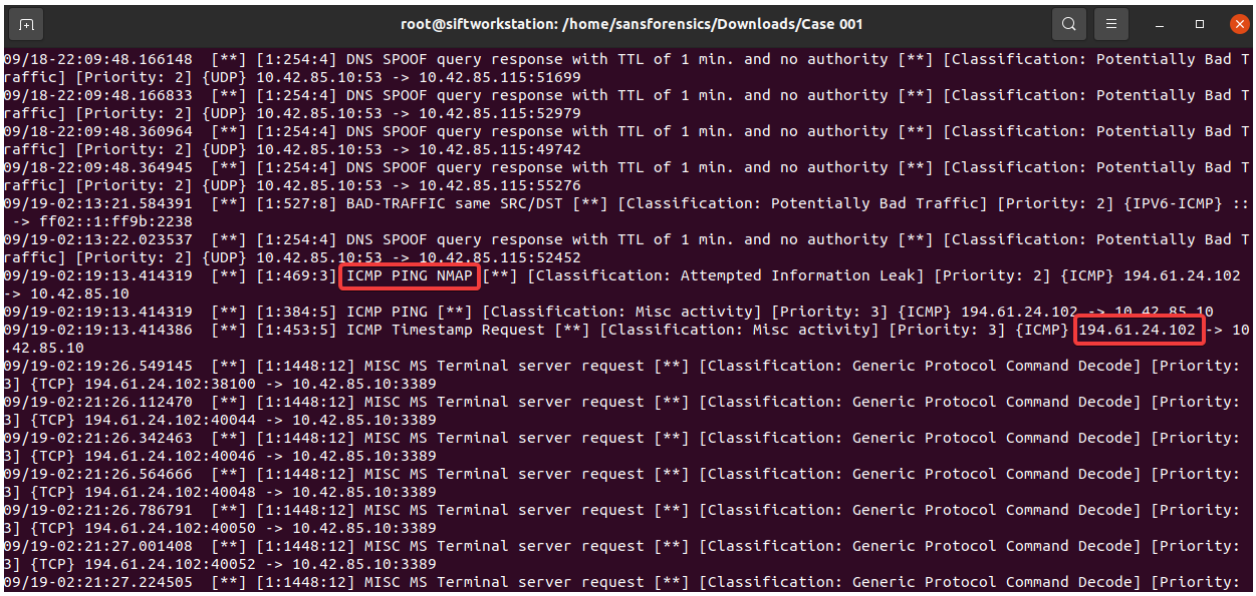
The local time is Pacific Standard Time PST. The Time Zone information was determined by downloading the registry files from the disk image. Location of the system reg file: 20200918_0347_CDrive.E01/Partition2[11168MB]/NONAME[NTFS]/[root]/Windows/System32/config/SYSTEM. FTK Imager was used for downloading the files, then the downloaded files were examined in RegistryExplorer.



4. Was there a breach?

***Tools Used*: Snort**

We determined that there was a breach after using Snort to analyze the PCAP data. There was a Nmap ICMP ping from IP: 193.61.24.102 probing the network. We used this command: snort -c /etc/snort/snort.conf -r case001.pcap -q -K none -A console | tee snort.out



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

***Tools Used*: Snort and TCPDump**

Moments after determining that there was a breach, we observed rapid connections from an outside source to an inside source - in this case the Domain Controller; IP: 10.42.85.10 on port 3389. Furthermore, that remote IP address, 194.61.24.102 originated in Russia. The RDP connection was then established.

```
sansforensics@siftworkstation: ~/Downloads/Case 001
$ tcpdump -nttttr case001.pcap 'tcp port 3389 and (dst net 10.42.85.0/24 and not src net 10.42.85.0/24)' -c5
reading from file case001.pcap, link-type EN10MB (Ethernet)
2020-09-19 02:19:26.469203 IP 194.61.24.102.38088 > 10.42.85.10.3389: Flags [S], seq 304134196, win 64240, options [mss 1460,sackOK,TS val 2976250824 ecr 0,nop,wscale 7], length 0
2020-09-19 02:19:26.469759 IP 194.61.24.102.38088 > 10.42.85.10.3389: Flags [.], ack 2792490071, win 502, options [nop,nop,TS val 2976250824 ecr 701188], length 0
2020-09-19 02:19:26.469897 IP 194.61.24.102.38088 > 10.42.85.10.3389: Flags [R.], seq 0, ack 1, win 502, options [nop,nop,TS val 2976250824 ecr 701188], length 0
2020-09-19 02:19:26.472244 IP 194.61.24.102.38090 > 10.42.85.10.3389: Flags [S], seq 83770137, win 64240, options [mss 1460,sackOK,TS val 2976250827 ecr 0,nop,wscale 7], length 0
2020-09-19 02:19:26.472579 IP 194.61.24.102.38090 > 10.42.85.10.3389: Flags [.], ack 897565919, win 502, options [nop,nop,TS val 2976250827 ecr 701188], length 0
```

```
09/19-02:19:13.414319  [**] [1:384:5] ICMP PING [**] [Classification: Misc activity] [Priority: 3] {ICMP} 194.61.24.102 -> 10.42.85.10
09/19-02:19:13.414386  [**] [1:453:5] ICMP Timestamp Request [**] [Classification: Misc activity] [Priority: 3] {ICMP} 194.61.24.102 -> 10.42.85.10
09/19-02:19:26.549145  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:38100 -> 10.42.85.10:3389
09/19-02:21:26.112470  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40044 -> 10.42.85.10:3389
09/19-02:21:26.342463  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40046 -> 10.42.85.10:3389
09/19-02:21:26.564666  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40048 -> 10.42.85.10:3389
09/19-02:21:26.786791  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40050 -> 10.42.85.10:3389
09/19-02:21:27.001408  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40052 -> 10.42.85.10:3389
09/19-02:21:27.224505  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40054 -> 10.42.85.10:3389
09/19-02:21:27.437501  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40056 -> 10.42.85.10:3389
09/19-02:21:27.661672  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40058 -> 10.42.85.10:3389
09/19-02:21:27.887579  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40060 -> 10.42.85.10:3389
09/19-02:21:28.099029  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40062 -> 10.42.85.10:3389
09/19-02:21:28.322016  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40064 -> 10.42.85.10:3389
09/19-02:21:28.546732  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40066 -> 10.42.85.10:3389
09/19-02:21:28.761526  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40068 -> 10.42.85.10:3389
09/19-02:21:28.983910  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40070 -> 10.42.85.10:3389
09/19-02:21:29.197633  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40072 -> 10.42.85.10:3389
09/19-02:21:29.419680  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40074 -> 10.42.85.10:3389
09/19-02:21:29.633132  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40076 -> 10.42.85.10:3389
09/19-02:21:29.857974  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40078 -> 10.42.85.10:3389
09/19-02:21:30.080671  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40080 -> 10.42.85.10:3389
09/19-02:21:30.307257  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40082 -> 10.42.85.10:3389
09/19-02:21:30.519633  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40084 -> 10.42.85.10:3389
09/19-02:21:30.746101  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40086 -> 10.42.85.10:3389
09/19-02:21:30.972217  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40088 -> 10.42.85.10:3389
09/19-02:21:31.197246  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40090 -> 10.42.85.10:3389
09/19-02:21:31.411328  [**] [1:1448:12] MISC MS Terminal server request [**] [Classification: Generic Protocol Command Decode] [Priority: 3] {TCP} 194.61.24.102:40092 -> 10.42.85.10:3389
```

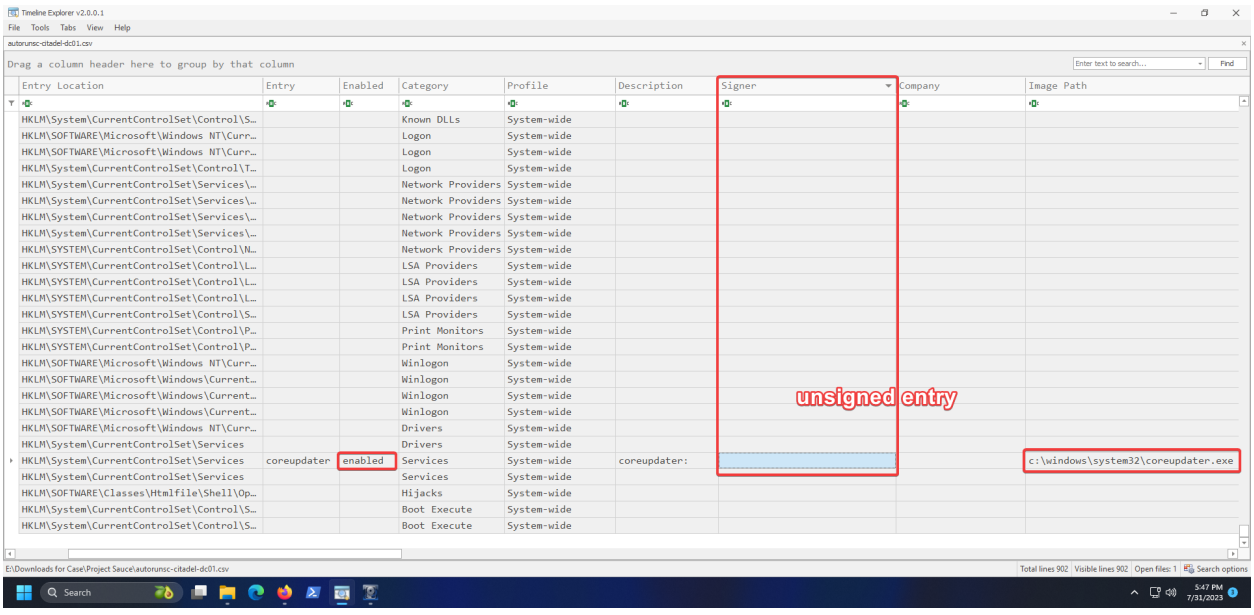
6. **Was malware used? If so, what was it? If there was malware answer the following:**

   - **What process was malicious?**

     coreupdater.exe and spoolsv.exe

Tools Used: Timeline Explorer and Volatility

We found out from the autorun that this program was unsigned and was being run from a privileged location. The situation is intriguing for several reasons. Upon each computer boot, there may be a requirement for updates. However, it remains uncertain whether this is a legitimate process or not. The concerning aspect is that the program originates from a revered directory, System32, which is typically accessible only to privileged users and contains signed software. If the binary is malicious, it might have been placed there by someone with elevated access, such as a System or Administrator level user, indicating a serious security breach. Moreover, the usage of services is a common tactic employed by attackers to establish persistence in the system.



coreupdater was the initial process, it was then migrated to spoolsv.exe.

We can look for evidence of reflective or hidden code injection since this is what Meterpreter typically does in processes. I used volatility

Using the command –

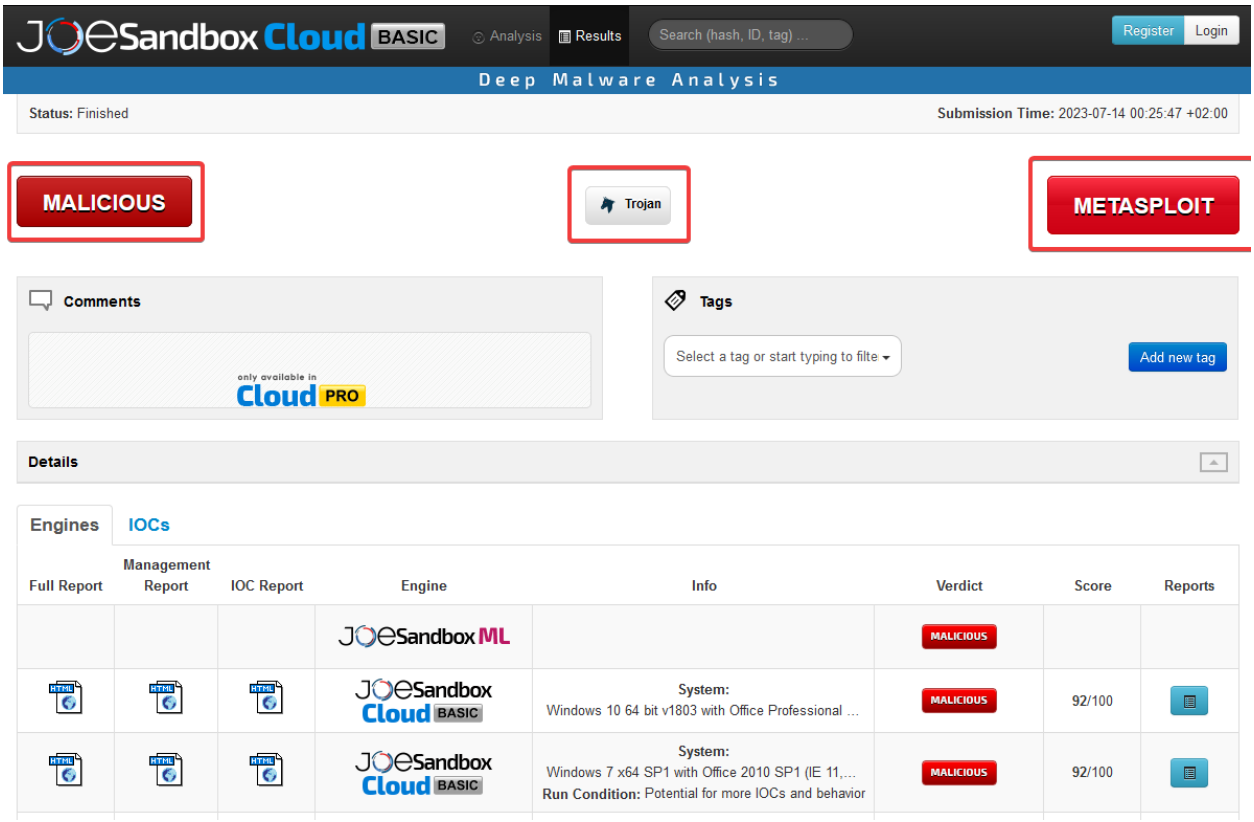
```
vol.py -f citadeldc01.mem --profile=Win2012R2x64_18340 malfind
```

```
Process: spoolsv.exe Pid: 3724 Address: 0x4afc1f0000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: PrivateMemory: 1, Protection: 6

0x0000004afc1f0000  4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00   MZ..............
0x0000004afc1f0010  b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00   ........@.......
0x0000004afc1f0020  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00   ................
0x0000004afc1f0030  00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 00   ................

0x00000000fc1f0000 4d              DEC EBP
0x00000000fc1f0001 5a              POP EDX
0x00000000fc1f0002 90              NOP
0x00000000fc1f0003 0003            ADD [EBX], AL
0x00000000fc1f0005 0000            ADD [EAX], AL
0x00000000fc1f0007 000400          ADD [EAX+EAX], AL
0x00000000fc1f000a 0000            ADD [EAX], AL
0x00000000fc1f000c ff              DB 0xff
0x00000000fc1f000d ff00            INC DWORD [EAX]
0x00000000fc1f000f 00b800000000    ADD [EAX+0x0], BH
0x00000000fc1f0015 0000            ADD [EAX], AL
0x00000000fc1f0017 004000          ADD [EAX+0x0], AL
0x00000000fc1f001a 0000            ADD [EAX], AL
0x00000000fc1f001c 0000            ADD [EAX], AL
0x00000000fc1f001e 0000            ADD [EAX], AL
0x00000000fc1f0020 0000            ADD [EAX], AL
0x00000000fc1f0022 0000            ADD [EAX], AL
0x00000000fc1f0024 0000            ADD [EAX], AL
0x00000000fc1f0026 0000            ADD [EAX], AL
0x00000000fc1f0028 0000            ADD [EAX], AL
0x00000000fc1f002a 0000            ADD [EAX], AL
0x00000000fc1f002c 0000            ADD [EAX], AL
0x00000000fc1f002e 0000            ADD [EAX], AL
0x00000000fc1f0030 0000            ADD [EAX], AL
0x00000000fc1f0032 0000            ADD [EAX], AL
0x00000000fc1f0034 0000            ADD [EAX], AL
0x00000000fc1f0036 0000            ADD [EAX], AL
0x00000000fc1f0038 0000            ADD [EAX], AL
0x00000000fc1f003a 0000            ADD [EAX], AL
0x00000000fc1f003c 0001            ADD [ECX], AL
0x00000000fc1f003e 0000            ADD [EAX], AL
```

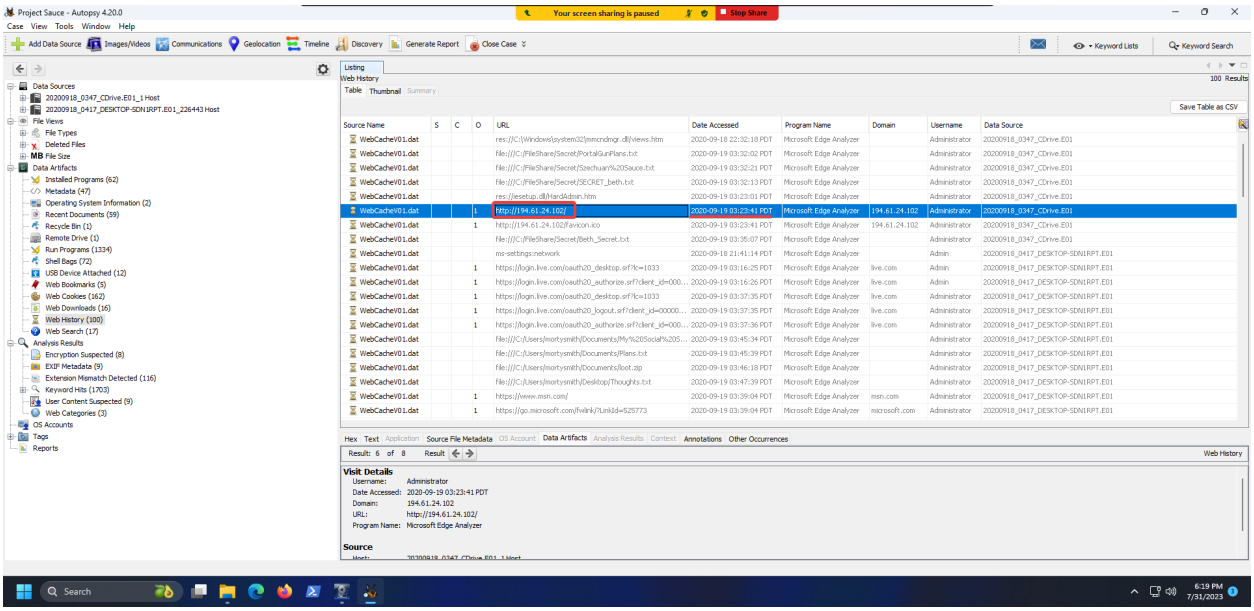
We used JoeSandbox to analyze the malware at https://www.joesandbox.com/#windows. It was determined to be a trojan delivery method and Metasploit clearly.



- **Identify the IP Address that delivered the payload.**

  Tools Used: Autopsy

  Investigating inside Web History Logs on the disk image using Autopsy the IP: 194.61.24.102 was determined via Internet Explorer when the attacker RDP'd in.



- **What IP Address is the malware calling to?**

  IP: 203.78.103.109

  This was found when the malware was analyzed using the Joesandbox report.

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.78.103.109	unknown	Thailand		18362	NETWAY-AS-APNetwayCommunicationCoLtdTH	true

Also after digging in the memory files,

```
nsforensics@siftworkstation: ~/Downloads/Case 001
vol.py -f citadeldc01.mem --profile=Win2012R2x64 netscan |tee netscan.out
```

Using VOLATILITY 2, looking at connections not related to dns.exe with: grep -v dns.exe netscan.out|less

I found this suspicious ip again related to coreupdater.exe

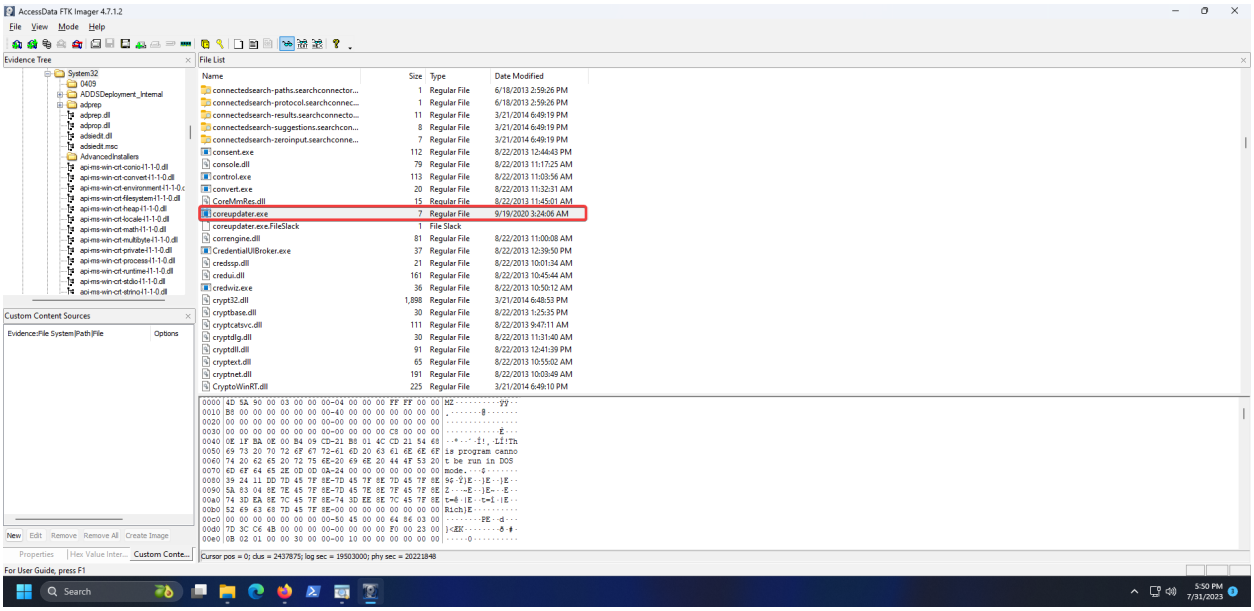
```
0x1b6d06d0       TCPv6    fe80::2dcf:e660:be73:d220:49193 fe80::2dcf:e660:be73:d220:49155 ESTABLISHED     1332     dfsrs.exe
0x1f94a3b0       TCPv6    ::1:62782                       ::1:389                 CLOSED           1292     Microsoft.Acti
0x20471ed0       TCPv4    0.0.0.0:62475                   0.0.0.0:0               LISTENING        3724     spoolsv.exe
0x205cc4f0       TCPv6    fe80::2dcf:e660:be73:d220:49174 fe80::2dcf:e660:be73:d220:49155 ESTABLISHED     1660     dfssvc.exe
0x20fffe50       TCPv4    0.0.0.0:62475                   0.0.0.0:0               LISTENING        3724     spoolsv.exe
0x20fffe50       TCPv6    :::62475                        :::0                    LISTENING        3724     spoolsv.exe
0x20e28d10       TCPv6    fe80::2dcf:e660:be73:d220:49155 fe80::2dcf:e660:be73:d220:62777 CLOSED           460      lsass.exe
0x20f52a00       TCPv6    fe80::2dcf:e660:be73:d220:135   fe80::2dcf:e660:be73:d220:62779 CLOSED           684      svchost.exe
0x20fc7590       TCPv4    10.42.85.10:62613               203.78.103.109:443      ESTABLISHED      3644     coreupdater.ex
0x2253d010       TCPv6    ::1:49160                       ::1:389                 ESTABLISHED      1392     ismserv.exe
0x251e0640       TCPv6    ::1:49161                       ::1:389                 ESTABLISHED      1392     ismserv.exe
0x2bbced10       TCPv6    fe80::2dcf:e660:be73:d220:49155 fe80::2dcf:e660:be73:d220:49193 ESTABLISHED     460      lsass.exe
0x2eaf9d10       TCPv6    fe80::2dcf:e660:be73:d220:62777 fe80::2dcf:e660:be73:d220:49155 CLOSED           460      lsass.exe
0x3111ea70       TCPv6    ::1:389                         ::1:49161               ESTABLISHED      460      lsass.exe
0x3c594880       UDPv4    0.0.0.0:0                       *:*                                      460      lsass.exe      2020-09-19 01:22:50 UTC+0000
0x3c522500       TCPv4    0.0.0.0:636                     0.0.0.0:0               LISTENING        460      lsass.exe
```

- **Where is this malware on disk?**

  Tools Used: FTK Imager

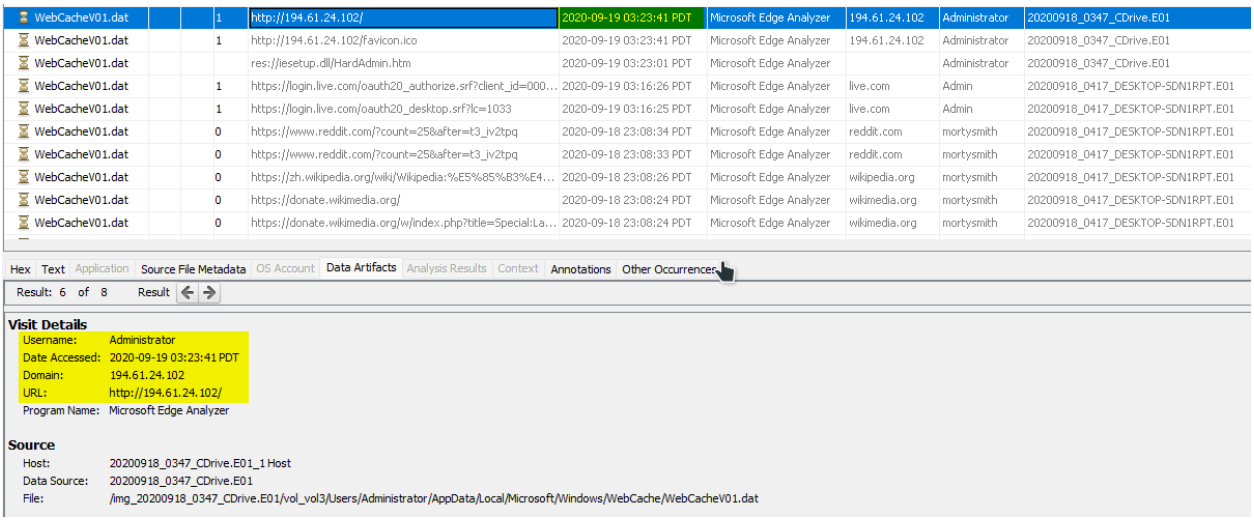
  Image Path = c:\windows\system32\coreupdater.exe

  This was found using FTK Imager when I tried to look for the coreupdater file. The location was cross-referenced with the location provided in the autoruns.



- **When did it first appear?**
  Tools Used: TimeLine Explorer

The malware was downloaded at 03:23:41 PDT from internet explorer into the downloads folder. We can see the time matches as seen in the web cache and the usrclass.dat file below.



WebCacheV01.dat			1	http://194.61.24.102/	2020-09-19 03:23:41 PDT	Microsoft Edge Analyzer	194.61.24.102	Administrator	20200918_0347_CDrive.E01
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.E01
WebCacheV01.dat				res://iesetup.dll/HardAdmin.htm	2020-09-19 03:23:01 PDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat			1	https://login.live.com/oauth20_authorize.srf?client_id=000...	2020-09-19 03:16:26 PDT	Microsoft Edge Analyzer	live.com	Admin	20200918_0417_DESKTOP-SDN1RPT.E01
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-SDN1RPT.E01
WebCacheV01.dat			0	https://www.reddit.com/?count=25&after=t3_jv2tpq	2020-09-18 23:08:34 PDT	Microsoft Edge Analyzer	reddit.com	mortysmith	20200918_0417_DESKTOP-SDN1RPT.E01
WebCacheV01.dat			0	https://www.reddit.com/?count=25&after=t3_jv2tpq	2020-09-18 23:08:33 PDT	Microsoft Edge Analyzer	reddit.com	mortysmith	20200918_0417_DESKTOP-SDN1RPT.E01
WebCacheV01.dat			0	https://zh.wikipedia.org/wiki/Wikipedia:%E5%85%B3%E4...	2020-09-18 23:08:26 PDT	Microsoft Edge Analyzer	wikipedia.org	mortysmith	20200918_0417_DESKTOP-SDN1RPT.E01
WebCacheV01.dat			0	https://donate.wikimedia.org/	2020-09-18 23:08:24 PDT	Microsoft Edge Analyzer	wikimedia.org	mortysmith	20200918_0417_DESKTOP-SDN1RPT.E01
WebCacheV01.dat			0	https://donate.wikimedia.org/w/index.php?title=Special:La...	2020-09-18 23:08:24 PDT	Microsoft Edge Analyzer	wikimedia.org	mortysmith	20200918_0417_DESKTOP-SDN1RPT.E01

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

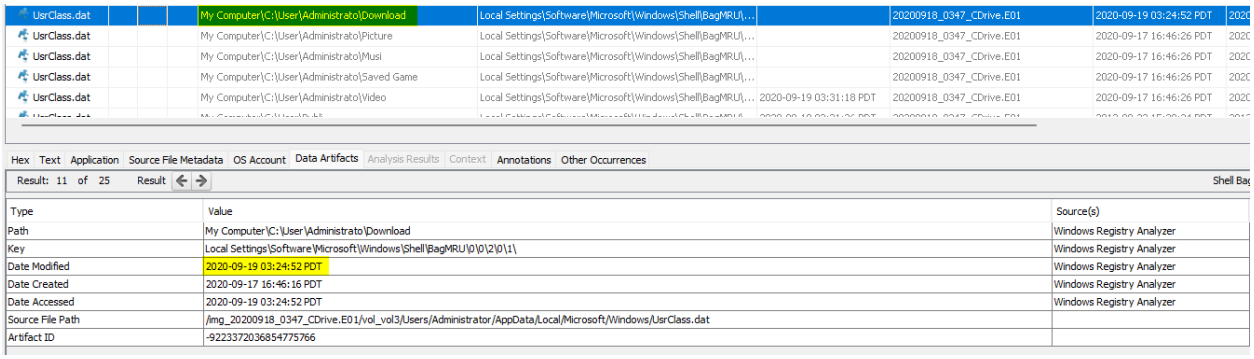
Result: 6 of 8 Result

Visit Details

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

Source

Host:	20200918_0347_CDrive.E01_1 Host
Data Source:	20200918_0347_CDrive.E01
File:	/img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat



UsrClass.dat			My Computer\C:\User\Administrato\Download	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...		20200918_0347_CDrive.E01	2020-09-19 03:24:52 PDT
UsrClass.dat			My Computer\C:\User\Administrato\Picture	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...		20200918_0347_CDrive.E01	2020-09-17 16:46:26 PDT
UsrClass.dat			My Computer\C:\User\Administrato\Musi	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...		20200918_0347_CDrive.E01	2020-09-17 16:46:26 PDT
UsrClass.dat			My Computer\C:\User\Administrato\Saved Game	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...		20200918_0347_CDrive.E01	2020-09-17 16:46:26 PDT
UsrClass.dat			My Computer\C:\User\Administrato\Video	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\...	2020-09-19 03:31:18 PDT	20200918_0347_CDrive.E01	2020-09-17 16:46:26 PDT

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

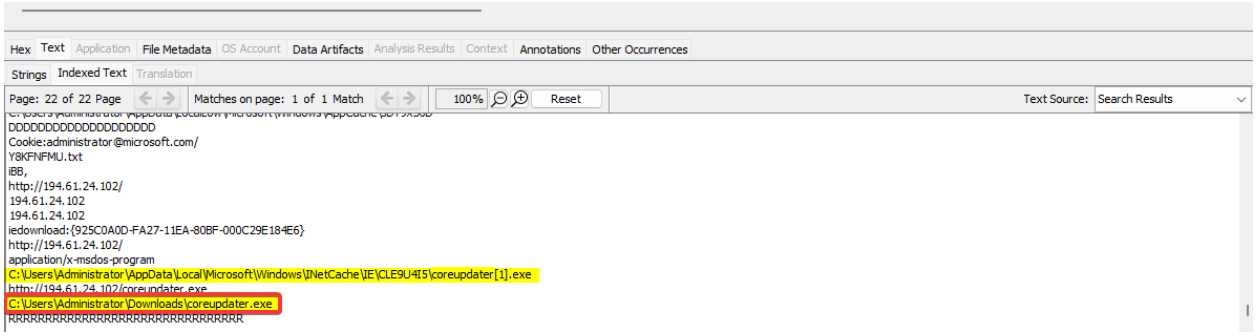
Result: 11 of 25 Result

Type	Value	Source(s)
Path	My Computer\C:\User\Administrato\Download	Windows Registry Analyzer
Key	Local Settings\Software\Microsoft\Windows\Shell\BagMRU\0\0\2\0\1\	Windows Registry Analyzer
Date Modified	2020-09-19 03:24:52 PDT	Windows Registry Analyzer
Date Created	2020-09-17 16:46:16 PDT	Windows Registry Analyzer
Date Accessed	2020-09-19 03:24:52 PDT	Windows Registry Analyzer
Source File Path	/img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/AppData/Local/Microsoft/Windows/UsrClass.dat	
Artifact ID	-9223372036854775766	

- **Did someone move it?**
  Tools Used: **Autopsy**

Yes, it appears to be moved from the Administrator/Downloads to Windows/System32/. This info was found by looking at the web cache file.

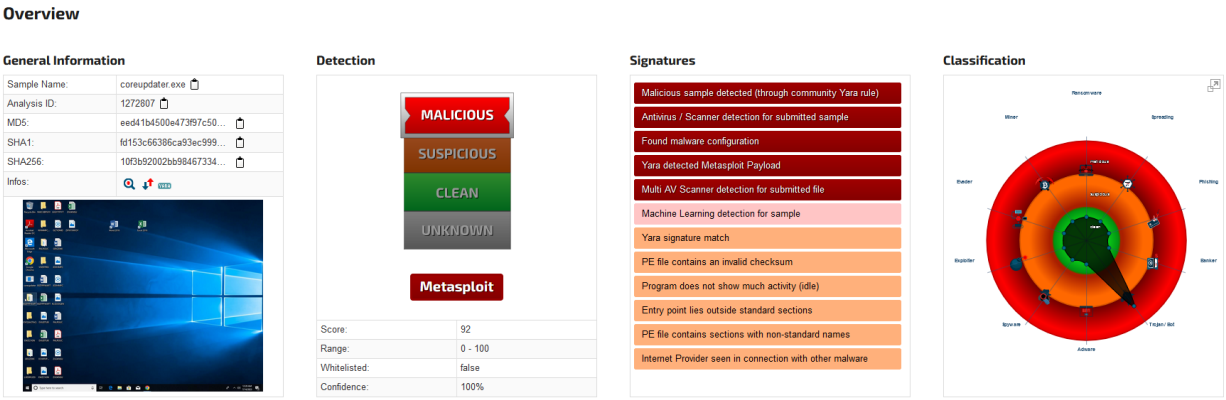
Name	Keyword Preview	Location
WebCacheV01.dat	tCache\IE\CLE9U4I5\«coreupdater«[1].exehttp://194.61	/img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/AppData/L
V01.log	102/coreupdater.exe«coreupdater«[1].exeHTTP/1.0 200	/img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/AppData/L
pagefile.sys	be stopped.WudfPf«coreupdater«ShareListViewModelTemplate	/img_20200918_0347_CDrive.E01/vol_vol3/pagefile.sys
SYSTEM	b6d912}000Ank t.«coreupdater«vk HImagePathC:\W	/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config/SYS
$LogFile	(@h@(8`8^RCRD(«coreupdater«[1].exeCOREUP~1.EXER	/img_20200918_0347_CDrive.E01/vol_vol3/$LogFile
$UsnJrnl:$J	<UsrClass.dat$<«coreupdater«[1].exe`$<«coreupdater«[1].exe`	/img_20200918_0347_CDrive.E01/vol_vol3/$Extend/$UsnJrnl:$J
SYSTEM.LOG1	b6d912}000Ank t.«coreupdater«vk HImagePathC:\W	/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config/SYS
SYSTEM.LOG2	b6d912}000Ank t.«coreupdater«vk HImagePathC:\W	/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config/SYS
RegRipper /img_20200918_0347_CDrive.E01/vol_vol3/V	2020Z Name = «coreupdater« Display = ImagePath	RegRipper /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32



- **What were the capabilities of this malware?**
  Tools Used: JoeSandbox

  Many. It's Metasploit and is quite versatile. It is capable of process migration, credential theft, keylogging, screen scraping, many many modules…

  Using Joesandbox reports⟶ The malware is meterpreter



- **Is this malware easily obtained?**

  Yes. It comes with Metasploit Framework which is free to download and use.

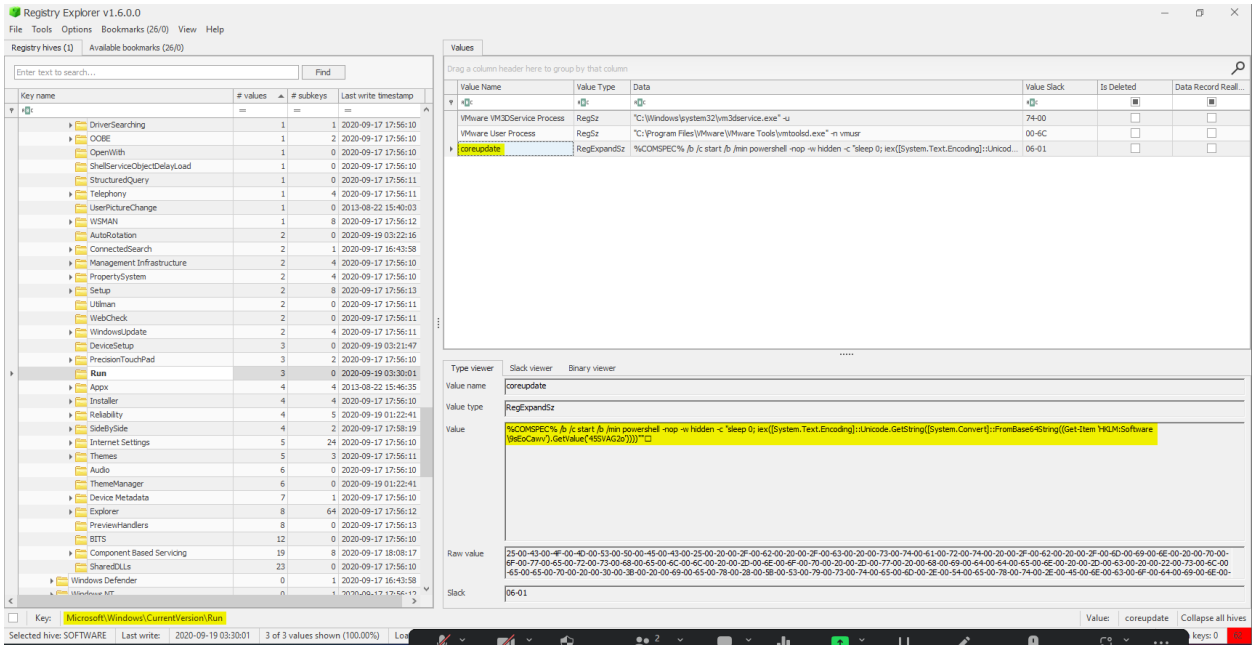
- **Was this malware installed with persistence on any machine?**
  Tools Used: Registry Explorer

- When? The last write in the registry seems to be updated at 3:30 on September 19, as shown in the picture below.

Microsoft\Windows\CurrentVersion\Run		
SOFTWARE	Last write:	2020-09-19 03:30:01

Tools Used: Registry Explorer

- Where? Persistence in the registry at CurrentVersion\Run and installed as a service. I found the following in the registry files using registry explorer.exe

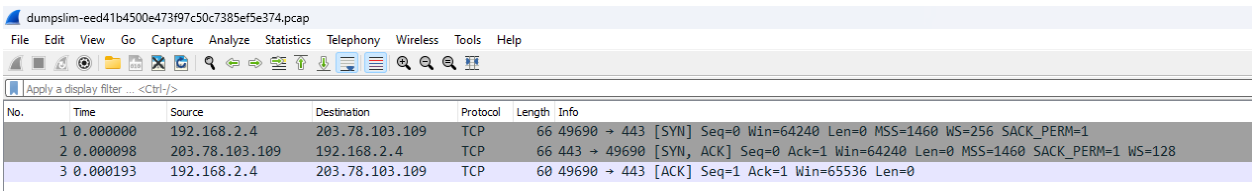


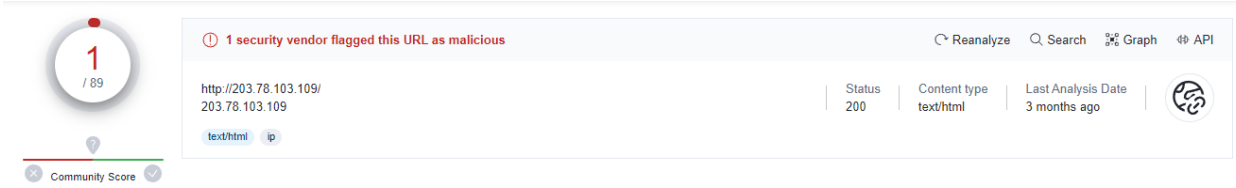
7. What malicious IP Addresses were involved?

Tools Used: **Wireshark**

- **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.





- **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**

- 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.

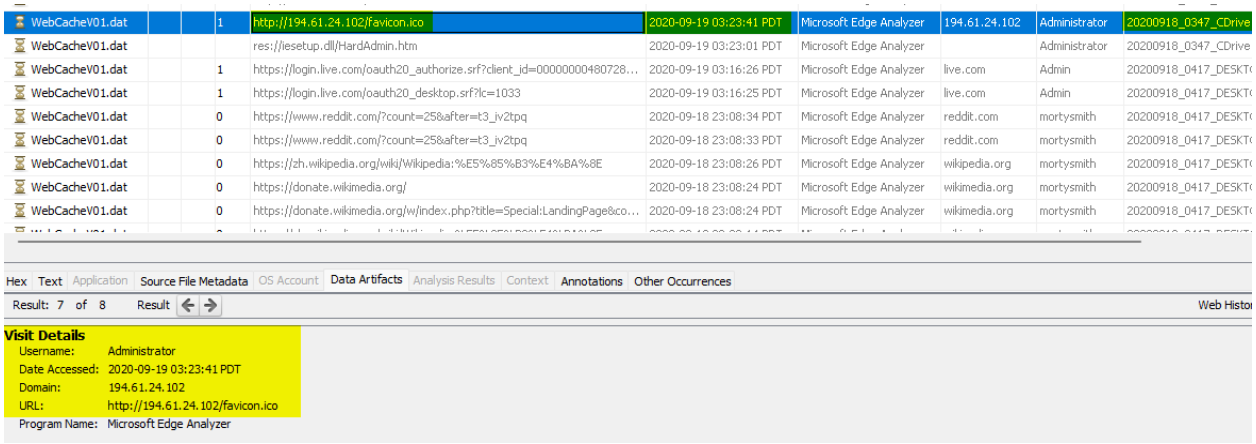
```
sansforensics@siftworkstation: ~/Downloads/Case 001
$ tcpdump -nttttr case001.pcap 'tcp port 3389 and (src net 10.42.85.0/24 and dst net 10.42.85.0/24)' -c15
reading from file case001.pcap, link-type EN10MB (Ethernet)
2020-09-19 02:35:55.285340 IP 10.42.85.10.62514 > 10.42.85.115.3389: Flags [SEW], 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
```

- When?

Tools Used: **Autopsy**

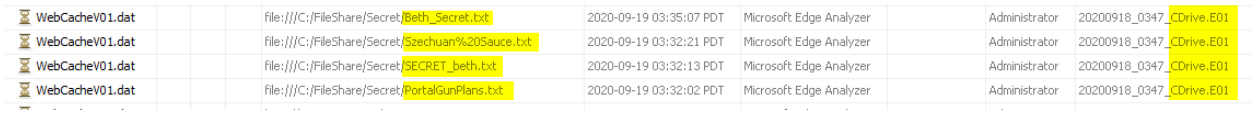
The compromised Domain Administrator account initiated a connection to the Desktop-SDN1RPT machine from Domain Controller, CITADEL-DC01, at 02:35:55 UTC on 19 September 2020 according to the PCAP, or 03:35:54 on 19 September 2020 according to the Super Timeline when left uncorrected. In reality, it was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

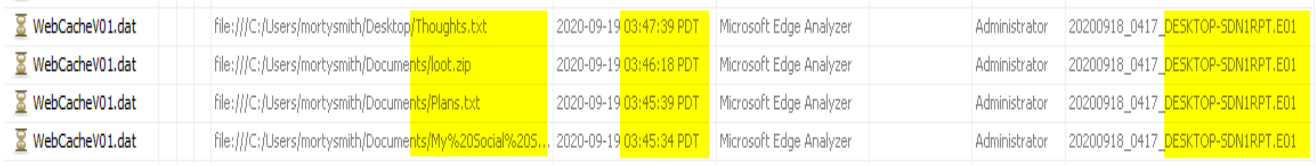


- Did the attacker steal or access any data?

  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?

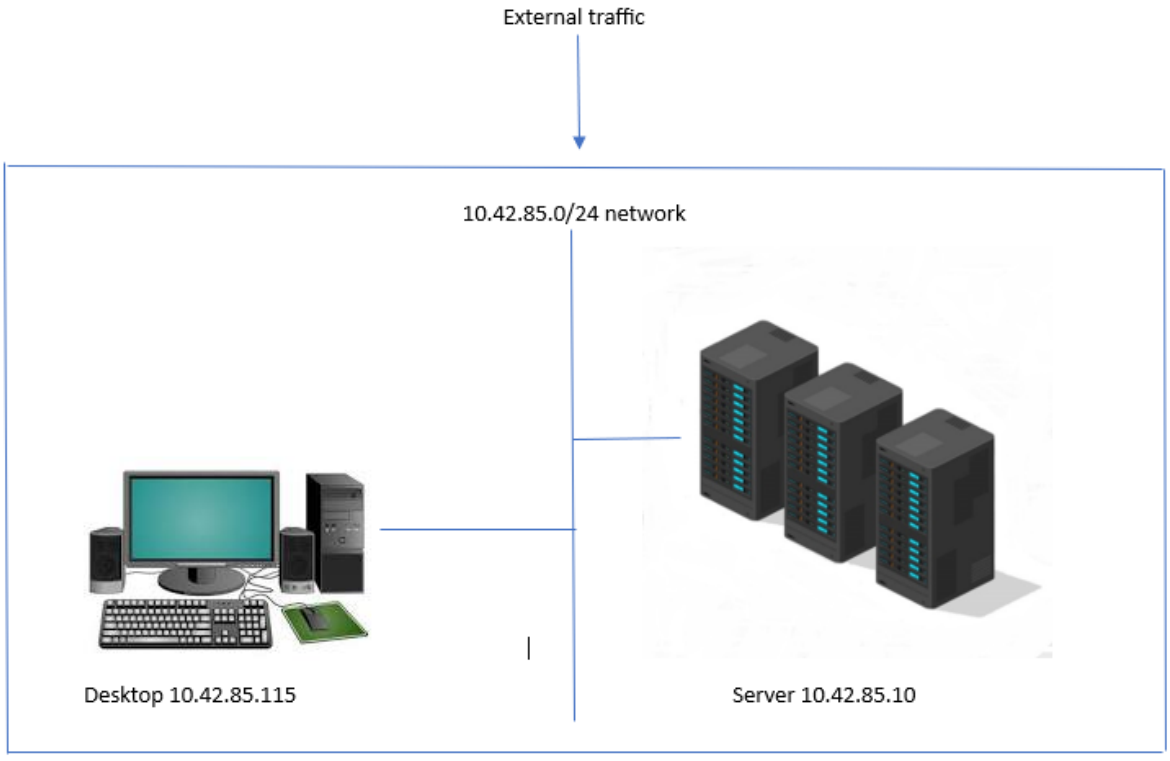
The network layout you provided is a small local area network (LAN) with a subnet of 10.42.85.0/24. This means the network can accommodate up to 256 IP addresses (from 10.42.85.0 to 10.42.85.255), where the first three octets (10.42.85) represent the network address, and the last octet can be assigned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

Joe Security LLC. (2016). *Automated Malware Analysis - Joe Sandbox Cloud Basic*. Joesandbox.com. https://www.joesandbox.com/#windows

Snort - Network Intrusion Detection & Prevention System. (2023). Snort.org. https://www.snort.org/

Home | TCPDUMP & LIBPCAP. (2023). Tcpdump.org. https://www.tcpdump.org/

Autopsy | Digital Forensics. (2023, June 23). Autopsy. https://www.autopsy.com/

Overview. Metasploit Documentation Penetration Testing Software, Pen Testing Security. (2017). https://docs.metasploit.com/docs/using-metasploit/advanced/meterpreter/meterpreter.html

Wireshark · Go Deep. (2023). Wireshark. https://www.wireshark.org/

Registry Explorer | SANS Institute. (2023, August 5). Sans.org. https://www.sans.org/tools/registry-explorer/

FTK® Imager - Exterro. (2023). Exterro. https://www.exterro.com/ftk-imager

Timeline Explorer | SANS Institute. (2023, August 5). Sans.org. https://www.sans.org/tools/timeline-explorer/

VirusTotal. (2000). Virustotal.com. https://www.virustotal.com/