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

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 (“coreupdater.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.

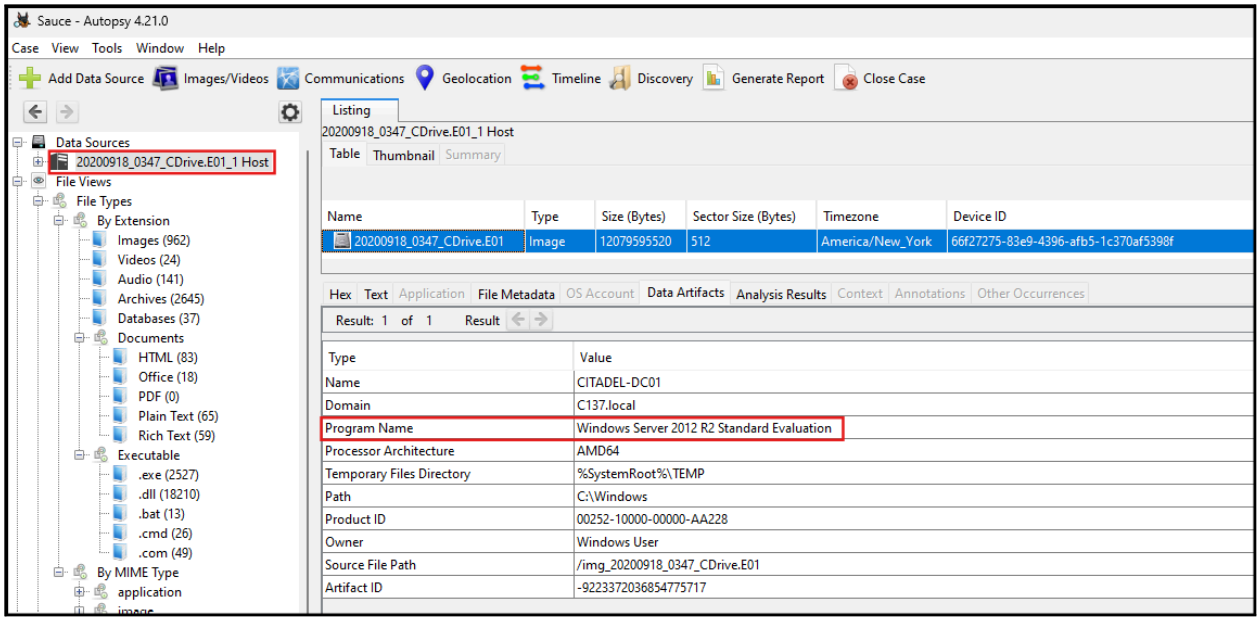

Figure 1: Windows Server 2012 R2 (determined using Autopsy on DC01 Disk Image) - Courtesy of Jenz Kim

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

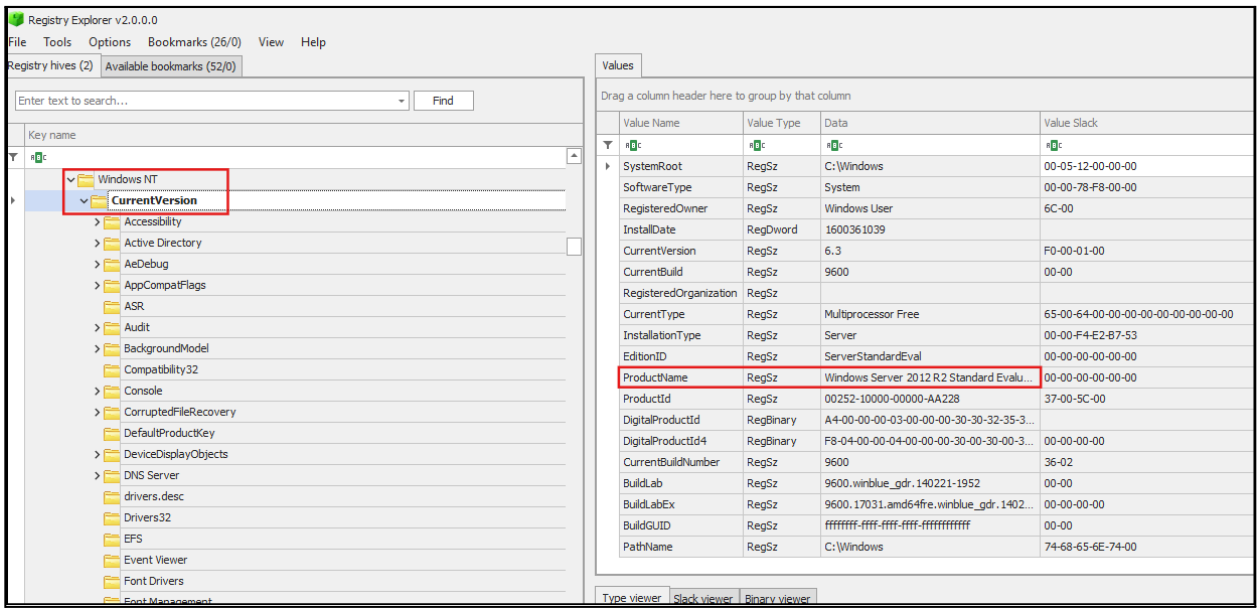

Figure 2: Windows Server 2012 R2 SE (using Registry Explorer on the disk image) - Courtesy of Jenz Kim

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/81BC5C377C525081645F9958F209C527-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf801636232a8
Major/Minor     15.19041
MachineType     34404
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      34404
PE TimeDateStamp        Sun Aug 11 05:47:24 2069
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*

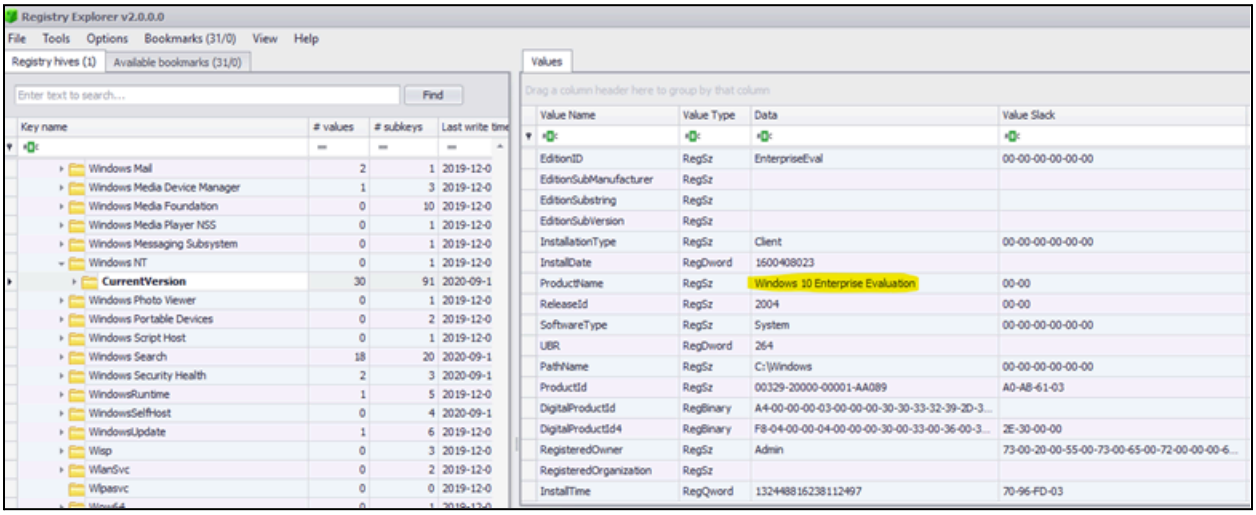

Figure 4: Windows CurrentVersion - Product Name (using Registry Explorer)

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

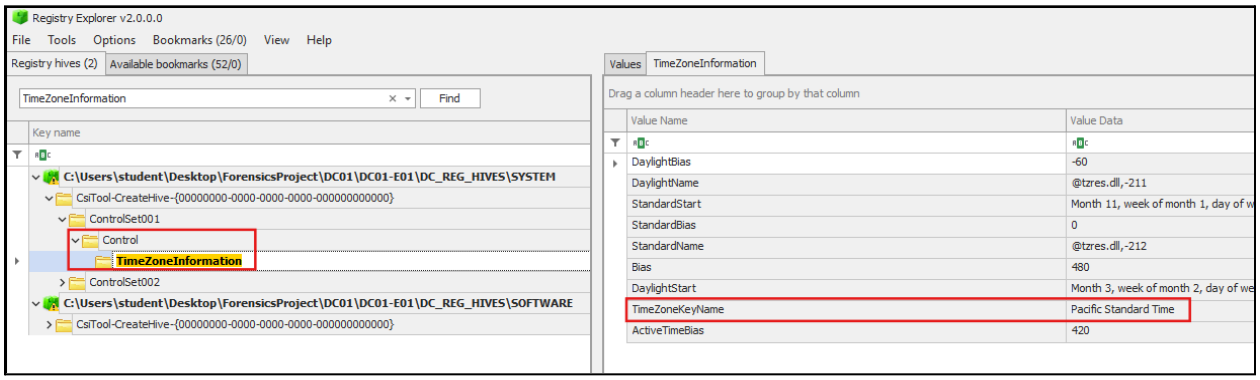

Figure 5: TimeZone Information (Registry Explorer)

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)

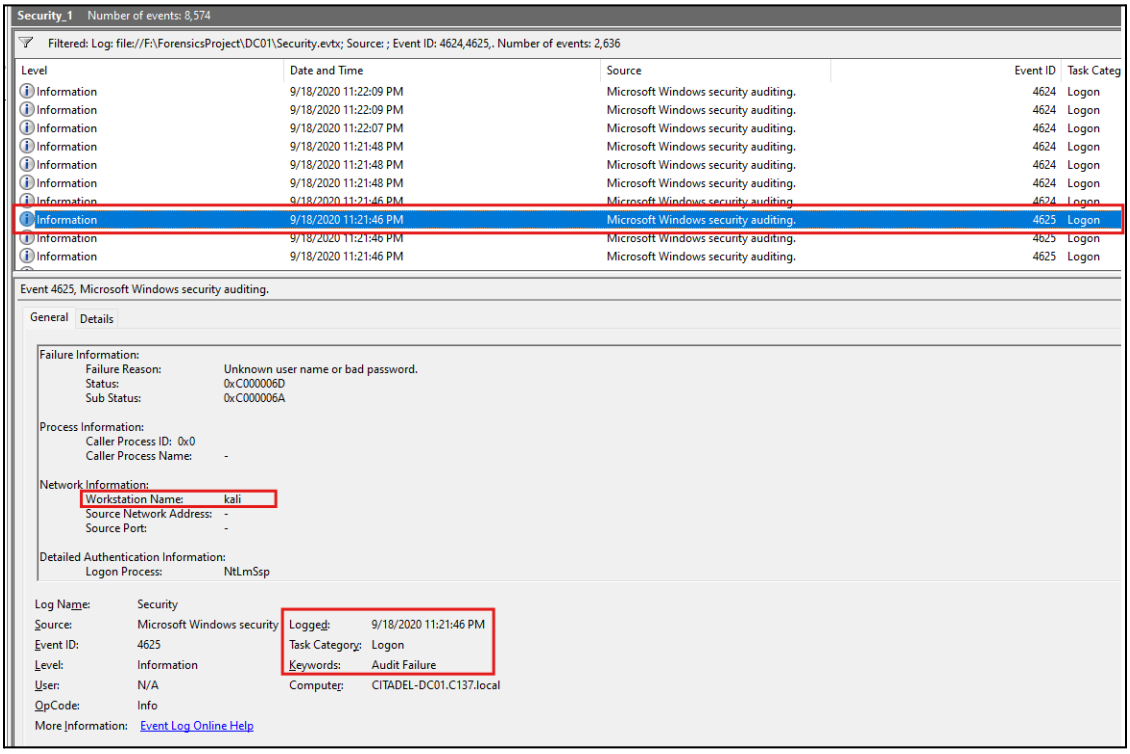

Figure 6: Windows Event Viewer - Security logs (Event ID: 4625)

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)

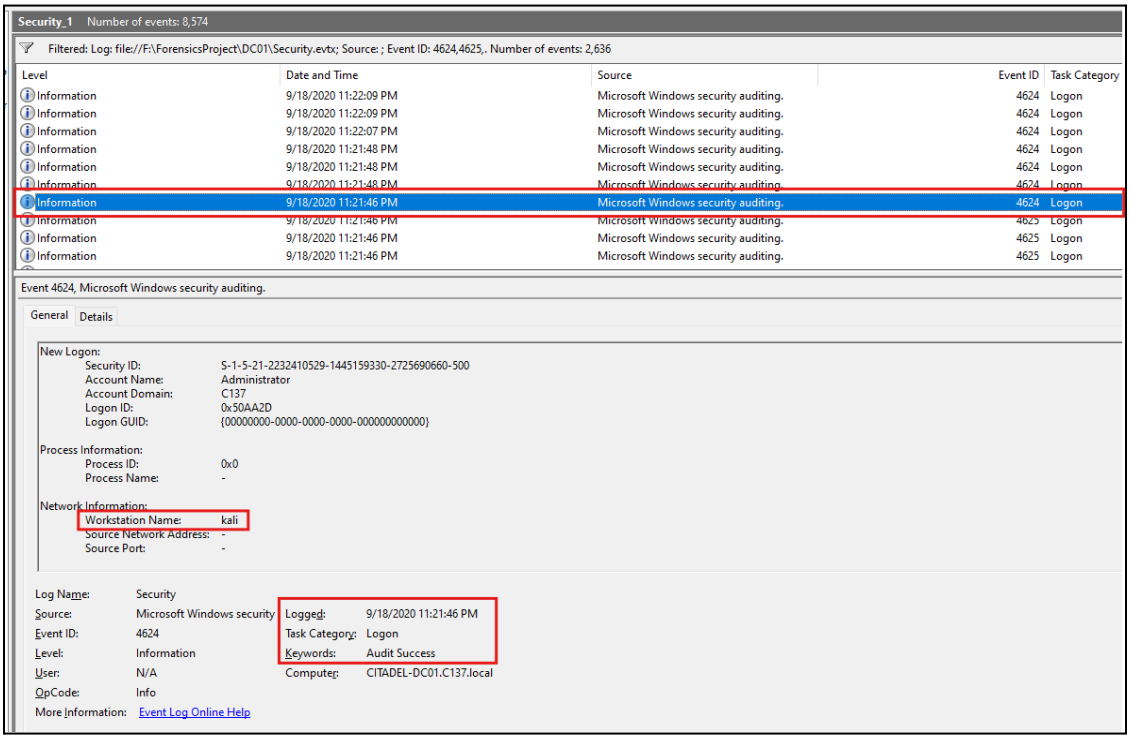

Figure 7: Windows Event Viewer - Security logs (Event ID: 4624)

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.

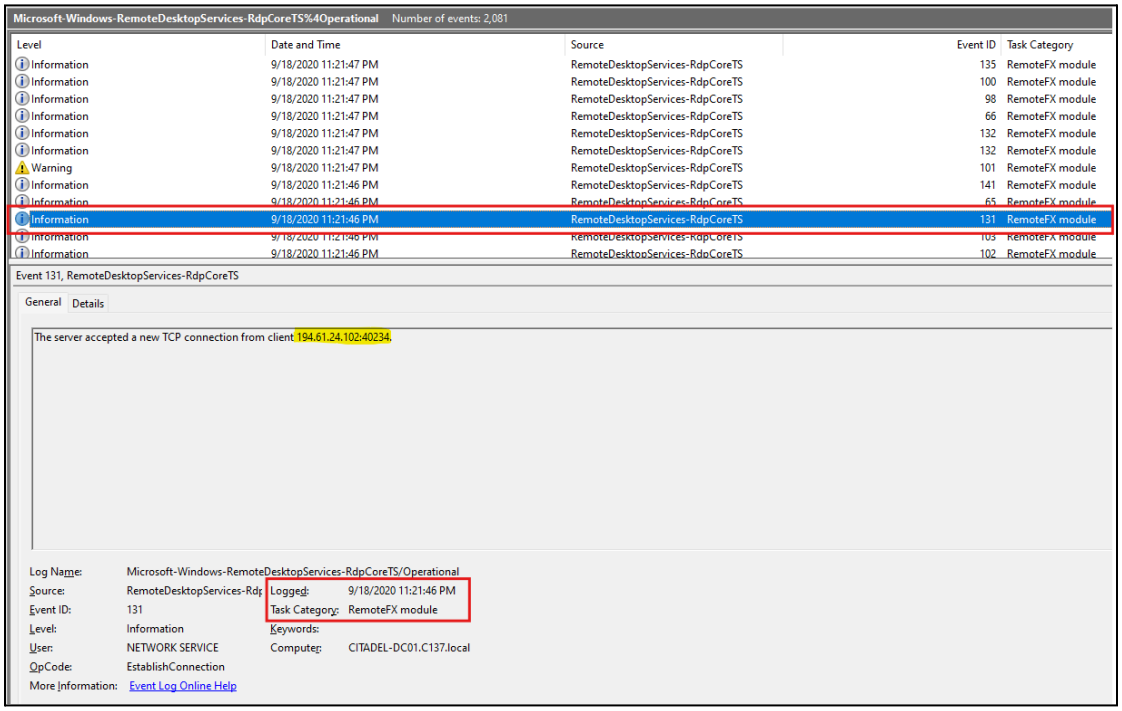

Figure 8: Windows Event Viewer - RDS Operational logs

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)

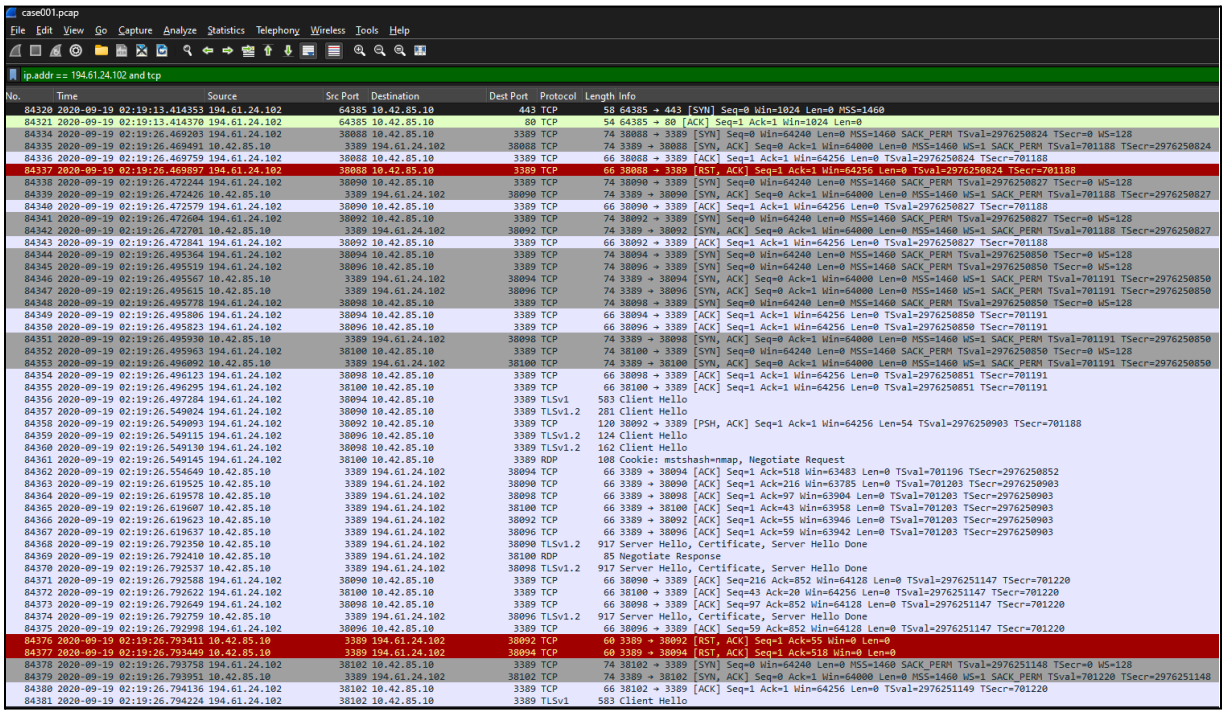

Figure 9: IP address and TCP filter applied in Case001.pcap - Courtesy of Matthew Egharevba

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)

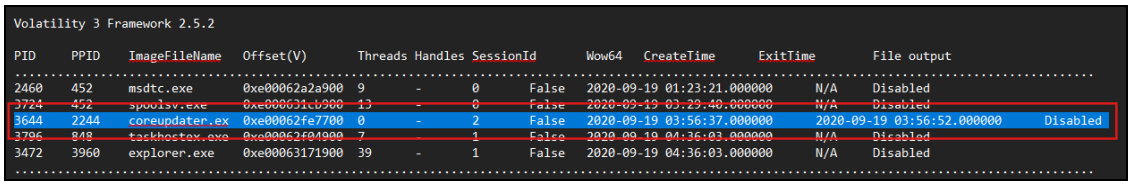

Figure 10: vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.pslist - Courtesy of Jenz Kim

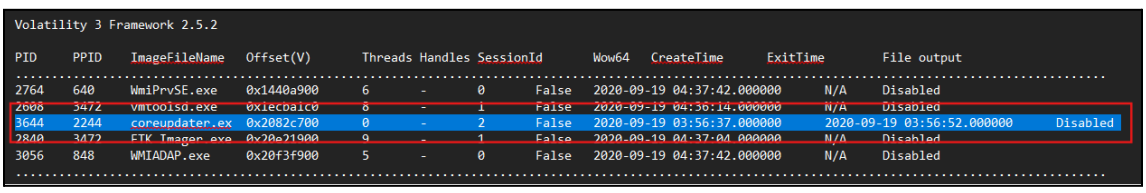

Figure 11: vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.pscan - Courtesy of Jenz Kim

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)

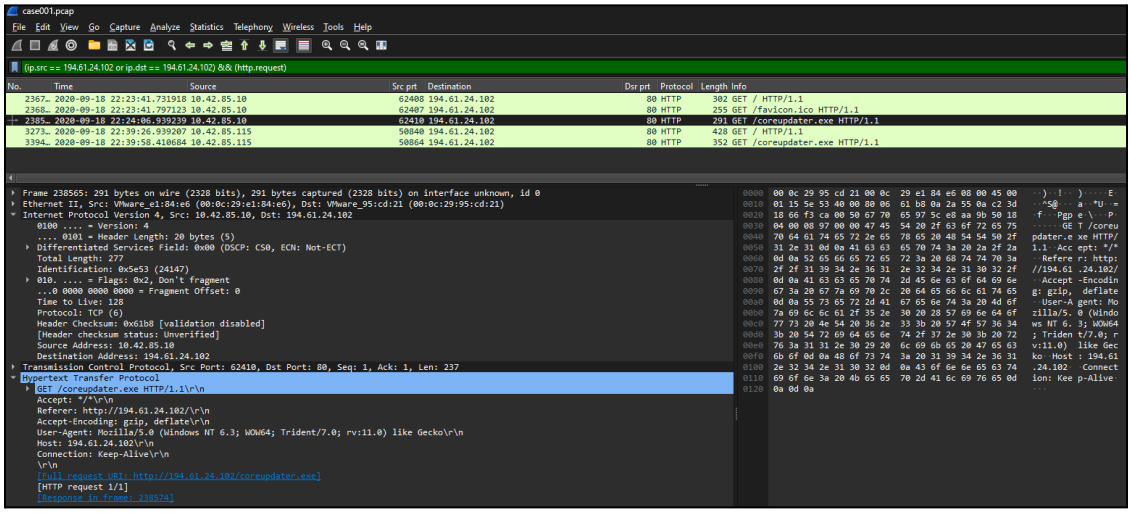

Figure 12: PCAP using display filter (The attack hosted malware on a HTTP server)

- 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
0x6006fba0	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.ex 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.**

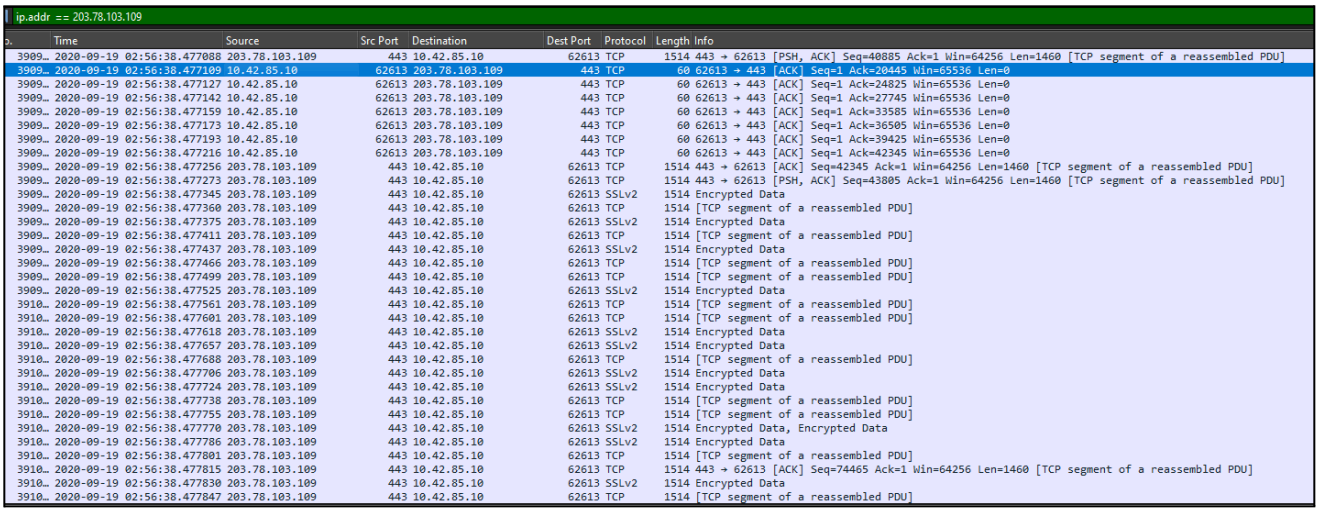

Figure 14: PCAP using display filter (The attack hosted malware on a HTTP server) - Courtesy of Matthew Egharevba

- 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.

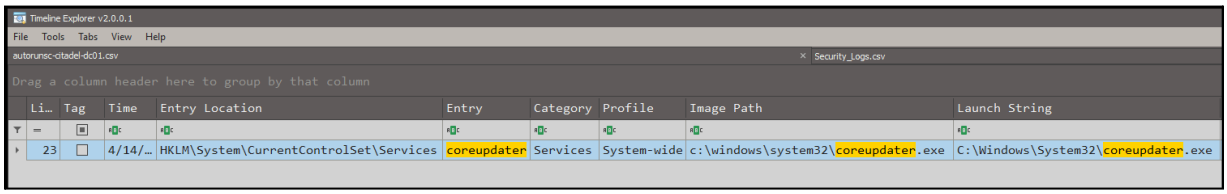

Figure 15: Malware found in DC-01 C:\Windows\System32\coreupdate.exe (Timeline Explorer)

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

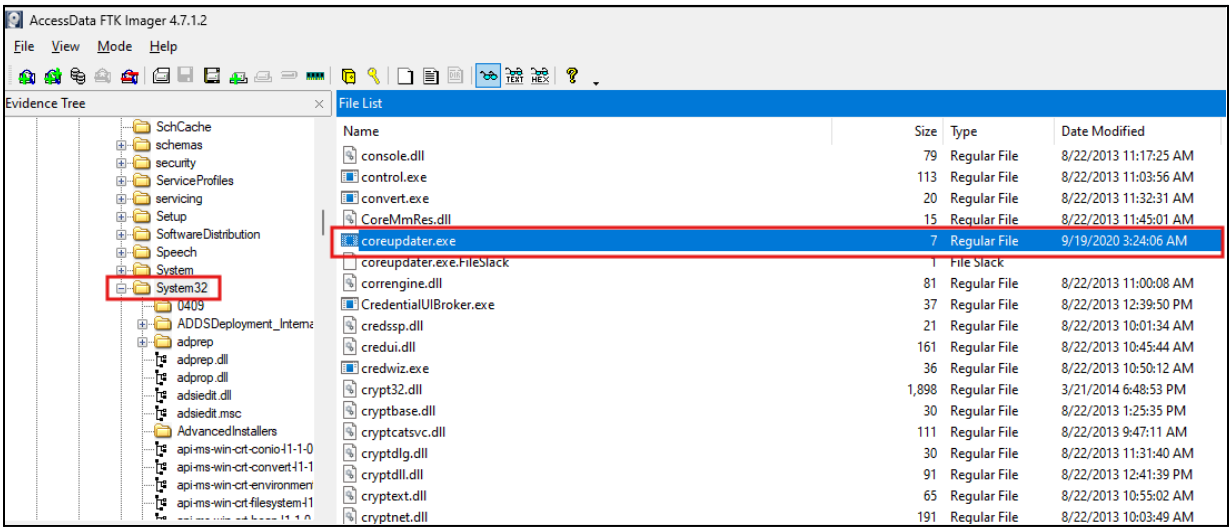

Figure 15: Malware found in DC-01 C:\Windows\System32\coreupdate.exe (FTK Imager)

- 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)

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.

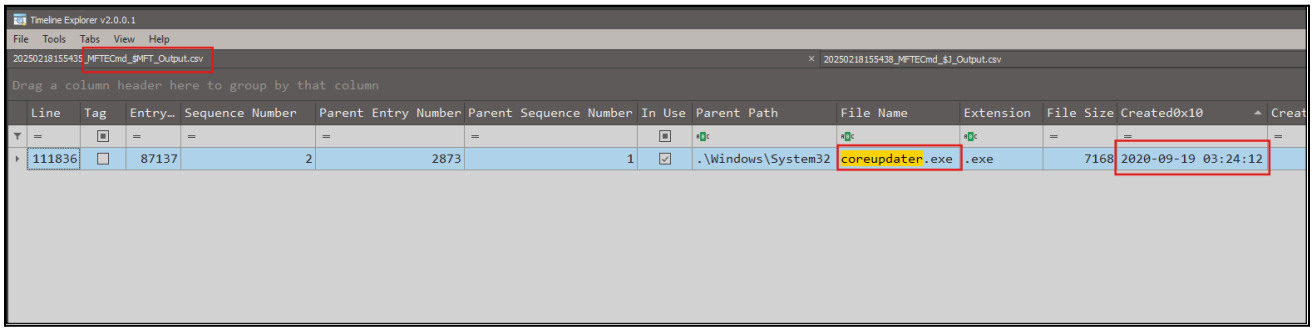

Figure 17: coreupdater.exe searched for in the MTF Output file (Timeline Explorer) - Courtesy of Jenz Kim

- 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.

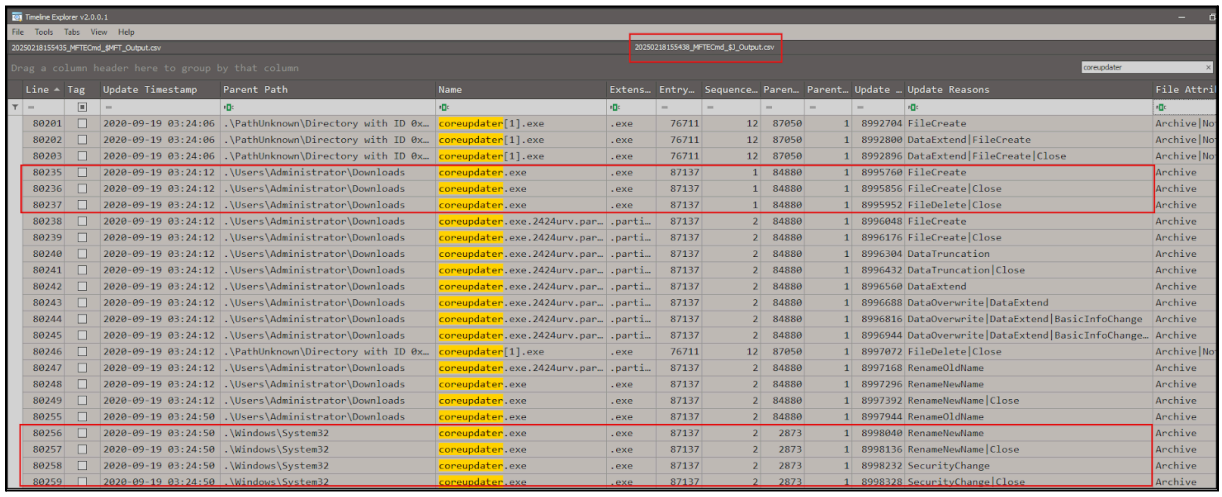

Figure 18: coreupdater.exe searched for in the MTF $J Output file (Timeline Explorer) - Courtesy of Jenz Kim

- 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

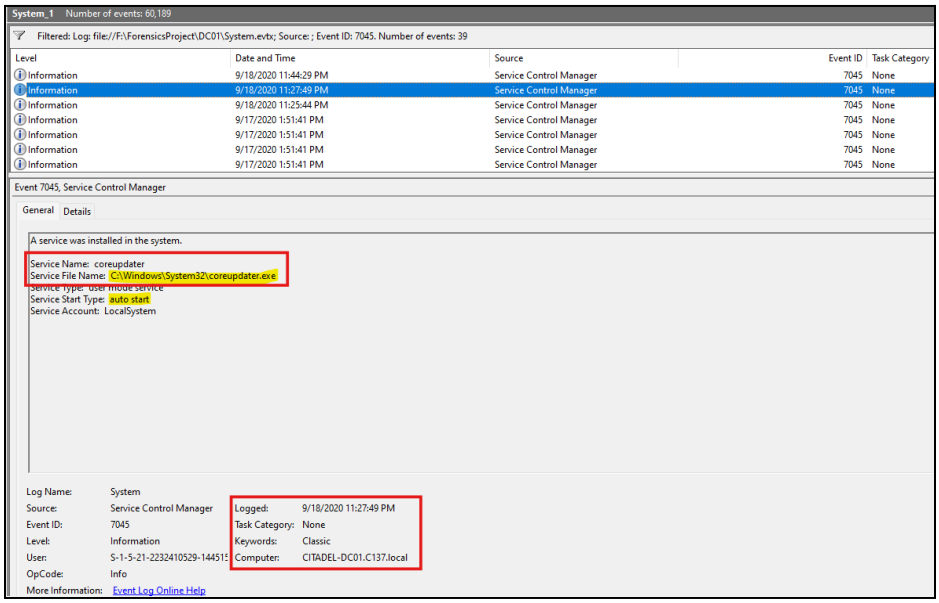

Figure 19: Windows System logs - Server (Event ID 7045)

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

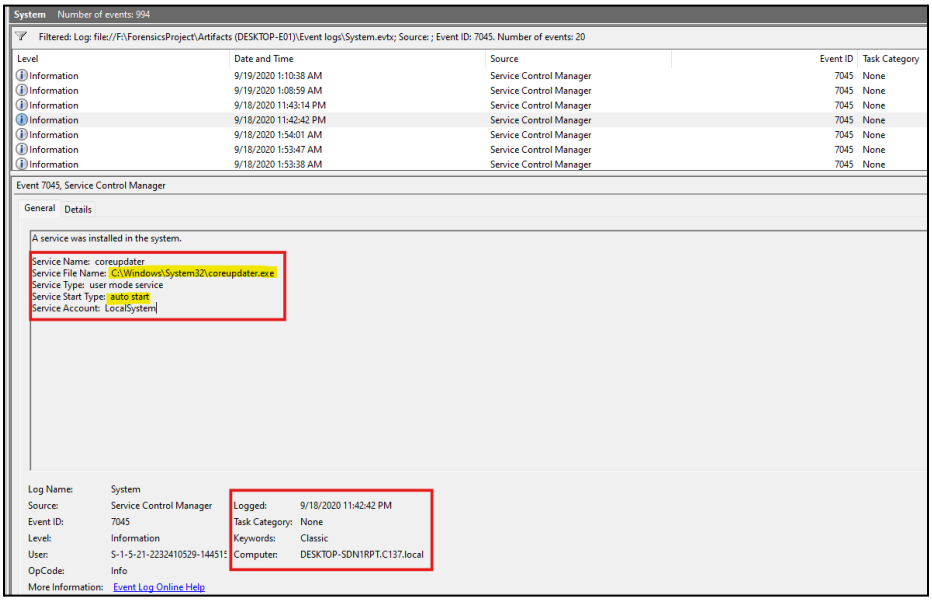

Figure 20: Windows System logs - Desktop (Event ID 7045)

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).

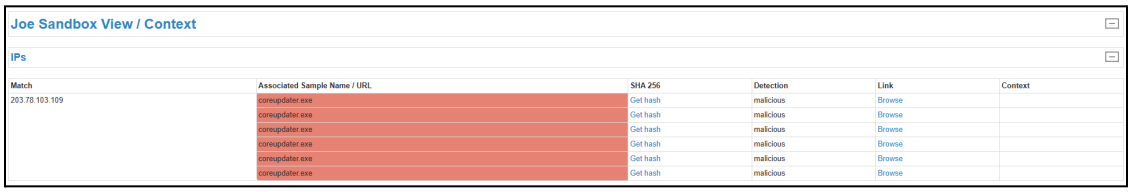

Figure 21: 203.78.103.109 listed on Joe Sandbox.

- 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.**

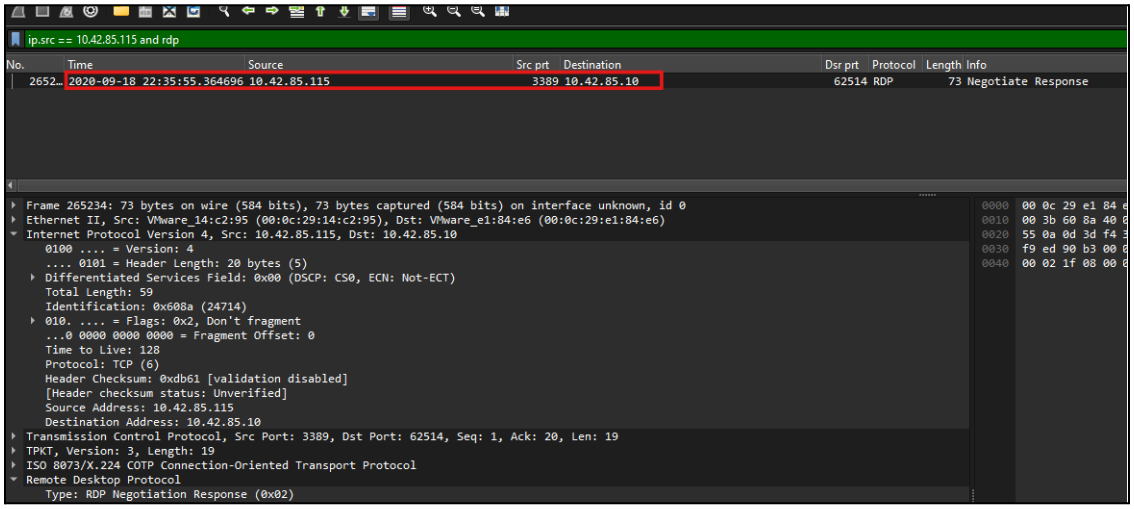

Figure 22: Display filter used to capture RDP movement from Server to Desktop

   - 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.

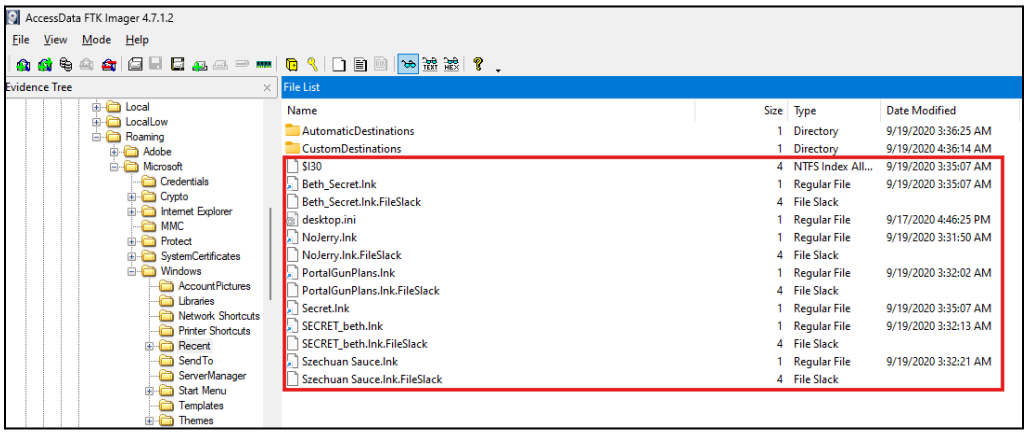

Figure 24: Recent directory - CITADEL-DC01 (FTK Imager)

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

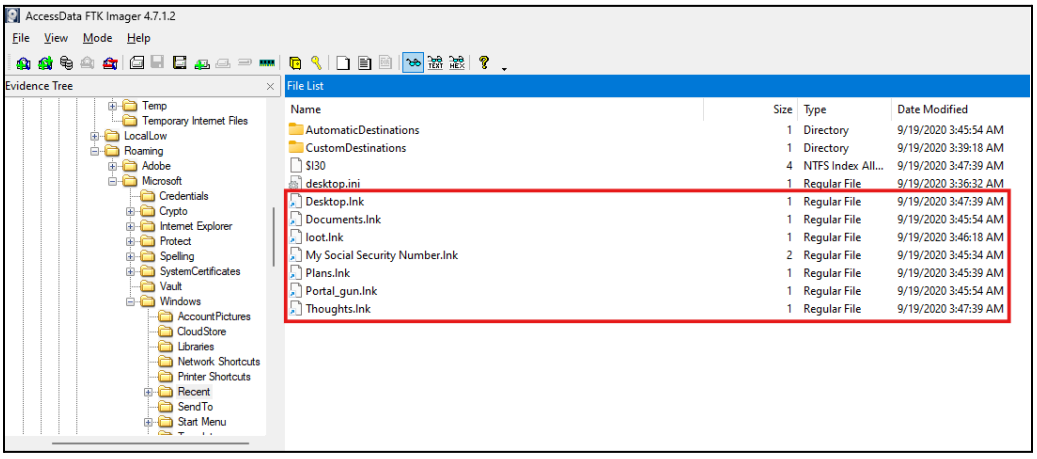

Figure 25: Recent directory - SDN1RPT (FTK Imager)

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)

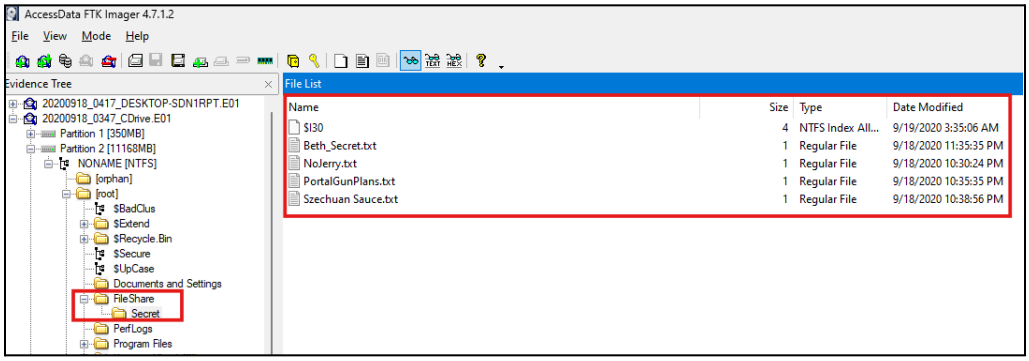

Figure 26:C:\FileShare\Secret.zip (Server)

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

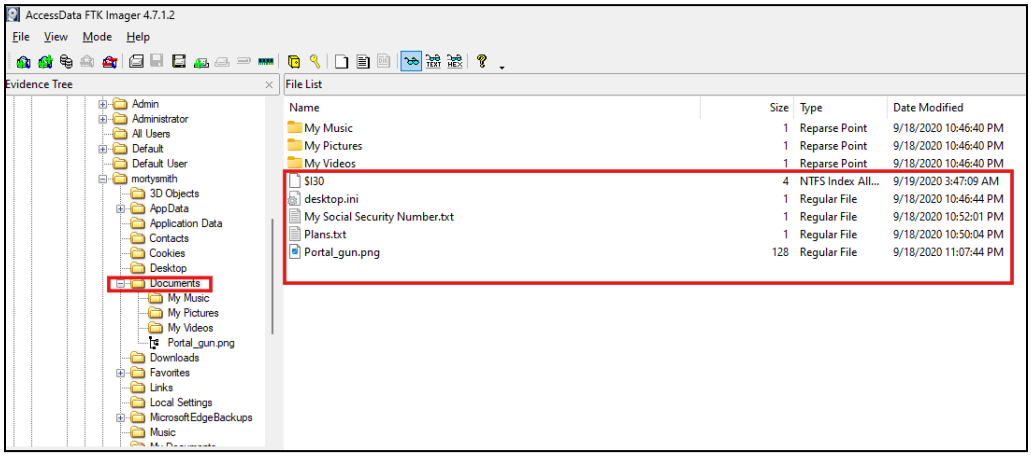

Figure 27:C:\Users\mortysmith\Documents\loot.zip (Desktop)

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)

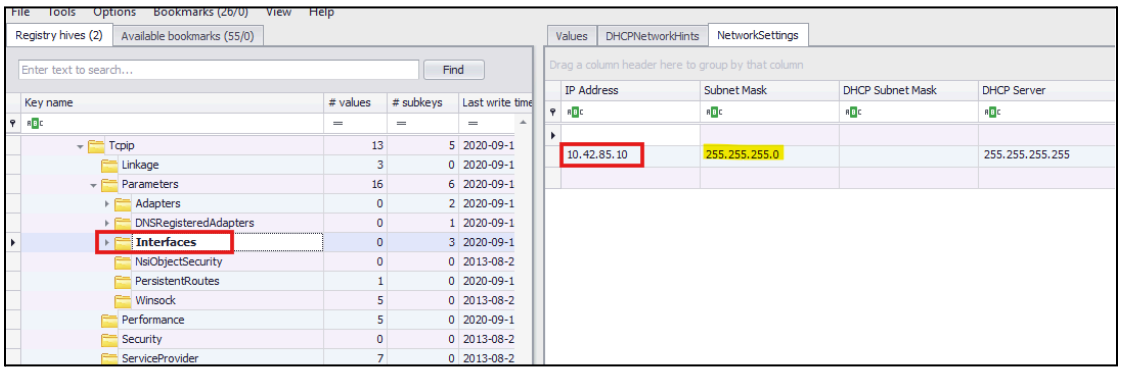

Figure 28: Network Settings using Registry Explorer (Server)

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

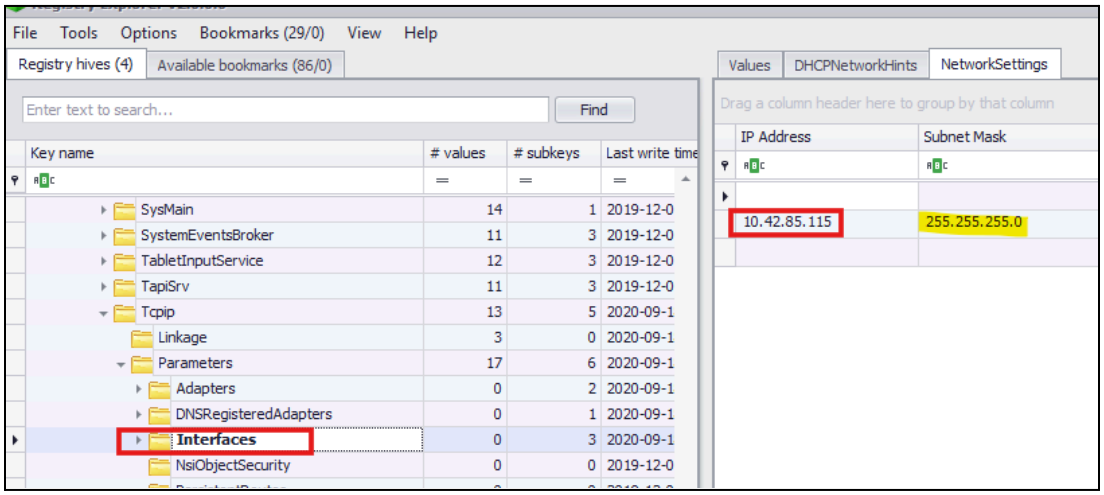

Figure 29: Network Settings using Registry Explorer (Desktop)

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.onfvp.com/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 coreupdater.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