By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This document aims to provide a detailed overview of the attack that occurred on September 19, 2020 at approximately 2:30:00 UTC, including its scope and relevant information regarding the adversaries involved. The primary objectives were to identify the attack vector, assess the extent of system compromise, and determine if sensitive data, including the "Szechuan sauce recipe," was exfiltrated from the client's IT infrastructure.

Analysis of security logs and network traffic captured by Wireshark revealed unauthorized access to both the server and a desktop system. The investigation determined that the breach originated from a brute-force attack targeting Remote Desktop Protocol (RDP) from a suspicious IP address. The analysis uncovered the presence of malware on the compromised systems. This malware facilitated persistent access across the network, enabling data exfiltration. Network traffic analysis identified encrypted data being transmitted to an external Command and Control (C2) server, strongly indicating data exfiltration. While specific file names within the encrypted traffic were not discernible, system drive analysis confirmed that the "Szechuan sauce recipe" and other sensitive files were accessed and likely exfiltrated.

The investigation confirmed a successful cyberattack that compromised the client's systems and resulted in the likely exfiltration of sensitive data, including the "Szechuan sauce recipe." The breach was initiated through a brute-force attack targeting RDP.

TOOLS USED

Below is a summary of the specific tools and versions used to analyze the data provided.

Tool	Version	Analyzed Data
Autopsy	4.21.0	20200918_0347_CDrive.E01
		20200918_0417_DESKTOP-SDN1RPT.E01
FLOSS	2.0	process.0xffffe000631cb900.0x4afbf20000.dmp (dmp file from malfind results)
FTK Imager	4.7.1.2	20200918_0347_CDrive.E01
Registry Explorer	2.0.	Server SOFTWARE.hive
		Server SYSTEM.hive
		Desktop SOFTWARE.hive
		Desktop SYSTEM.hive
RegRipper	3.0	DesktopAmcache.hive
Volatility	2.6	citadeldc01.mem
		DESKTOP-SDN1RPT.mem
Wireshark	4.4.3	Case001.pcap

*TIME NOTE – the machine used is located in an area using EST, as such the screenshots presented through any application apart from Wireshark will present the time in EST rather than UTC. EST is UTC plus one hour (i.e. if the time says "3:00AM" it is "02:00 UTC). The screen shots' captions within this report will refer to the times as UTC.

SYSTEM INFORMATION

This section will cover what information about the local network and its systems that could be gleaned from the files provided. Following the overview of what information was discovered about the local network, a summary table and diagram has been provided.

OPERATING SYSTEM OF THE SERVER

It has been found that the operating system of the server is **Windows 12** as discovered by inputting the domain controller disk image files into Autopsy as seen in Figure 1.1.
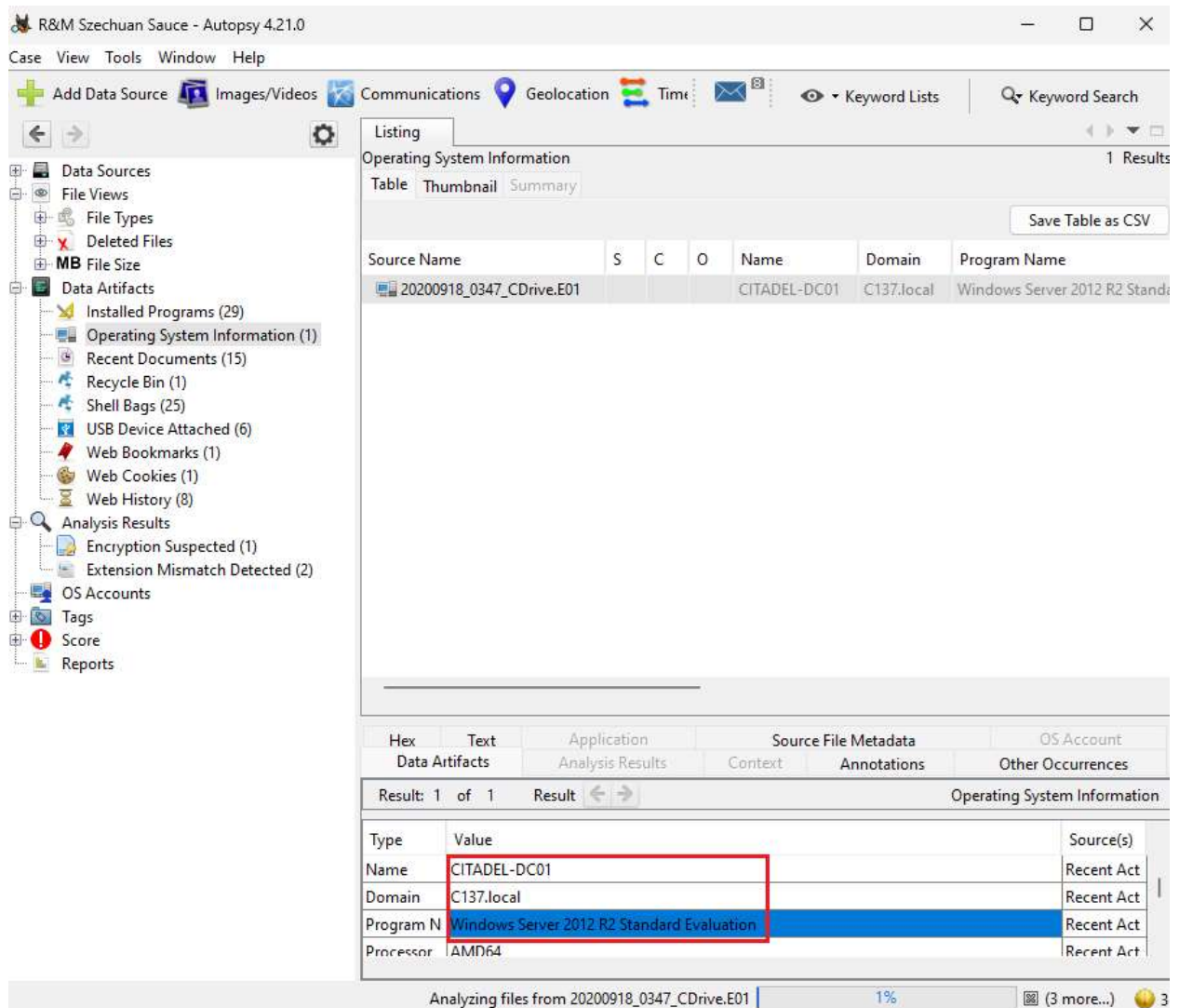
Figure 1.1 The operating system of the server found in the Autopsy tool.

OPERATING SYSTEM OF DESKTOP

Using Registry Explorer with the imported *SOFTWARE* hive originally from the Desktop image file (e01), the operating system was determined to be **Windows 10** as seen in Figure 1.2.

Value Name	Value Type	Data	V...	I...	Data Record R...
EditionSubstring	RegSz			☐	☐
EditionSubVersion	RegSz			☐	☐
InstallationType	RegSz	Client	0...	☐	☐
InstallDate	RegDword	1600408023		☐	☐
ProductName	RegSz	Windows 10 Enterprise Evaluation	0...	☐	☐
ReleaseId	RegSz	2004	0...	☐	☐
SoftwareType	RegSz	System	0...	☐	☐
UBR	RegDword	264		☐	☐
PathName	RegSz	C:\Windows	0...	☐	☐
ProductId	RegSz	00329-20000-00001-AA089	A...	☐	☐
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-33...		☐	☐
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-30-33...	2...	☐	☐
RegisteredOwner	RegSz	Admin	7...	☐	☐
RegisteredOrganization	RegSz			☐	☐
InstallTime	RegQword	132448816238112497	7...	☐	☐

Figure 1.2 – Desktop operating system found in *SOFTWARE* hive opened in Registry Explorer.

LOCAL TIME OF SERVER

It was found that the local time zone of the server was **Pacific Standard Time (PST)** using Registry Explorer viewing the SYSTEM hive that was found in the domain controllers image disk (e01 files). The path to the hive file was within *Partition2\root\Windows\System32\config* which was then exported to the virtual machine to then import the hive into Registry Explorer. The time zone was found in the bookmarks under *TimeZoneInformation* which can be seen in Figure 1.3.
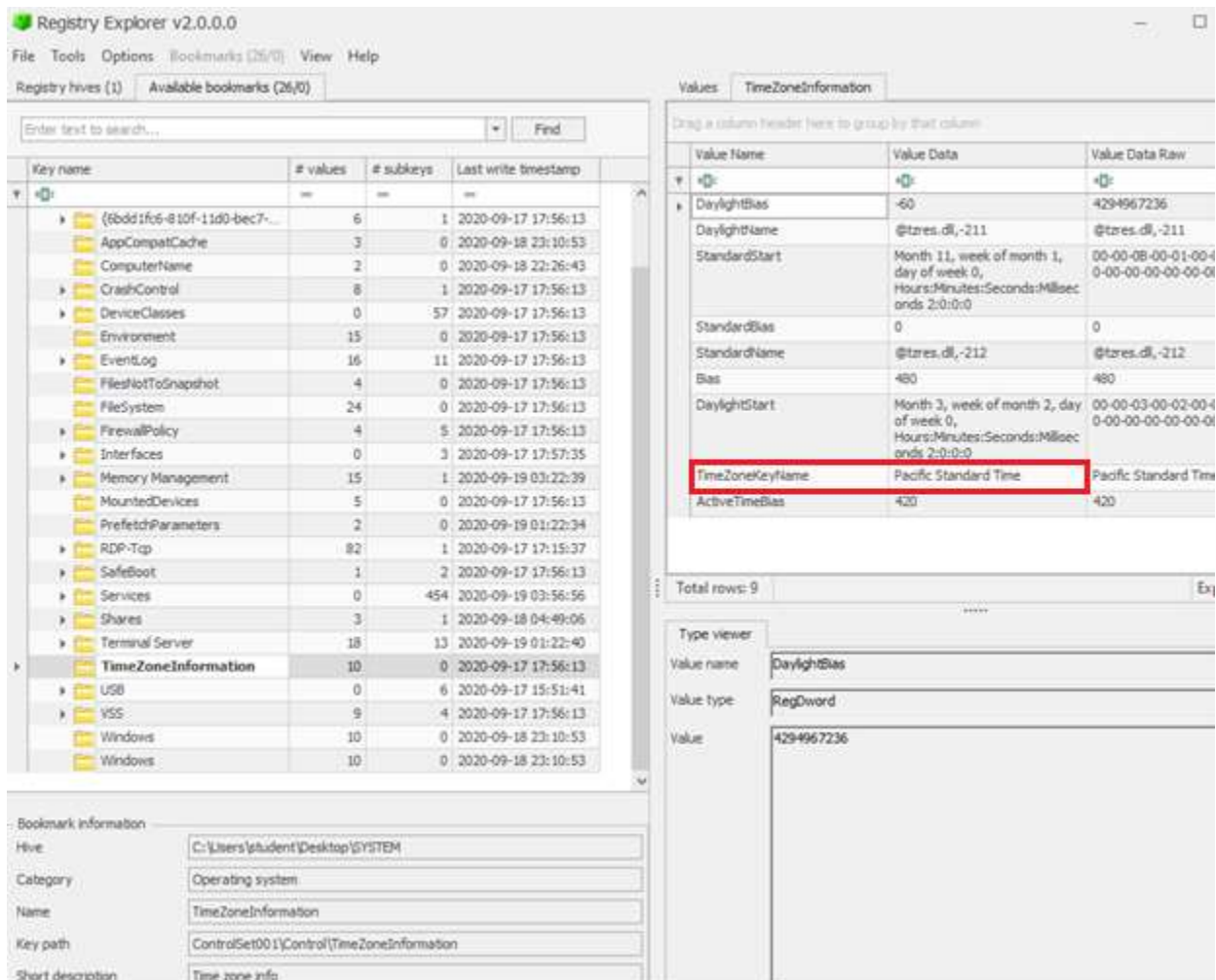
Figure 1.3 – the local time zone of the machine found in Registry Explorer

NETWORK LAYOUT

Using what was gathered from Figures 1.1-1.7, the network layout and associated IP addresses have been summarized in the table following the figures. Additionally, a simple diagram of the local network has also been drafted and included after the table. The path used to find the IP address information was

$Windows\backslash System32\backslash config\backslash System\backslash Controlset\backslash Services\backslash Tcpip\backslash parameters\backslash interfaces$ within the Autopsy tool. The path used to find the computer name for the Server was

ContolSet002\Control\ComputerName\ComputerName. For the Desktop's computer name, the path

used was *ContolSet001\Control\ComputerName\ComputerName*.
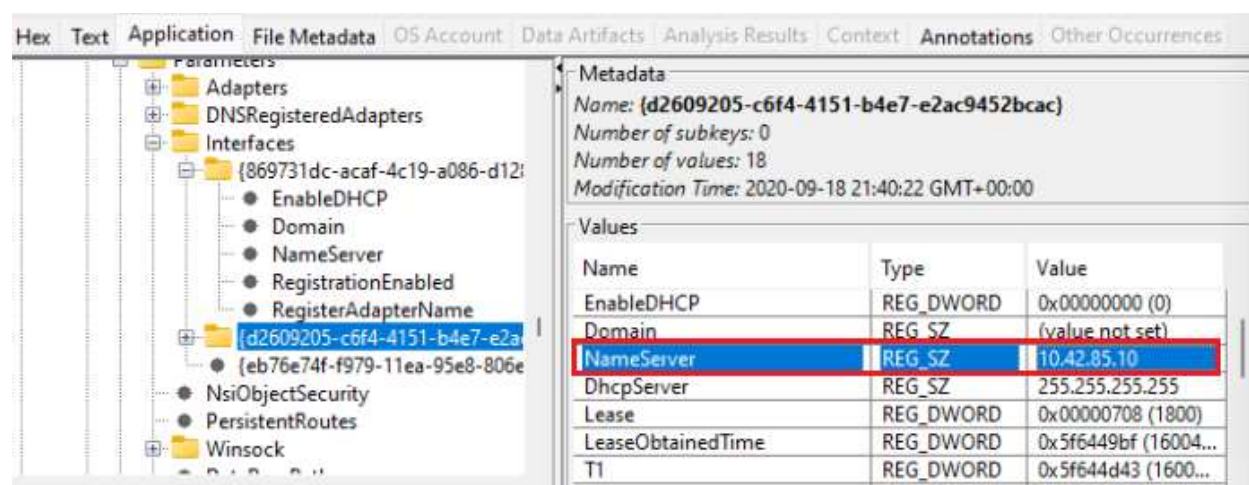
Figure 1.4 – Server IP address found in Autopsy.
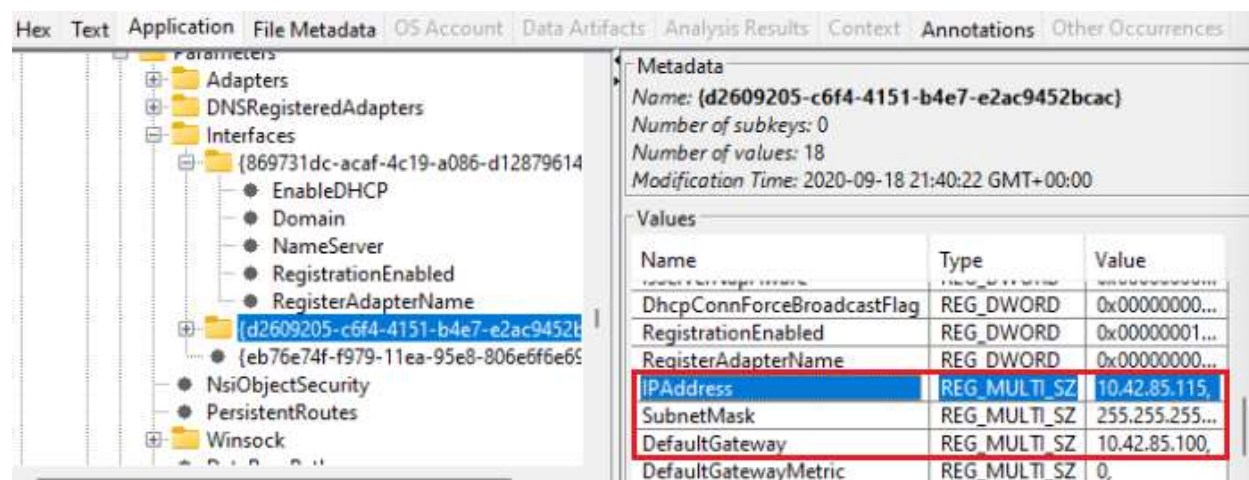
Figure 1.5 – Desktop IP address, default gateway IP address, Subnet Mask found in Autopsy.
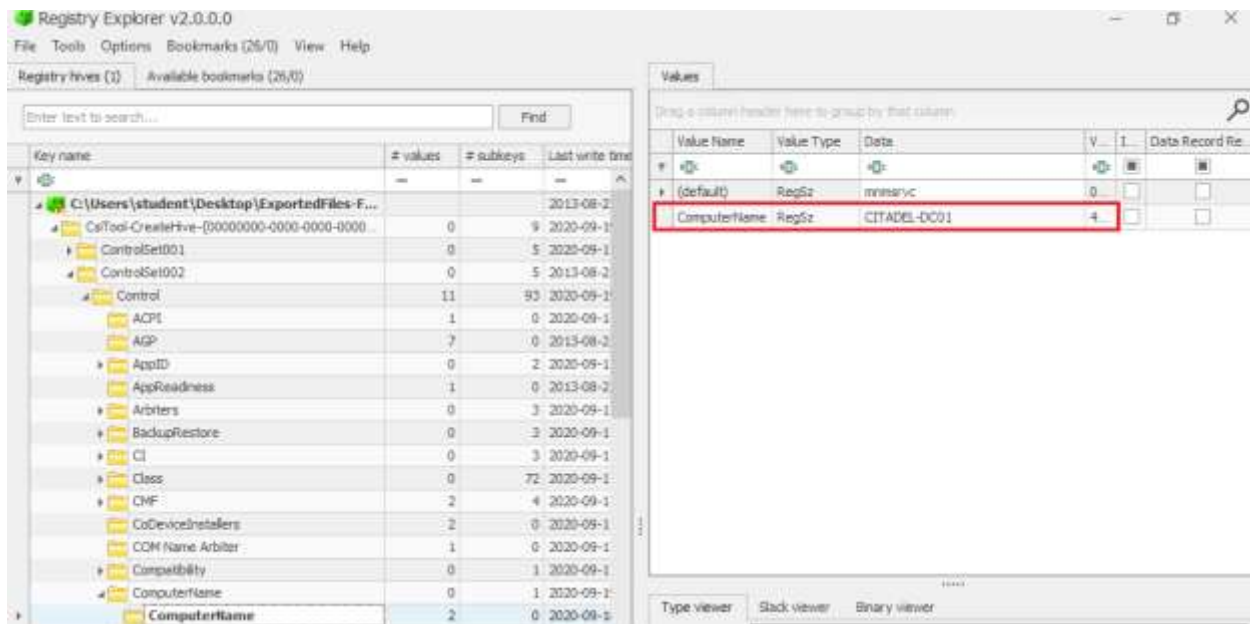
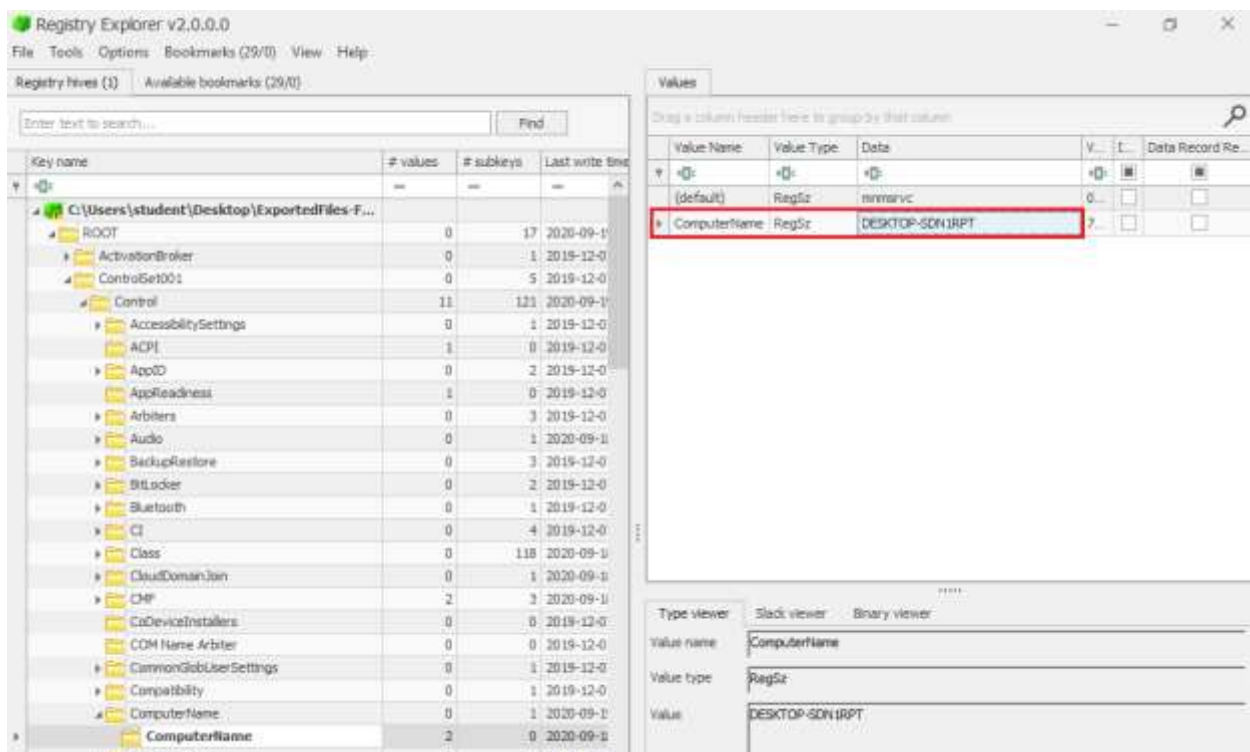**Figure 1.6** – Server name found in Registry Explorer from *SYSTEM* hive file.

Figure 1.7 – Desktop name in network found in Registry Explorer from *SYSTEM* hive file.

Below is a summary of what could be determined regarding the local network layout from the information gathered.

	IPv4 Address	Computer Name
Server	10.42.85.10	CITADEL – DC01
Desktop	10.42.85.115	DESKTOP – SDN1RT
Default Gateway	10.42.85.100	-
Subnet Mask	255.255.255.0	-
IP Address Range of Network	10.42.85.0/24	-
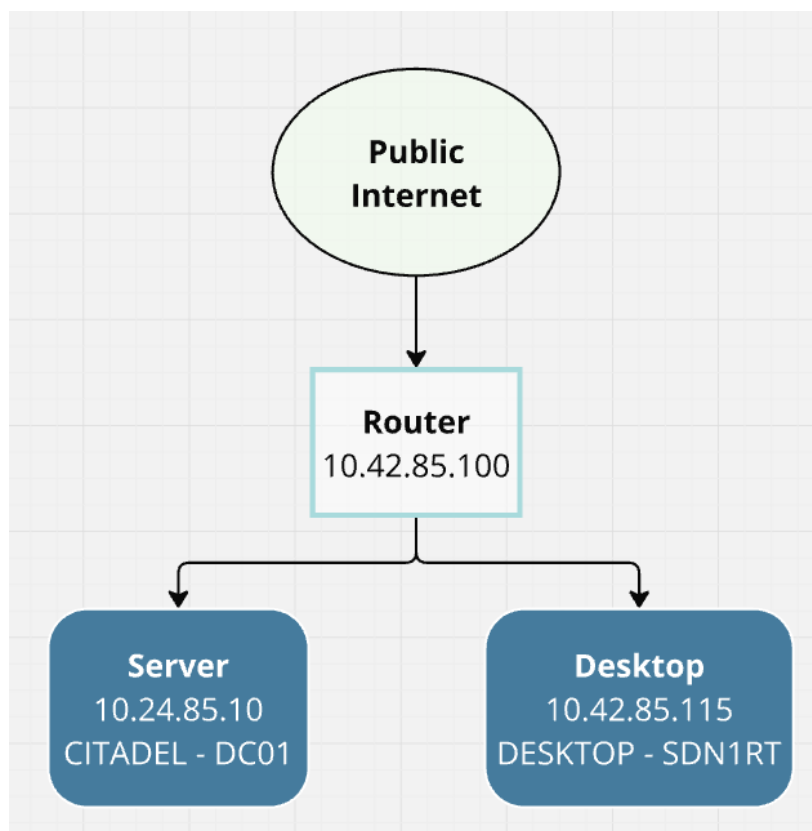
Figure 1.7 – An assumption of the local network layout.

INCIDENT OVERVIEW

This section aims to cover all the forensic evidence discovered during analysis of the files provided as well as the inferred facts of the incidents that were gathered from the main pieces of data during analysis. Following the comprehensive overview of the incident, a succinct summary of the incident has been provided to answer the main questions of concern regarding this incident.

DISK IMAGE, MEMORY AND AUTORUN FILE ANALYSIS

This subsection will cover the key pieces of information gleaned from the disk image files, memory files, and autorun files of the Server and Desktop. The methodology as well as the thought processes when going through these pieces of evidence will also permeate through this section in order to justify the answers to the Summary section's questions.

IP ADDRESS 194.61.24.102

One of the first pieces of data examined was the web history data viewable in the Autopsy tool. As the main point of concern was the stolen Szechuan recipe that was within the Local Server's disk, it seemed prudent to take a look at the web history in addition to registries and disk images in order to rule out certain vectors of attack and narrow down the artifact data worth further investigation. As seen in Figures 2.1 and 2.2, a suspicious http address was listed within the Cache. Since it was with the more insecure http rather than the standard https for websites, the IP address was looked into on VirusTotal as seen in Figure 2.3 which revealed that it is an IP address originating from Russia and seemingly malicious. This IP address was noted during further stages of analysis into other artifacts - to either keep an eye on the further actions of the IP or to definitively disprove its supposed malicious intent.

Figure 2.1 – Suspicious http URL found in Web History heading of the Local Server disk image information using Autopsy.

Figure 2.2 – The same suspicious IP address found in the web cache of the Desktop as viewed through Autopsy.
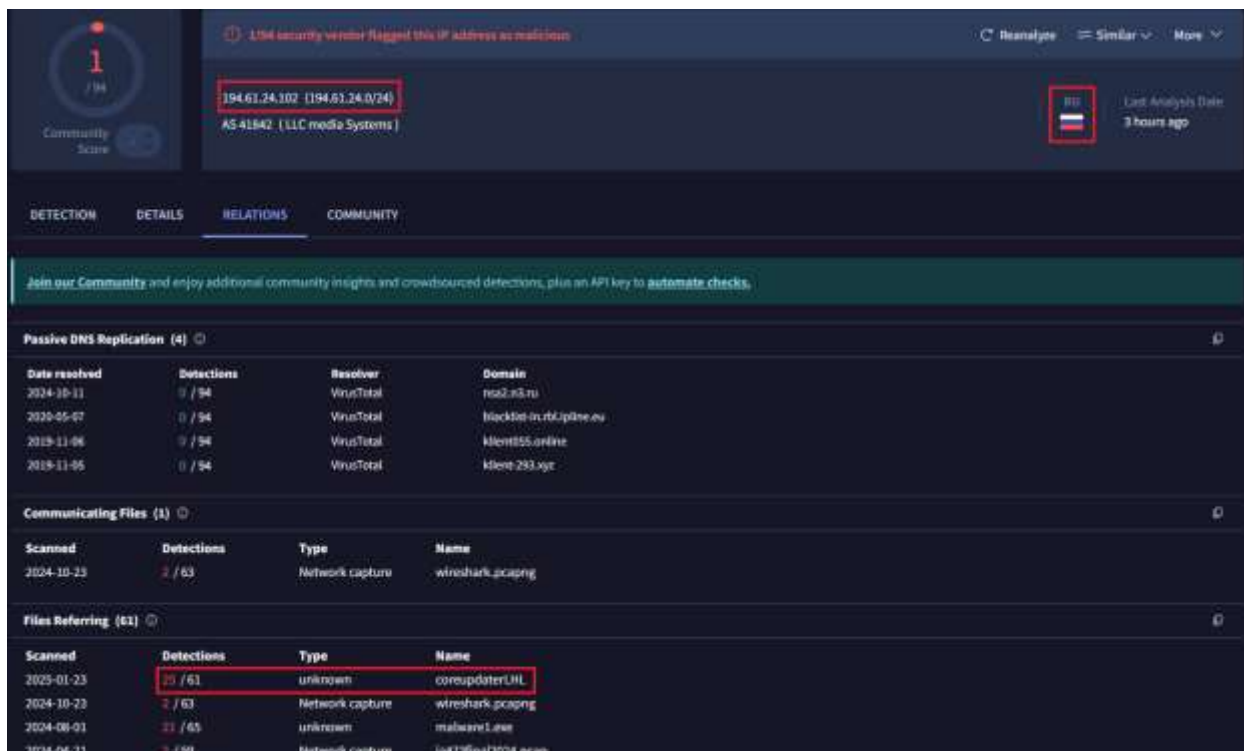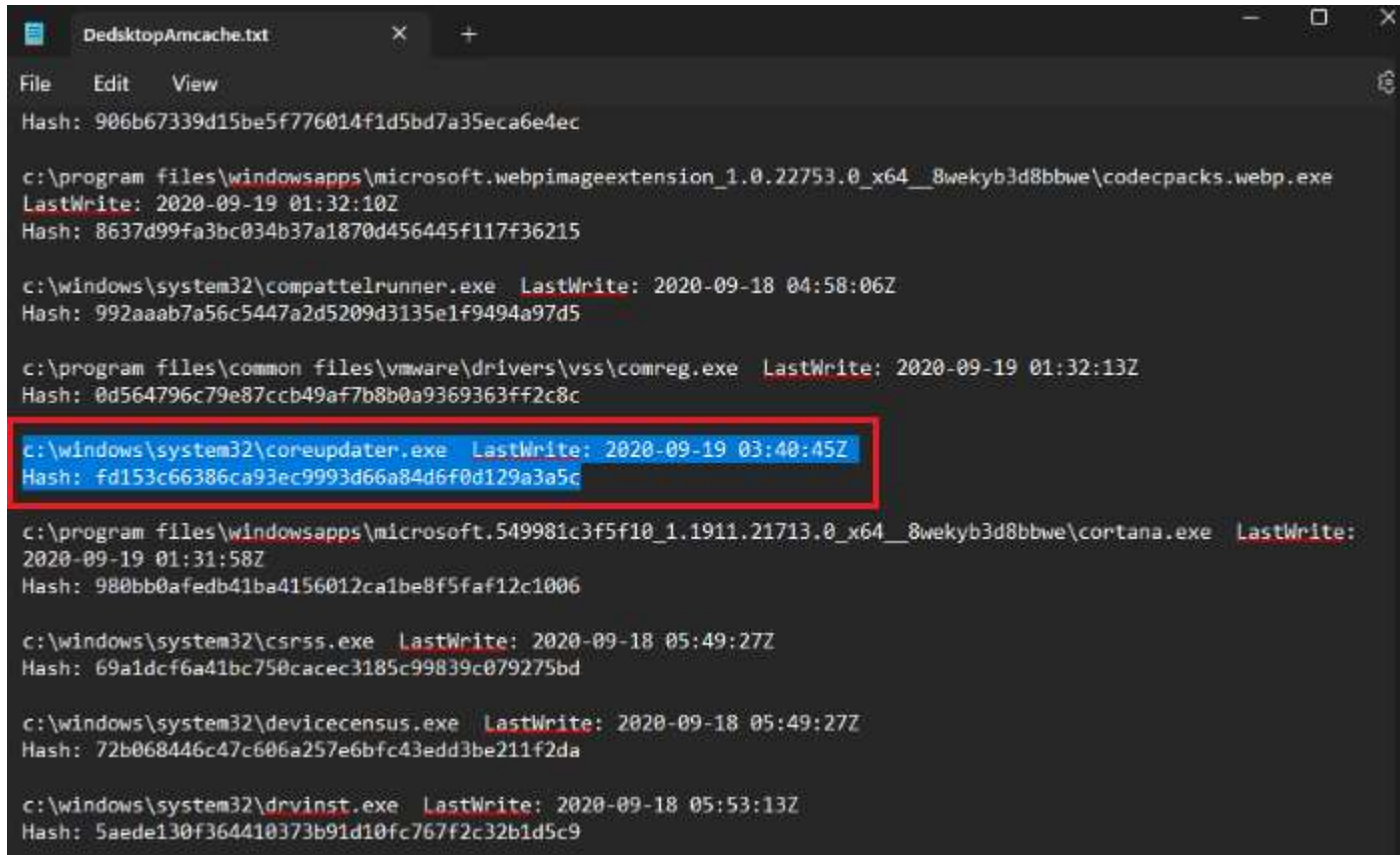
Figure 2.3 – Virus total results for the IP address 194.61.24.102 which originates from Russia.

COREUPDATER.EXE

Application Activity Cache (AmCache) is a forensic artifact in Windows operating systems that tracks metadata about executables and other files that have been run on, or interacted with, the system (Magnet Forensics, 2024). Given what useful information AmCache holds; this file was exported from the Local Server's image disk file for further analysis of any potential malicious executables present in the system. AmCache is found in

Windows\AppCompat\Programs\Amcache.hve. The RegRipper GUI was used to parse through the hive which then compiled the results into a .txt file to easily manually parse through and search for any specific terms and copy text. When parsing through the results, apart from the vmware related files and other legitimate applications, one .exe file did not seem to be a legitimate application present after researching the application name *coreupdater.exe*. The results of the RegRipper output is shown in Figure 2.4. As seen in Figure 2.5, **after looking into the hash of**

coreupdater.exe observed in the AmCache analysis, **VirusTotal revealed that it is malware**.

After further parsing of the disk image file of the Server through FTK Imager, it was found that the

malware was found in the path: *C:\Windows\System32\coreupdate.exe* as seen in Figure 2.6

and 2.7. Given that it is malware, it is unlikely that its original folder as System32 only contains

critical Windows system files for proper functioning of the operating system (Brithny, 2025).

Figure 2.4 – Desktop AmCache analysis through RegRipper revealed this suspicious executable file
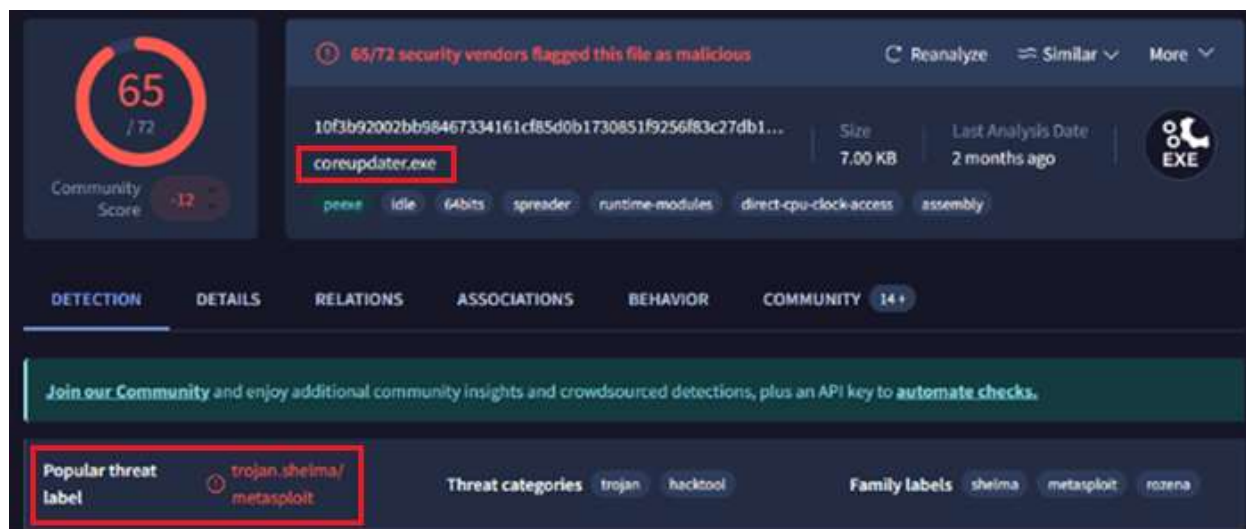that is not a legitimate application within Windows system.

Figure 2.5 – VirusTotal results of the *coreupdater.exe* hash reveal it is Metasploit/Trojan malware.
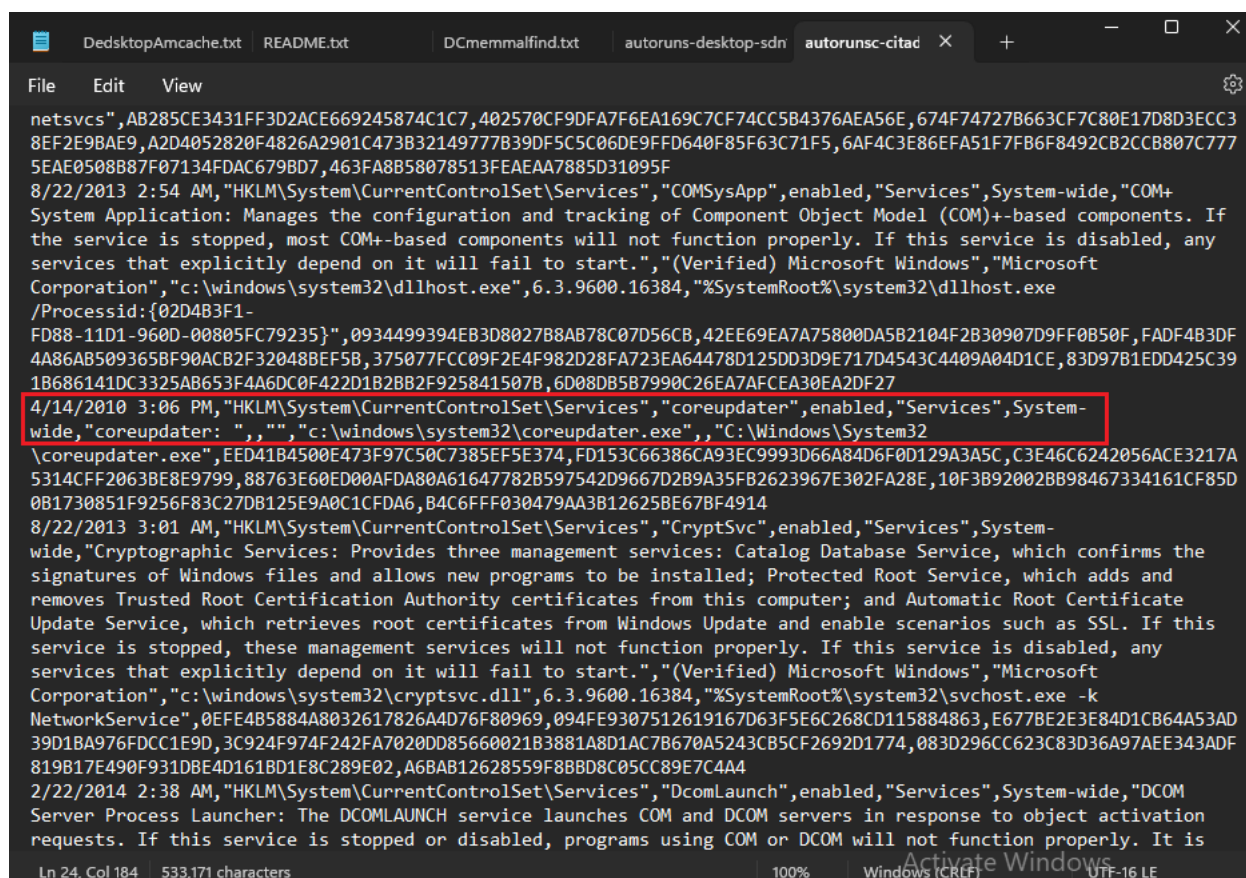

Figure 2.6 – From both the Server and Desktop autorun files, the location of the *coreupdater.exe* is shown to be in the following path: *C:\Windows\System32\coreupdater.exe.*
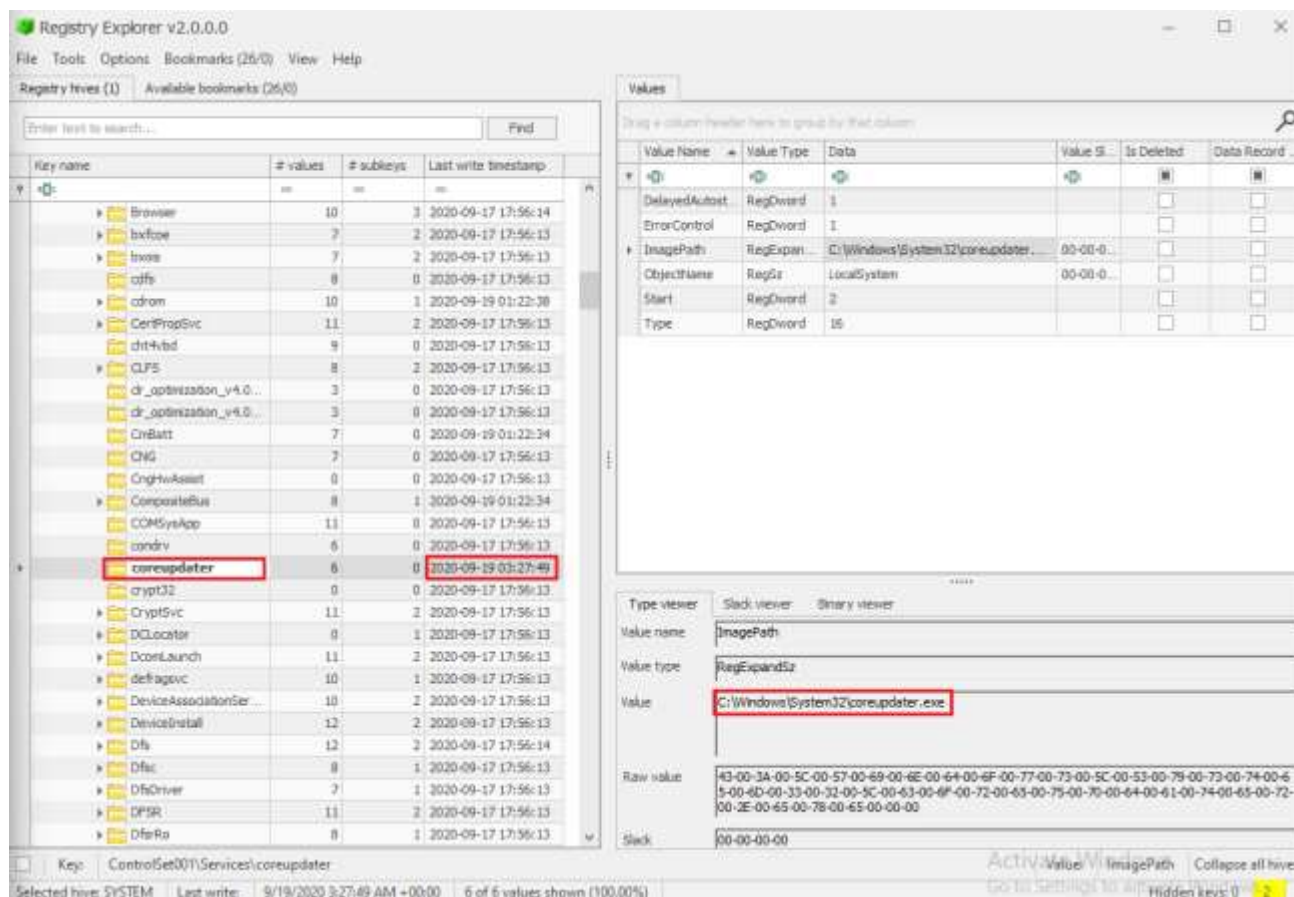
Figure 2.7 – DC *SYSTEM* hive file opened in Registry Explorer. The location of *coreupdater.exe* present in the Local Server machine. It appears to have been written into the registry at 2020-09-19 02:27:49 UTC.

<div align="center">IP ADDRESS 203.78.103.109</div>

After discovering the presence of the malware, the memory files of the Server were analyzed with the Volatility tool in order to see if and how it was interacting with the system. As seen in Figure 2.8 and 2.9, the memory dumps using Volatility reveal that from the local server the ***coreupdater.exe* executable was used to communicate to IP address 203.78.103.109**. It was confirmed as a **malicious IP address** as evident in Figure 2.1.1.

Figure 2.8 – The Volatility memory dump results show that the *coreupdater.exe* stands out among other executables as it had an exit time. Command used: *volatility_2.6_win64_standalone.exe --profile=Win2012R2x64 pslist -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem*

Figure 2.9 – Netscan results (used see network connections and open ports from the memory dump) of the memory using Volatility revealing the suspicious *coreupdater.exe* application being executed between the Server and another IP address 203.78.103.109. Command used: *volatility_2.6_win64_standalone.exe --profile=Win2012R2x64 netscan -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem > netscan.txt*
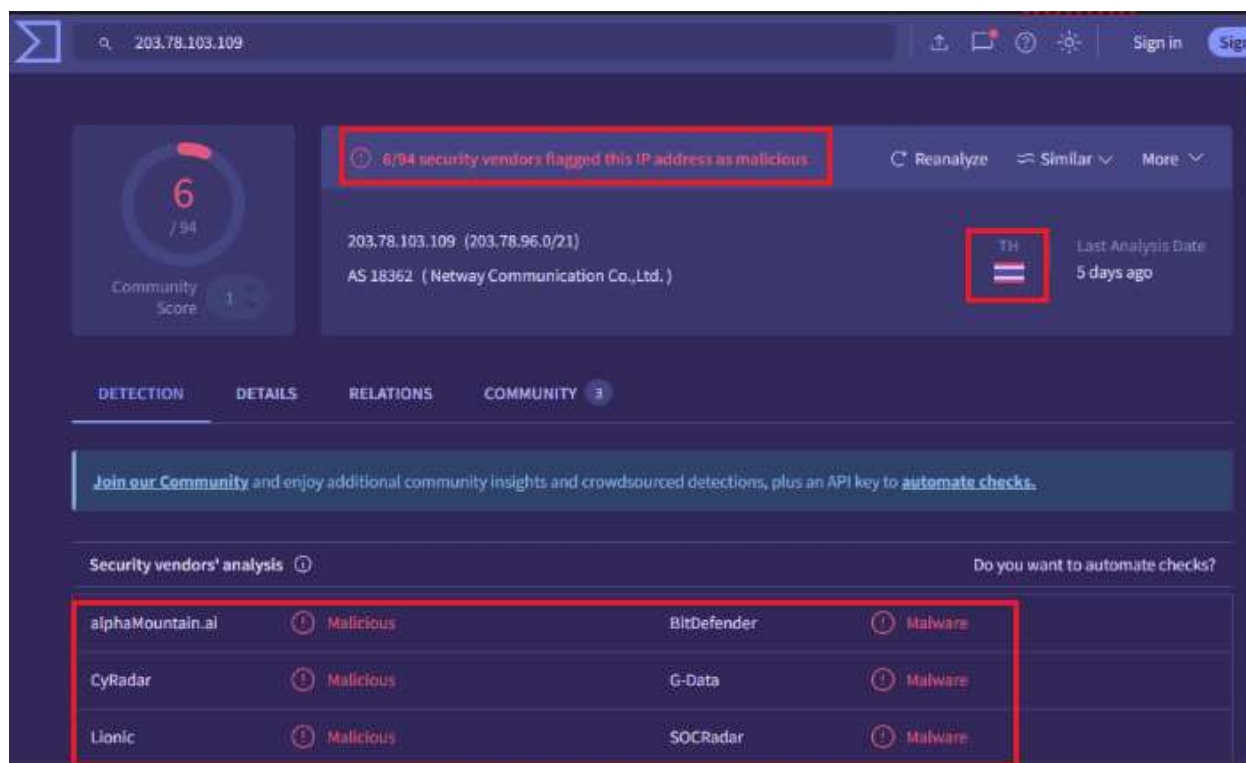
Figure 2.1.1 – VirusTotal results of the associated IP address 203.78.103.109 which originates from Thailand.

SPOOLSV.EXE

Following the discovery of the malware and the IP address 203.78.103.109, the malfind command was used in Volatility to detect and identify any potential malicious code in the memory dump. The results of which are found in Figure 2.1.2 which leads to the discovery of the Meterpreter as seen in Figure 2.1.3. **Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore a target machine and execute code** (Meterpreter, 2023). It is deployed using in-memory DLL injection and as a result, Meterpreter resides entirely in memory and writes nothing to disk – no new processes are created as Meterpreter injects itself into the compromised process, from which it can migrate to other running processes (Meterpreter, 2023). In this case, it can be inferred from Figure 2.1.4 that the **compromised process** that the Meterpreter injected itself into **was *spoolsv.exe***. The application

spoolsv.exe is not inherently malicious as it is a legitimate Windows application for managing the

printing process for computers (Computer Hope, 2020).

Figure 2.1.2 – malfind command used in Volatility resulted in the discovery of this executable files that appeared three times. Command used: volatility_2.6_win64_standalone.exe --profile=Win2012R2x64 malfind -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem > DCmemmalfind.txt

Figure 2.1.3 – After entering a malfind dump command, the Windows VM was able to recognize it as malicious and had indicated the detected threat was Meterpreter. Command used to trigger this: volatility_2.6_win64_standalone.exe --profile=Win2012R2x64 malfind -D . -f C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem > DCmalfindmaldump.txt

```
zh-tw
zu-za
CONOUT$
tcp://203.78.103.109:443
```

Figure 2.1.4 – FLOSS results of a malfind data dmp file reveal the IP address 203.78.103.109 as an outward (TCP) connection (CONOUTS). Command used: *floss.exe C:\Users\student\Desktop\volatility_2.6_win64_standalone\process.0xffffe000631cb900.0x4afbf2000 0.dmp --format sc64 > DCmaldumpfloss.txt*

PCAP ANALYSIS

After analyzing the TCP conversations to determine any abnormal activity between any IP addresses or specific ports, it was observed in Figure 3.1 that the notable ports used by the local network was 3389 which is used for Remote Desktop Protocol native to Windows machines. Additionally, the network seemed very actively communicating with the IP address 194.61.24.109. as seen in Figure 3.2 it can be observed that this IP address was attempting to gain access to the Administrator account of the Local Server. This implies that the inciting incident was a **brute force attack in order to manipulate the open 3389 port of the local machines**. In regards to the time of entry, in Figures 3.3, 3.4, and 3.5, the date and time of *coreupdater.exe's* original entry into the local network can be observed on both the Local Server and Desktop.

Address A	Port A	Address B	Port B	Packets ▼	Bytes	Stream ID	Packets A → B	Bytes A → B	Packets B → A	Bytes B → A
194.61.24.102	40238	10.42.85.10	3389	71,289	18 MB	30442	36,909	5 MB	34,380	13 MB
10.42.85.115	50731	104.119.185.124	443	33,699	40 MB	30502	7,407	446 kB	26,292	39 MB
10.42.85.10	62514	10.42.85.115	3389	15,553	1 MB	30465	9,414	875 kB	6,139	453 kB
194.61.24.102	40240	10.42.85.10	3389	4,683	1 MB	30688	2,173	266 kB	2,510	1 MB
10.42.85.115	50132	151.101.1.67	443	4,511	4 MB	458	1,615	107 kB	2,896	4 MB
10.42.85.115	50614	104.18.12.165	443	3,928	5 MB	940	609	39 kB	3,319	5 MB
10.42.85.115	50354	23.47.193.50	443	3,661	5 MB	680	435	31 kB	3,226	5 MB
10.42.85.115	50408	143.204.131.79	443	3,338	4 MB	734	373	23 kB	2,965	4 MB
10.42.85.115	49803	13.107.21.200	443	3,074	2 MB	129	1,218	204 kB	1,856	2 MB
10.42.85.115	50782	23.47.52.14	443	3,050	3 MB	30553	825	52 kB	2,225	3 MB
10.42.85.115	49751	23.47.48.60	443	2,992	3 MB	77	855	54 kB	2,137	3 MB
10.42.85.115	51002	23.47.52.90	443	2,612	3 MB	30781	764	47 kB	1,848	3 MB
10.42.85.115	50875	203.78.103.109	443	2,556	2 MB	30646	904	280 kB	1,652	2 MB
10.42.85.115	49884	34.96.91.138	443	1,777	2 MB	210	459	30 kB	1,318	2 MB
10.42.85.10	62613	203.78.103.109	443	1,581	1 MB	30689	604	89 kB	977	961 kB
10.42.85.115	49841	23.32.45.41	443	1,567	1 MB	167	639	60 kB	928	1 MB
10.42.85.115	50440	74.120.184.194	443	1,420	1 MB	766	516	37 kB	904	1 MB
10.42.85.115	49736	172.232.42.32	443	1,416	1 MB	62	497	41 kB	919	1 MB

Figure 3.1 – Wireshark pcap file's TCP conversations. The most active ports are 3389 of both the local Server and Desktop computers with the other IP address involved being 194.61.24.102.
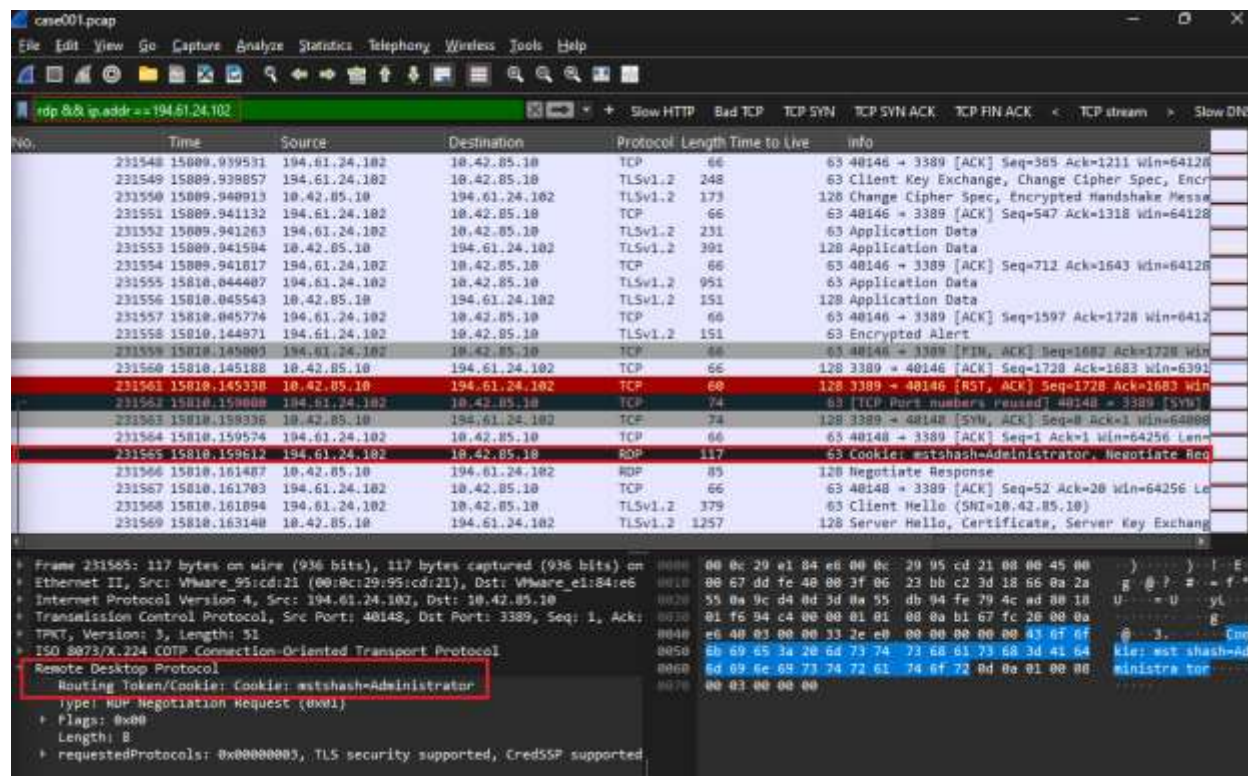
Figure 3.2 – Wireshark pcap results after filtering for RDP (port 3389) and the IP address 194.61.24.109. The filter reveals a series of attempts to gain access to the administrator account, implying it was a brute force attack taking place.
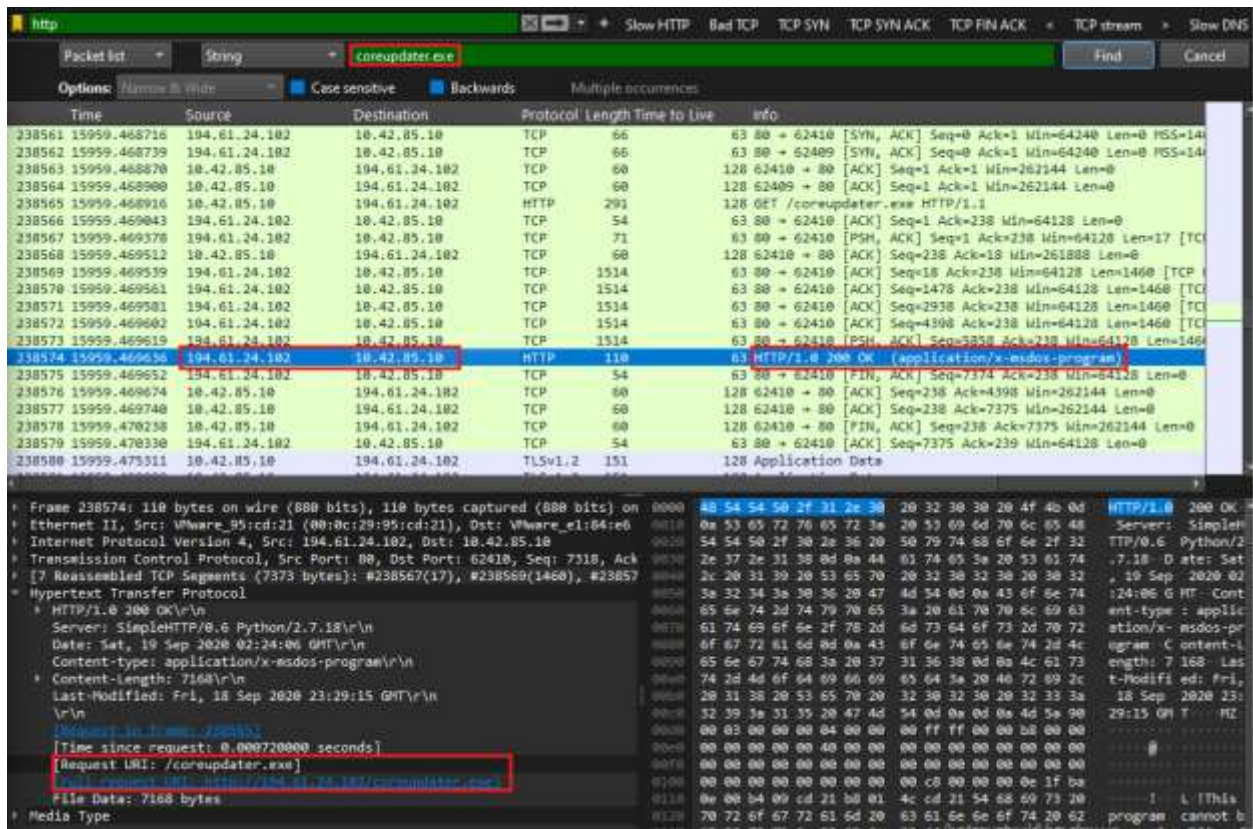
Figure 3.3 – After filtering for the string "coreupdater.exe" reveals the successful transfer of this file from the malicious IP to the breached local system.
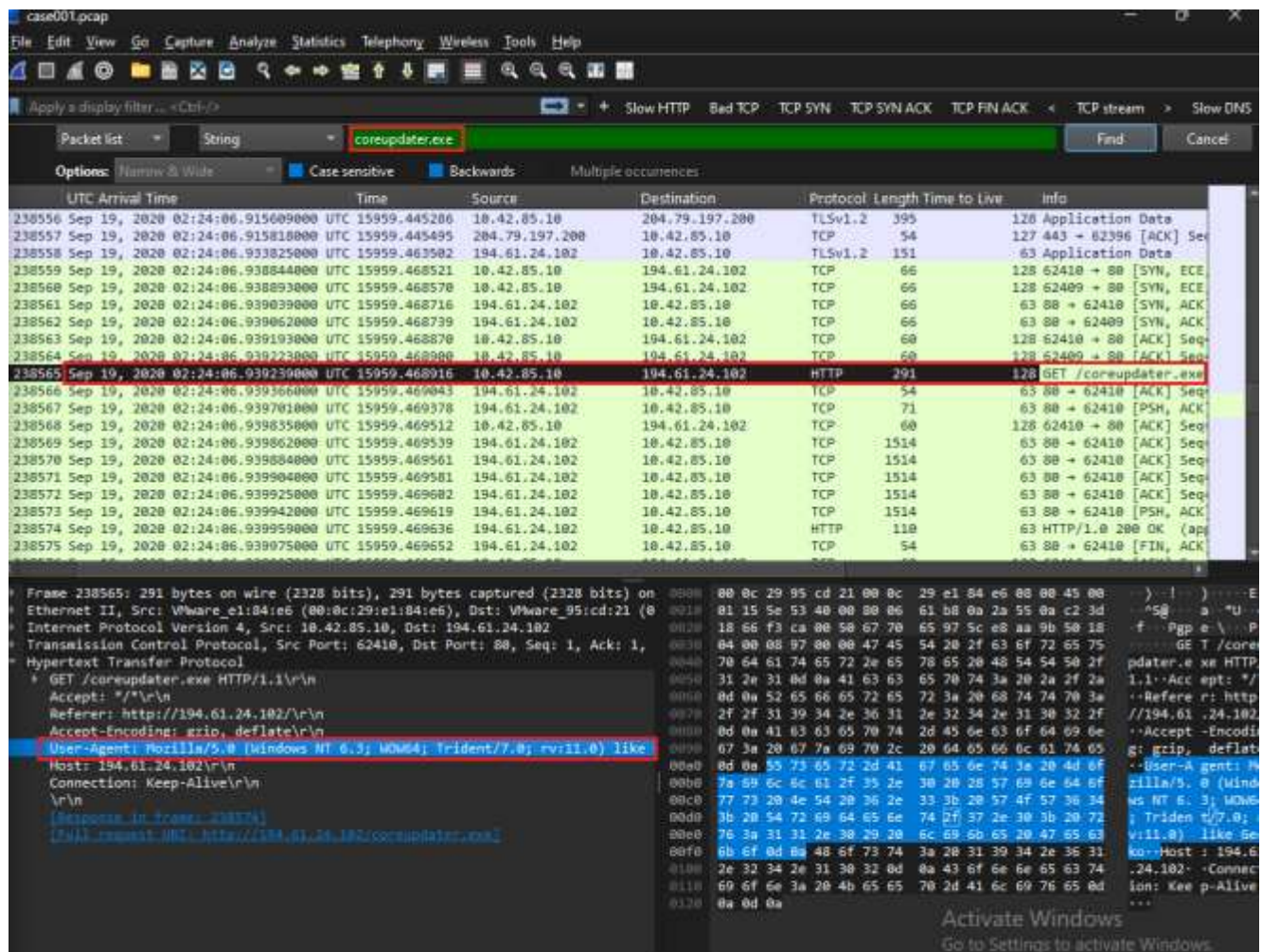
Figure 3.4 – Within the strings filter of *coreupdater.exe*, it was found that the malware was delivered by 194.61.24.102 through an Internet Explorer download (rv:11.0). The first time it appeared on the Local Server: 2020-09-19 02:24:06:939239 UTC.
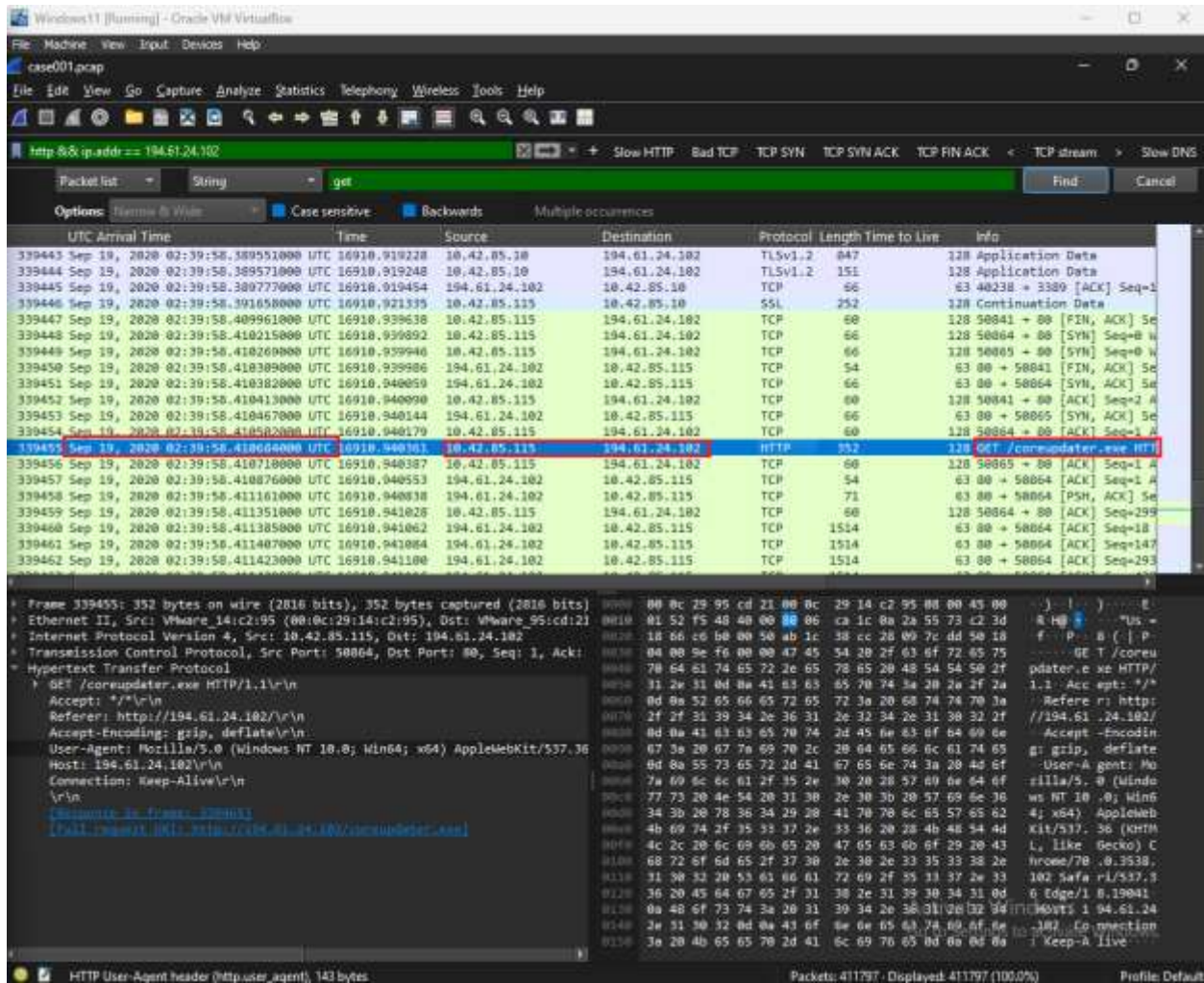
Figure 3.5 – The time that the malware appeared on the Desktop as seen by the *GET* request. Time of entry on Desktop: 2020-09-19 02:39:58:410684 UTC.
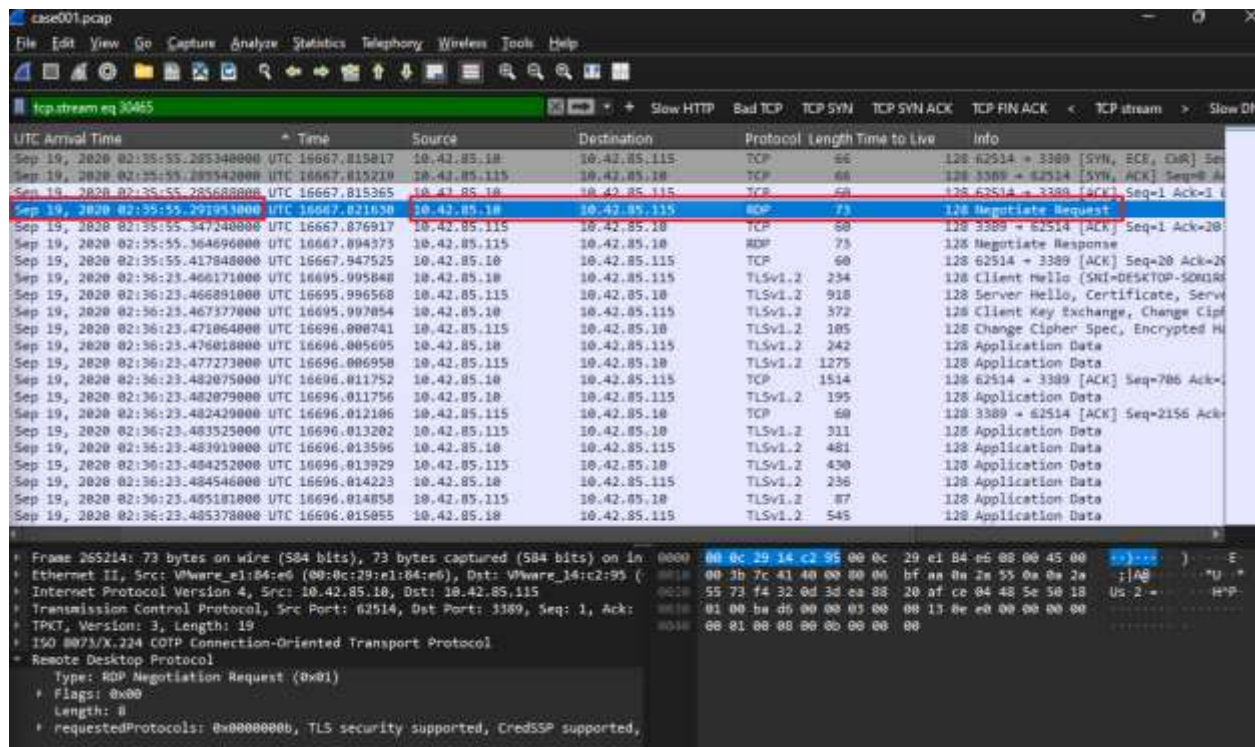
Figure 3.6 – Following a stream where RDP was a negotiated request between the Local Server's port 62514 and Desktop's port 3389 revealed it was successful and what followed was a series of TCP and TLS communications.

SUMMARY

INITIAL BREACH

1. Was there a breach?

   a. Yes

2. What was the initial entry vector?

   a. It was confirmed that there was a breach and evidence suggested that its attack vector was through a brute force attack that manipulated the open Remote Desktop Protocol (RDP) port – port 3389 – as evident in the PCAP file analysis.

3. Was malware used? If so, what was it?

    a.   Metasploit.

4. What Process was Malicious?

    a.   coreupdater.exe.

       Hash: fd153c66386ca93ec9993d66a84d6f0d129a3a5c.

5. Identify the IP Address that delivered the payload.

    a.   194.61.24.102 (attacker).

6. What IP Address is the malware calling to?

    a.   203.78.103.109 (C2 server).

7. Where is this malware on disk?

    a.   C:\windows\system32\coreupdater.exe.

    b.   Injected Meterpreter in *spoolsv.exe.*

8. When did it first appear?

    a.   On the server: 2020-09-19 02:24:06:939239 UTC.

    b.   On the desktop: 2020-09-19 02:39:58:410684 UTC.

9. Did someone move it?

    a.   Yes, was observed to be first downloaded via Internet Explorer as seen in Figure 3.4 yet it is later found within the System32 folder on the Local Server.

10. What were the capabilities of this malware?

    a.   The *coreupdater.exe* malware, associated with the Metasploit framework, is a powerful and versatile payload used for post-exploitation activities. Most notable capabilities include (Rapid7, 2023):

        i.   Remote access control – provides attackers with remote access to targeted systems.

      ii.   Privilege escalation – exploit vulnerabilities to elevate attackers to administrator privileges.

     iii.   Data exfiltration – enables attackers to find and exfiltrate sensitive data via encrypted channels.

     iv.   Keylogging and credential theft – captures keystrokes and collects stored credentials for further exploitation.

      v.   C2 communications – maintains communication with a remote C2 server to receive instructions and retrieve the exfiltrated data.

11. Is this malware easily obtained?

    a.   Yes, this originates from the Metasploit vulnerability framework used by red team penetrations testers (Rapid7, 2023).

12. Was this malware installed with persistence on any machine?

    a.   Yes, as seen in Figures 2.6 and 2.7, it seems that after its initial download, it was moved to the System32 folder of applications that automatically run in the background without the need for user interaction to trigger.

    b.   First download via Internet Explorer

      i.   On the server: 2020-09-19 02:24:06:939239 UTC

     ii.   On the desktop: 2020-09-19 02:39:58:410684 UTC

    c.   Movement to System32 folder:

      i.   2020-09-19 03:27:49 UTC

ATTACKERS

13. What malicious IP Addresses were involved?

    a.   194.61.24.102 (attacker)

    b.   203.78.103.109 (C2 server)

14. Were any IP Addresses from known adversary infrastructure?

   a. Though it cannot be confirmed with utmost confidence that the resolved IP addresses are from a known adversary infrastructure, the two resolved IP addresses involved in the malware attack have been reported as malicious by VirusTotal contributors.

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

   a. From the data recovered and analyzed, it cannot be definitively determined if this attack is in conjunction with other attacks around the time.

POST-BREACH ACTIVITY

16. Did the attacker access any other systems?

   a. Yes, as seen in Figure 3.6, there was a successful connection and proceeding TCP and TLS communications between the Local Server's port 62514 and Desktop's port 3389. This is classified as Lateral Movement under the MITRE ATT&CK Framework (MITRE ATT&CK, 2019).

   b. As seen in Figure 3.6, it is seen that this lateral movement first occurred at 2020-09-19 02:35:55:291953 UTC

17. Did the attacker steal or access any data? When?

   a. Yes. As seen in Figures 4.1-4.4, it can be inferred that these data files were accessed and potentially stolen between the time of 02:35:06-02:46:15 UTC on the date of 2020-09-19.

18. What architecture changes should be made immediately?

    a. Enhance network security posture

        i. Isolate the server from the public internet as much as possible to minimize the possibility of compromise directly impacting the main server.

        ii. Refine firewall files and configuration to limit incoming traffic and block unnecessary and unused ports.

    b. Secure RDP access if unnecessary or only allow the use of it through a Virtual Private Network (VPN) to ensure the encryption of traffic.

    c. Configure the server settings to limit the number of login attempts from a single IP address within a specific timeframe to deter automated brute-force attacks

19. Did the attacker steal the Szechuan sauce? If so, what time?

    a. As seen in Figure 4.1, the folder was accessed within the duration of the attack and that folder contains the Szechuan sauce recipe. As such, it can be assumed that the recipe was stolen at 2020-09-19 02:35:06 UTC.

20. Did the attacker steal or access any other sensitive files? If so, what times?

    a. Please refer to the answer to question 17.

21. Finally, when was the last known contact with the adversary?

    a. As seen in Figure 4.5, it is seen that the last known contact with the adversary was at 2020-09-19 02:57:41:58551 UTC

TIMELINE

Below is a rough timeline of the information discovered from the data analyzed. The date of the attack being 2020-09-19. It is highly probable that more information was accessed than what was discovered in this report.

| Time (UTC)	Note	Accompanying Figure Number
02:24:06:939239	First contact between the Local Server and adversary	3.4
02:39:58:410684	First contact between the Desktop and adversary	3.5
02:35:55:291953	Successful RDP connection between Local Server to Desktop – lateral movement	3.6
02:35:06	Secret folder on LocalServer, which contains the Szechuan Sauce recipe file, was accessed	4.1
02:46:15	File within Desktop was accessed: portal_gun.png	4.2
	File within Desktop was accessed: plans.txt	4.3
	File within Desktop was accessed: My Social Security Number.txt	4.4
02:57:41:58551	Last known contact between adversary and local network	4.5
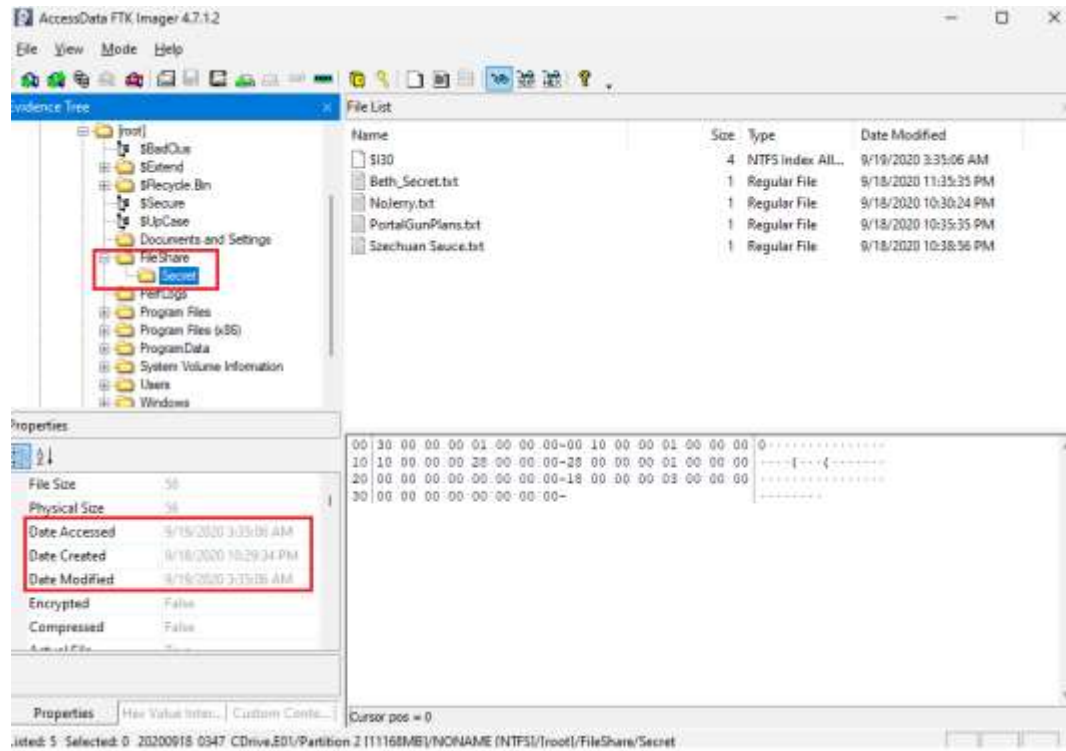
Figure 4.1 – the Secret Folder within the Local Server image disk. The date accessed is 2020-09-19 02:35:06 UTC.
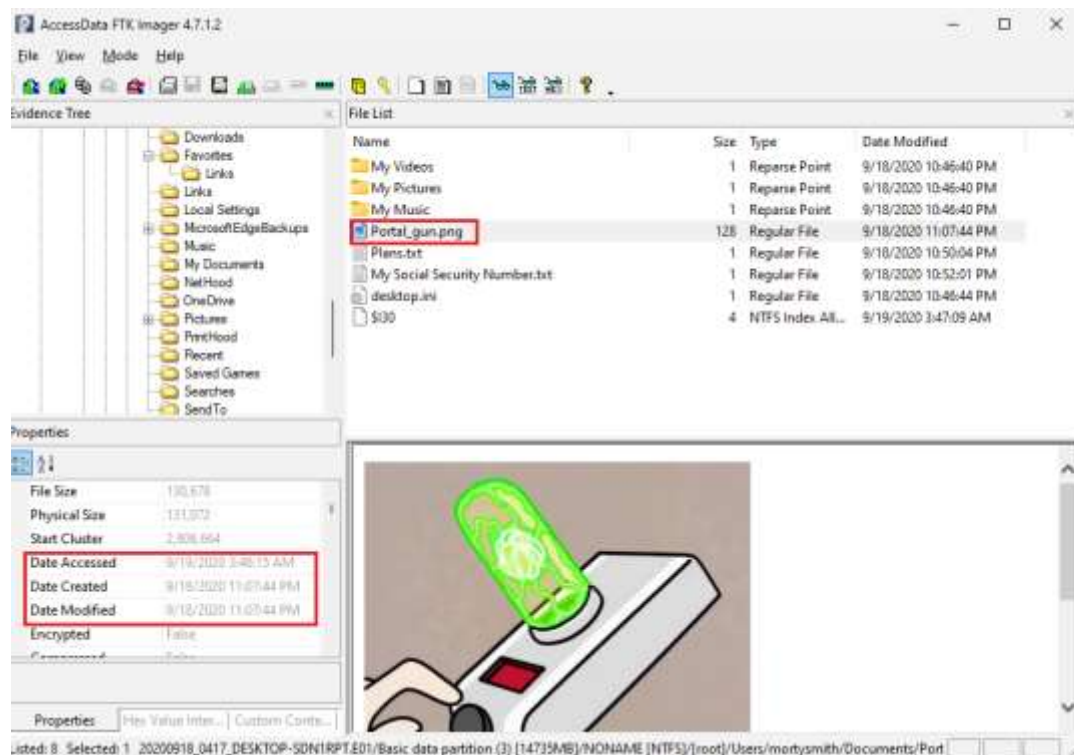
Figure 4.2 – A file within the Desktop's disk image under the morty user. The date accessed is 2020-09-19 02:46:15 UTC.
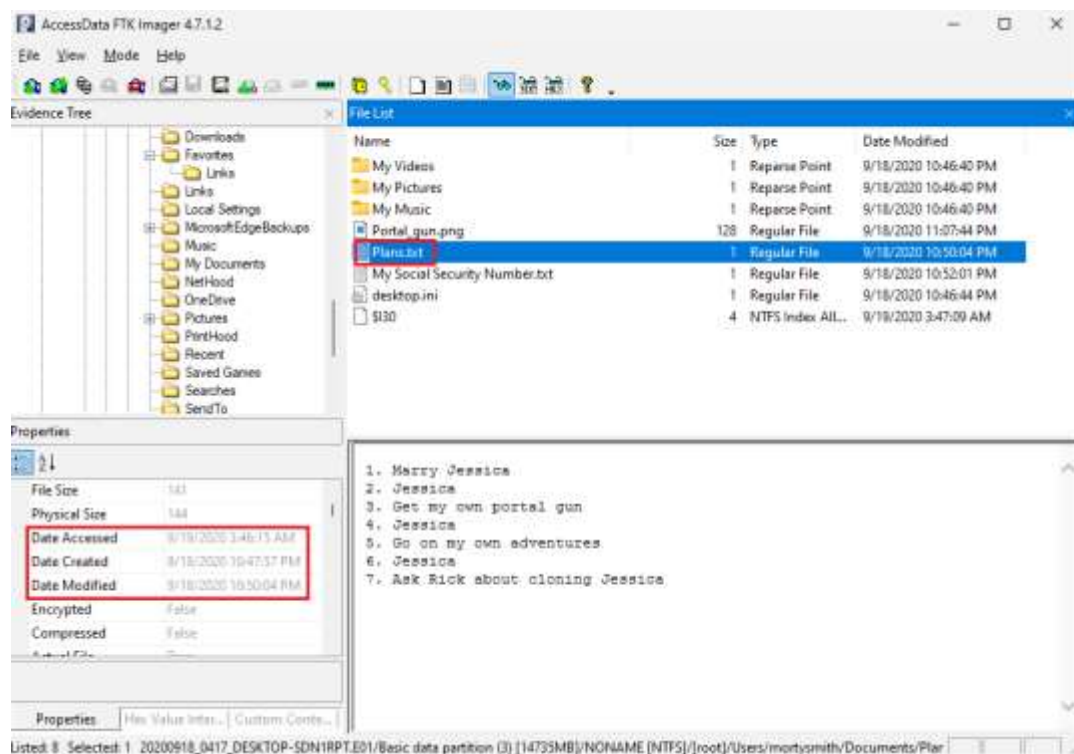

Figure 4.3 – A file within the Desktop's disk image under the morty user. The date accessed is 2020-09-19 02:46:15 UTC.
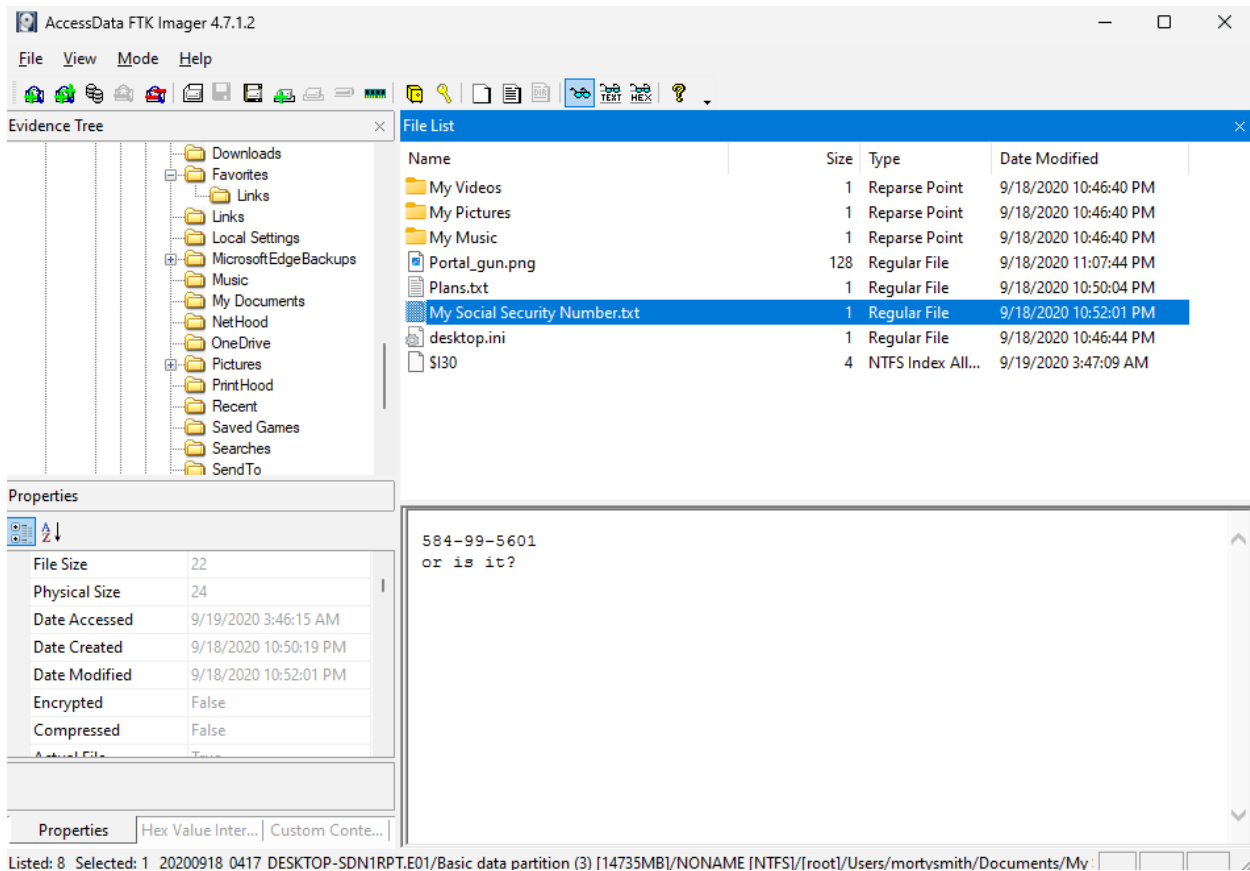
Figure 4.4 – A file within the Desktop's disk image under the morty user. The date accessed is 2020-09-19 02:46:15 UTC.
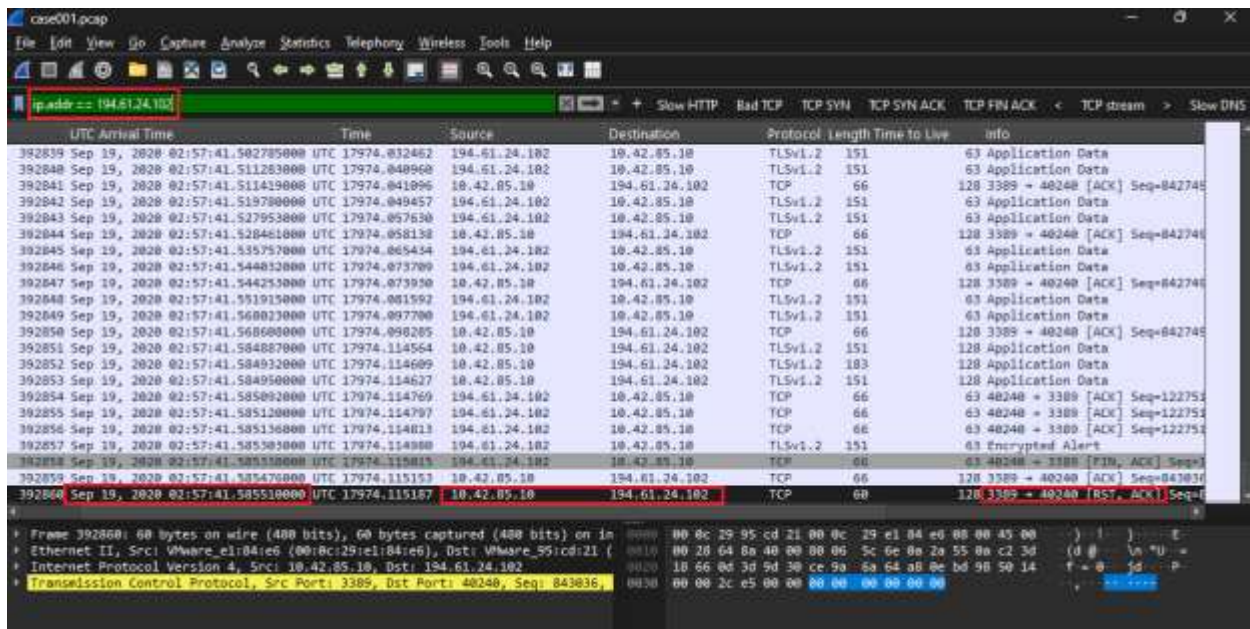

Figure 4.5 – The last known contact with the IP address 194.61.24.202 at 2020-09-19 02:57:41:58551 UTC

REFERENCES

Brithny. (2025, January 24). *What Happens If You Delete the System32 Folder? Here Are the Answers*. Retrieved from EaseUS: https://www.easeus.com/computer-instruction/delete-system32.html

Computer Hope. (2020, August 31). *What is the Windows spoolsv.exe file and process?* Retrieved from Computer Hope: https://www.computerhope.com/issues/ch000914.htm

Magnet Forensics. (2024, October 25). *ShimCache vs AmCache: Key Windows Forensic Artifacts*. Retrieved from Magnet Forensics: https://www.magnetforensics.com/blog/shimcache-vs-amcache-key-windows-forensic-artifacts/

Mandiant. (2024, September 26). *mandiant /flare-floss*. Retrieved from GitHub: https://github.com/mandiant/flare-floss

Meterpreter. (2023). Retrieved from Secret Double Octopus: https://doubleoctopus.com/security-wiki/threats-and-tools/meterpreter/

MITRE ATT&CK. (2019, July 19). *Lateral Movement* . Retrieved from MITRE ATT&CK: https://attack.mitre.org/tactics/TA0008/

Rapid7. (2023). *Get Started with Metasploit*. Retrieved from Metasploit: https://www.metasploit.com/get-started

Rapid7. (2023). *Getting Started*. Retrieved from Rapid7: https://docs.rapid7.com/metasploit/getting-started/