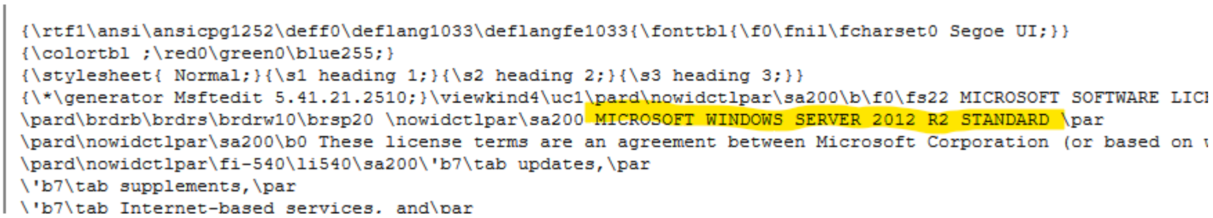
Seena Davoodi Scott Maclean

Questions to Answer and Goals from the Case

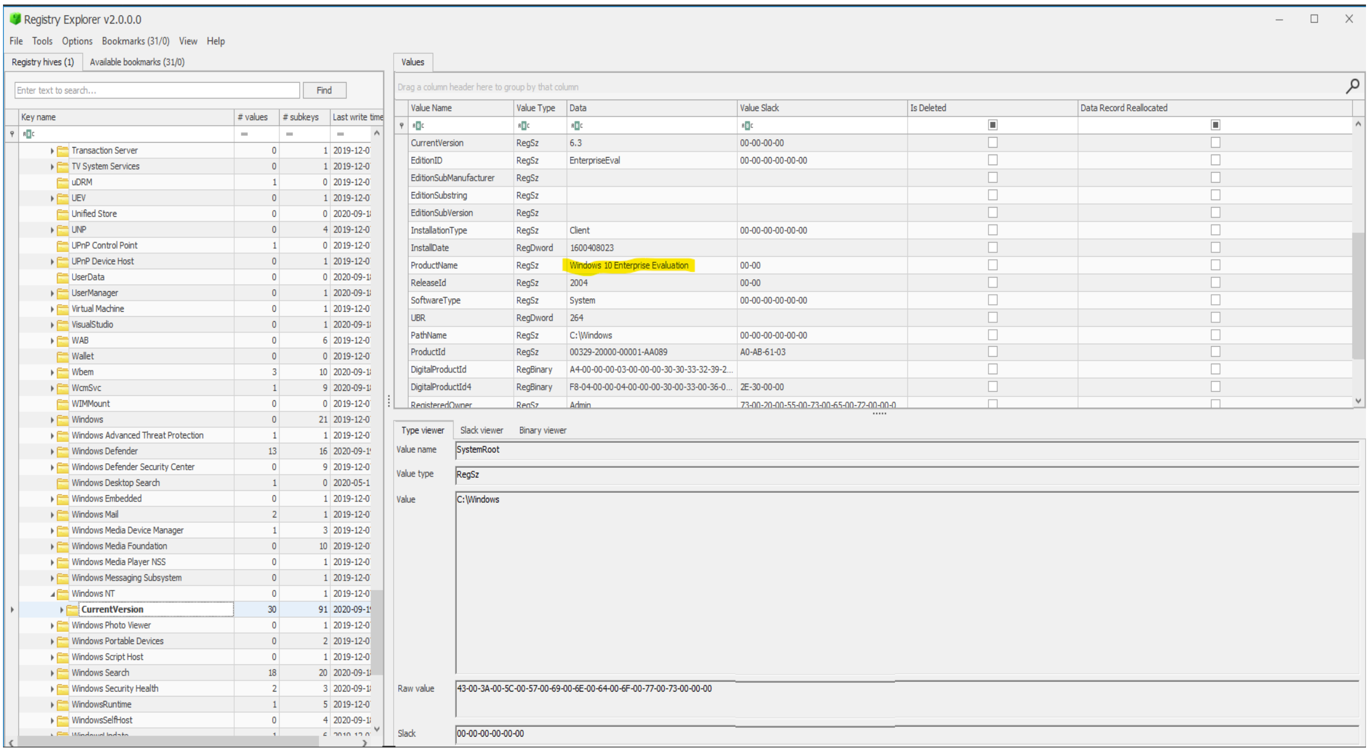
Answer the following questions and use the submission guidelines below to ensure you are providing an explanation of your process, screen captures of where you found each answer and the tools and artifacts you used.

1. What's the Operating System of the Server? Scott Maclean
   - ○ Windows Server 2012 R2 Standard Evaluation
   - ○ Path Using FTKImager, we have mounted the disk image of the DC01 drive into the system and navigate to -> C:\Windows\System32\License



```
{\rtf1\ansi\ansicpg1252\deff0\deflang1033\deflangfe1033{\fonttbl{\f0\fnil\fcharset0 Segoe UI;}}
{\colortbl ;\red0\green0\blue255;}
{\stylesheet{ Normal;}{\s1 heading 1;}{\s2 heading 2;}{\s3 heading 3;}}
{\*\generator Msftedit 5.41.21.2510;}\viewkind4\uc1\pard\nowidctlpar\sa200\b\f0\fs22 MICROSOFT SOFTWARE LICI
\pard\brdrb\brdrs\brdrw10\brsp20 \nowidctlpar\sa200 MICROSOFT WINDOWS SERVER 2012 R2 STANDARD \par
\pard\nowidctlpar\sa200\b0 These license terms are an agreement between Microsoft Corporation (or based on t
\pard\nowidctlpar\fi-540\li540\sa200\'b7\tab updates,\par
\'b7\tab supplements,\par
\'b7\tab Internet-based services, and\par
```

2. What's the Operating System of the Desktop? Seena Davoodi
   - ○ Windows 10 Enterprise Evaluation
   - ○ Exported SOFTWARE hive from desktop registry, uploaded to registry explorer. Path -> KHLM-SOFTWARE-Microsoft-Windows NT-Current Version



Registry Explorer v2.0.0.0
File Tools Options Bookmarks (31/0) View Help
Registry hives (1) Available bookmarks (31/0)
Enter text to search...
Find
Values
Drag a column header here to group by that column
Type viewer Slack viewer Binary viewer

Key name	# values	# subkeys	Last write time
Transaction Server	0	1	2019-12-0
TV System Services	0	1	2019-12-0
uDRM	1	0	2019-12-0
UEV	0	1	2019-12-0
Unified Store	0	0	2020-09-1
UNP	0	4	2019-12-0
UPnP Control Point	1	0	2019-12-0
UPnP Device Host	0	1	2019-12-0
UserData	0	0	2020-09-1
UserManager	0	1	2020-09-1
Virtual Machine	0	1	2019-12-0
VisualStudio	0	1	2020-09-1
WAB	0	6	2019-12-0
Wallet	0	0	2019-12-0
Wbem	3	10	2020-09-1
WcmSvc	1	9	2020-09-1
WIMMount	0	0	2019-12-0
Windows	0	21	2019-12-0
Windows Advanced Threat Protection	1	1	2019-12-0
Windows Defender	13	16	2020-09-1
Windows Defender Security Center	0	9	2019-12-0
Windows Desktop Search	1	0	2020-05-1
Windows Embedded	0	1	2019-12-0
Windows Mail	2	1	2019-12-0
Windows Media Device Manager	1	3	2019-12-0
Windows Media Foundation	0	10	2019-12-0
Windows Media Player NSS	0	1	2019-12-0
Windows Messaging Subsystem	0	1	2019-12-0
Windows NT	0	1	2019-12-0
CurrentVersion	30	91	2020-09-1
Windows Photo Viewer	0	1	2019-12-0
Windows Portable Devices	0	2	2019-12-0
Windows Script Host	0	1	2019-12-0
Windows Search	18	20	2020-09-1
Windows Security Health	2	3	2020-09-1
WindowsRuntime	1	5	2019-12-0
WindowsSelfHost	0	4	2020-09-1

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
CurrentVersion	RegSz	6.3	00-00-00-00	☐	☐
EditionID	RegSz	EnterpriseEval	00-00-00-00-00-00	☐	☐
EditionSubManufacturer	RegSz			☐	☐
EditionSubstring	RegSz			☐	☐
EditionSubVersion	RegSz			☐	☐
InstallationType	RegSz	Client	00-00-00-00-00-00	☐	☐
InstallDate	RegDword	1600408023		☐	☐
ProductName	RegSz	Windows 10 Enterprise Evaluation	00-00	☐	☐
ReleaseId	RegSz	2004	00-00	☐	☐
SoftwareType	RegSz	System	00-00-00-00-00-00	☐	☐
UBR	RegDword	264		☐	☐
PathName	RegSz	C:\Windows	00-00-00-00-00-00	☐	☐
ProductId	RegSz	00329-20000-00001-AA089	A0-AB-61-03	☐	☐
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33-32-39-2...		☐	☐
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-33-00-36-0...	2E-30-00-00	☐	☐
RegisteredOwner	RegSz	Admin	73-00-20-00-55-00-73-00-65-00-72-00-00-0	☐	☐

Value name: SystemRoot

Value type: RegSz

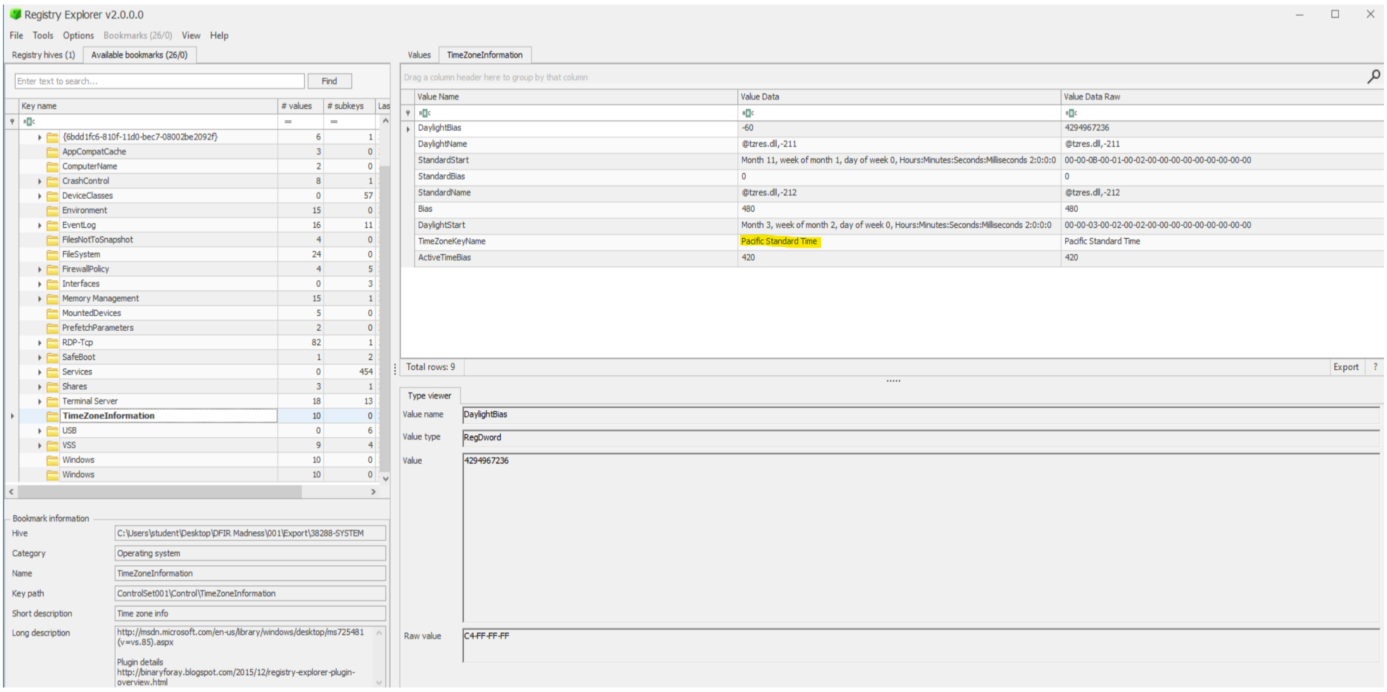
Value: C:\Windows

Raw value: 43-00-3A-00-5C-00-57-00-69-00-6E-00-64-00-6F-00-77-00-73-00-00-00

Slack: 00-00-00-00-00-00

3. What was the local time of the Server? Scott Maclean

    - Pacific Standard Time
    - We extracted the SYSTEM hive from the Server Registry using FTKImager by going into CDriveE01-Partition 2-Root-Windows-System32-Config. From there we saw the SYSTEM hive, exported it to our desktop and uploaded that file into Eric Zimmermans Registry Explorer. From there we took the Path->HKLM-ControlSet001-TimeZoneInformation


Registry Explorer v2.0.0.0
File Tools Options Bookmarks (26/0) View Help
Registry hives (1)
Available bookmarks (26/0)
Enter text to search...
Find
Values
TimeZoneInformation
Drag a column header here to group by that column
Export
?
Type viewer

Key name	# values	# subkeys
{6bdd1fc6-810f-11d0-bec7-08002be2092f}	6	1
AppCompatCache	3	0
ComputerName	2	0
CrashControl	8	1
DeviceClasses	0	57
Environment	15	0
EventLog	16	11
FilesNotToSnapshot	4	0
FileSystem	24	0
FirewallPolicy	4	5
Interfaces	0	3
Memory Management	15	1
MountedDevices	5	0
PrefetchParameters	2	0
RDP-Tcp	82	1
SafeBoot	1	2
Services	0	454
Shares	3	1
Terminal Server	18	13
TimeZoneInformation	10	0
USB	0	6
VSS	9	4
Windows	10	0
Windows	10	0

Bookmark information

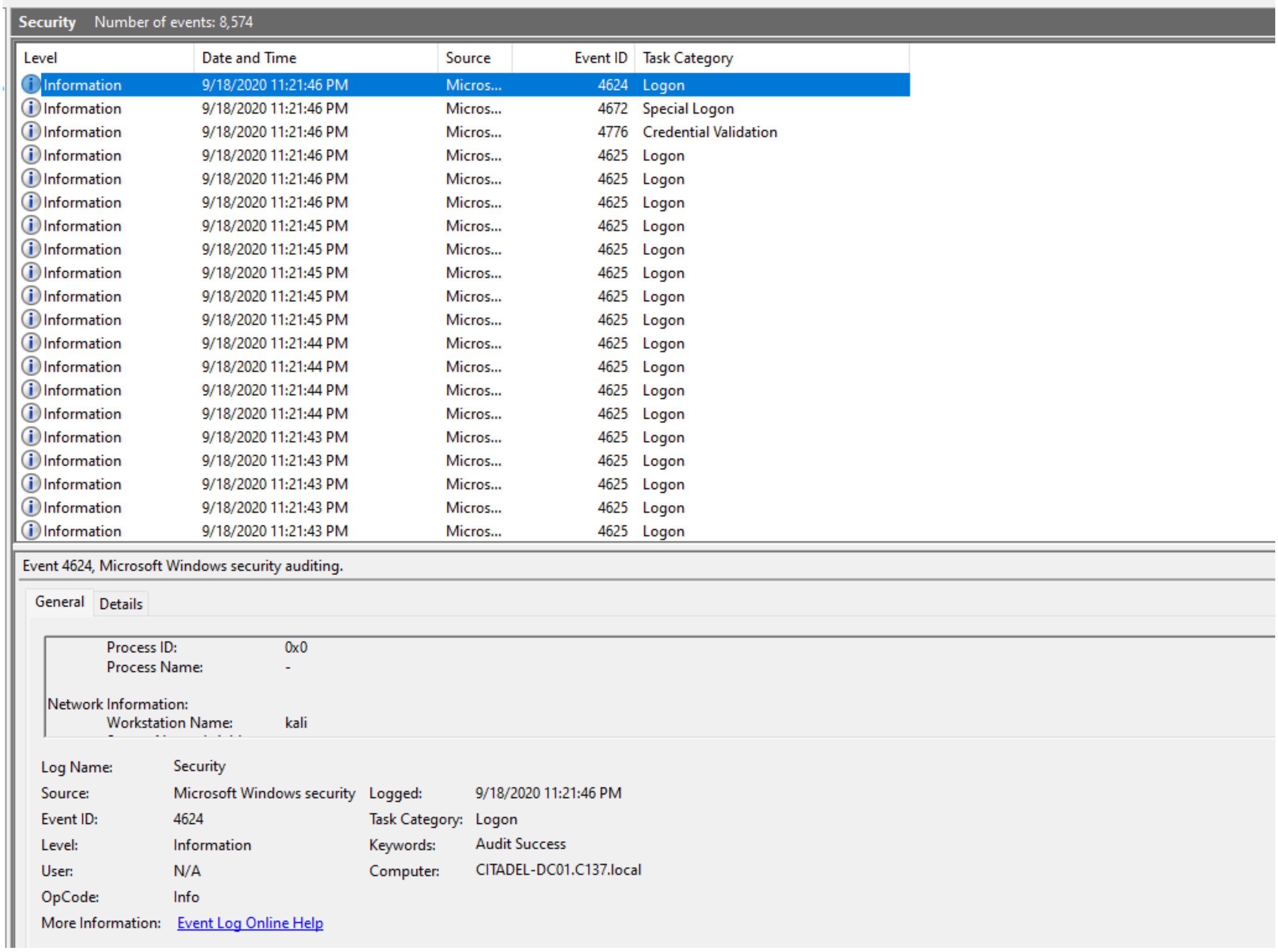
Hive	C:\Users\student\Desktop\DFIR Madness\001\Export\38288-SYSTEM
Category	Operating system
Name	TimeZoneInformation
Key path	ControlSet001\Control\TimeZoneInformation
Short description	Time zone info
Long description	http://msdn.microsoft.com/en-us/library/windows/desktop/ms725481(v=vs.85).aspx Plugin details http://binaryforay.blogspot.com/2015/12/registry-explorer-plugin-overview.html

Value Name	Value Data	Value Data Raw
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-211	@tzres.dll,-211
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0B-00-01-00-02-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
Bias	480	480
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time
ActiveTimeBias	420	420

Total rows: 9

Value name	DaylightBias
Value type	RegDword
Value	4294967236
Raw value	C4-FF-FF-FF

4. Was there a breach?
    - Yes, FBI was involved in confirming the breach.
5. What was the initial entry vector (how did they get in)? **Scott Maclean**
    - RDP Brute Force Attack. We extracted the HKLM (Local Machine) Security Hive security event logs into the Windows event viewer tool. Filtered for failed login attempts using event ID 4625. Noted first failed login attempt was at 9/18/2020 11:21:25PM from a kali machine. Numerous failed login attempts were recorded in less than a minute. At 11:21:46PM the attacker assigned themselves new privileges and successfully logged into the server.



Security   Number of events: 8,574

Level	Date and Time	Source	Event ID	Task Category
Information	9/18/2020 11:21:46 PM	Micros...	4624	Logon
Information	9/18/2020 11:21:46 PM	Micros...	4672	Special Logon
Information	9/18/2020 11:21:46 PM	Micros...	4776	Credential Validation
Information	9/18/2020 11:21:46 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:46 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:46 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:45 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:45 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:45 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:45 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:45 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:44 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:44 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:44 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:44 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:43 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:43 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:43 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:43 PM	Micros...	4625	Logon
Information	9/18/2020 11:21:43 PM	Micros...	4625	Logon

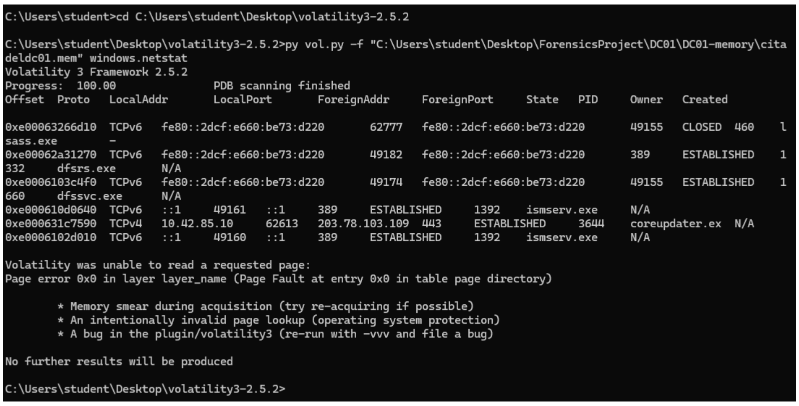
Event 4624, Microsoft Windows security auditing.

Process ID: 0x0
Process Name: -

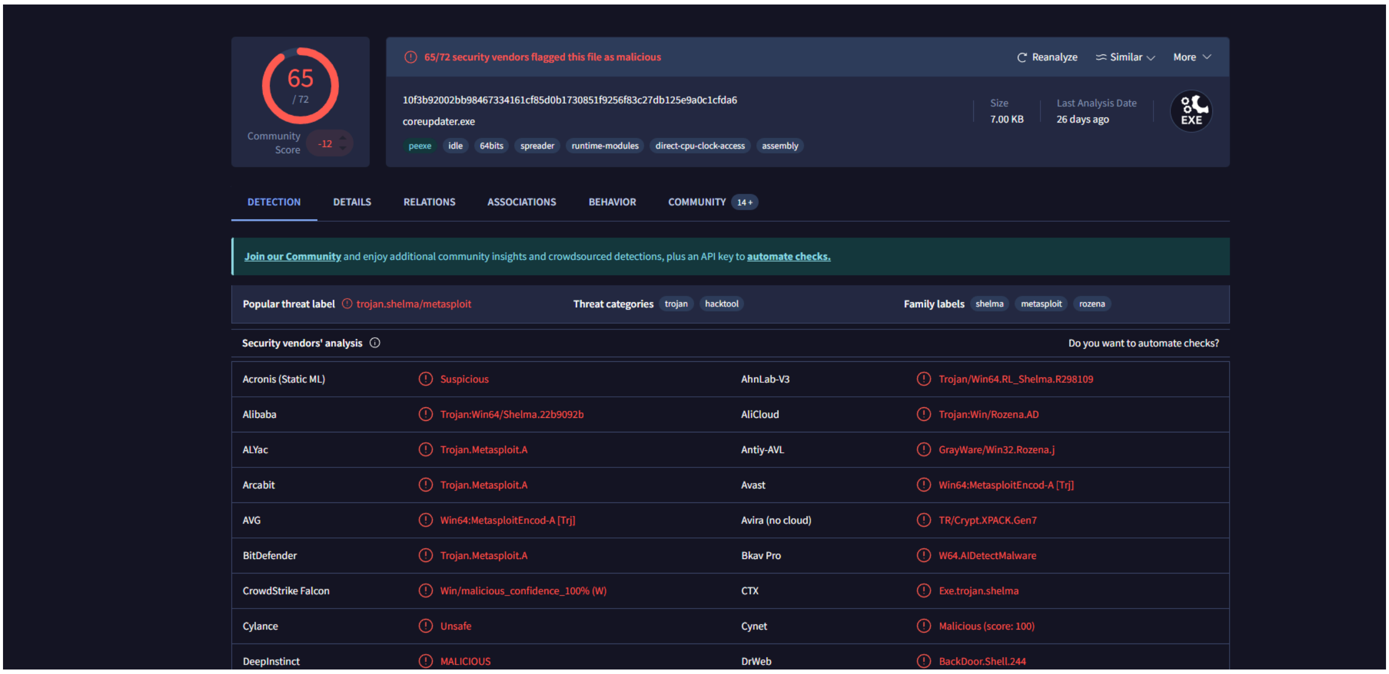
Network Information:
Workstation Name: kali

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	9/18/2020 11:21:46 PM
Event ID:	4624	Task Category:	Logon
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	CITADEL-DC01.C137.local
OpCode:	Info		
More Information:	Event Log Online Help		

6. Was malware used? If so, what was it? If there was malware answer the following: Seena Davoodi
    - What process was malicious?
        - Coreupdater.exe
        - Using the volatility 3 tool, we were able to analyze the memory dump for the DC using various plugins. Once we loaded the file into volatility and used the plugin windows.netstat, we were able to see that an executable "coreupdater" was offloaded onto IP 10.42.85.10 by IP address 203.78.103.109:



```
C:\Users\student>cd C:\Users\student\Desktop\volatility3-2.5.2

C:\Users\student\Desktop\volatility3-2.5.2>py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\cita
deldc01.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe00063266d10  TCPv6   fe80::2dcf:e660:be73:d220       62777   fe80::2dcf:e660:be73:d220       49155   CLOSED  460     l
sass.exe        -
0xe00062a31270  TCPv6   fe80::2dcf:e660:be73:d220       49182   fe80::2dcf:e660:be73:d220       389     ESTABLISHED     1
332     dfsrs.exe       N/A
0xe0006103c4f0  TCPv6   fe80::2dcf:e660:be73:d220       49174   fe80::2dcf:e660:be73:d220       49155   ESTABLISHED     1
660     dfssvc.exe      N/A
0xe000610d0640  TCPv6   ::1     49161   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A
0xe000631c7590  TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0xe0006102d010  TCPv6   ::1     49160   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A

Volatility was unable to read a requested page:
Page error 0x0 in layer layer_name (Page Fault at entry 0x0 in table page directory)

        * Memory smear during acquisition (try re-acquiring if possible)
        * An intentionally invalid page lookup (operating system protection)
        * A bug in the plugin/volatility3 (re-run with -vvv and file a bug)

No further results will be produced

C:\Users\student\Desktop\volatility3-2.5.2>
```



65 / 72

Community Score -12

65/72 security vendors flagged this file as malicious

10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

coreupdater.exe

Size 7.00 KB

Last Analysis Date 26 days ago

Popular threat label trojan.shelma/metasploit

Threat categories trojan hacktool

Family labels shelma metasploit rozena

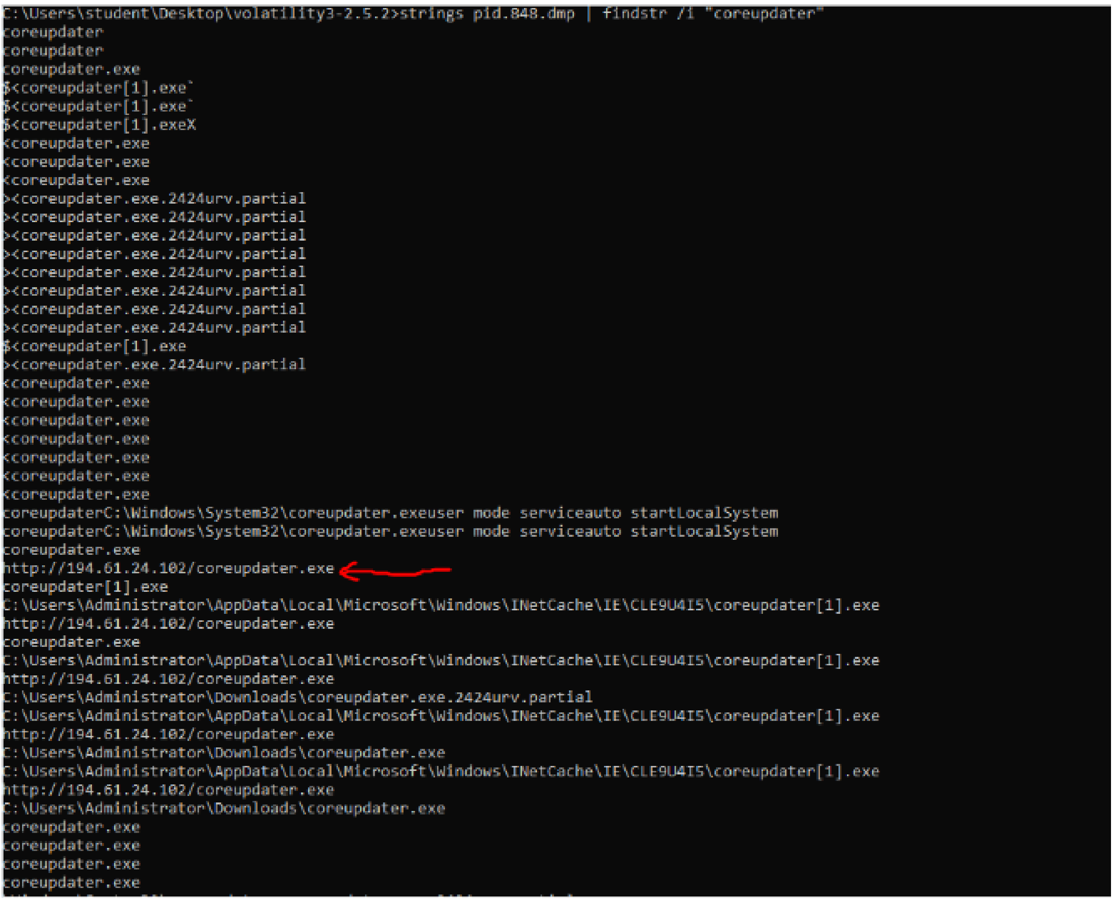
Security vendors' analysis

Do you want to automate checks?

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win64.RL_Shelma.R298109
Alibaba	Trojan:Win64/Shelma.22b9092b	AliCloud	Trojan:Win/Rozena.AD
ALYac	Trojan.Metasploit.A	Antiy-AVL	GrayWare/Win32.Rozena.j
Arcabit	Trojan.Metasploit.A	Avast	Win64:MetasploitEncod-A [Trj]
AVG	Win64:MetasploitEncod-A [Trj]	Avira (no cloud)	TR/Crypt.XPACK.Gen7
BitDefender	Trojan.Metasploit.A	Bkav Pro	W64.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Exe.trojan.shelma
Cylance	Unsafe	Cynet	Malicious (score: 100)
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Shell.244

We can see after adding the hash to virus total that the malware has been identified as Metasploit.

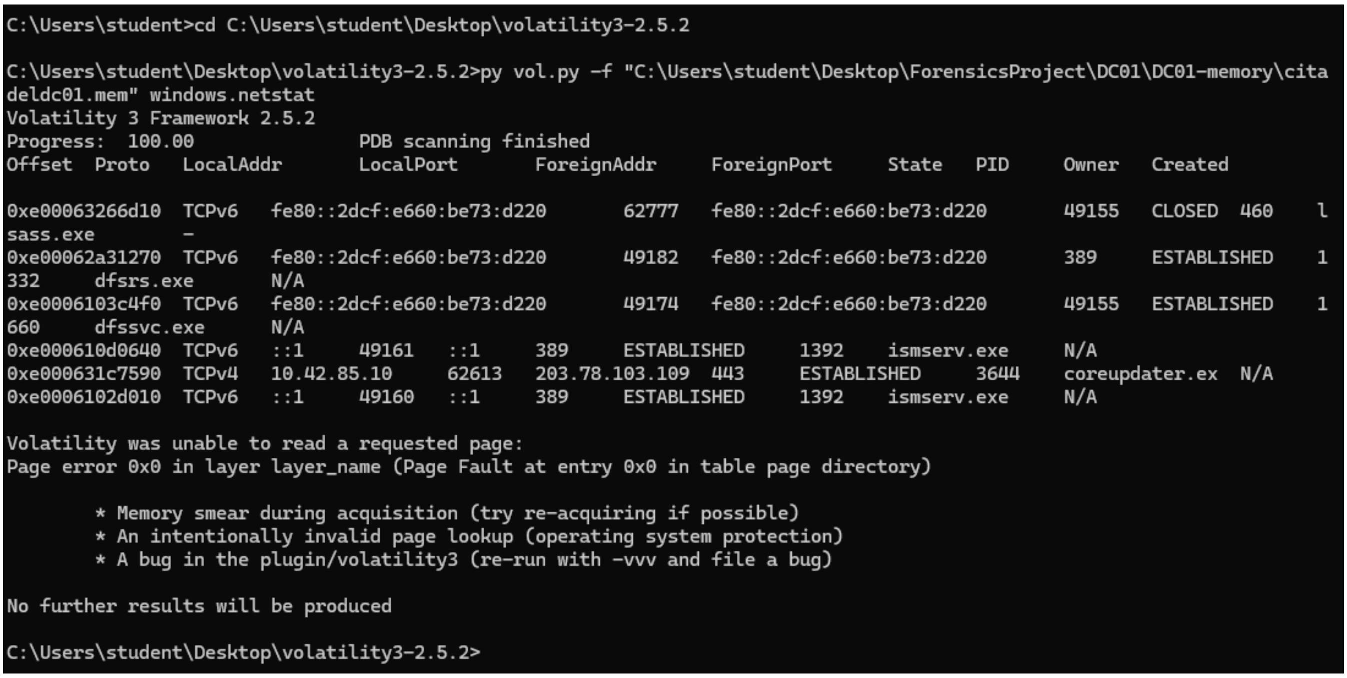
- ○ Identify the IP Address that delivered the payload. Seena Davoodi
  - ■ 194.61.24.102



```
C:\Users\student\Desktop\volatility3-2.5.2>strings pid.848.dmp | findstr /i "coreupdater"
coreupdater
coreupdater
coreupdater.exe
$<coreupdater[1].exe`
$<coreupdater[1].exe`
$<coreupdater[1].exeX
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
$<coreupdater[1].exe
><coreupdater.exe.2424urv.partial
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
coreupdaterC:\Windows\System32\coreupdater.exeuser mode serviceauto startLocalSystem
coreupdaterC:\Windows\System32\coreupdater.exeuser mode serviceauto startLocalSystem
coreupdater.exe
http://194.61.24.102/coreupdater.exe
coreupdater[1].exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
coreupdater.exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe.2424urv.partial
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
```

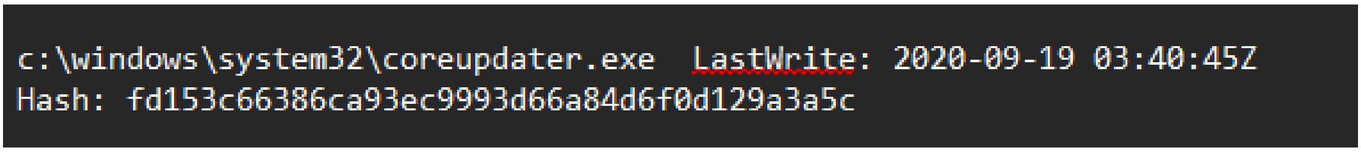
- What IP Address is the malware calling to? Scott Maclean
  - 203.78.103.109

We can see that by running the windows.netstat plugin in Volatility 3 that coreupdater.exe is calling to IP 203.78.103.109



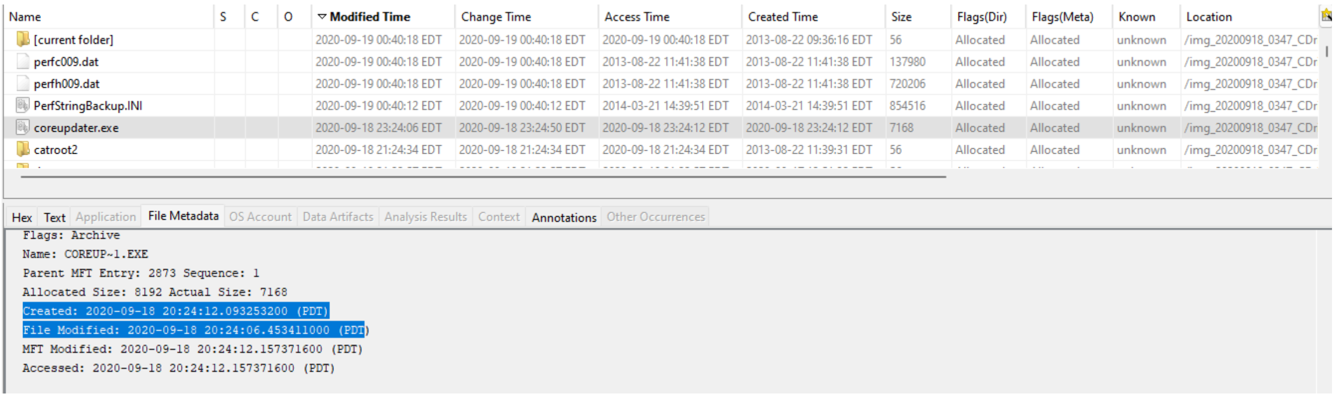
```
C:\Users\student>cd C:\Users\student\Desktop\volatility3-2.5.2

C:\Users\student\Desktop\volatility3-2.5.2>py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\cita
deldc01.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe00063266d10  TCPv6   fe80::2dcf:e660:be73:d220       62777   fe80::2dcf:e660:be73:d220       49155   CLOSED  460     l
sass.exe        -
0xe00062a31270  TCPv6   fe80::2dcf:e660:be73:d220       49182   fe80::2dcf:e660:be73:d220       389     ESTABLISHED     1
332     dfsrs.exe       N/A
0xe0006103c4f0  TCPv6   fe80::2dcf:e660:be73:d220       49174   fe80::2dcf:e660:be73:d220       49155   ESTABLISHED     1
660     dfssvc.exe      N/A
0xe000610d0640  TCPv6   ::1     49161   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A
0xe000631c7590  TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0xe0006102d010  TCPv6   ::1     49160   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A

Volatility was unable to read a requested page:
Page error 0x0 in layer layer_name (Page Fault at entry 0x0 in table page directory)

        * Memory smear during acquisition (try re-acquiring if possible)
        * An intentionally invalid page lookup (operating system protection)
        * A bug in the plugin/volatility3 (re-run with -vvv and file a bug)

No further results will be produced

C:\Users\student\Desktop\volatility3-2.5.2>
```

- Where is this malware on disk? Seena Davoodi
  - C:windows\system32\coreupdater.exe
    1. Found in Desktop Amcache using RegRipper. Checked the hash on VirusTotal.



```
c:\windows\system32\coreupdater.exe  LastWrite: 2020-09-19 03:40:45Z
Hash: fd153c66386ca93ec9993d66a84d6f0d129a3a5c
```

- When did it first appear? Seena Davoodi/Scott Maclean
  - 20:24 PDT 2020-09-18
  - Found the core updater.exe in DC's system32 and looked at the file's metadata



Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2020-09-19 00:40:18 EDT	2020-09-19 00:40:18 EDT	2020-09-19 00:40:18 EDT	2013-08-22 09:36:16 EDT	56	Allocated	Allocated	unknown	/img_20200918_0347_CDr
perfc009.dat				2020-09-19 00:40:18 EDT	2020-09-19 00:40:18 EDT	2013-08-22 11:41:38 EDT	2013-08-22 11:41:38 EDT	137980	Allocated	Allocated	unknown	/img_20200918_0347_CDr
perfh009.dat				2020-09-19 00:40:18 EDT	2020-09-19 00:40:18 EDT	2013-08-22 11:41:38 EDT	2013-08-22 11:41:38 EDT	720206	Allocated	Allocated	unknown	/img_20200918_0347_CDr
PerfStringBackup.INI				2020-09-19 00:40:12 EDT	2020-09-19 00:40:12 EDT	2014-03-21 14:39:51 EDT	2014-03-21 14:39:51 EDT	854516	Allocated	Allocated	unknown	/img_20200918_0347_CDr
coreupdater.exe				2020-09-18 23:24:06 EDT	2020-09-18 23:24:50 EDT	2020-09-18 23:24:12 EDT	2020-09-18 23:24:12 EDT	7168	Allocated	Allocated	unknown	/img_20200918_0347_CDr
catroot2				2020-09-18 21:24:34 EDT	2020-09-18 21:24:34 EDT	2020-09-18 21:24:34 EDT	2013-08-22 11:39:31 EDT	56	Allocated	Allocated	unknown	/img_20200918_0347_CDr

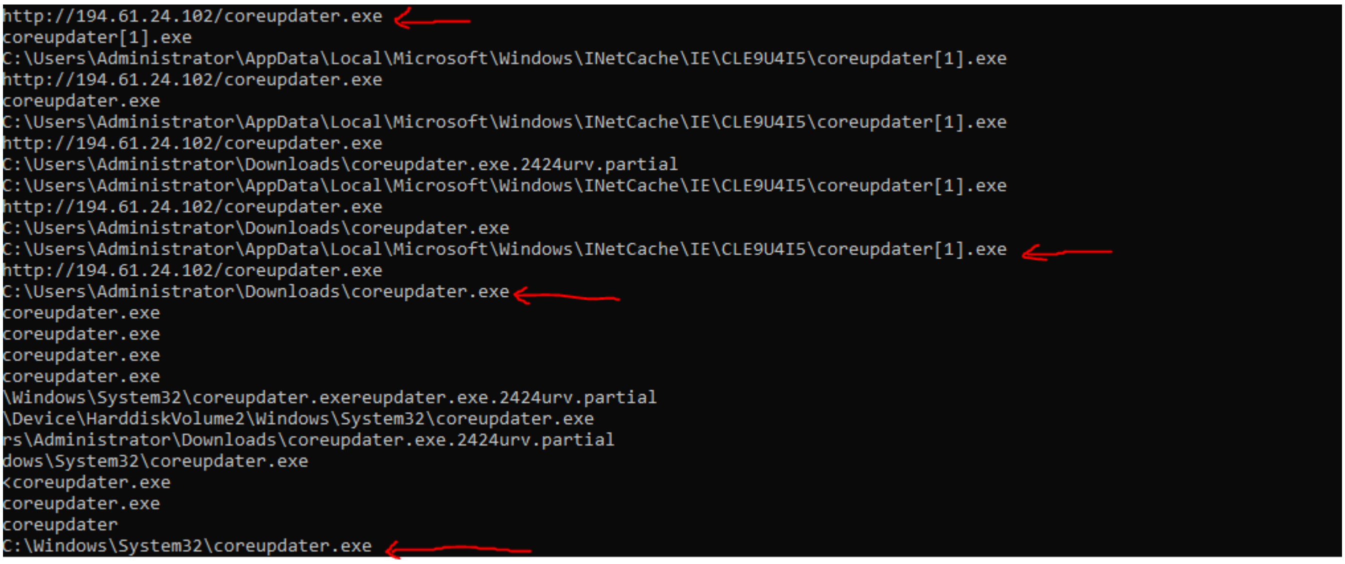
```
Flags: Archive
Name: COREUP~1.EXE
Parent MFT Entry: 2873 Sequence: 1
Allocated Size: 8192 Actual Size: 7168
Created: 2020-09-18 20:24:12.093253200 (PDT)
File Modified: 2020-09-18 20:24:06.453411000 (PDT)
MFT Modified: 2020-09-18 20:24:12.157371600 (PDT)
Accessed: 2020-09-18 20:24:12.157371600 (PDT)
```

- Did someone move it? Seena Davoodi
    - Yes - It was initially downloaded to C:\Users\Administrator\Downloads\coreupdater.exe.2424urv.partial

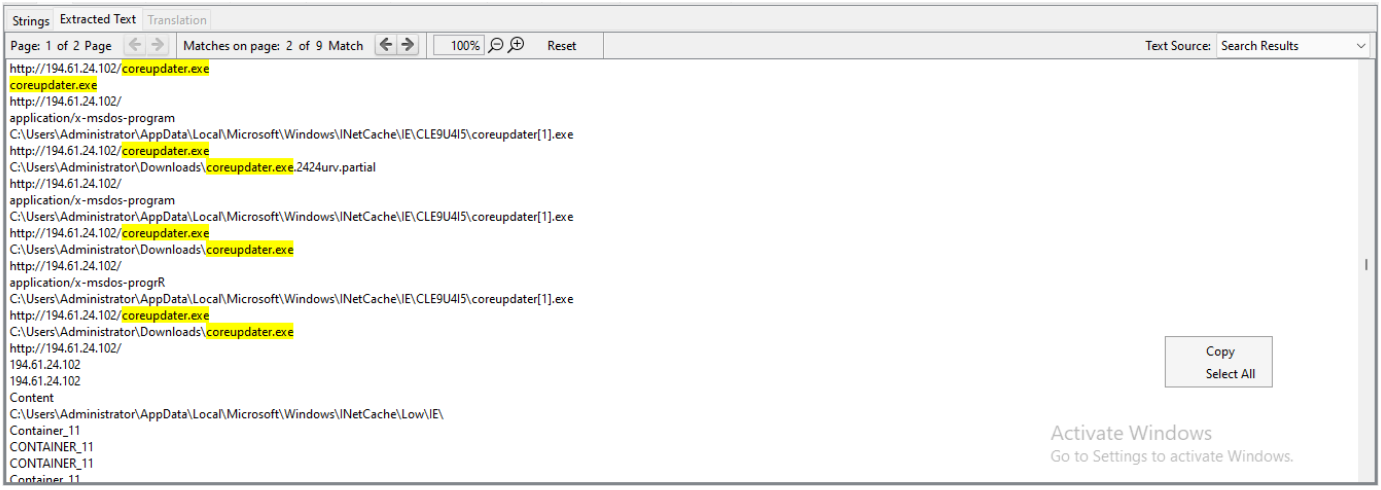
      It was cached in IE's cache:

      C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe

      Finally moved to: C:\Windows\System32\coreupdater.exe



```
http://194.61.24.102/coreupdater.exe
coreupdater[1].exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
coreupdater.exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe.2424urv.partial
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
\Windows\System32\coreupdater.exereupdater.exe.2424urv.partial
\Device\HarddiskVolume2\Windows\System32\coreupdater.exe
rs\Administrator\Downloads\coreupdater.exe.2424urv.partial
dows\System32\coreupdater.exe
<coreupdater.exe
coreupdater.exe
coreupdater
C:\Windows\System32\coreupdater.exe
```


Strings
Extracted Text
Translation
Page: 1 of 2 Page
Matches on page: 2 of 9 Match
100%
Reset
Text Source: Search Results
Copy
Select All
Activate Windows
Go to Settings to activate Windows.

```
http://194.61.24.102/coreupdater.exe
coreupdater.exe
http://194.61.24.102/
application/x-msdos-program
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe.2424urv.partial
http://194.61.24.102/
application/x-msdos-program
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
http://194.61.24.102/
application/x-msdos-progrR
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
http://194.61.24.102/
194.61.24.102
194.61.24.102
Content
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\Low\IE\
Container_11
CONTAINER_11
CONTAINER_11
Container_11
```

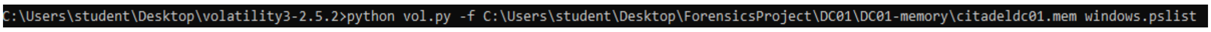
- What were the capabilities of this malware? Seena Davoodi
  - Lateral movement within the victim’s network, privilege escalation/creating Administrator account, it enabled autostart on system boot by modifying the registry, exfiltration, remote desktop access
- Is this malware easily obtained? **Scott Maclean**
  - Yes, Metasploit is generally easily obtainable. Here's why:

  1. Open-Source Framework: The Metasploit Framework is open-source, meaning its source code is freely available to the public. You can download it from the official Metasploit website or its GitHub repository.

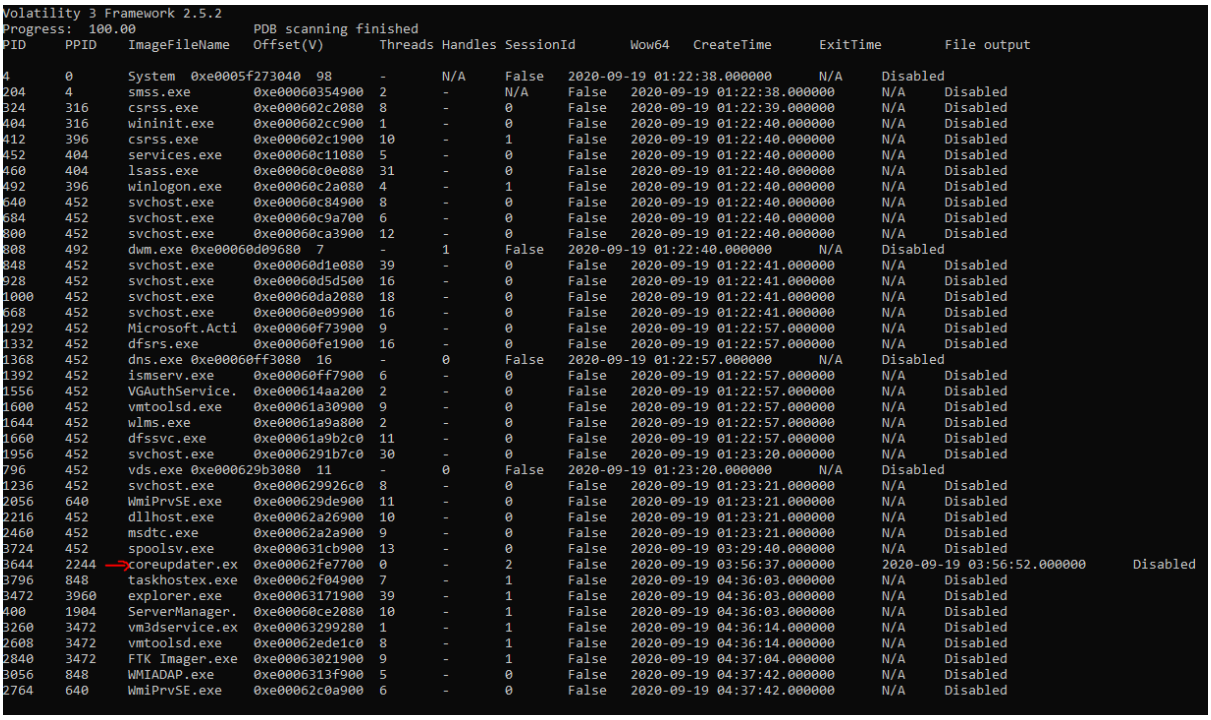
  2. Included in Kali Linux: Kali Linux, a popular penetration testing distribution, comes with Metasploit pre-installed. This makes it readily accessible to anyone using Kali.

- Was this malware installed with persistence on any machine? Seena Davoodi
  - When?
  - Where?

Ran this command to see a list of processes in memory dump and found the previously identified malicious exe named “coreupdater”:

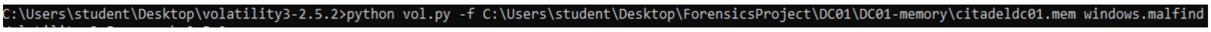


```
C:\Users\student\Desktop\volatility3-2.5.2>python vol.py -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem windows.pslist
```

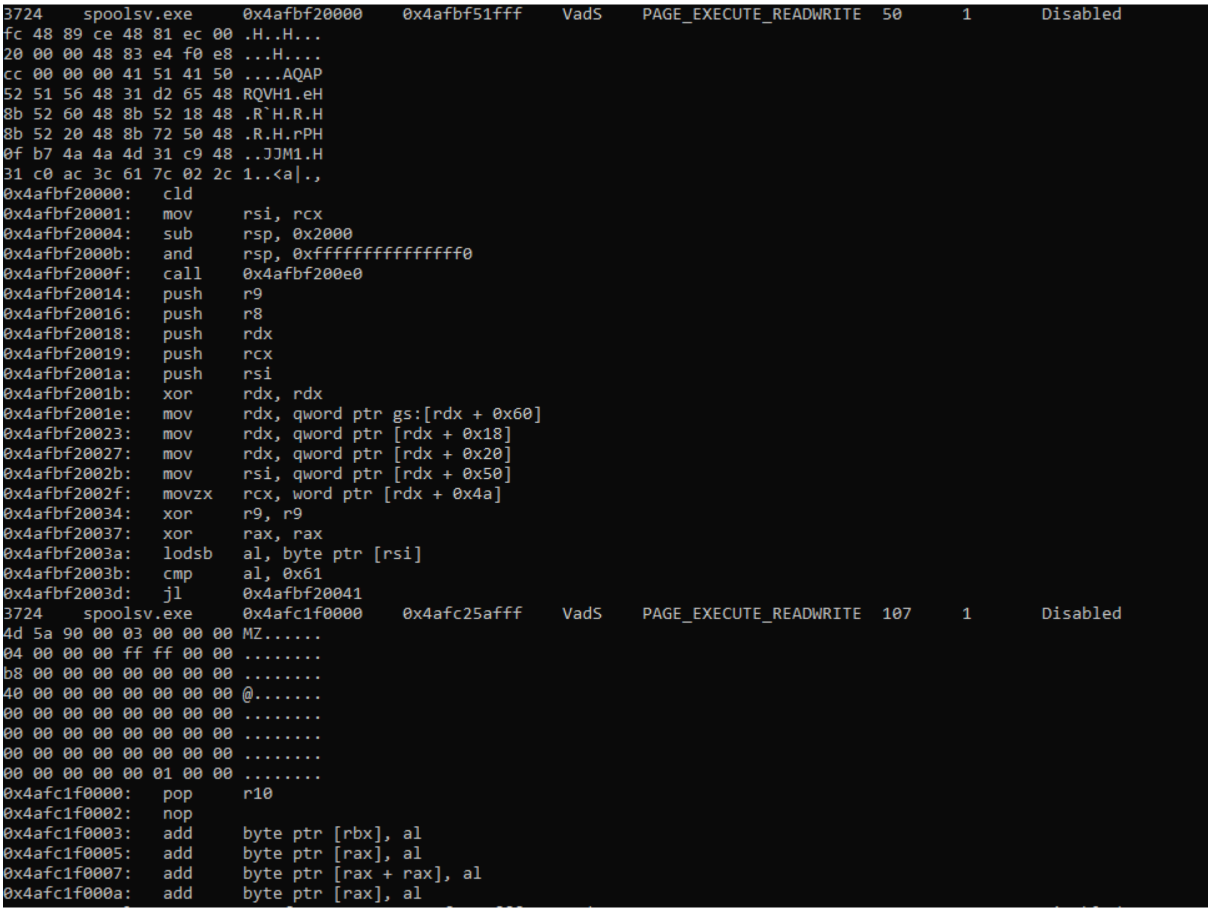


```
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xe0005f273040  98      -       N/A     False   2020-09-19 01:22:38.000000      N/A     Disabled
204     4       smss.exe        0xe00060354900  2       -       N/A     False   2020-09-19 01:22:38.000000      N/A     Disabled
324     316     csrss.exe       0xe000602c2080  8       -       0       False   2020-09-19 01:22:39.000000      N/A     Disabled
404     316     wininit.exe     0xe000602cc900  1       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
412     396     csrss.exe       0xe000602c1900  10      -       1       False   2020-09-19 01:22:40.000000      N/A     Disabled
452     404     services.exe    0xe00060c11080  5       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
460     404     lsass.exe       0xe00060c0e080  31      -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
492     396     winlogon.exe    0xe00060c2a080  4       -       1       False   2020-09-19 01:22:40.000000      N/A     Disabled
640     452     svchost.exe     0xe00060c84900  8       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
684     452     svchost.exe     0xe00060c9a700  6       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
800     452     svchost.exe     0xe00060ca3900  12      -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
808     492     dwm.exe 0xe00060d09680  7       -       1       False   2020-09-19 01:22:40.000000      N/A     Disabled
848     452     svchost.exe     0xe00060d1e080  39      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
928     452     svchost.exe     0xe00060d5d500  16      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
1000    452     svchost.exe     0xe00060da2080  18      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
668     452     svchost.exe     0xe00060e09900  16      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
1292    452     Microsoft.Acti  0xe00060f73900  9       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1332    452     dfsrs.exe       0xe00060fe1900  16      -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1368    452     dns.exe 0xe00060ff3080  16      -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1392    452     ismserv.exe     0xe00060ff7900  6       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1556    452     VGAuthService.  0xe000614aa200  2       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1600    452     vmtoolsd.exe    0xe00061a30900  9       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1644    452     wlms.exe        0xe00061a9a800  2       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1660    452     dfssvc.exe      0xe00061a9b2c0  11      -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1956    452     svchost.exe     0xe0006291b7c0  30      -       0       False   2020-09-19 01:23:20.000000      N/A     Disabled
796     452     vds.exe 0xe000629b3080  11      -       0       False   2020-09-19 01:23:20.000000      N/A     Disabled
1236    452     svchost.exe     0xe000629926c0  8       -       0       False   2020-09-19 01:23:21.000000      N/A     Disabled
2056    640     WmiPrvSE.exe    0xe000629de900  11      -       0       False   2020-09-19 01:23:21.000000      N/A     Disabled
2216    452     dllhost.exe     0xe00062a26900  10      -       0       False   2020-09-19 01:23:21.000000      N/A     Disabled
2460    452     msdtc.exe       0xe00062a2a900  9       -       0       False   2020-09-19 01:23:21.000000      N/A     Disabled
3724    452     spoolsv.exe     0xe000631cb900  13      -       0       False   2020-09-19 03:29:40.000000      N/A     Disabled
3644    2244  →coreupdater.ex   0xe00062fe7700  0       -       2       False   2020-09-19 03:56:37.000000      2020-09-19 03:56:52.000000      Disabled
3796    848     taskhostex.exe  0xe00062f04900  7       -       1       False   2020-09-19 04:36:03.000000      N/A     Disabled
3472    3960    explorer.exe    0xe00063171900  39      -       1       False   2020-09-19 04:36:03.000000      N/A     Disabled
400     1904    ServerManager.  0xe00060ce2080  10      -       1       False   2020-09-19 04:36:03.000000      N/A     Disabled
3260    3472    vm3dservice.ex  0xe00063299280  1       -       1       False   2020-09-19 04:36:14.000000      N/A     Disabled
2608    3472    vmtoolsd.exe    0xe00062ede1c0  8       -       1       False   2020-09-19 04:36:14.000000      N/A     Disabled
2840    3472    FTK Imager.exe  0xe00063021900  9       -       1       False   2020-09-19 04:37:04.000000      N/A     Disabled
3056    848     WMIADAP.exe     0xe0006313f900  5       -       0       False   2020-09-19 04:37:42.000000      N/A     Disabled
2764    640     WmiPrvSE.exe    0xe00062c0a900  6       -       0       False   2020-09-19 04:37:42.000000      N/A     Disabled
```

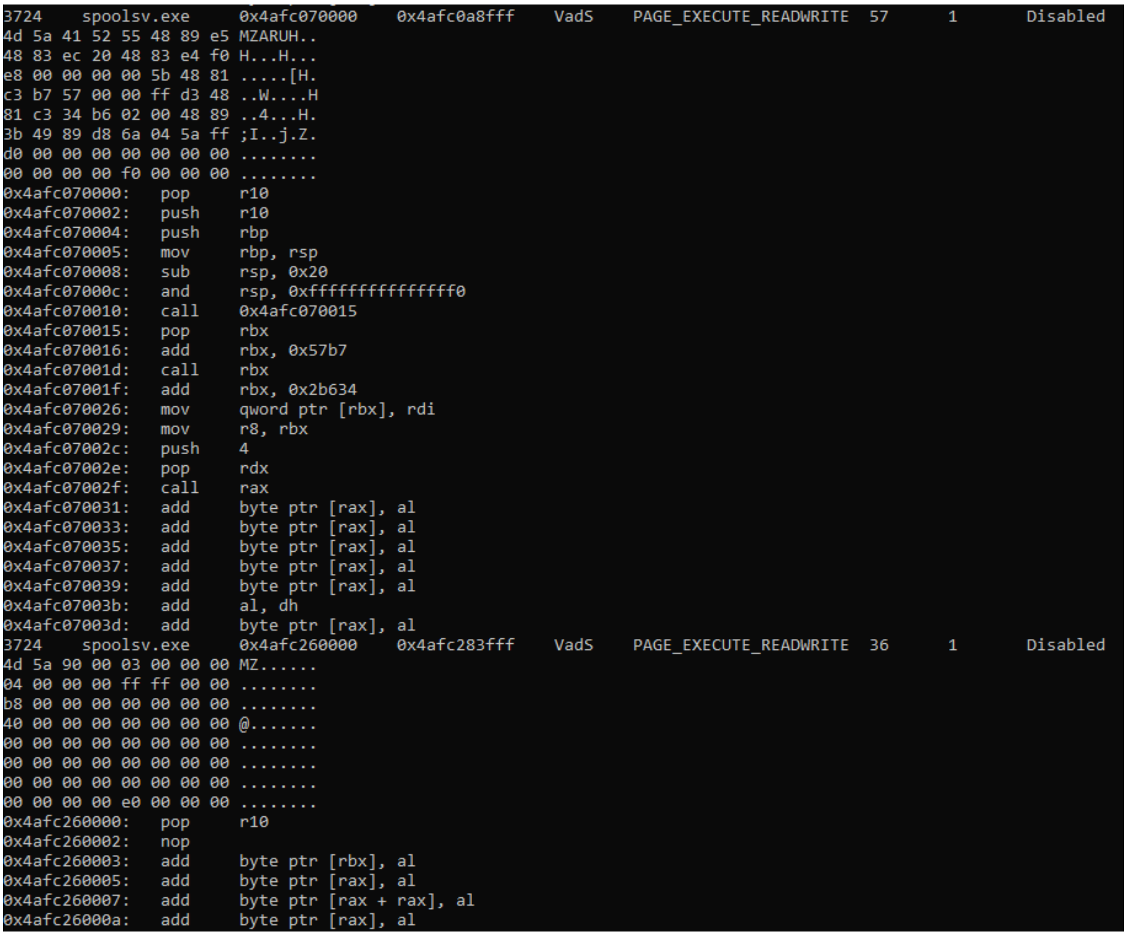
Using windows.malfind to see if we can detect suspicious memory regions:



```
C:\Users\student\Desktop\volatility3-2.5.2>python vol.py -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem windows.malfind
```

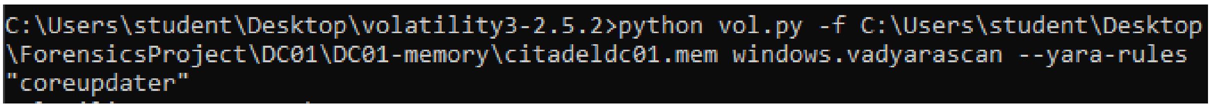


```
3724    spoolsv.exe     0x4afbf20000    0x4afbf51fff    VadS    PAGE_EXECUTE_READWRITE  50      1       Disabled
fc 48 89 ce 48 81 ec 00 .H..H...
20 00 00 48 83 e4 f0 e8 ...H....
cc 00 00 00 41 51 41 50 ....AQAP
52 51 56 48 31 d2 65 48 RQVH1.eH
8b 52 60 48 8b 52 18 48 .R`H.R.H
8b 52 20 48 8b 72 50 48 .R.H.rPH
0f b7 4a 4a 4d 31 c9 48 ..JJM1.H
31 c0 ac 3c 61 7c 02 2c 1..<a|.,
0x4afbf20000:   cld
0x4afbf20001:   mov     rsi, rcx
0x4afbf20004:   sub     rsp, 0x2000
0x4afbf2000b:   and     rsp, 0xfffffffffffffff0
0x4afbf2000f:   call    0x4afbf200e0
0x4afbf20014:   push    r9
0x4afbf20016:   push    r8
0x4afbf20018:   push    rdx
0x4afbf20019:   push    rcx
0x4afbf2001a:   push    rsi
0x4afbf2001b:   xor     rdx, rdx
0x4afbf2001e:   mov     rdx, qword ptr gs:[rdx + 0x60]
0x4afbf20023:   mov     rdx, qword ptr [rdx + 0x18]
0x4afbf20027:   mov     rdx, qword ptr [rdx + 0x20]
0x4afbf2002b:   mov     rsi, qword ptr [rdx + 0x50]
0x4afbf2002f:   movzx   rcx, word ptr [rdx + 0x4a]
0x4afbf20034:   xor     r9, r9
0x4afbf20037:   xor     rax, rax
0x4afbf2003a:   lodsb   al, byte ptr [rsi]
0x4afbf2003b:   cmp     al, 0x61
0x4afbf2003d:   jl      0x4afbf20041
3724    spoolsv.exe     0x4afc1f0000    0x4afc25afff    VadS    PAGE_EXECUTE_READWRITE  107     1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 01 00 00 ........
0x4afc1f0000:   pop     r10
0x4afc1f0002:   nop
0x4afc1f0003:   add     byte ptr [rbx], al
0x4afc1f0005:   add     byte ptr [rax], al
0x4afc1f0007:   add     byte ptr [rax + rax], al
0x4afc1f000a:   add     byte ptr [rax], al
```

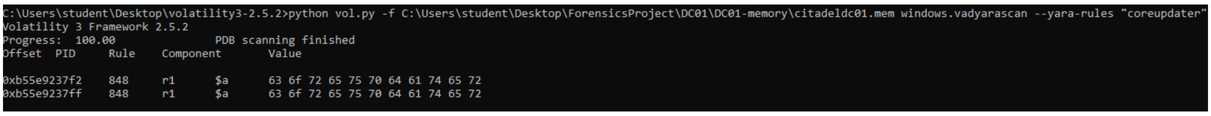


```
3724    spoolsv.exe     0x4afc070000    0x4afc0a8fff    VadS    PAGE_EXECUTE_READWRITE  57      1       Disabled
4d 5a 41 52 55 48 89 e5 MZARUH..
48 83 ec 20 48 83 e4 f0 H...H...
e8 00 00 00 00 5b 48 81 .....[H.
c3 b7 57 00 00 ff d3 48 ..W....H
81 c3 34 b6 02 00 48 89 ..4...H.
3b 49 89 d8 6a 04 5a ff ;I..j.Z.
d0 00 00 00 00 00 00 00 ........
00 00 00 00 f0 00 00 00 ........
0x4afc070000:   pop     r10
0x4afc070002:   push    r10
0x4afc070004:   push    rbp
0x4afc070005:   mov     rbp, rsp
0x4afc070008:   sub     rsp, 0x20
0x4afc07000c:   and     rsp, 0xfffffffffffffff0
0x4afc070010:   call    0x4afc070015
0x4afc070015:   pop     rbx
0x4afc070016:   add     rbx, 0x57b7
0x4afc07001d:   call    rbx
0x4afc07001f:   add     rbx, 0x2b634
0x4afc070026:   mov     qword ptr [rbx], rdi
0x4afc070029:   mov     r8, rbx
0x4afc07002c:   push    4
0x4afc07002e:   pop     rdx
0x4afc07002f:   call    rax
0x4afc070031:   add     byte ptr [rax], al
0x4afc070033:   add     byte ptr [rax], al
0x4afc070035:   add     byte ptr [rax], al
0x4afc070037:   add     byte ptr [rax], al
0x4afc070039:   add     byte ptr [rax], al
0x4afc07003b:   add     al, dh
0x4afc07003d:   add     byte ptr [rax], al
3724    spoolsv.exe     0x4afc260000    0x4afc283fff    VadS    PAGE_EXECUTE_READWRITE  36      1       Disabled
4d 5a 90 00 03 00 00 00 MZ......
04 00 00 00 ff ff 00 00 ........
b8 00 00 00 00 00 00 00 ........
40 00 00 00 00 00 00 00 @.......
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 00 00 00 00 ........
00 00 00 00 e0 00 00 00 ........
0x4afc260000:   pop     r10
0x4afc260002:   nop
0x4afc260003:   add     byte ptr [rbx], al
0x4afc260005:   add     byte ptr [rax], al
0x4afc260007:   add     byte ptr [rax + rax], al
0x4afc26000a:   add     byte ptr [rax], al
```

Use yarascan to search for any references to this name:

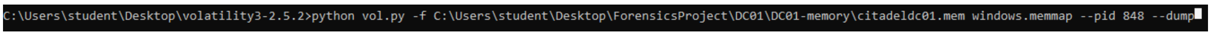


```
C:\Users\student\Desktop\volatility3-2.5.2>python vol.py -f C:\Users\student\Desktop
\ForensicsProject\DC01\DC01-memory\citadeldc01.mem windows.vadyarascan --yara-rules
"coreupdater"
```



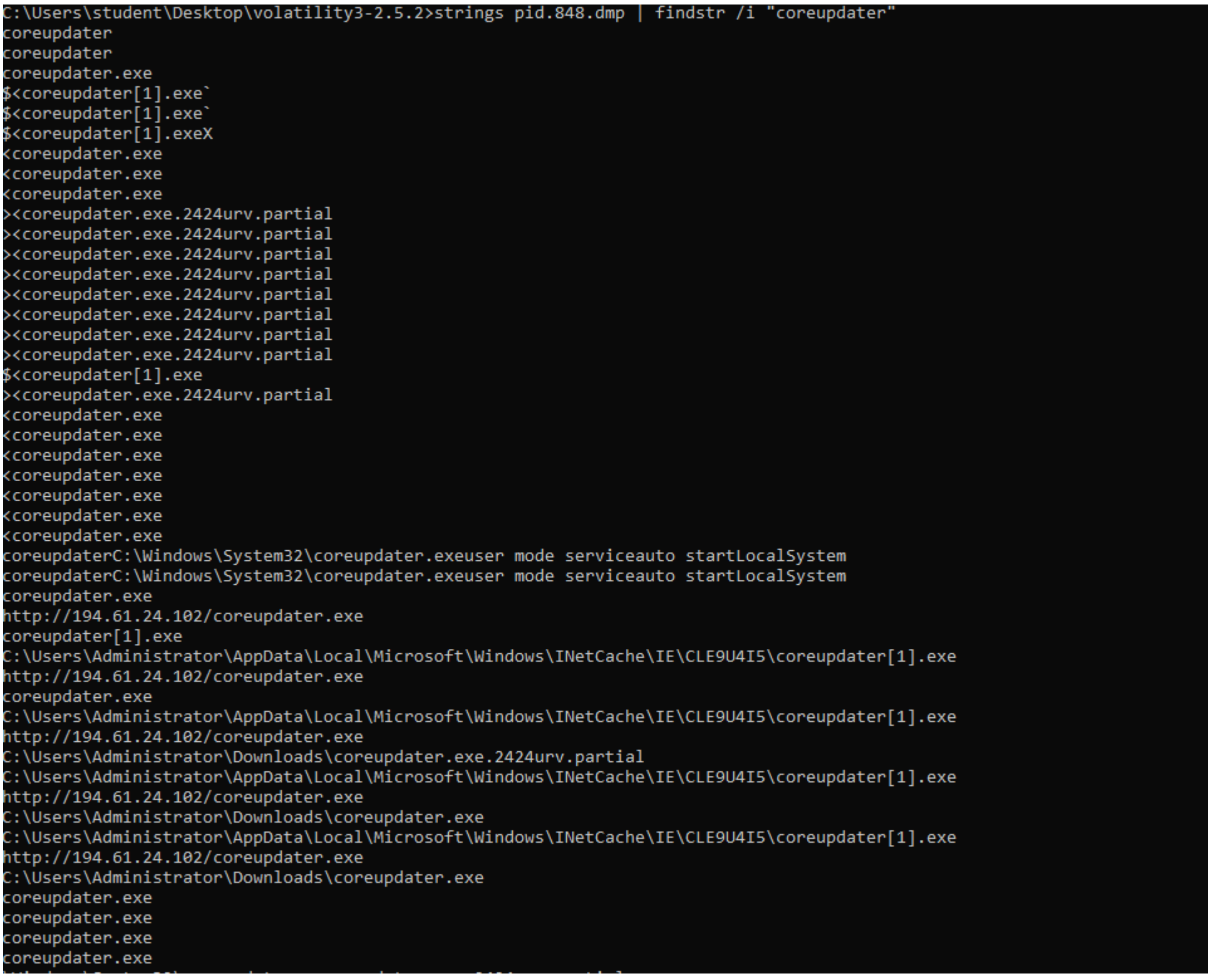
```
C:\Users\student\Desktop\volatility3-2.5.2>python vol.py -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem windows.vadyarascan --yara-rules "coreupdater"
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  PID     Rule    Component       Value

0xb55e9237f2    848     r1      $a      63 6f 72 65 75 70 64 61 74 65 72
0xb55e9237ff    848     r1      $a      63 6f 72 65 75 70 64 61 74 65 72
```

Dumping the entire process memory to examine:

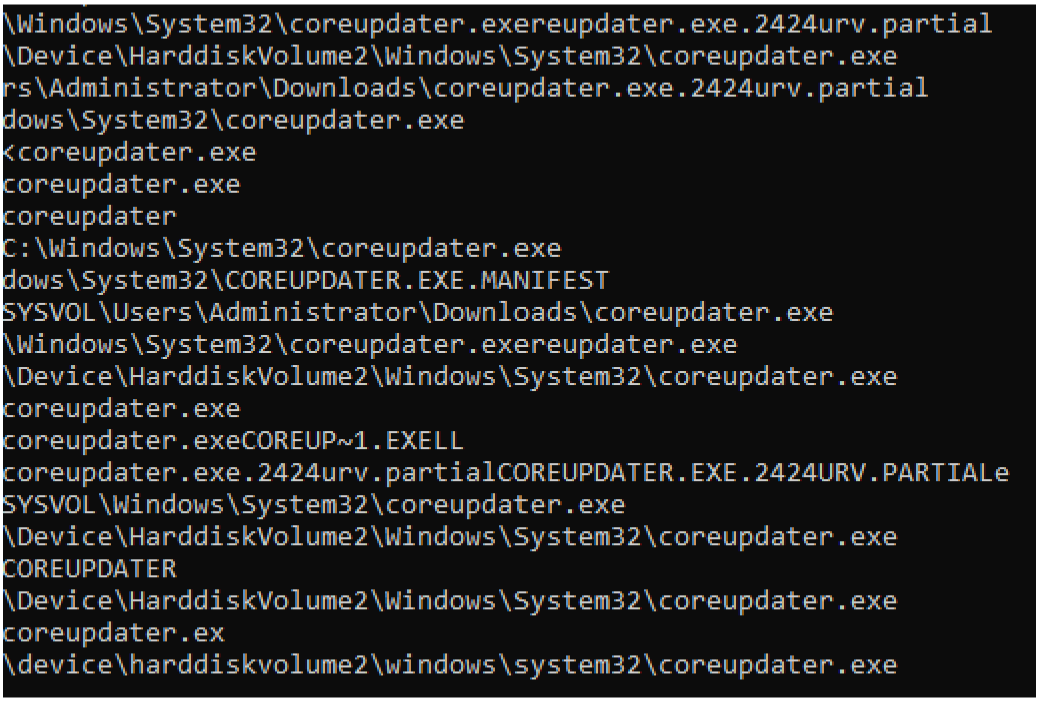


```
C:\Users\student\Desktop\volatility3-2.5.2>python vol.py -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem windows.memmap --pid 848 --dump
```

Use strings at the content around the offset in the dumped memory file:



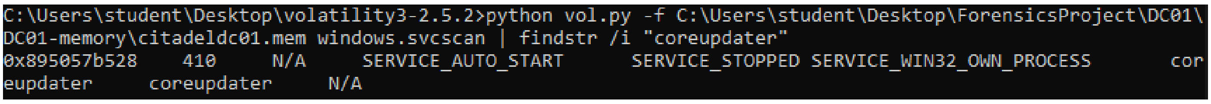
```
C:\Users\student\Desktop\volatility3-2.5.2>strings pid.848.dmp | findstr /i "coreupdater"
coreupdater
coreupdater
coreupdater.exe
$<coreupdater[1].exe`
$<coreupdater[1].exe`
$<coreupdater[1].exeX
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
><coreupdater.exe.2424urv.partial
$<coreupdater[1].exe
><coreupdater.exe.2424urv.partial
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
<coreupdater.exe
coreupdaterC:\Windows\System32\coreupdater.exeuser mode serviceauto startLocalSystem
coreupdaterC:\Windows\System32\coreupdater.exeuser mode serviceauto startLocalSystem
coreupdater.exe
http://194.61.24.102/coreupdater.exe
coreupdater[1].exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
coreupdater.exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe.2424urv.partial
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
http://194.61.24.102/coreupdater.exe
C:\Users\Administrator\Downloads\coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
coreupdater.exe
```



```
\Windows\System32\coreupdater.exereupdater.exe.2424urv.partial
\Device\HarddiskVolume2\Windows\System32\coreupdater.exe
rs\Administrator\Downloads\coreupdater.exe.2424urv.partial
dows\System32\coreupdater.exe
<coreupdater.exe
coreupdater.exe
coreupdater
C:\Windows\System32\coreupdater.exe
dows\System32\COREUPDATER.EXE.MANIFEST
SYSVOL\Users\Administrator\Downloads\coreupdater.exe
\Windows\System32\coreupdater.exereupdater.exe
\Device\HarddiskVolume2\Windows\System32\coreupdater.exe
coreupdater.exe
coreupdater.exeCOREUP~1.EXELL
coreupdater.exe.2424urv.partialCOREUPDATER.EXE.2424URV.PARTIALe
SYSVOL\Windows\System32\coreupdater.exe
\Device\HarddiskVolume2\Windows\System32\coreupdater.exe
COREUPDATER
\Device\HarddiskVolume2\Windows\System32\coreupdater.exe
coreupdater.ex
\device\harddiskvolume2\windows\system32\coreupdater.exe
```

The file was downloaded from a malicious URL:
http:// 194 . 61 . 24 . 102 /coreupdater.exe
It was initially downloaded to:
C:\Users\Administrator\Downloads\coreupdater.exe.2424urv.partial

It was cached in IE's cache:
C:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exe
Finally moved to:
C:\Windows\System32\coreupdater.exe
It appears to have been set up as a service with these parameters:
"user mode service auto start LocalSystem"
Lastly we analyzed the service configuration:

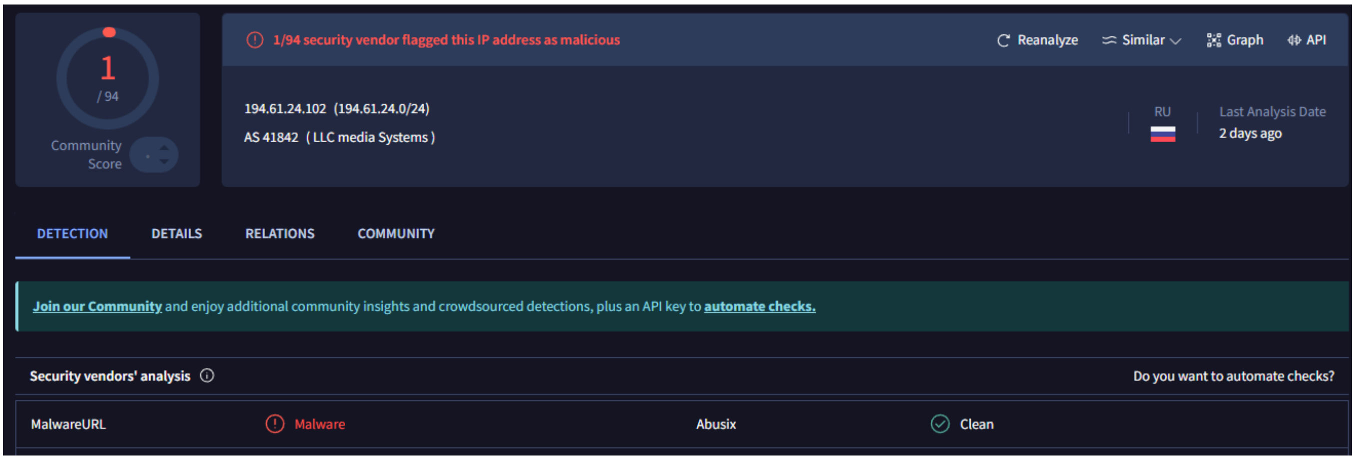


```
C:\Users\student\Desktop\volatility3-2.5.2>python vol.py -f C:\Users\student\Desktop\ForensicsProject\DC01\
DC01-memory\citadeldc01.mem windows.svcscan | findstr /i "coreupdater"
0x895057b528    410     N/A     SERVICE_AUTO_START      SERVICE_STOPPED SERVICE_WIN32_OWN_PROCESS       cor
eupdater     coreupdater     N/A
```

The service configuration is suspicious because:

Legitimate Windows services rarely use the same name for both service name and display name
The name tries to appear legitimate by suggesting it's a core update service
It was set to auto-start with SYSTEM privileges
The associated executable was downloaded from a suspicious IP (194.61.24.102)

7. What malicious IP Addresses were involved? Scott Maclean
    - Were any IP Addresses from known adversary infrastructure?
        - 194.61.24.102 - Found in IE Web History (autopsy data artifacts/web history)



1/94 security vendor flagged this IP address as malicious

194.61.24.102 (194.61.24.0/24)
AS 41842 (LLC media Systems)

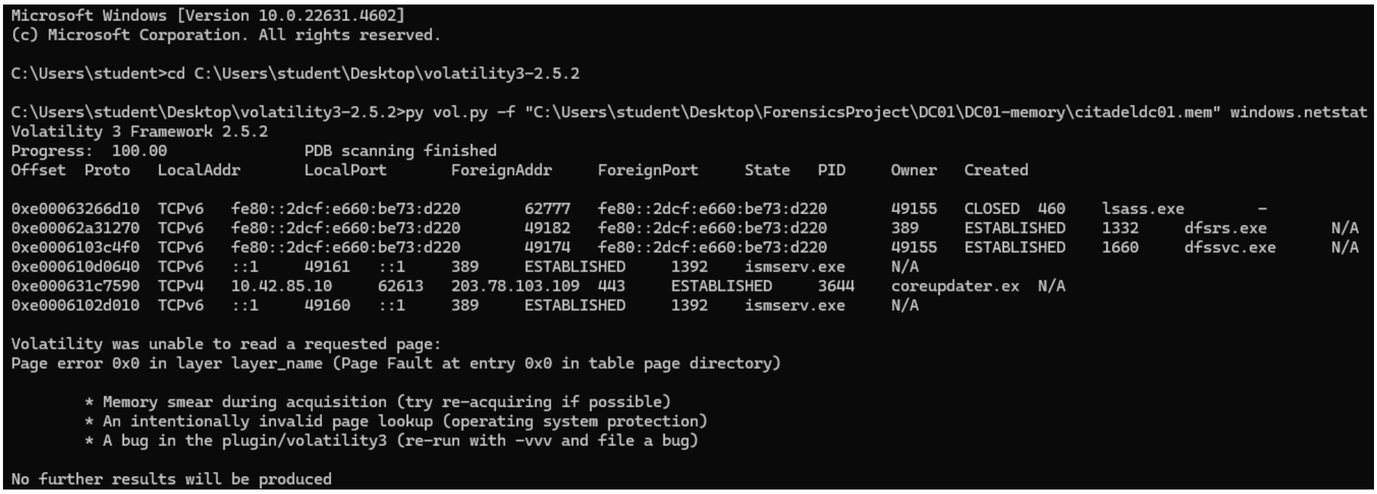
Last Analysis Date
2 days ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

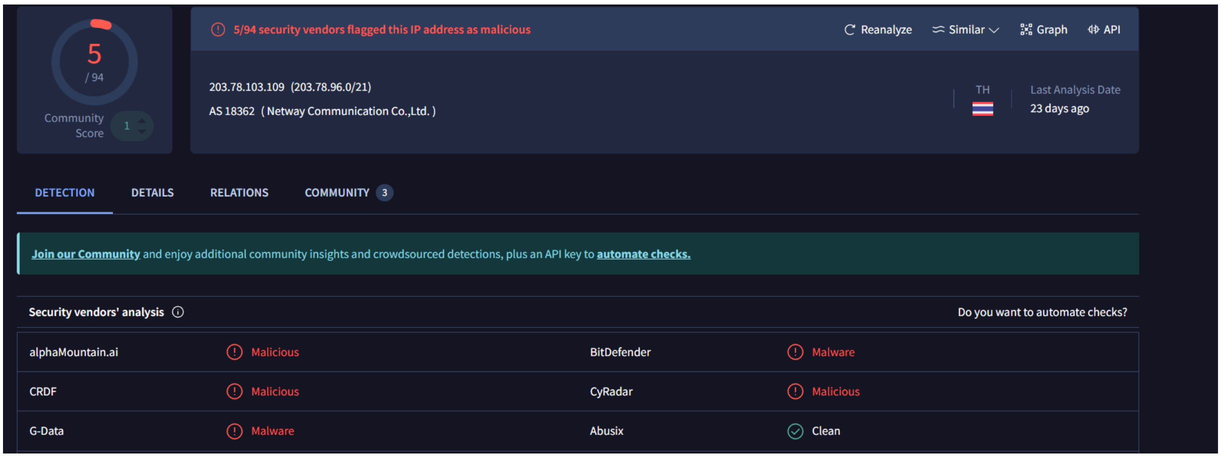
Security vendors' analysis — Do you want to automate checks?

MalwareURL — Malware — Abusix — Clean

203.78.103.109 - Memory Image: Volatility 3 - py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.netstat



```
Microsoft Windows [Version 10.0.22631.4602]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student>cd C:\Users\student\Desktop\volatility3-2.5.2

C:\Users\student\Desktop\volatility3-2.5.2>py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe00063266d10  TCPv6   fe80::2dcf:e660:be73:d220       62777   fe80::2dcf:e660:be73:d220       49155   CLOSED  460     lsass.exe       -
0xe00062a31270  TCPv6   fe80::2dcf:e660:be73:d220       49182   fe80::2dcf:e660:be73:d220       389     ESTABLISHED     1332    dfsrs.exe       N/A
0xe0006103c4f0  TCPv6   fe80::2dcf:e660:be73:d220       49174   fe80::2dcf:e660:be73:d220       49155   ESTABLISHED     1660    dfssvc.exe      N/A
0xe000610d0640  TCPv6   ::1     49161   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A
0xe000631c7590  TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0xe0006102d010  TCPv6   ::1     49160   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A

Volatility was unable to read a requested page:
Page error 0x0 in layer layer_name (Page Fault at entry 0x0 in table page directory)

        * Memory smear during acquisition (try re-acquiring if possible)
        * An intentionally invalid page lookup (operating system protection)
        * A bug in the plugin/volatility3 (re-run with -vvv and file a bug)

No further results will be produced
```



5/94 security vendors flagged this IP address as malicious

203.78.103.109 (203.78.96.0/21)

AS 18362 (Netway Communication Co.,Ltd.)

Last Analysis Date
23 days ago

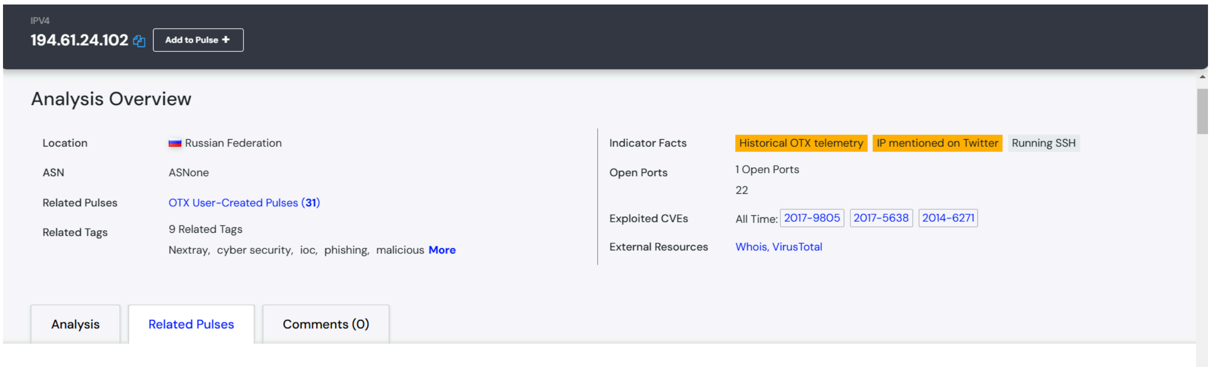
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis

Do you want to automate checks?

alphaMountain.ai	Malicious	BitDefender	Malware
CRDF	Malicious	CyRadar	Malicious
G-Data	Malware	Abusix	Clean

- ○ Are these pieces of adversary infrastructure involved in other attacks around the time of the attack? Scott Maclean
    - ■ It appears that IP 194.61.24.102 was involved in other exploitations around 2017 as indicated by alienvault.

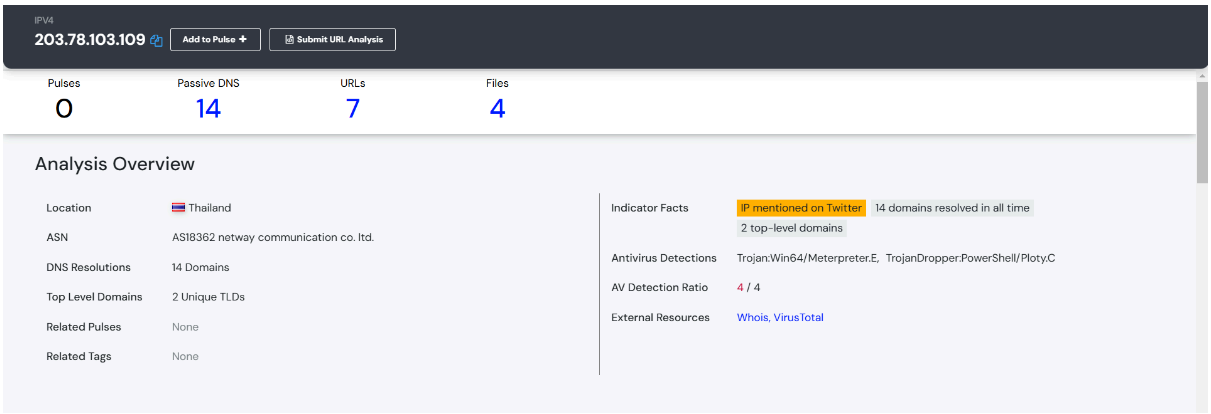


194.61.24.102

Analysis Overview

Location	Russian Federation
ASN	ASNone
Related Pulses	OTX User-Created Pulses (31)
Related Tags	9 Related Tags Nextray, cyber security, ioc, phishing, malicious More
Indicator Facts	Historical OTX telemetry IP mentioned on Twitter Running SSH
Open Ports	1 Open Ports 22
Exploited CVEs	All Time: 2017-9805 2017-5638 2014-6271
External Resources	Whois, VirusTotal

It also appears that IP 203.78.103.109 was involved in a trojan delivery named meterpreter associated with AV detections.



203.78.103.109

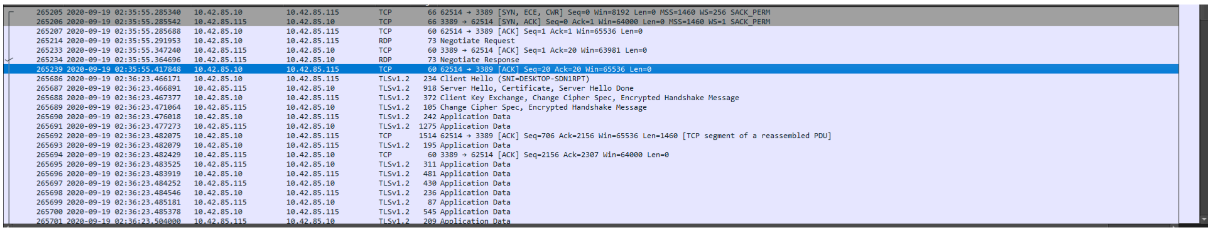
Pulses	Passive DNS	URLs	Files
0	14	7	4

Analysis Overview

Location	Thailand
ASN	AS18362 netway communication co. ltd.
DNS Resolutions	14 Domains
Top Level Domains	2 Unique TLDs
Related Pulses	None
Related Tags	None

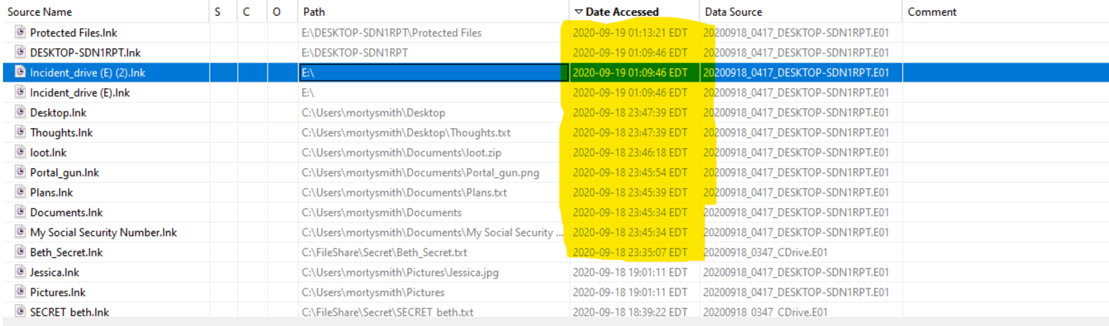
Indicator Facts	IP mentioned on Twitter 14 domains resolved in all time 2 top-level domains
Antivirus Detections	Trojan:Win64/Meterpreter.E, TrojanDropper:PowerShell/Ploty.C
AV Detection Ratio	4 / 4
External Resources	Whois, VirusTotal

- Did the attacker access any other systems? When?How? **Scott Maclean**
  - Using wireshark to filter for port 3389, which is used for RDP, we were able to see that the attacker started the 3 way TCP handshake from the DC to the desktop around 2:35 UDT on 2020/09/19. Once the ACK was received, the attacker initiated the request for Remote Desktop Protocol. At 2:36 UDT, a key was generated after the Server and Desktop said hello to each other to provide remote encryption. Once the link was established, application data was moved between the DC and the desktop.



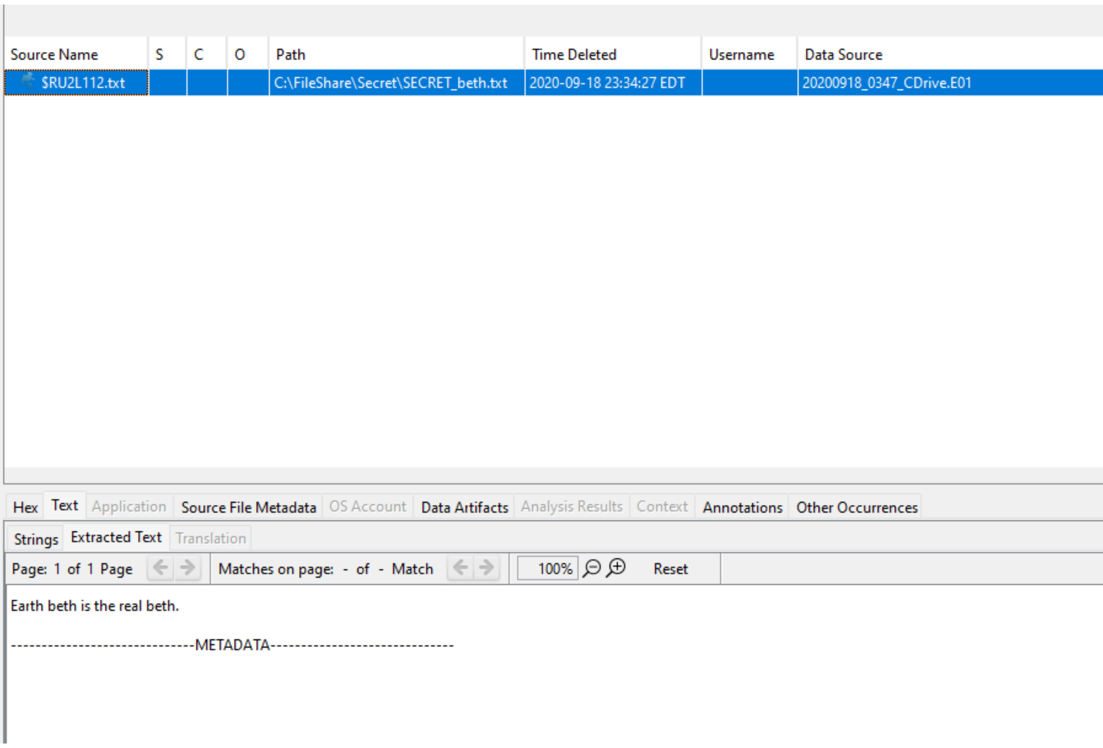
```
265205 2020-09-19 02:35:55.285340   10.42.85.10     10.42.85.115    TCP        66 62514 → 3389 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
265206 2020-09-19 02:35:55.285542   10.42.85.115    10.42.85.10     TCP        66 3389 → 62514 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM
265207 2020-09-19 02:35:55.285688   10.42.85.10     10.42.85.115    TCP        60 62514 → 3389 [ACK] Seq=1 Ack=1 Win=65536 Len=0
265214 2020-09-19 02:35:55.291953   10.42.85.10     10.42.85.115    RDP        73 Negotiate Request
265233 2020-09-19 02:35:55.347240   10.42.85.115    10.42.85.10     TCP        60 3389 → 62514 [ACK] Seq=1 Ack=20 Win=63981 Len=0
265234 2020-09-19 02:35:55.364696   10.42.85.115    10.42.85.10     RDP        73 Negotiate Response
265239 2020-09-19 02:35:55.417848   10.42.85.10     10.42.85.115    TCP        60 62514 → 3389 [ACK] Seq=20 Ack=20 Win=65536 Len=0
265686 2020-09-19 02:36:23.466171   10.42.85.10     10.42.85.115    TLSv1.2   234 Client Hello (SNI=DESKTOP-SDN1RPT)
265687 2020-09-19 02:36:23.466891   10.42.85.115    10.42.85.10     TLSv1.2   918 Server Hello, Certificate, Server Hello Done
265688 2020-09-19 02:36:23.467377   10.42.85.10     10.42.85.115    TLSv1.2   372 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
265689 2020-09-19 02:36:23.471064   10.42.85.115    10.42.85.10     TLSv1.2   105 Change Cipher Spec, Encrypted Handshake Message
265690 2020-09-19 02:36:23.476018   10.42.85.10     10.42.85.115    TLSv1.2   242 Application Data
265691 2020-09-19 02:36:23.477273   10.42.85.115    10.42.85.10     TLSv1.2  1275 Application Data
265692 2020-09-19 02:36:23.482075   10.42.85.10     10.42.85.115    TCP      1514 62514 → 3389 [ACK] Seq=706 Ack=2156 Win=65536 Len=1460 [TCP segment of a reassembled PDU]
265693 2020-09-19 02:36:23.482079   10.42.85.10     10.42.85.115    TLSv1.2   195 Application Data
265694 2020-09-19 02:36:23.482429   10.42.85.115    10.42.85.10     TCP        60 3389 → 62514 [ACK] Seq=2156 Ack=2307 Win=64000 Len=0
265695 2020-09-19 02:36:23.483525   10.42.85.115    10.42.85.10     TLSv1.2   311 Application Data
265696 2020-09-19 02:36:23.483919   10.42.85.10     10.42.85.115    TLSv1.2   481 Application Data
265697 2020-09-19 02:36:23.484252   10.42.85.115    10.42.85.10     TLSv1.2   430 Application Data
265698 2020-09-19 02:36:23.484546   10.42.85.10     10.42.85.115    TLSv1.2   236 Application Data
265699 2020-09-19 02:36:23.485181   10.42.85.115    10.42.85.10     TLSv1.2    87 Application Data
265700 2020-09-19 02:36:23.485378   10.42.85.10     10.42.85.115    TLSv1.2   545 Application Data
265701 2020-09-19 02:36:23.504000   10.42.85.115    10.42.85.10     TLSv1.2   209 Application Data
```

- Did the attacker steal or access any data? **Scott Maclean**
  - When? Going back into Autopsy, we looked into the recent documents folder and noticed that there were a number of files that had been modified after the DC connected to the Desktop.



Source Name	S	C	O	Path	Date Accessed	Data Source	Comment
Protected Files.lnk				E:\DESKTOP-SDN1RPT\Protected Files	2020-09-19 01:13:21 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
DESKTOP-SDN1RPT.lnk				E:\DESKTOP-SDN1RPT	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Incident_drive (E) (2).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Incident_drive (E).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Desktop.lnk				C:\Users\mortysmith\Desktop	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Thoughts.lnk				C:\Users\mortysmith\Desktop\Thoughts.txt	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
loot.lnk				C:\Users\mortysmith\Documents\loot.zip	2020-09-18 23:46:18 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Portal_gun.lnk				C:\Users\mortysmith\Documents\Portal_gun.png	2020-09-18 23:45:54 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Plans.lnk				C:\Users\mortysmith\Documents\Plans.txt	2020-09-18 23:45:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Documents.lnk				C:\Users\mortysmith\Documents	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
My Social Security Number.lnk				C:\Users\mortysmith\Documents\My Social Security ...	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Beth_Secret.lnk				C:\FileShare\Secret\Beth_Secret.txt	2020-09-18 23:35:07 EDT	20200918_0347_CDrive.E01	
Jessica.lnk				C:\Users\mortysmith\Pictures\Jessica.jpg	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
Pictures.lnk				C:\Users\mortysmith\Pictures	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01	
SECRET_beth.lnk				C:\FileShare\Secret\SECRET_beth.txt	2020-09-18 18:39:22 EDT	20200918_0347_CDrive.E01	

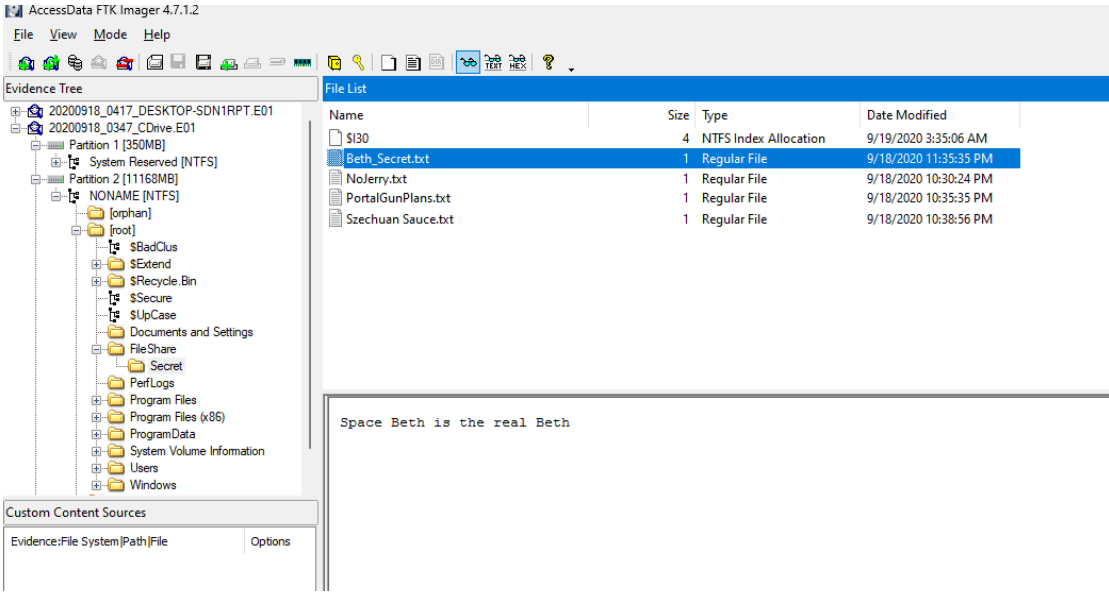
All of the highlighted portion was accessed after the connection was made and looking closer we can also see a file was added to the recycling bin after the RDP connection was made. The original file was a txt document that read “Earth beth is the real beth”.



Source Name	S	C	O	Path	Time Deleted	Username	Data Source
$RU2L112.txt				C:\FileShare\Secret\SECRET_beth.txt	2020-09-18 23:34:27 EDT		20200918_0347_CDrive.E01

```
Earth beth is the real beth.

-----------------------------METADATA-----------------------------
```

Going back to FTKImager, we can see now that the file has a new value with it being modified after the attacker connected to the desktop. That value is:

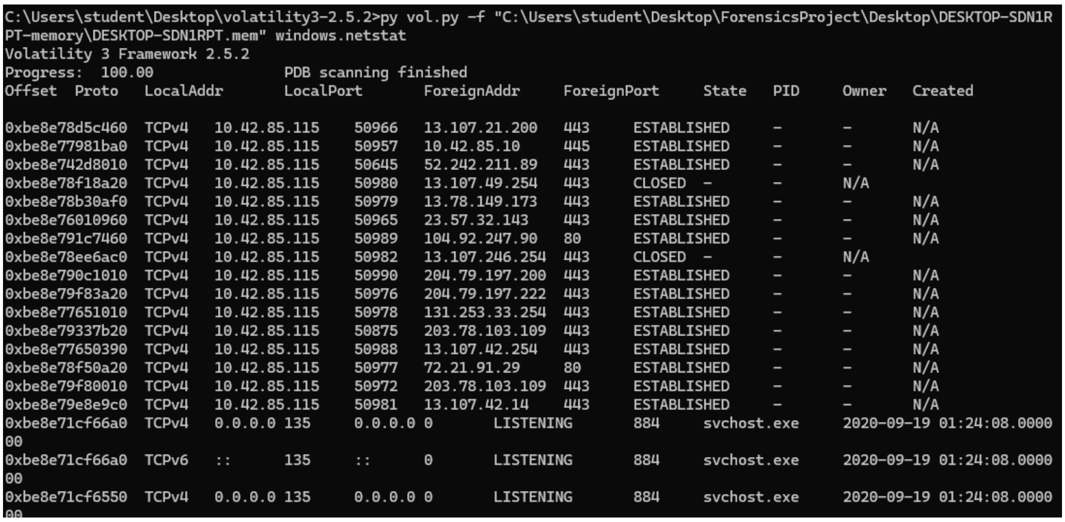


Name	Size	Type	Date Modified
$I30	4	NTFS Index Allocation	9/19/2020 3:35:06 AM
Beth_Secret.txt	1	Regular File	9/18/2020 11:35:35 PM
NoJerry.txt	1	Regular File	9/18/2020 10:30:24 PM
PortalGunPlans.txt	1	Regular File	9/18/2020 10:35:35 PM
Szechuan Sauce.txt	1	Regular File	9/18/2020 10:38:56 PM

```
Space Beth is the real Beth
```

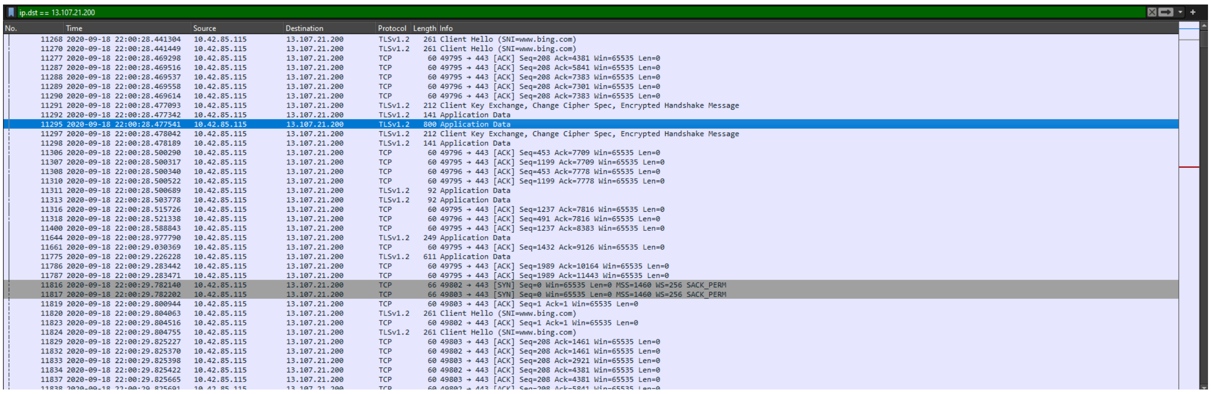
It appears that the attacker accessed and modified these files from 23:45 EDT 2020/09/18 until 01:13 EDT 2020/09/19.

Also looking at the memory dump using volatility 3 for the desktop, we can see that a number of IP addresses were captured for transferring information over the network:

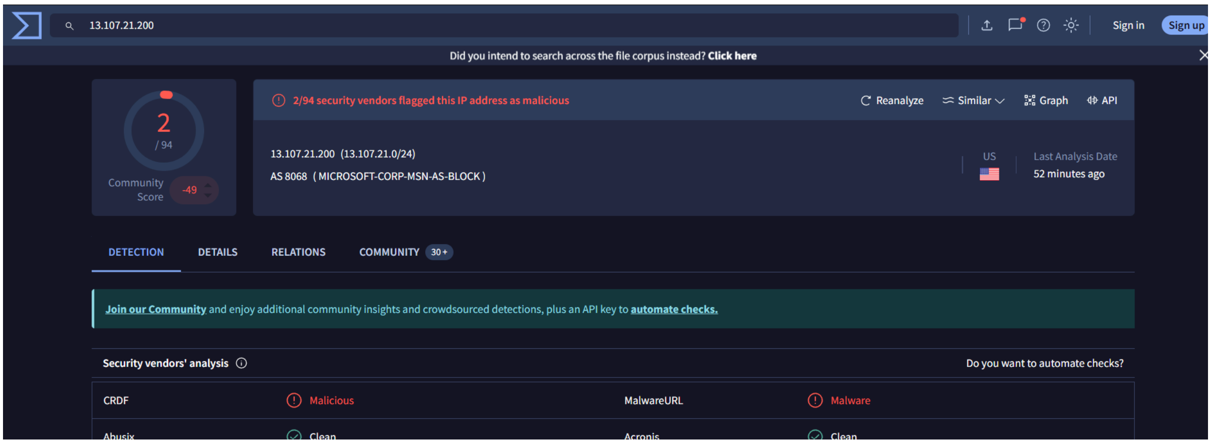


```
C:\Users\student\Desktop\volatility3-2.5.2>py vol.py -f "C:\Users\student\Desktop\ForensicsProject\Desktop\DESKTOP-SDN1R
PT-memory\DESKTOP-SDN1RPT.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xbe8e78d5c460  TCPv4   10.42.85.115    50966   13.107.21.200   443     ESTABLISHED     -       -       N/A
0xbe8e77981ba0  TCPv4   10.42.85.115    50957   10.42.85.10     445     ESTABLISHED     -       -       N/A
0xbe8e742d8010  TCPv4   10.42.85.115    50645   52.242.211.89   443     ESTABLISHED     -       -       N/A
0xbe8e78f18a20  TCPv4   10.42.85.115    50980   13.107.49.254   443     CLOSED  -       -       N/A
0xbe8e78b30af0  TCPv4   10.42.85.115    50979   13.78.149.173   443     ESTABLISHED     -       -       N/A
0xbe8e76010960  TCPv4   10.42.85.115    50965   23.57.32.143    443     ESTABLISHED     -       -       N/A
0xbe8e791c7460  TCPv4   10.42.85.115    50989   104.92.247.90   80      ESTABLISHED     -       -       N/A
0xbe8e78ee6ac0  TCPv4   10.42.85.115    50982   13.107.246.254  443     CLOSED  -       -       N/A
0xbe8e790c1010  TCPv4   10.42.85.115    50990   204.79.197.200  443     ESTABLISHED     -       -       N/A
0xbe8e79f83a20  TCPv4   10.42.85.115    50976   204.79.197.222  443     ESTABLISHED     -       -       N/A
0xbe8e77651010  TCPv4   10.42.85.115    50978   131.253.33.254  443     ESTABLISHED     -       -       N/A
0xbe8e79337b20  TCPv4   10.42.85.115    50875   203.78.103.109  443     ESTABLISHED     -       -       N/A
0xbe8e77650390  TCPv4   10.42.85.115    50988   13.107.42.254   443     ESTABLISHED     -       -       N/A
0xbe8e78f50a20  TCPv4   10.42.85.115    50977   72.21.91.29     80      ESTABLISHED     -       -       N/A
0xbe8e79f80010  TCPv4   10.42.85.115    50972   203.78.103.109  443     ESTABLISHED     -       -       N/A
0xbe8e79e8e9c0  TCPv4   10.42.85.115    50981   13.107.42.14    443     ESTABLISHED     -       -       N/A
0xbe8e71cf66a0  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     2020-09-19 01:24:08.0000
00
0xbe8e71cf66a0  TCPv6   ::      135     ::      0       LISTENING       884     svchost.exe     2020-09-19 01:24:08.0000
00
0xbe8e71cf6550  TCPv4   0.0.0.0 135     0.0.0.0 0       LISTENING       884     svchost.exe     2020-09-19 01:24:08.0000
00
```

Going back to wireshark, we can see that lots of application data was transferred from this IP address from our desktop.



```
ip.dst == 13.107.21.200
No.     Time                        Source          Destination     Protocol Length Info
  11268 2020-09-18 22:00:28.441304  10.42.85.115    13.107.21.200   TLSv1.2  261 Client Hello (SNI=www.bing.com)
  11270 2020-09-18 22:00:28.441449  10.42.85.115    13.107.21.200   TLSv1.2  261 Client Hello (SNI=www.bing.com)
  11277 2020-09-18 22:00:28.469298  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=208 Ack=4381 Win=65535 Len=0
  11287 2020-09-18 22:00:28.469516  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=208 Ack=5841 Win=65535 Len=0
  11288 2020-09-18 22:00:28.469537  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=208 Ack=7383 Win=65535 Len=0
  11289 2020-09-18 22:00:28.469558  10.42.85.115    13.107.21.200   TCP       60 49796 → 443 [ACK] Seq=208 Ack=7301 Win=65535 Len=0
  11290 2020-09-18 22:00:28.469614  10.42.85.115    13.107.21.200   TCP       60 49796 → 443 [ACK] Seq=208 Ack=7383 Win=65535 Len=0
  11291 2020-09-18 22:00:28.477093  10.42.85.115    13.107.21.200   TLSv1.2  212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  11292 2020-09-18 22:00:28.477342  10.42.85.115    13.107.21.200   TLSv1.2  141 Application Data
  11295 2020-09-18 22:00:28.477541  10.42.85.115    13.107.21.200   TLSv1.2  800 Application Data
  11297 2020-09-18 22:00:28.478042  10.42.85.115    13.107.21.200   TLSv1.2  212 Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
  11298 2020-09-18 22:00:28.478189  10.42.85.115    13.107.21.200   TLSv1.2  141 Application Data
  11306 2020-09-18 22:00:28.500290  10.42.85.115    13.107.21.200   TCP       60 49796 → 443 [ACK] Seq=453 Ack=7709 Win=65535 Len=0
  11307 2020-09-18 22:00:28.500317  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=1199 Ack=7709 Win=65535 Len=0
  11308 2020-09-18 22:00:28.500340  10.42.85.115    13.107.21.200   TCP       60 49796 → 443 [ACK] Seq=453 Ack=7778 Win=65535 Len=0
  11310 2020-09-18 22:00:28.500522  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=1199 Ack=7778 Win=65535 Len=0
  11311 2020-09-18 22:00:28.500689  10.42.85.115    13.107.21.200   TLSv1.2   92 Application Data
  11313 2020-09-18 22:00:28.503778  10.42.85.115    13.107.21.200   TLSv1.2   92 Application Data
  11316 2020-09-18 22:00:28.515726  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=1237 Ack=7816 Win=65535 Len=0
  11318 2020-09-18 22:00:28.521338  10.42.85.115    13.107.21.200   TCP       60 49796 → 443 [ACK] Seq=491 Ack=7816 Win=65535 Len=0
  11400 2020-09-18 22:00:28.588843  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=1237 Ack=8383 Win=65535 Len=0
  11644 2020-09-18 22:00:28.977790  10.42.85.115    13.107.21.200   TLSv1.2  249 Application Data
  11661 2020-09-18 22:00:29.030369  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=1432 Ack=9126 Win=65535 Len=0
  11775 2020-09-18 22:00:29.226228  10.42.85.115    13.107.21.200   TLSv1.2  611 Application Data
  11786 2020-09-18 22:00:29.283442  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=1989 Ack=10164 Win=65535 Len=0
  11787 2020-09-18 22:00:29.283471  10.42.85.115    13.107.21.200   TCP       60 49795 → 443 [ACK] Seq=1989 Ack=11443 Win=65535 Len=0
  11816 2020-09-18 22:00:29.782140  10.42.85.115    13.107.21.200   TCP       66 49802 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  11817 2020-09-18 22:00:29.782202  10.42.85.115    13.107.21.200   TCP       66 49803 → 443 [SYN] Seq=0 Win=65535 Len=0 MSS=1460 WS=256 SACK_PERM
  11819 2020-09-18 22:00:29.800944  10.42.85.115    13.107.21.200   TCP       60 49803 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  11820 2020-09-18 22:00:29.804063  10.42.85.115    13.107.21.200   TLSv1.2  261 Client Hello (SNI=www.bing.com)
  11823 2020-09-18 22:00:29.804516  10.42.85.115    13.107.21.200   TCP       60 49802 → 443 [ACK] Seq=1 Ack=1 Win=65535 Len=0
  11824 2020-09-18 22:00:29.804755  10.42.85.115    13.107.21.200   TLSv1.2  261 Client Hello (SNI=www.bing.com)
  11829 2020-09-18 22:00:29.825227  10.42.85.115    13.107.21.200   TCP       60 49803 → 443 [ACK] Seq=208 Ack=1461 Win=65535 Len=0
  11832 2020-09-18 22:00:29.825370  10.42.85.115    13.107.21.200   TCP       60 49802 → 443 [ACK] Seq=208 Ack=1461 Win=65535 Len=0
  11833 2020-09-18 22:00:29.825398  10.42.85.115    13.107.21.200   TCP       60 49803 → 443 [ACK] Seq=208 Ack=2921 Win=65535 Len=0
  11834 2020-09-18 22:00:29.825422  10.42.85.115    13.107.21.200   TCP       60 49802 → 443 [ACK] Seq=208 Ack=4381 Win=65535 Len=0
  11837 2020-09-18 22:00:29.825665  10.42.85.115    13.107.21.200   TCP       60 49803 → 443 [ACK] Seq=208 Ack=4381 Win=65535 Len=0
  11838 2020-09-18 22:00:29.825691  10.42.85.115    13.107.21.200   TCP       60 49802 → 443 [ACK] Seq=208 Ack=5841 Win=65535 Len=0
```



Did you intend to search across the file corpus instead? **Click here**

2 / 94

Community Score -49

2/94 security vendors flagged this IP address as malicious

13.107.21.200 (13.107.21.0/24)

AS 8068 (MICROSOFT-CORP-MSN-AS-BLOCK)

US

Last Analysis Date 52 minutes ago

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to **automate checks.**

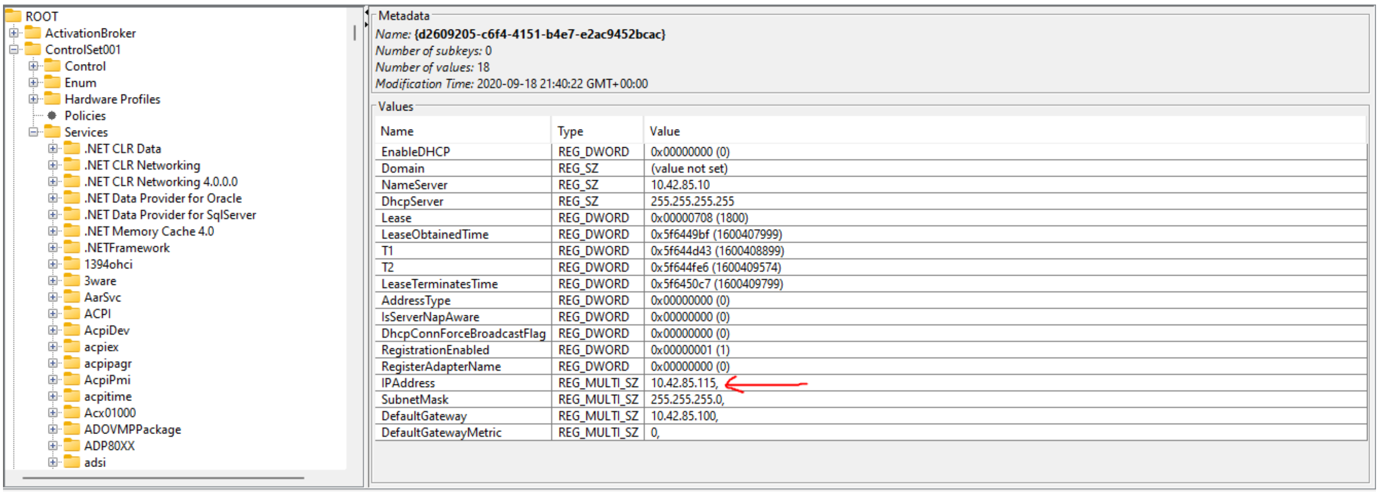
Security vendors' analysis

Do you want to automate checks?

CRDF	Malicious	MalwareURL	Malware
Abusix	Clean	Acronis	Clean

8. What was the network layout of the victim network? 10.42.85.0/24 Seena Davoodi

- 10.42.85.115 - Desktop
    - On Desktop Image: C:\Windows\System32\config
        1. SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\



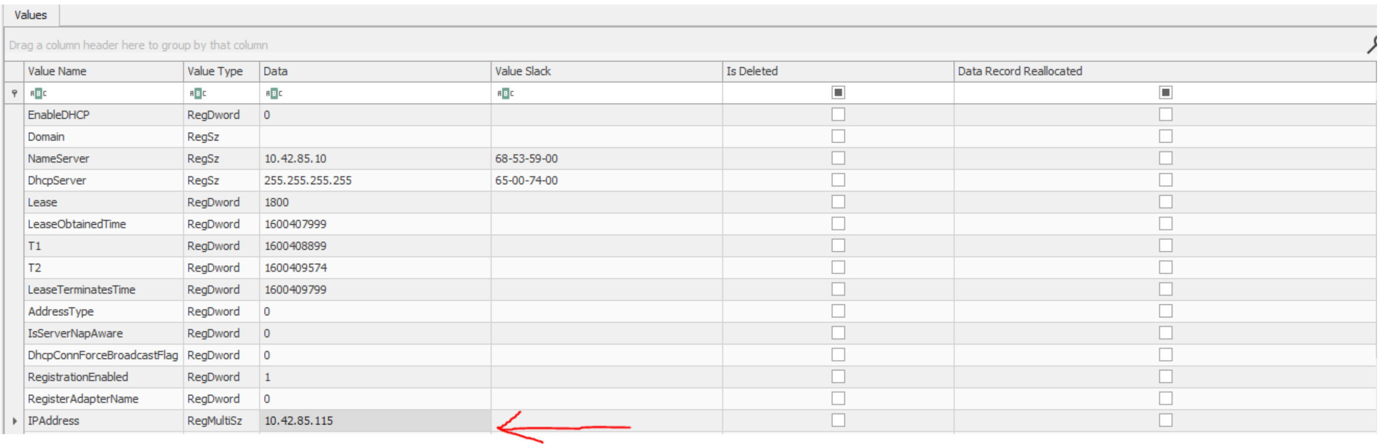
ROOT
- ActivationBroker
- ControlSet001
    - Control
    - Enum
    - Hardware Profiles
    - Policies
    - Services
        - .NET CLR Data
        - .NET CLR Networking
        - .NET CLR Networking 4.0.0.0
        - .NET Data Provider for Oracle
        - .NET Data Provider for SqlServer
        - .NET Memory Cache 4.0
        - .NETFramework
        - 1394ohci
        - 3ware
        - AarSvc
        - ACPI
        - AcpiDev
        - acpiex
        - acpipagr
        - AcpiPmi
        - acpitime
        - Acx01000
        - ADOVMPPackage
        - ADP80XX
        - adsi

Metadata

Name: {d2609205-c6f4-4151-b4e7-e2ac9452bcac}
Number of subkeys: 0
Number of values: 18
Modification Time: 2020-09-18 21:40:22 GMT+00:00

Values

Name	Type	Value
EnableDHCP	REG_DWORD	0x00000000 (0)
Domain	REG_SZ	(value not set)
NameServer	REG_SZ	10.42.85.10
DhcpServer	REG_SZ	255.255.255.255
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtainedTime	REG_DWORD	0x5f6449bf (1600407999)
T1	REG_DWORD	0x5f644d43 (1600408899)
T2	REG_DWORD	0x5f644fe6 (1600409574)
LeaseTerminatesTime	REG_DWORD	0x5f6450c7 (1600409799)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000 (0)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
IPAddress	REG_MULTI_SZ	10.42.85.115,
SubnetMask	REG_MULTI_SZ	255.255.255.0,
DefaultGateway	REG_MULTI_SZ	10.42.85.100,
DefaultGatewayMetric	REG_MULTI_SZ	0,

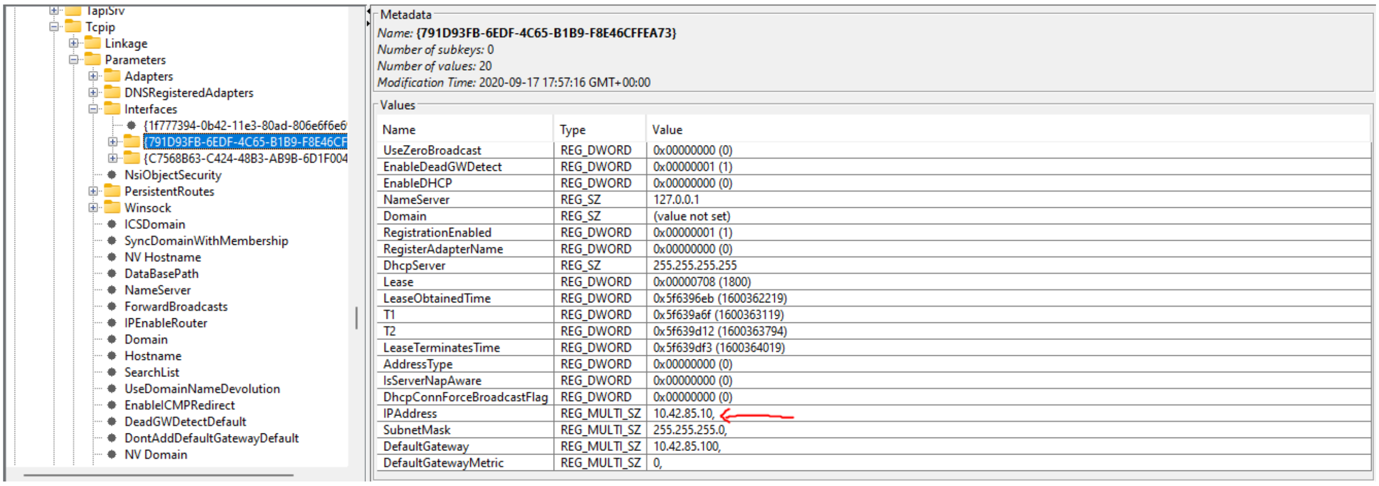


Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
EnableDHCP	RegDword	0		☐	☐
Domain	RegSz			☐	☐
NameServer	RegSz	10.42.85.10	68-53-59-00	☐	☐
DhcpServer	RegSz	255.255.255.255	65-00-74-00	☐	☐
Lease	RegDword	1800		☐	☐
LeaseObtainedTime	RegDword	1600407999		☐	☐
T1	RegDword	1600408899		☐	☐
T2	RegDword	1600409574		☐	☐
LeaseTerminatesTime	RegDword	1600409799		☐	☐
AddressType	RegDword	0		☐	☐
IsServerNapAware	RegDword	0		☐	☐
DhcpConnForceBroadcastFlag	RegDword	0		☐	☐
RegistrationEnabled	RegDword	1		☐	☐
RegisterAdapterName	RegDword	0		☐	☐
IPAddress	RegMultiSz	10.42.85.115		☐	☐

- 10.42.85.10 - DC Seena Davoodi
    - On server Image: C:\Windows\System32\config
        1. SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\



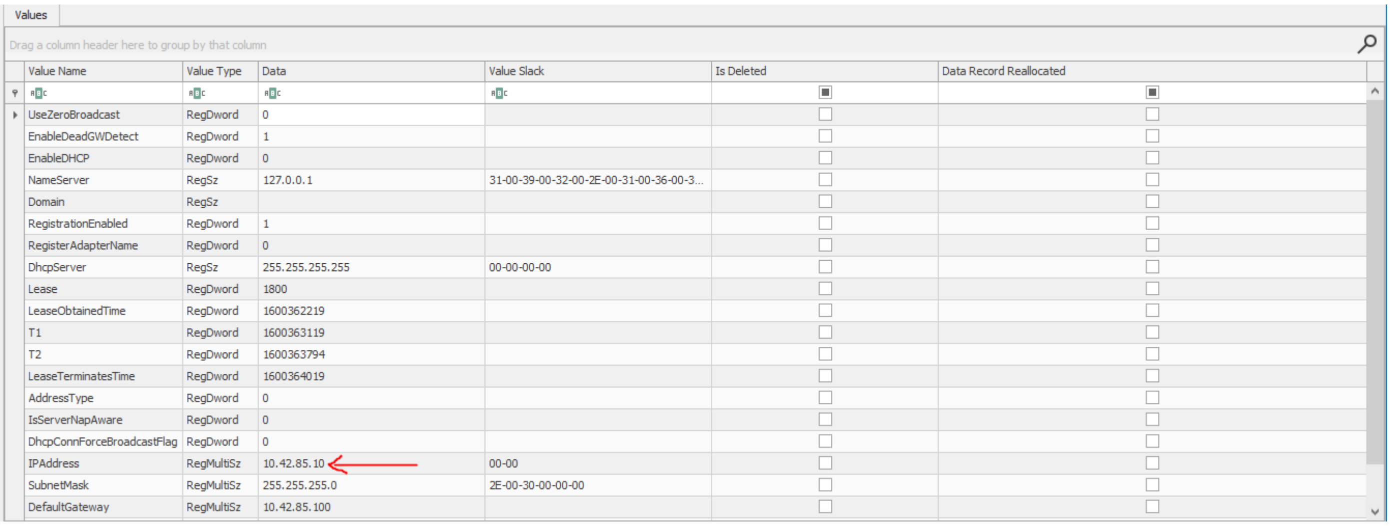
```
TapiSrv
Tcpip
  Linkage
  Parameters
    Adapters
    DNSRegisteredAdapters
    Interfaces
      {1f777394-0b42-11e3-80ad-806e6f6e6
      {791D93FB-6EDF-4C65-B1B9-F8E46CF
      {C7568B63-C424-48B3-AB9B-6D1F004
    NsiObjectSecurity
    PersistentRoutes
    Winsock
    ICSDomain
    SyncDomainWithMembership
    NV Hostname
    DataBasePath
    NameServer
    ForwardBroadcasts
    IPEnableRouter
    Domain
    Hostname
    SearchList
    UseDomainNameDevolution
    EnableICMPRedirect
    DeadGWDetectDefault
    DontAddDefaultGatewayDefault
    NV Domain
```

Metadata

Name: **{791D93FB-6EDF-4C65-B1B9-F8E46CFFEA73}**
Number of subkeys: 0
Number of values: 20
Modification Time: 2020-09-17 17:57:16 GMT+00:00

Values

Name	Type	Value
UseZeroBroadcast	REG_DWORD	0x00000000 (0)
EnableDeadGWDetect	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000000 (0)
NameServer	REG_SZ	127.0.0.1
Domain	REG_SZ	(value not set)
RegistrationEnabled	REG_DWORD	0x00000001 (1)
RegisterAdapterName	REG_DWORD	0x00000000 (0)
DhcpServer	REG_SZ	255.255.255.255
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtainedTime	REG_DWORD	0x5f6396eb (1600362219)
T1	REG_DWORD	0x5f639a6f (1600363119)
T2	REG_DWORD	0x5f639d12 (1600363794)
LeaseTerminatesTime	REG_DWORD	0x5f639df3 (1600364019)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNapAware	REG_DWORD	0x00000000 (0)
DhcpConnForceBroadcastFlag	REG_DWORD	0x00000000 (0)
IPAddress	REG_MULTI_SZ	10.42.85.10,
SubnetMask	REG_MULTI_SZ	255.255.255.0,
DefaultGateway	REG_MULTI_SZ	10.42.85.100,
DefaultGatewayMetric	REG_MULTI_SZ	0,



Values

Drag a column header here to group by that column

Value Name	Value Type	Data	Value Slack	Is Deleted	Data Record Reallocated
				■	■
UseZeroBroadcast	RegDword	0		□	□
EnableDeadGWDetect	RegDword	1		□	□
EnableDHCP	RegDword	0		□	□
NameServer	RegSz	127.0.0.1	31-00-39-00-32-00-2E-00-31-00-36-00-3...	□	□
Domain	RegSz			□	□
RegistrationEnabled	RegDword	1		□	□
RegisterAdapterName	RegDword	0		□	□
DhcpServer	RegSz	255.255.255.255	00-00-00-00	□	□
Lease	RegDword	1800		□	□
LeaseObtainedTime	RegDword	1600362219		□	□
T1	RegDword	1600363119		□	□
T2	RegDword	1600363794		□	□
LeaseTerminatesTime	RegDword	1600364019		□	□
AddressType	RegDword	0		□	□
IsServerNapAware	RegDword	0		□	□
DhcpConnForceBroadcastFlag	RegDword	0		□	□
IPAddress	RegMultiSz	10.42.85.10	00-00	□	□
SubnetMask	RegMultiSz	255.255.255.0	2E-00-30-00-00-00	□	□
DefaultGateway	RegMultiSz	10.42.85.100		□	□