

Case 001 – The Stolen Szechuan Sauce

Taken from: DFIR Madness (Author - James Smith)

Prepared by: Prinson D'silva
Team members: Jenz Kim, Matthew Egharevba
Date: February 18th, 2025

Table of Contents

Executive Summary	3
Questions/ Goals	4
1. What's the Operating System of the Server?	4
2. What's the Operating System of the Desktop?	5
3. What was the local time of the Server?	5
4. Was there a breach?	6
5. What was the initial entry vector (how did they get in)?	6
6. Was malware used? If so, what was it? If there was malware answer the following:	8
○ Identify the IP Address that delivered the payload.	9
○ What IP Address is the malware calling to?	9
○ Where is this malware on disk?	10
○ When did it first appear?	10
○ Did someone move it?	11
○ What were the capabilities of this malware?	11
○ Is this malware easily obtained?	12
○ Was this malware installed with persistence on any machine?	12
■ When?	12
■ Where?	12
7. What malicious IP Addresses were involved?	13
○ Were any IP Addresses from known adversary infrastructure?	13
○ Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?	14
8. Did the attacker access any other systems?	14
○ How?	14
○ When?	14
○ Did the attacker steal or access any data?	15
■ When?	15
9. What was the network layout of the victim network?	16
Recommendations	18
References	19

Executive Summary

The “Stolen Szechuan Sauce” digital forensics case focuses on analyzing a breach by employing advanced tools and methodologies. Through careful examination of system artifacts such as Disk Image, Volatile Memory, Autoruns of the Server (DC-01) as well as the Desktop (SDN1RPT), and packet capture of network traffic, the study of this case uncovers critical information about the breach, including the timeline, attack vectors, and malicious activities.

Key findings include the identification of the breach, initial entry vector through RDP brute force, presence of malware (“coreupdate.exe”), and the compromise of sensitive data. This study also recommends some preventive measures to fortify the security posture which was seen in this case.

Tools Used

- Volatility 3-2.5.2
- AccessData: FTK Imager 4.7.1.2
- Sauce - Autopsy 4.21.0
- Eric Zimmerman Tools: Registry Explorer v2.0.0.0, Timeline Explorer v2.0.0.1
- Windows: Event Viewer
- Wireshark
- Websites: Joe Sandbox, Virus Total

To prevent future attacks, the following mitigation strategies are recommended:

1. Account Use Policies
2. Multi-factor Authentication
3. Password Policies
4. User Account Management

Questions/ Goals

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

The Operating System on the Server is Windows Server 2012 R2.

This was determined by foraging on the Disk Image of CITADEL-DC01, using Autopsy.

Name	Type	Size (Bytes)	Sector Size (Bytes)	Timezone	Device ID
20200918_0347_CDrive.E01	image	12079595520	512	America/New_York	66f27275-83e9-4396-afb5-1c370af5398f

Figure 1: Windows Server 2012 R2 (determined using Autopsy on DC01 Disk Image) - Courtesy of Jenz Kim

This was alternatively confirmed using Registry Explorer of the SOFTWARE hive within the following directory of the Disk Image: \Microsoft\Windows\NT\CurrentVersion

Value Name	Value Type	Data	Value Slack
SystemRoot	RegSz	C:\Windows	00-05-12-00-00-00
SoftwareType	RegSz	System	00-00-F8-00-00
RegisteredOwner	RegSz	Windows User	6C-00
InstallDate	RegDword	1600361039	
CurrentVersion	RegSz	6.3	F0-00-01-00
CurrentBuild	RegSz	9600	00-00
RegisteredOrganization	RegSz		
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00-00-00
InstallationType	RegSz	Server	00-00-F4-E2-B7-53
EditionID	RegSz	ServerStandardEval	00-00-00-00-00-00
ProductName	RegSz	Windows Server 2012 R2 Standard Evaluation	00-00-00-00-00-00
ProductId	RegSz	00252-10000-00000-A228	37-00-5C-00
DigitalProductId	RegBinary	A4-00-00-03-00-00-00-30-30-32-35-3...	00-00-00-00
DigitalProductid4	RegBinary	F8-04-00-00-04-00-00-30-00-30-00-3...	00-00-00-00
CurrentBuildNumber	RegSz	9600	36-02
BuildLab	RegSz	9600.winblue_gdr.140221-1952	00-00
BuildLabEx	RegSz	9600.17031.amsdi4fre.winblue_gdr.1402...	00-00-00-00
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff	00-00
PathName	RegSz	C:\Windows	74-68-65-6E-74-00

Figure 2: Windows Server 2012 R2 SE (using Registry Explorer on the disk image) - Courtesy of Jenz Kim

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

The OS of the Desktop is Windows 10 Enterprise Evaluation.

This information was retrieved from the Desktop memory file by running the following Volatility 3 command in PowerShell: (Ashley Pearson, 2021)

`vol.py -f`

`"C:\Users\student\Desktop\ForensicsProject\Desktop\DESKTOP-SDN1RPT-memory\DESKTOP-SDN1RPT.mem" windows.info`

```
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\Desktop\DESKTOP-SDN1RPT-memory\DESKTOP-SDN1RPT.mem" windows.info
Volatility 3 Framework 2.5.2
Progress: 100.00          PDB scanning finished
Variable      Value
Kernel Base    0xf80162a14000
DTB     0x1ad000
Symbols file:///C:/Users/student/Desktop/volatility3-2.5.2/volatility3/symbols/windows/ntkrnlmp.pdb/81BC5C377C525081645F9958F289C527-1.json.xz
Is64Bit True
IsPAE False
Layer_name     0 WindowsIntel32e
Memory_layer   1 FileLayer
KdVersionBlock 0xf801636232a8
Major/Minor    15.19041
MachineType    34494
KeNumberProcessors 2
SystemTime     2020-09-19 05:10:39
NtSystemRoot   C:\Windows
NtProductType NtProductWinNt
NtMajorVersion 10
NtMinorVersion 0
PE MajorOperatingSystemVersion 10
PE MinorOperatingSystemVersion 0
PE Machine     34494
PE TimeDateStamp Sun Aug 11 05:47:24 2000
PS C:\Users\student\Desktop\volatility3-2.5.2>
```

Figure 3: Windows System Info (using Volatility 3)

This information was again confirmed in Registry Explorer, in the SOFTWARE hive following directory of the Desktop Disk Image: \Microsoft\WindowsNT\CurrentVersion

Value Name	Type	Data	Value Slack
EditionID	RegSz	EnterpriseEval	00-00-00-00-00-00
EditionSubManufacturer	RegSz		
EditionSubstring	RegSz		
EditionSubVersion	RegSz		
InstallationType	RegDword	Client	00-00-00-00-00-00
InstallDate	RegDword	1600408023	
ProductName	RegSz	Windows 10 Enterprise Evaluation	00-00
ReleasedId	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-A8-61-03
DigitalProductId	RegBinary	A4-00-00-03-00-00-00-30-30-33-32-39-2D-3...	
DigitalProductId64	RegBinary	F8-04-00-00-04-00-00-00-30-00-33-00-36-00-3...	2E-30-00-00
RegisteredOwner	RegSz	Admin	73-00-20-00-55-00-73-00-65-00-72-00-00-6...
RegisteredOrganization	RegSz		
InstallTime	RegQword	132448816238112497	70-96-FD-03

Figure 4: Windows CurrentVersion - Product Name (using Registry Explorer)

3. What was the local time of the Server?

The local time on the server was set in Pacific Standard Time as seen in Registry Explorer, within the following directory of the SYSTEM Hive:

\Microsoft\WindowsNT\CurrentVersion

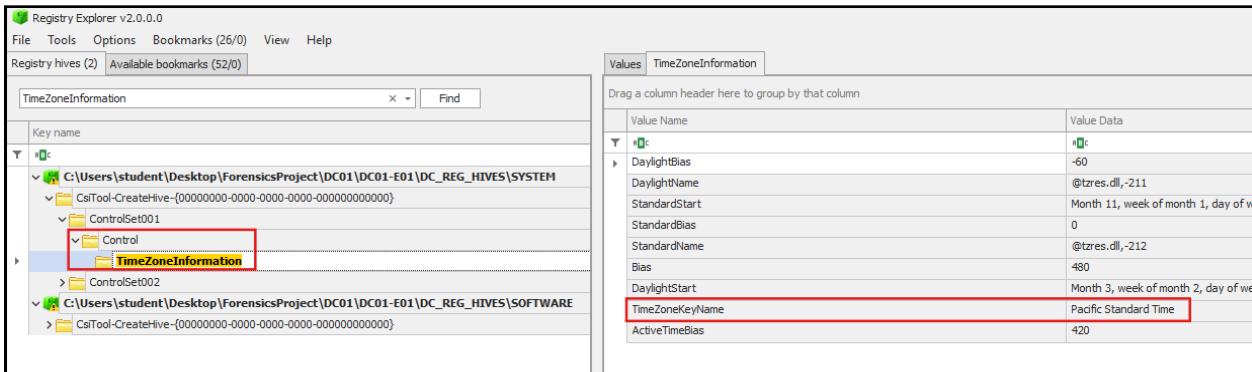


Figure 5: TimeZone Information (Registry Explorer)

4. Was there a breach?

Yes, as we can confirm from the case summary that the recipe was stolen. (DFIR, 2020) This theory is further backed up by the evidence from the answers provided in the following questions.

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

From the following evidence, we can confirm that the attack vector for initial entry in the server is Brute Force by RDP [Remote Desktop Protocol]. (MITRE, 2024)

While reviewing Event Logs in the server (DC-01), we noticed that the security logs had a large number of unsuccessful login attempts made from a suspected system named 'kali'. This was confirmed from Event ID 4625. (Microsoft, 2022)

The screenshot shows the Windows Event Viewer with the title 'Security_1 Number of events: 8,574'. A filter is applied: 'Filtered: Log: file:///F:/ForensicsProject/DC01/Security.evtx; Source: ; Event ID: 4624,4625., Number of events: 2,636'. The main table lists several event entries, with the last three highlighted by a red box. The details for Event ID 4625 are shown in the bottom half of the window:

Level	Date and Time	Source	Event ID	Task Categ
Information	9/18/2020 11:22:09 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:22:09 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:22:07 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:48 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:48 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:48 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4625	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4625	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4625	Logon

Event 4625, Microsoft Windows security auditing.

General Details

Failure Information:

- Failure Reason: Unknown user name or bad password.
- Status: 0xC000006D
- Sub Status: 0xC000006A

Process Information:

- Caller Process ID: 0x0
- Caller Process Name: -

Network Information:

- Workstation Name: kali
- Source Network Address: -
- Source Port: -

Detailed Authentication Information:

- Logon Process: NtLmssp

Log Name: Security

Source: Microsoft Windows security

Event ID: 4625

Level: Information

User: N/A

OpCode: Info

Keywords: Audit Failure

Logged: 9/18/2020 11:21:46 PM

Task Category: Logon

Compute: CITADEL-DC01.C137.local

More Information: [Event Log Online Help](#)

Figure 6: Windows Event Viewer - Security logs (Event ID: 4625)

After a number of failed attempts, the user from the kali system was finally able to login successfully as seen in log of Event ID 4624. (Microsoft, 2021)

Security_1 Number of events: 8,574				
Filtered: Log file:///F:\ForensicsProject\DC01\Security.evtx; Source: ; Event ID: 4624,4625, Number of events: 2,636				
Level	Date and Time	Source	Event ID	Task Category
Information	9/18/2020 11:22:09 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:22:09 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:22:07 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:48 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:48 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:48 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4624	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4625	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4625	Logon
Information	9/18/2020 11:21:46 PM	Microsoft Windows security auditing.	4625	Logon

Event 4624, Microsoft Windows security auditing.

General Details

New Logon:

- Security ID: S-1-5-21-2232410529-1445159330-2725690660-500
- Account Name: Administrator
- Account Domain: C137
- Logon ID: 0x50AA2D
- Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:

- Process ID: 0x0
- Process Name: -

Network Information:

- Workstation Name: kali
- Source Network Address: -
- Source Port: -

Log Name: Security

Source: Microsoft Windows security

Event ID: 4624

Level: Information

User: N/A

OpCode: Info

Logged: 9/18/2020 11:21:46 PM

Task Category: Logon

Keywords: Audit Success

Computer: CITADEL-DC01.C137.local

More Information: [Event Log Online Help](#)

Figure 7: Windows Event Viewer - Security logs (Event ID: 4624)

The event was then used to compare a TCP Connection established by this system, as seen in the RDS logs. The IP Address 194.61.24.102 was suspected to be a threat actor.

Microsoft-Windows-RemoteDesktopServices-RdpCoreTS%Operational Number of events: 2,081				
Level	Date and Time	Source	Event ID	Task Category
Information	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	135	RemoteFX module
Information	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	100	RemoteFX module
Information	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	98	RemoteFX module
Information	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	66	RemoteFX module
Information	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	132	RemoteFX module
Information	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	132	RemoteFX module
Information	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	101	RemoteFX module
Warning	9/18/2020 11:21:47 PM	RemoteDesktopServices-RdpCoreTS	141	RemoteFX module
Information	9/18/2020 11:21:46 PM	RemoteDesktopServices-RdpCoreTS	65	RemoteFX module
Information	9/18/2020 11:21:46 PM	RemoteDesktopServices-RdpCoreTS	131	RemoteFX module
Information	9/18/2020 11:21:46 PM	RemoteDesktopServices-RdpCoreTS	105	RemoteFX module
Information	9/18/2020 11:21:46 PM	RemoteDesktopServices-RdpCoreTS	102	RemoteFX module

Event 131, RemoteDesktopServices-RdpCoreTS

General Details

The server accepted a new TCP connection from client 194.61.24.102:40234.

Log Name: Microsoft-Windows-RemoteDesktopServices-RdpCoreTS/Operational

Source: RemoteDesktopServices-Rdp

Event ID: 131

Level: Information

User: NETWORK SERVICE

OpCode: EstablishConnection

Logged: 9/18/2020 11:21:46 PM

Task Category: RemoteFX module

Keywords:

Computer: CITADEL-DC01.C137.local

More Information: [Event Log Online Help](#)

Figure 8: Windows Event Viewer - RDS Operational logs

This can also be confirmed in the Wireshark capture file after applying the following display filter: ip.addr == 194.61.24.102 and tcp. (Wireshark, 2020)

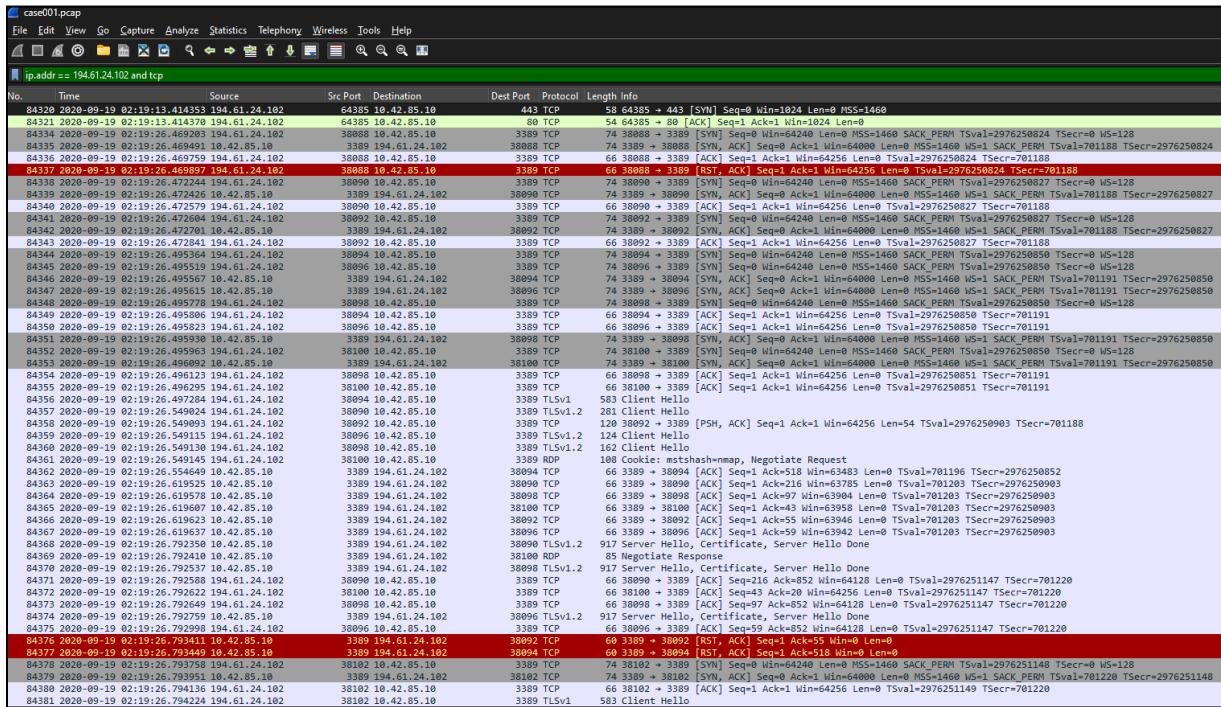


Figure 9: IP address and TCP filter applied in Case001.pcap - Courtesy of Matthew Egharevba

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

- What process was malicious?

The identified malicious process was coreupdater.exe which was confirmed running the following volatility 3 commands: (Ashley Pearson, 2021)

Volatility 3 Framework 2.5.2										
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
2460	452	msdtc.exe	0xe00062a2a900	9	-	0	False	2020-09-19 01:23:21.000000	N/A	Disabled
3724	452	spoolsv.exe	0xe00061cb300	13	-	0	False	2020-09-19 02:29:40.000000	N/A	Disabled
3644	2244	coreupdater.exe	0xe00062fe7700	0	-	2	False	2020-09-19 03:56:37.000000	2020-09-19 03:56:52.000000	Disabled
3706	848	taskhostw.exe	0xe00062f64900	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

Figure 10: vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.pslist - Courtesy of Jenz Kim

Volatility 3 Framework 2.5.2										
PID	PPID	ImageFileName	Offset(V)	Threads	Handles	SessionId	Wow64	CreateTime	ExitTime	File output
2764	640	WmiPrvSE.exe	0x1440a900	6	-	0	False	2020-09-19 04:37:42.000000	N/A	Disabled
2668	3472	vmtoolsd.exe	0x1e0cb1c0	8	-	1	False	2020-09-19 04:36:14.000000	N/A	Disabled
3644	2244	coreupdater.exe	0x2082c700	0	-	2	False	2020-09-19 03:56:37.000000	2020-09-19 03:56:52.000000	Disabled
2840	3472	FTK Imager.exe	0x20a2c1900	9	-	1	False	2020-09-19 04:37:04.000000	N/A	Disabled
3056	848	WMIADAP.exe	0x20f3f900	5	-	0	False	2020-09-19 04:37:42.000000	N/A	Disabled

Figure 11: vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.pscan - Courtesy of Jenz Kim

According to [Joe Sandbox](#) (2025), this program was confirmed as a **Malicious Metasploit**.

This was further verified by comparing its SHA256 hash value on [Virustotal](#) (2025).

- Identify the IP Address that delivered the payload.

As identified in question 5, we see that the kali system with IP **194.61.24.102** was involved in the initial entry of the attack.

We can confirm this from the Wireshark pcap file where the malware was downloaded from 194.61.24.102 using HTTP GET Method. The filter used is **(ip.src == 194.61.24.102 or ip.dst == 194.61.24.102) && (http.request)**.
(Wireshark, 2020)

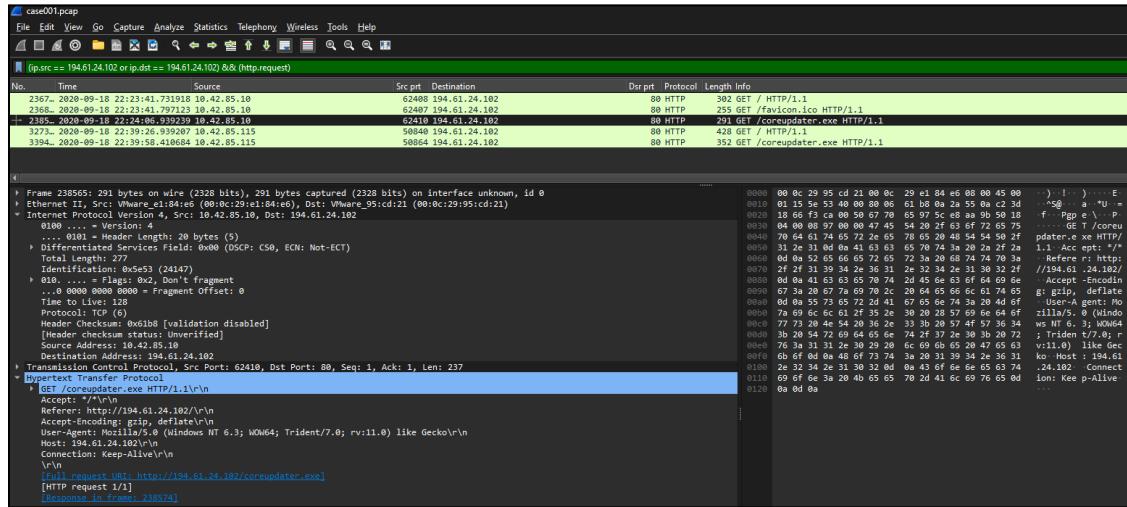


Figure 12: PCAP using display filter (The attack hosted malware on a HTTP server)

- What IP Address is the malware calling to?

By using the netscan Volatility 3 command (Ashley Pearson, 2021) on the server, we can identify that the malware coreupdater.exe is calling out to an IP address **203.78.103.109**.

0x5ffe1d10	TCPv6	fe80::2dcf:e660:be73:d220	49155	fe80::2dcf:e660:be73:d220	62777	CLOSED	460
0x6006f490	UDPV4	0.0.0.0 49437 * 0	1368	dns.exe	2020-09-19 01:22:57.000000		
0x6006fbba0	UDPV4	0.0.0.0 49436 * 0	1368	dns.exe	2020-09-19 01:22:57.000000		
0x60182590	TCPv4	10.42.85.10 62613 203.78.103.109 443	ESTABLISHED	3644	coreupdater.exe	N/A	
0x601cda00	TCPv6	fe80::2dcf:e660:be73:d220 135	fe80::2dcf:e660:be73:d220	62779	CLOSED	684	
0x601fae50	TCPv4	0.0.0.0 62475 0.0.0.0 0	LISTENING	3724	spoolsv.exe	N/A	
0x601fae50	TCPv6	:: 62475 :: 0	LISTENING	3724	spoolsv.exe	N/A	

Figure 13: vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.netscan - Courtesy of Jenz Kim

This was confirmed in the pcap file by using the ip address display filter **ip.addr == 203.78.103.109**.

Figure 14: PCAP using display filter (The attack hosted malware on a HTTP server) - Courtesy of Matthew Egharevba

- Where is this malware on disk?

The malware was found in the following directory by looking at the autorun of the server, in Timeline Explorer.

Li...	Tag	Time	Entry Location	Entry	Category	Profile	Image Path	Launch String
T	=							
23	<input type="checkbox"/>	4/14/...	HKLM\System\CurrentControlSet\Services	coreupdater	Services	System-wide	c:\windows\system32\coreupdater.exe	C:\Windows\System32\coreupdater.exe

Figure 15: Malware found in DC-01 C:\Windows\System32\coreupdate.exe (Timeline Explorer)

Also verified when the server disk file directory was triaged in FTK Imager.

The screenshot displays the AccessData FTK Imager interface. The Evidence Tree pane on the left shows a hierarchical file system structure, with the 'System32' folder under the root highlighted by a red box. The File List pane on the right shows a detailed list of files from the 'System32' folder, with 'coreupdater.exe' highlighted by a blue box. The table below provides the details for the listed files.

Name	Size	Type	Date Modified
console.dll	79	Regular File	8/22/2013 11:17:25 AM
control.exe	113	Regular File	8/22/2013 11:03:56 AM
convert.exe	20	Regular File	8/22/2013 11:32:31 AM
CoreMmRes.dll	15	Regular File	8/22/2013 11:45:01 AM
coreupdater.exe	7	Regular File	9/19/2010 3:24:06 AM
coreupdater.exe.\$fileslack	1	File Slack	
corregine.dll	81	Regular File	8/22/2013 11:00:08 AM
CredentialUIBroker.exe	37	Regular File	8/22/2013 12:39:50 PM
credssp.dll	21	Regular File	8/22/2013 10:01:34 AM
credui.dll	161	Regular File	8/22/2013 10:45:44 AM
credwiz.exe	36	Regular File	8/22/2013 10:50:12 AM
crypt32.dll	1,898	Regular File	3/21/2014 6:48:53 PM
cryptbase.dll	30	Regular File	8/22/2013 1:25:35 PM
cryptcatsvc.dll	111	Regular File	8/22/2013 9:47:11 AM
cryptdlg.dll	30	Regular File	8/22/2013 11:31:40 AM
cryptdll.dll	91	Regular File	8/22/2013 12:41:39 PM
cryptext.dll	65	Regular File	8/22/2013 10:55:02 AM
cryptnet.dll	191	Regular File	8/22/2013 10:03:49 AM

Figure 15: Malware found in DC-01 C:\Windows\System32\coreupdate.exe (FTK Imager)

- When did it first appear?

It first appeared at 3:24:12 on 2020-09-19 (UTC) which was confirmed using an MFT Scan in Volatility 3, of the server memory file.
 (ForensicXlab, November 2023)

```
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "F:\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.mftscan.MFTScan | Select-String -Pattern 'coreupdater.exe'
Progress: 100.00      PDB scanning finished
* 0xb001cd18528    FILE 87137 2 File Archive FILE_NAME 2020-09-19 03:24:12.000000 2020-09-19 03:24:06.000000 2020-09-19 03:24:12.000000 2020-09-19 03:24:12.000000 coreupdater.exe
```

Figure 16: MFT Scan including Select-String to filter out coreupdater.exe (Volatility 3)

This can also be confirmed by looking at the MFT output file of the Server in timeline explorer which reflects the exact same date & time.

Timeline Explorer v2.0.0.1													
File Tools Tabs View Help													
20200218155435_MFTECmd_\$J_Output.csv													
Drag a column header here to group by that column													
Line	Tag	Entry...	Sequence Number	Parent Entry Number	Parent Sequence Number	In Use	Parent Path	File Name	Extension	File Size	Created@x10	Updated@x10	Deleted@x10
111836			87137	2	2873	1	.\Windows\System32	coreupdater.exe	.exe	7168	2020-09-19 03:24:12		

Figure 17: coreupdater.exe searched for in the MFT Output file (Timeline Explorer) - Courtesy of Jenz Kim

- Did someone move it?

Yes, It was originally located in the `Users\Administrator\Downloads` directory which was then moved to the `Windows\System32` directory. This was found by analysing USNJournal of the Server, using the `$J` output file in Timeline Explorer.

Timeline Explorer v2.0.0.1													
File Tools Tabs View Help													
20200218155435_MFTECmd_\$J_Output.csv													
Drag a column header here to group by that column													
Line	Tag	Update Timestamp	Parent Path	Name	Extens...	Entry...	Sequence...	Parent...	Parent...	Update ...	Update ...	Reasons	File Attrrib...
80281		2020-09-19 03:24:06	.\PathUnknown\Directory with ID 0x...	coreupdater[1].exe	.exe	76711	12	87050	1	8992704	1	FileCreate	Archive No
80292		2020-09-19 03:24:06	.\PathUnknown\Directory with ID 0x...	coreupdater[1].exe	.exe	76711	12	87050	1	8992800	1	DataExtend FileCreate	Archive No
80293		2020-09-19 03:24:06	.\PathUnknown\Directory with ID 0x...	coreupdater[1].exe	.exe	76711	12	87050	1	8992896	1	DataExtend FileCreate Close	Archive No
80235		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe	.exe	87137	1	84880	1	8995760	1	FileCreate	Archive
80236		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe	.exe	87137	1	84880	1	8995856	1	FileCreate Close	Archive
80237		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe	.exe	87137	1	84880	1	8995952	1	FileDelete Close	Archive
80238		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996048	1	FileCreate	Archive
80239		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996176	1	FileCreate Close	Archive
80240		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996304	1	DataTruncation	Archive
80241		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996432	1	DataTruncation Close	Archive
80242		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996560	1	DataExtend	Archive
80243		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996688	1	DataOverwrite DataExtend	Archive
80244		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996816	1	DataOverwrite DataExtend BasicInfoChange	Archive
80245		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8996944	1	DataOverwrite DataExtend BasicInfoChange	Archive
80246		2020-09-19 03:24:12	.\PathUnknown\Directory with ID 0x...	coreupdater[1].exe	.exe	76711	12	87050	1	8997072	1	FileDelete Close	Archive No
80247		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urn.par...	.parti...	87137	2	84880	1	8997168	1	RenameOldName	Archive
80248		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe	.exe	87137	2	84880	1	8997296	1	RenameNewName	Archive
80249		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe	.exe	87137	2	84880	1	8997392	1	RenameNewName Close	Archive
80255		2020-09-19 03:24:50	.\Users\Administrator\Downloads	coreupdater.exe	.exe	87137	2	84880	1	8997944	1	RenameOldName	Archive
80256		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe	.exe	87137	2	2873	1	8998804	1	RenameNewName	Archive
80257		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe	.exe	87137	2	2873	1	8998136	1	RenameNewName Close	Archive
80258		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe	.exe	87137	2	2873	1	8998232	1	SecurityChange	Archive
80259		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe	.exe	87137	2	2873	1	8998328	1	SecurityChange Close	Archive

Figure 18: coreupdater.exe searched for in the MTF \$J Output file (Timeline Explorer) - Courtesy of Jenz Kim

- What were the capabilities of this malware?

According to [Joe Sandbox](#) (2025), coreupdater.exe is capable of the following:

- Remote Access control: Giving the attacker access through a backdoor so they can take control of the compromised machine from a distance.

- Privilege escalation: Coreupdater.exe can be used to elevate privileges on a computer system.

It is also capable of data-manipulation by encode data using XOR, as mentioned by [Virus Total](#) (2025).

- Is this malware easily obtained?

Although this malware is flagged as a malicious trojan by most security vendors (Anti-Virus and Sandbox Reports), it is part of the Metasploit framework and intended as an information security tool to test the vulnerability of computer systems. (Virus Total, 2025)

It is a Ruby based open-source framework that allows penetration testing so it is safe to assume that this malware can be obtained easily.

- Was this malware installed with persistence on any machine?

- When?

The program was installed on both machines (i.e. the server and desktop) for auto start and since it has already been deemed malicious, it could allow attackers to maintain persistence.

This was detected by looking into the Windows System event logs (Event ID 7045) which indicates a new service installed.

(Splunk, 2025)

- Server (CITADEL-DC-01) - 9/18/2020 11:27:49 PM local (9/19/2020 3:27:49 PM UTC)
- Desktop (SDN1RPT) - 9/18/2020 11:42:42 PM local (9/19/2020 3:42:42 PM UTC)

- Where?

- Server (CITADEL-DC-01) - C:\Windows\System32\coreupdater.exe

Level	Date and Time	Source	Event ID	Task Category
Information	9/18/2020 11:44:29 PM	Service Control Manager	7045	None
Information	9/18/2020 11:27:49 PM	Service Control Manager	7045	None
Information	9/18/2020 11:25:44 PM	Service Control Manager	7045	None
Information	9/17/2020 1:51:41 PM	Service Control Manager	7045	None
Information	9/17/2020 1:51:41 PM	Service Control Manager	7045	None
Information	9/17/2020 1:51:41 PM	Service Control Manager	7045	None
Information	9/17/2020 1:51:41 PM	Service Control Manager	7045	None

Event 7045, Service Control Manager

General Details

A service was installed in the system.

Service Name: coreupdater
 Service File Name: C:\Windows\System32\coreupdater.exe
 Service Type: user mode service
 Service Start Type: auto start
 Service Account: LocalSystem

Log Name: System
 Source: Service Control Manager
 Event ID: 7045
 Level: Information
 User: S-1-5-21-232410529-144515
 OpCode: Info
 More Information: [Event Log](#) [Online Help](#)

Logged: 9/18/2020 11:27:49 PM
 Task Category: None
 Keywords: Classic
 Computer: CITADEL-DC01.C137.local

Figure 19: Windows System logs - Server (Event ID 7045)

- Desktop (SDN1RPT) - C:\Windows\System32\coreupdater.exe

System Number of events: 994					
Filtered: Log: file:///F:/ForensicsProject/Artifacts/(DESKTOP-E01)\Event logs\System.evtx; Source: ; Event ID: 7045. Number of events: 20					
Level	Date and Time	Source		Event ID	Task Category
(I) Information	9/19/2020 1:10:38 AM	Service Control Manager		7045	None
(I) Information	9/19/2020 1:08:59 AM	Service Control Manager		7045	None
(I) Information	9/18/2020 11:43:14 PM	Service Control Manager		7045	None
(I) Information	9/18/2020 11:42:42 PM	Service Control Manager		7045	None
(I) Information	9/18/2020 1:54:01 AM	Service Control Manager		7045	None
(I) Information	9/18/2020 1:53:47 AM	Service Control Manager		7045	None
(I) Information	9/18/2020 1:53:38 AM	Service Control Manager		7045	None

Event 7045, Service Control Manager					
General	Details				
A service was installed in the system.					
Service Name:	coreupdate				
Service File Name:	C:\Windows\System32\coreupdate.exe				
Service Type:	user mode service				
Service Start Type:	auto_start				
Service Account:	LocalSystem				

Log Name:	System
Source:	Service Control Manager
Event ID:	7045
Level:	Information
User:	S-1-5-21-2232410529-14451!
OpCode:	Info
More Information:	Event Log Online Help

Figure 20: Windows System logs - Desktop (Event ID 7045)

7. What malicious IP Addresses were involved?

- Were any IP Addresses from known adversary infrastructure?

Among the two malicious IP addresses identified (refer to Fig. 12 and Fig. 14), one of the IP Addresses **203.78.103.109** has been blacklisted multiple times by both [Joe Sandbox](#) (2025) and [Virus Total](#) (2025) while **194.61.24.102** is listed as safe on either of these websites, it has been once reported for a Brute Force attack in November 2020 by [Clean Talk](#) (2020).

Joe Sandbox View / Context						
IPs						
Match	Associated Sample Name / URL	SHA 256	Detection	Link	Context	
203.78.103.109	coreupdate.exe coreupdate.exe coreupdate.exe coreupdate.exe coreupdate.exe coreupdate.exe coreupdate.exe	Get hash Get hash Get hash Get hash Get hash Get hash Get hash	malicious malicious malicious malicious malicious malicious malicious	Browse Browse Browse Browse Browse Browse Browse		

Figure 21: 203.78.103.109 listed on Joe Sandbox.

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

As per the websites mentioned above, these IP addresses/ adversaries were not involved in other simultaneous attacks during the time when this attack was carried out.

8. Did the attacker access any other systems?

- How?

The attacker seemed to have moved from the server to the desktop using RDP. The initial attempts were made using a Brute Force attack (refer to 5.) This can be confirmed in the Wireshark pcap using the display filter `ip.src == 10.42.85.10 and rdp`.

ip.src == 10.42.85.115 and rdp						
No.	Time	Source	Src prt	Destination	Dsr prt	Protocol
2652...	2020-09-18 22:35:55.364696	10.42.85.115	3389	10.42.85.10	62514	RDP
<pre> Frame 265234: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface unknown, id 0 Ethernet II, Src: VMware_14:c2:95 (00:0c:29:14:c2:95), Dst: VMware_e1:84:e6 (00:0c:29:e1:84:e6) Internet Protocol Version 4, Src: 10.42.85.115, Dst: 10.42.85.10 0100 = Version: 4 0101 = Header Length: 20 bytes (5) Differentiated Services Field: 0x00 (DSQoS: CS0, ECN: Not-ECT) Total Length: 59 Identification: 0x608a (24714) > 010. = Flags: 0x2, Don't fragment ...0 0000 0000 0000 = Fragment Offset: 0 Time to Live: 128 Protocol: TCP (6) Header Checksum: 0xdbb6 [validation disabled] [Header checksum status: Unverified] Source Address: 10.42.85.115 Destination Address: 10.42.85.10 Transmission Control Protocol, Src Port: 3389, Dst Port: 62514, Seq: 1, Ack: 20, Len: 19 TPKT, Version: 3, Length: 19 ISO 8073/X.224 COTP Connection-Oriented Transport Protocol Remote Desktop Protocol Type: RDP Negotiation Response (0x02)</pre>						

Figure 22: Display filter used to capture RDP movement from Server to Desktop

- When?

The pcap shows the local timestamp of 2020-09-18 22:35:55 which means the RDP connection was made at around 19-09-2020 3:35:55 pm UTC.

It can also be confirmed in Timeline Explorer that the attacker moved from the server to the desktop using the admin account, around the same time.

DESKTOP-SDN1RPT.C137.local | 2020-09-19 03:36:24 4624 DESKTOP-SDN1RPT (10.42.85.10) Target: C137\Administrator

Figure 23: Lateral movement captured in Timeline Explorer - Courtesy of Jenz Kim

- Did the attacker steal or access any data?
 - When?
 - Server (CITADEL-DC-01) - As the attacker made a move using the admin account, we looked at the Recent directory (C:\Users\Administrator\AppData\Roaming\Windows\Recent) which showed the following files were last accessed by the attacker.

The screenshot shows the FTK Imager interface with the Evidence Tree on the left and a File List on the right. The Evidence Tree shows a folder structure including Local, Roaming, and Recent. The File List displays a list of files from the Recent directory, with several files highlighted in red. A red box highlights the list of files in the File List pane.

Name	Type	Date Modified
AutomaticDestinations	Directory	9/19/2020 3:36:25 AM
CustomDestinations	Directory	9/19/2020 4:36:14 AM
\$130	NTFS Index All...	9/19/2020 3:35:07 AM
Beth_Secret.Ink	Regular File	9/19/2020 3:35:07 AM
Beth_Secret.Ink.FileSlack	File Slack	
desktop.ini	Regular File	9/17/2020 4:46:25 PM
NoJerry.Ink	Regular File	9/19/2020 3:31:50 AM
NoJerry.Ink.FileSlack	File Slack	
PortalGunPlans.Ink	Regular File	9/19/2020 3:32:02 AM
PortalGunPlans.Ink.FileSlack	File Slack	
Secret.Ink	Regular File	9/19/2020 3:35:07 AM
SECRET_beth.Ink	Regular File	9/19/2020 3:32:13 AM
SECRET_beth.Ink.FileSlack	File Slack	
Szechuan Sauce.Ink	Regular File	9/19/2020 3:32:21 AM
Szechuan Sauce.Ink.FileSlack	File Slack	

Figure 24: Recent directory - CITADEL-DC01 (FTK Imager)

- Desktop (SDN1RPT) - The same directory was accessed for the Desktop.

The screenshot shows the FTK Imager interface with the Evidence Tree on the left and a File List on the right. The Evidence Tree shows a folder structure including Temp, Roaming, and Recent. The File List displays a list of files from the Recent directory, with several files highlighted in red. A red box highlights the list of files in the File List pane.

Name	Type	Date Modified
AutomaticDestinations	Directory	9/19/2020 3:45:54 AM
CustomDestinations	Directory	9/19/2020 3:39:18 AM
\$130	NTFS Index All...	9/19/2020 3:47:39 AM
desktop.ini	Regular File	9/19/2020 3:36:32 AM
Desktop.Ink	Regular File	9/19/2020 3:47:39 AM
Documents.Ink	Regular File	9/19/2020 3:45:54 AM
loot.Ink	Regular File	9/19/2020 3:46:18 AM
My Social Security Number.Ink	Regular File	9/19/2020 3:45:34 AM
Plans.Ink	Regular File	9/19/2020 3:45:39 AM
Portal_gun.Ink	Regular File	9/19/2020 3:45:54 AM
Thoughts.Ink	Regular File	9/19/2020 3:47:39 AM

Figure 25: Recent directory - SDN1RPT (FTK Imager)

After looking at the last accessed files from both the systems, we located their directories to confirm the data that was accessed by the attacker.

- Secret.zip - 9/19/2020 3:35:06 AM UTC (Stolen)

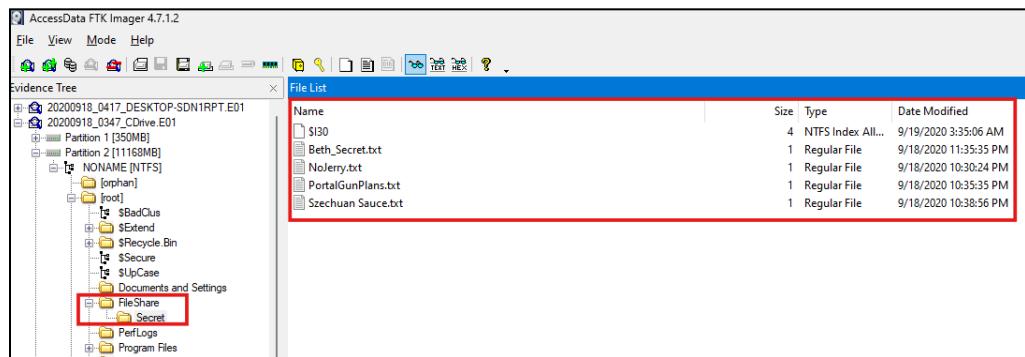


Figure 26:C:\FileShare\Secret.zip (Server)

- loot.zip - 9/19/2020 3:47:09 AM UTC (Missing - most likely stolen)

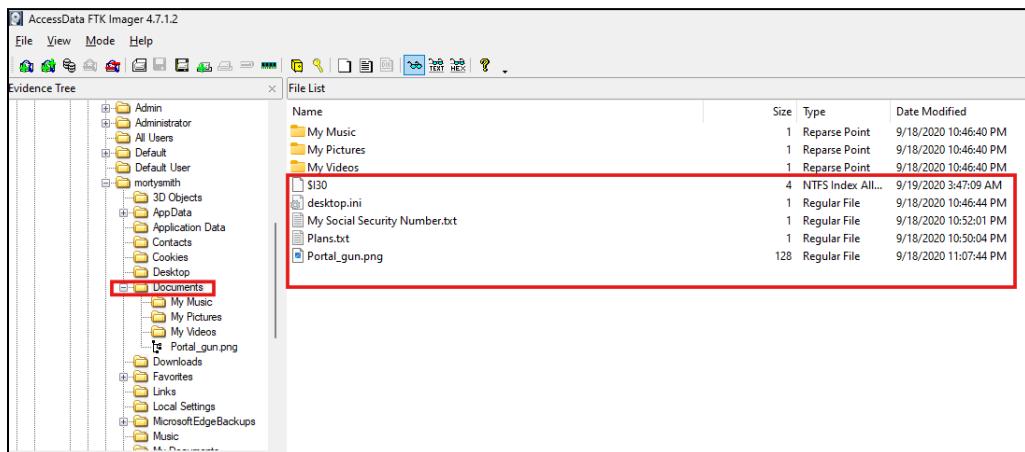


Figure 27:C:\Users\mortysmith\Documents\loot.zip (Desktop)

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

We can determine the network configuration of both systems in Registry Explorer, in the following directory:

SYSTEM\Root\ControlSet001\Services\Tcpip\Parameters\Interfaces

- Server: -
 - IP Address = 10.42.85.10
 - Subnet mask = 255.255.255.0 (10.42.85.0/24)

Registry hives (2) Available bookmarks (55/0)				Values	DHCPNetworkHints	NetworkSettings
Enter text to search... Find						
Key name	# values	# subkeys	Last write time	IP Address	Subnet Mask	DHCP Subnet Mask
Tcpip Linkage Parameters Adapters DNSRegisteredAdapters Interfaces NsiObjectSecurity PersistentRoutes Winsock Performance Security ServiceProvider	= 3 16 0 0 0 0 0 5 1 7	= 0 6 2 1 3 0 0 0 0 0	= 2020-09-1 2020-09-1 2020-09-1 2020-09-1 2020-09-1 2013-08-2 2020-09-1 2013-08-2 2013-08-2 2013-08-2	10.42.85.10 255.255.255.0	255.255.255.255	

Figure 28: Network Settings using Registry Explorer (Server)

- Desktop: -
 - IP Address = 10.42.85.115
 - Subnet mask = 255.255.255.0 (10.42.85.0/24)

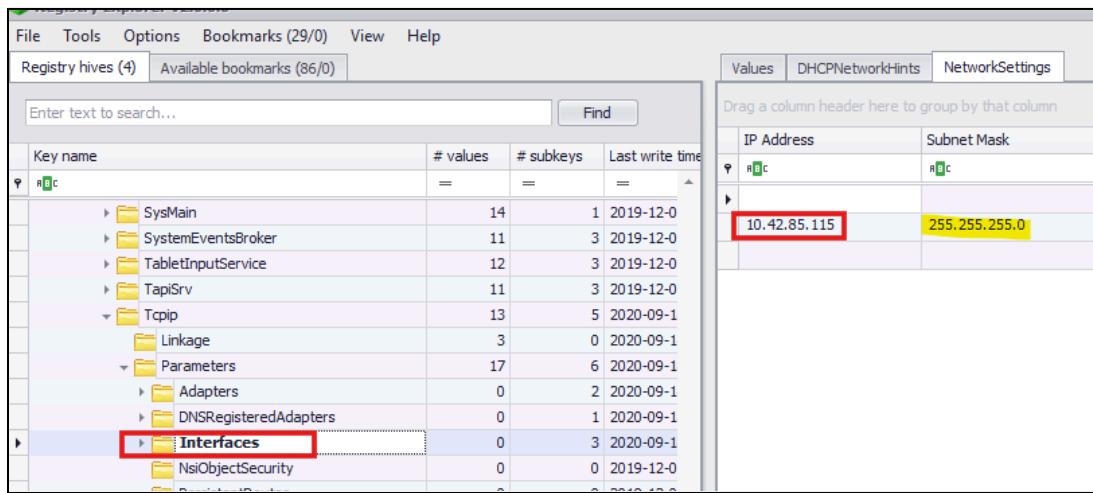


Figure 29: Network Settings using Registry Explorer (Desktop)

As we can see, both systems share the same subnet mask, i.e. 255.255.255.0. Thus, we can safely say that the two hosts CITADEL-DC01 (10.42.85.10) and Desktop (SDN1RPT) are in the same subnet 10.42.85.0/24.

Recommendations

According to MITRE (2025), following are some recommended mitigation strategies against RDP Brute Force Attacks: -

1. Account Use Policies:
 - a. Set account lockout policies after a certain number of failed login attempts to prevent passwords from being guessed. Too strict a policy may create a denial of service condition, with all accounts used in the brute force being locked-out.
 - b. Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges.
 - c. Consider blocking risky authentication requests, such as those originating from anonymous services/proxies.
2. Multi-factor Authentication: Use and enable multi-factor authentication, especially on externally facing services.
3. Password Policies: Refer to NIST guidelines when creating password policies. (NIST Special Publication 800-63B, October 2023)
4. User Account Management: Proactively reset accounts that are known to be part of breached credentials either immediately, or after detecting brute force attempts.

References

- James Smith (September 21, 2020) - *The Case of the Stolen Szechuan Sauce*. DFIR Madness. Retrieved from <https://dfirmadness.com/the-stolen-szechuan-sauce/>
- Ashley Pearson (May, 2021) - A Basic DFIR Blog: Volatility Cheat Sheet. ONFV Blog. Retrieved from <https://blog.onfv.org/post/volatility-cheatsheet/>
- MITRE (October 2024) - Techniques > Enterprise > Brute Force. MITRE. Retrieved from <https://attack.mitre.org/techniques/T1110/>
- Microsoft Windows Learn (March 2022) - *Security Auditing*. Microsoft. Retrieved from <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4625>
- Microsoft Windows Learn (July 2021) - *Security Auditing*. Microsoft. Retrieved from <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624>
- Wireshark Wiki (August, 2020) - *Display Filters*. Wireshark. Retrieved from <https://wiki.wireshark.org/DisplayFilters>
- JoeSandbox Cloud (Retrieved February, 2025) - *Analysis Report coreupdate.exe*. Retrieved from <https://www.joesandbox.com/analysis/398583/0/html>
- Virustotal (Retrieved February, 2025). Retrieved from <https://www.virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6>
- ForensicXlab (November, 2023) - Volatility3 : Alternate Data Stream Scan. Retrieved from <https://www.forensicxlab.com/posts/volads/>
- Splunk (January, 2025) - *Detection: Windows Service Created with Suspicious Service Path*. Retrieved from <https://research.splunk.com/endpoint/429141be-8311-11eb-adb6-acde48001122/#:~:text=Splunk%20Enterprise%20Security-,Description,severe%20threat%20to%20the%20environment>
- Clean Talk (November, 2020) - *Who is 194.61.24.102*. Retrieved from <https://cleantalk.org/blacklists/194.61.24.102#brute-force-log>
- NIST (October, 2023) - *NIST Special Publication 800-63B: Digital Identity Guidelines*. Retrieved from <https://pages.nist.gov/800-63-3/sp800-63b.html>