

LIGHTHOUSE LAB
CYBERSECURITY
FORENSICS REPORT & DOCUMENTATION
OLADAPO OLUWAYALE

Contents	Page
Executive Summary	3
Introduction	4
Methodology	4
Investigative Findings	6
Recommendations	23
References	24

Executive Summary

This report presents the results of a forensic investigation into a cyber security breach that occurred in September 2020, impacting both a server and a desktop within the organization. The investigation involved the use of various forensic tools to examine memory dumps, network traffic, and disk images, revealing crucial details about the nature of the attack.

Key Findings:

- The attack originated from a brute-force attempt targeting the server's RDP (Remote Desktop Protocol) service, which enabled the attackers to gain administrative access to the domain controller.
- Malware (coreupdater.exe) was discovered in system directories on both the server and desktop, and it was found to be communicating with a remote command-and-control server to ensure persistence and potentially exfiltrate data.
- Evidence of sensitive data being exfiltrated was uncovered, suggesting that the attackers successfully accessed and transferred confidential information from the system.

Recommendations:

- Implement multi-factor authentication (MFA) for all RDP access points to prevent unauthorized access.
- Restrict RDP access to internal networks only and use VPNs to facilitate secure remote access.
- Install endpoint detection and response (EDR) tools to continuously monitor for suspicious activities and malware.
- Regularly apply system updates and patches to address any existing vulnerabilities.
- Enhance incident response protocols to address RDP-related threats and provide training for staff to identify phishing attempts and other social engineering tactics.

The investigation highlights the key findings from the breach, as well as the critical steps that must be taken to reduce the likelihood of future incidents.

Introduction

A digital forensic investigation was launched in response to a potential security breach involving the theft of a proprietary Szechuan sauce recipe. This investigation, codenamed "The Stolen Szechuan Sauce," aimed to determine the specifics and scope of the breach, understand the methods used by the attackers, and assess its impact on the organization (James, Case 001 - The Stolen Szechuan Sauce, 2021).

The primary goals of this investigation are as follows:

- **Identify the Breach:** Confirm whether a breach occurred by thoroughly analyzing system logs, memory dumps, and network traffic.
- **Determine the Initial Entry Vector:** Investigate how the attackers first gained access to the servers and workstations, focusing on potential methods such as phishing emails, malicious downloads, or the use of USB devices.
- **Assess the Impact:** Evaluate the scale of the compromise, including identifying any malware involved, determining which systems were affected, and understanding what data was exfiltrated.
- **Examine Persistence Mechanisms:** Investigate how the attackers maintained continued access to the systems over time.
- **Provide Recommendations:** Based on the findings, offer immediate and long-term recommendations to prevent future breaches and strengthen the organization's overall security framework.

The purpose of this investigation is to collect thorough evidence, reconstruct the events that transpired, and provide actionable insights to protect the organization's valuable assets and sensitive information.

Methodology

Tools

The following forensic tools and artifacts were employed during this investigation:

- **Volatility:** Used to analyze memory dumps in order to identify malicious processes, network activity, and other artifacts.
- **Registry Explorer:** this is used to examine and analyze the Windows registry.
- **Wireshark:** Used to capture and examine network traffic for signs of suspicious or malicious behavior.
- **VirusTotal:** Employed to detect malicious files by cross-referencing them with multiple security vendor databases.

- FTK Imager: Used to acquire disk images and extract critical evidence from storage devices.

Artifacts

- Case001 PCAP: A file capturing network traffic during the incident, offering valuable insights into the actions of the attackers.
- Server/Desktop Disk Image: A disk image from the involved systems, providing file system data for in-depth analysis.
- Server/Desktop Memory and PageFile: Memory dumps analyzed to reveal the running processes and the system state at the time of the breach.
- Server/Desktop Protected Files: Registry files extracted from the systems to examine system configurations and identify potentially altered or compromised settings.

Approach

The investigation concentrated on the following critical areas:

- Memory Analysis: This involved identifying active processes, detecting malicious activities, analyzing network details, and uncovering any anomalies.
- Network Traffic Analysis: In-depth packet analysis was performed to trace communication between the attacker and the targeted systems.
- Disk and Registry Analysis: Files and registry entries were reviewed to detect malware and configuration modifications that may have been made during the attack.

Key Findings

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

Ans: Windows Server 2012 R2 Standard Evaluation

Process: this was located in the registry part

(Root\Microsoft\WindowsNT\CurrentVersion\ProductName) which was exported from the server image loaded on FTK with path(C:\root\windows\system32\Config\software

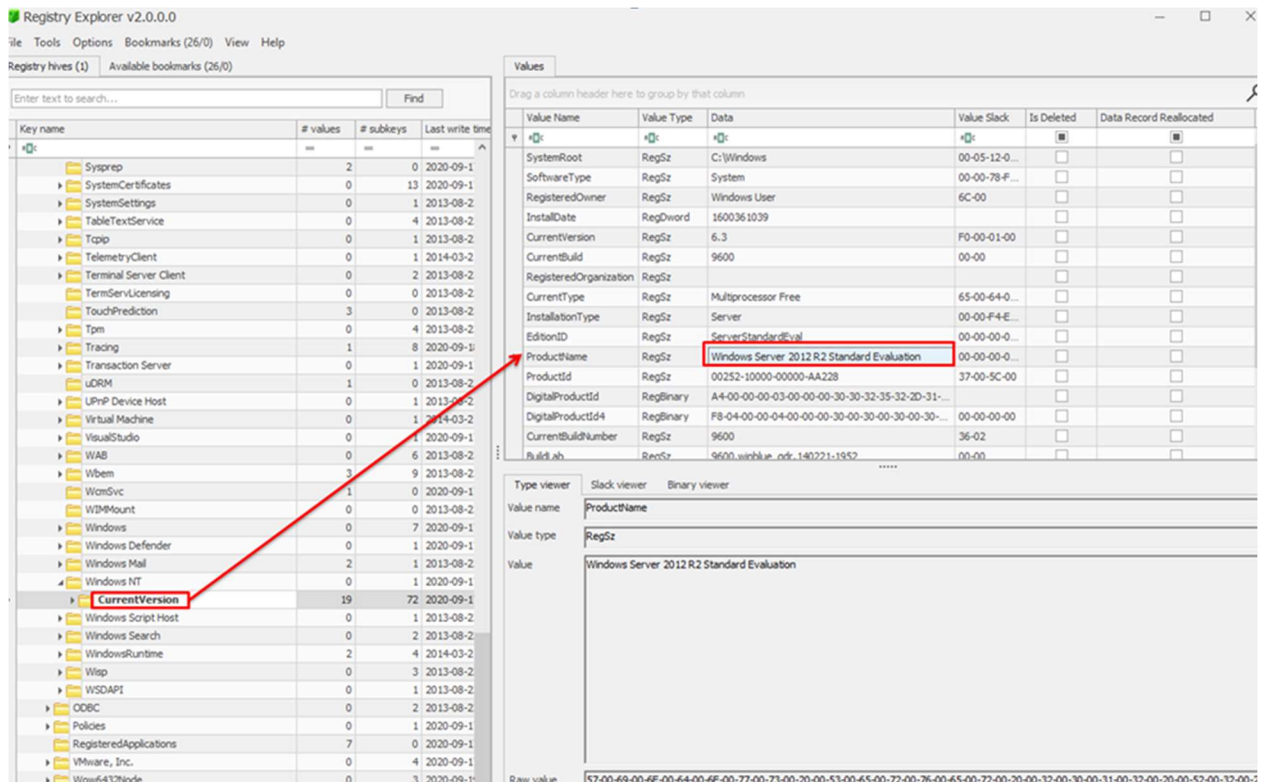


Fig 1: Server OS

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

Ans: Windows 10 Enterprise evaluation

Process: Loaded the desktop image on FTK, searched for the software file with file path C:\root\windows\System32\Config\software and exported it to registry explorer and got the OS and its version going through path Microsoft\Windows NT\CurrentVersion

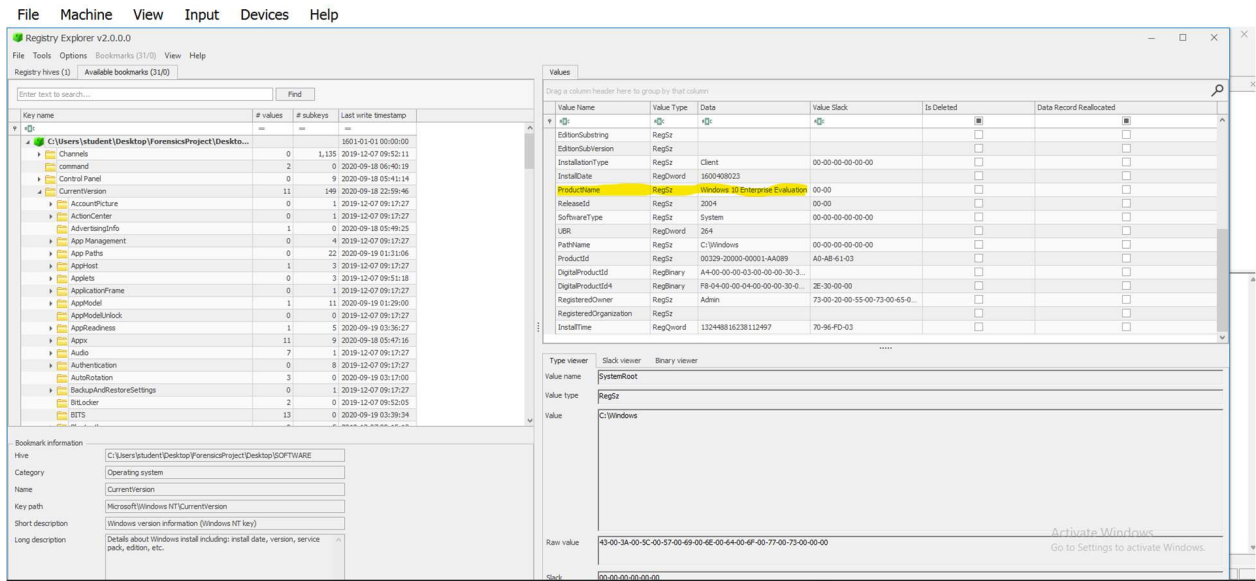


Fig 2: Desktop OS

3. What was the local time of the server?

Ans: 420 Pacific Standard Time

Process: the file `C:\Users\student\Desktop\ForensicsProject\DC01\DC01-ProtectedFiles\Protected\system` was checked and time zone was found in the registry:
Control

4. Was there a breach?

Ans: Yes

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

Ans: destination port used was port 3389 which suggest it was through remote desktop protocol (RDP)

Process: PCAP was loaded on Wireshark and the malicious IP was filtered and port detail was looked into.

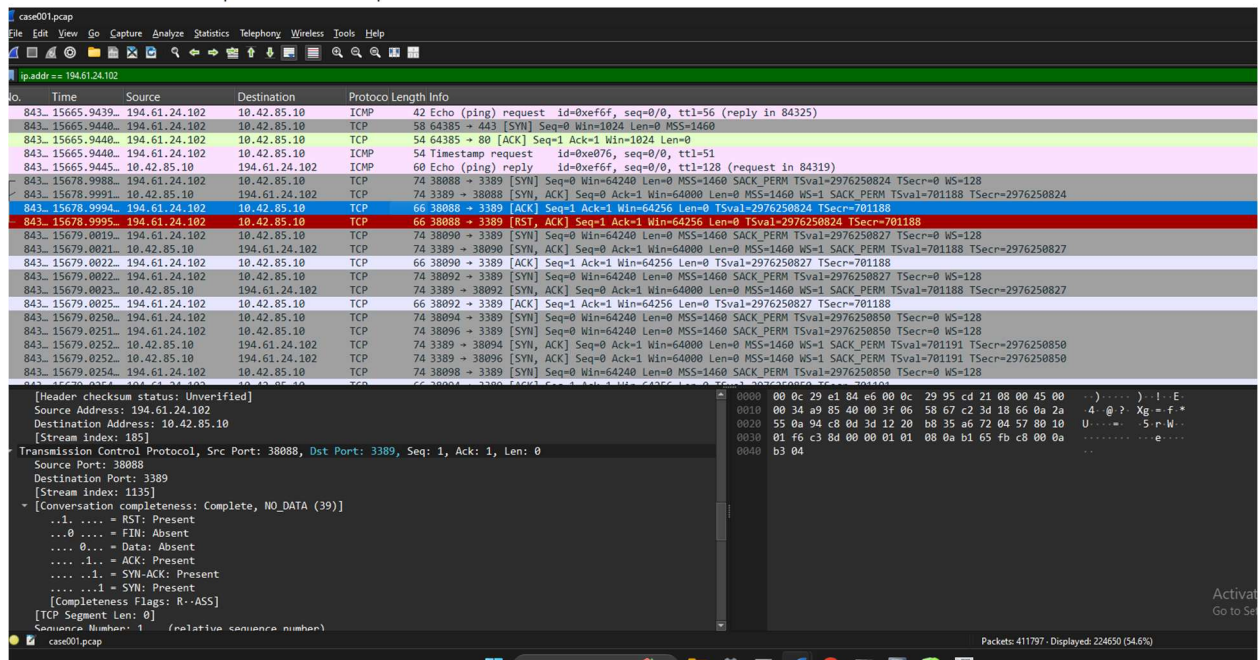


Fig 4: Initial entry vector

6. Was malware used? Yes, it was used.

Ans: The malicious process is “coreupdater.exe”

Process: Loaded desktop memory image on Volatility workbench, googled the processes that appeared fishy and found coreupdater.exe reported malicious, filtered it on Wireshark to get the IPs involve and plug them into VirusTotal to identify the malicious ones, got the process executable hash also and plugged it into VirusTotal to get more details about the malware.

PassMark Volatility Workbench

Image file: C:\Users\student\Desktop\ForensicsProject\Desktop\DESKTC
 Platform: Windows
 Command: windows.pscan.PsScan
 Command parameters:
☐ Display physical offsets
☐ Process ID

Browse Image
 Refresh Process List
 Command Info
 Run

Command Description:
 Scans for processes present in a particular windows memory image

2188	616	spoolsv.exe	0xbe8e75c2c200	10	-	0	False	2020-09-19 01:24:09.000000	N/A	Disabled
2248	616	svchost.exe	0xbe8e75c43240	9	-	0	False	2020-09-19 01:24:09.000000	N/A	Disabled
2364	616	vmtoolsd.exe	0xbe8e74364280	9	-	0	False	2020-09-19 01:24:09.000000	N/A	Disabled
2372	616	VGAuthService.exe	0xbe8e75cdd300	2	-	0	False	2020-09-19 01:24:09.000000	N/A	Disabled
2396	616	wlms.exe	0xbe8e75cde080	2	-	0	False	2020-09-19 01:24:09.000000	N/A	Disabled
2404	616	MsMpEng.exe	0xbe8e75c0e080	9	-	0	False	2020-09-19 01:24:09.000000	N/A	Disabled
2952	616	dilhost.exe	0xbe8e7600a280	10	-	0	False	2020-09-19 01:24:11.000000	N/A	Disabled
2548	764	WinPrvSE.exe	0xbe8e75d97280	11	-	0	False	2020-09-19 01:24:11.000000	N/A	Disabled
3520	616	msdtc.exe	0xbe8e763282c0	9	-	0	False	2020-09-19 01:24:13.000000	N/A	Disabled
2684	616	svchost.exe	0xbe8e760b7080	7	-	0	False	2020-09-19 01:24:30.000000	N/A	Disabled
2748	616	SgrmBroker.exe	0xbe8e7654b080	7	-	0	False	2020-09-19 01:26:10.000000	N/A	Disabled
2208	616	svchost.exe	0xbe8e7654f240	1	-	0	False	2020-09-19 01:26:11.000000	N/A	Disabled
2216	616	svchost.exe	0xbe8e76485300	11	-	0	False	2020-09-19 01:26:11.000000	N/A	Disabled
3708	616	SearchIndexer.exe	0xbe8e762ef3240	19	-	0	False	2020-09-19 01:26:11.000000	N/A	Disabled
1608	616	svchost.exe	0xbe8e711952c0	3	-	0	False	2020-09-19 01:28:10.000000	N/A	Disabled
4092	616	svchost.exe	0xbe8e77ee2080	4	-	0	False	2020-09-19 01:31:39.000000	N/A	Disabled
4592	764	MicrosoftEdge.exe	0xbe8e770f0080	0	-	1	False	2020-09-19 03:16:05.000000	2020-09-19 03:17:00.000000	Disabled
5664	616	SecurityHealth	0xbe8e79004280	14	-	0	False	2020-09-19 03:16:17.000000	N/A	Disabled
6384	4084	csrss.exe	0xbe8e779b9080	11	-	2	False	2020-09-19 03:17:00.000000	N/A	Disabled
6456	4084	winlogon.exe	0xbe8e7773ef080	5	-	2	False	2020-09-19 03:17:00.000000	N/A	Disabled
1768	6456	dwm.exe	0xbe8e78cab080	15	-	2	False	2020-09-19 03:17:01.000000	N/A	Disabled
4808	6456	fontdrvhost.exe	0xbe8e75cb4080	5	-	2	False	2020-09-19 03:17:01.000000	N/A	Disabled
860	764	MicrosoftEdge.exe	0xbe8e790c2080	0	-	3	False	2020-09-19 03:36:40.000000	2020-09-19 03:43:52.000000	Disabled
8324	4008	coreupdater.exe	0xbe8e7a447080	0	-	3	False	2020-09-19 03:40:49.000000	2020-09-19 03:43:10.000000	Disabled
3232	448	smss.exe	0xbe8e767d080	20	-	2	False	2020-09-19 05:08:13.000000	N/A	Disabled
1172	616	svchost.exe	0xbe8e778ef080	16	-	2	False	2020-09-19 05:08:15.000000	N/A	Disabled
6756	448	taskhostw.exe	0xbe8e790d7080	11	-	2	False	2020-09-19 05:08:16.000000	N/A	Disabled
5204	6456	userinit.exe	0xbe8e79130080	0	-	2	False	2020-09-19 05:08:16.000000	2020-09-19 05:08:42.000000	Disabled
5896	5204	explorer.exe	0xbe8e764d7080	75	-	2	False	2020-09-19 05:08:16.000000	N/A	Disabled
4096	1070858240		0xbe8e7607f080	4096	-	1217158537	False	-	-	Disabled
4312	616	svchost.exe	0xbe8e789d0080	33	-	0	False	2020-09-19 05:08:16.000000	N/A	Disabled
2904	764	dilhost.exe	0xbe8e757e2080	8	-	2	False	2020-09-19 05:08:18.000000	N/A	Disabled

Fig 5: Malicious process in Volatility

JoeSandboxCloud BASIC

Overview Signatures Startup Domains / IPs Dropped Static Net

Analysis Report coreupdater.exe

Overview

General Information

Sample Name:	coreupdater.exe
Analysis ID:	398583
MD5:	eed41b4500e473f97c50c7...
SHA1:	fd153c66386ca93ec9993d...
SHA256:	10f3b92002bb9846733416...
Infos:	

Most interesting Screenshot:

Detection

MALICIOUS

SUSPICIOUS

CLEAN

UNKNOWN

Metasploit

Score:	68
Range:	0 - 100
Whitelisted:	false
Confidence:	100%

Signatures

- Antivirus / Scanner detection for submitted sample
- Multi AV Scanner detection for submitted file
- Yara detected Metasploit Payload
- Machine Learning detection for sample
- Antivirus or Machine Learning detection for unpacked file
- Entry point lies outside standard sections
- IP address seen in connection with other malware
- PE file contains an invalid checksum
- PE file contains sections with non-standard names
- Program does not show much activity (idle)

Startup

- System is w10x64
- coreupdater.exe (PID: 6948 cmdline: "C:\Users\user\Desktop\coreupdater.exe" MD5: EED41B4500E473F97C50C7385EF5E374)
- cleanup

Fig 6: Record of the process reported malicious

```

Windows PowerShell (x86)
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows

PS C:\Users\student> cd Desktop
PS C:\Users\student\Desktop> Get-fileHash .\coreupdater.exe

Algorithm      Hash
-----
SHA256         10F3B92002BB98467334161CF85D0B1730851F9256F83C27DB125E9A0C1CFDA6
Path
-----
C:\Users\student\Desktop\core...

PS C:\Users\student\Desktop>

```

Fig 7: Malicious process hash

- IP address that delivered the payload is (194.61.24.102)

Process: Loaded the PCAP file on Wireshark, filtered out the malicious process using “Frame contains “coreupdater”” and got an IP address (194.61.24.102) initiating connection with the desktop IP address. Plugged the IP into Virus total and found out it’s malicious. Filtered out the malicious IP address and port 3389 that revealed the payload pushed successfully

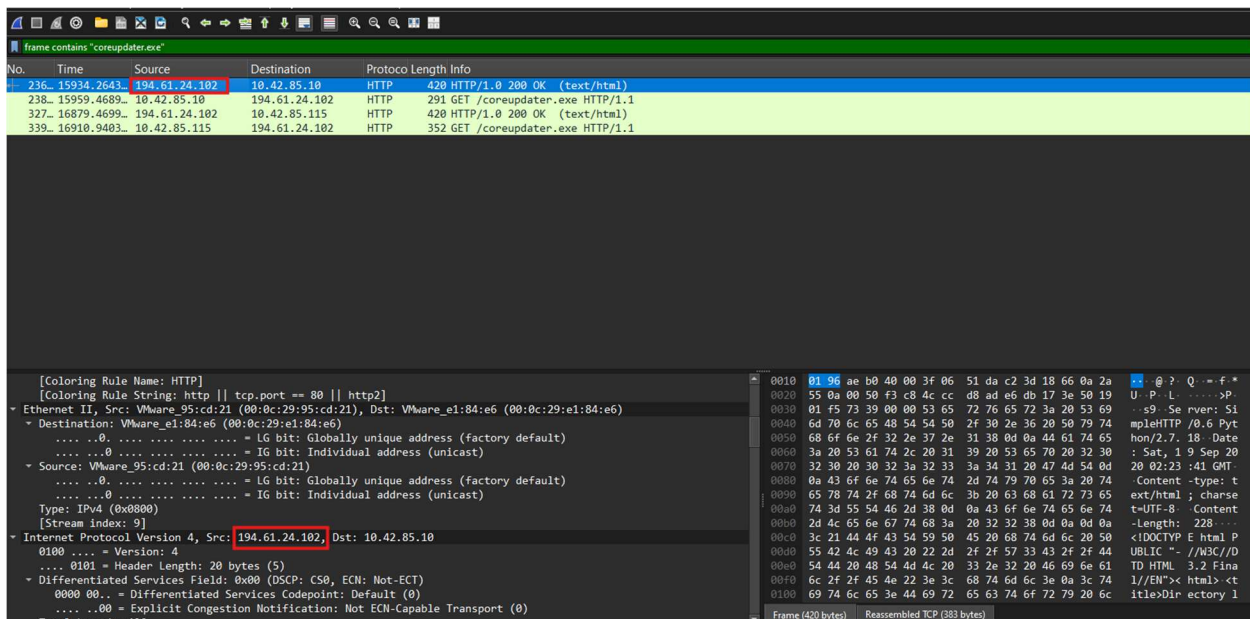


Fig 8: Malicious process filter

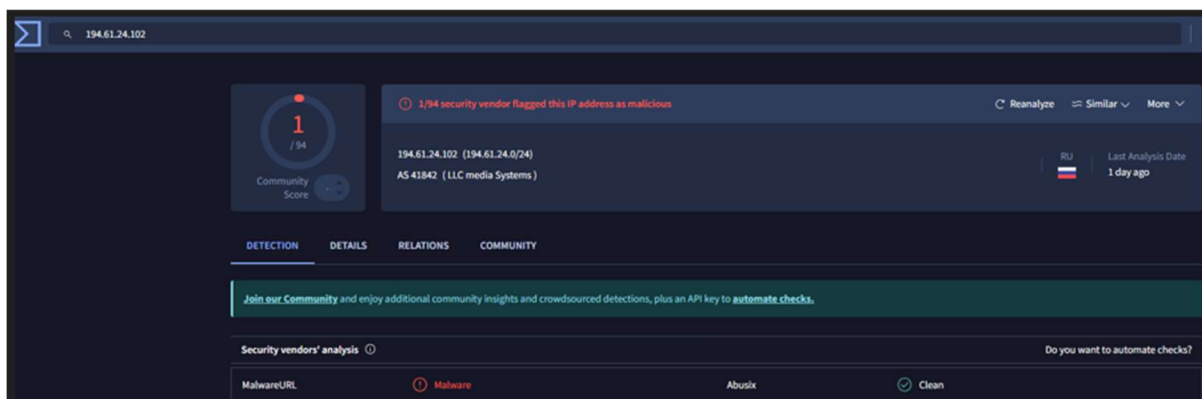


Fig 9: Virustotal revealing malicious IP

- The IP address the malware is calling to is (203.78.103.109)
Process: Used cmd in the volatility3 plugin with the command –
C:\Users\student\Desktop\ForensicsProject\DC01\DC01-
memory\citadeldc01.mem windows.netstat

```
C:\Windows\System32\cmd.exe
Microsoft Windows [Version 10.0.22631.4751]
(c) Microsoft Corporation. All rights reserved.

C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadelcdc01.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress: 100.00
PDB scanning finished
Offset Proto LocalAddr LocalPort ForeignAddr ForeignPort State PID Owner Created
0xe00063266d10 TCPv6 fe80::2dcf:e660:be73:d220 62777 fe80::2dcf:e660:be73:d220 49155 CLOSED 460 sass.exe -
0xe00062a31270 TCPv6 fe80::2dcf:e660:be73:d220 49182 fe80::2dcf:e660:be73:d220 389 ESTABLISHED 1 332 dfsrs.exe N/A
0xe0006103c4f0 TCPv6 fe80::2dcf:e660:be73:d220 49174 fe80::2dcf:e660:be73:d220 49155 ESTABLISHED 1 660 dfssvc.exe N/A
0xe000610d0640 TCPv6 ... #0161 ... 389 ESTABLISHED 1392 lsass.exe N/A
0xe000631c7590 TCPv4 10.42.85.10 62613 203.78.103.109 443 ESTABLISHED 3644 coreupdater.exe N/A
0xe0006102d010 TCPv6 ... 49100 ... 389 ESTABLISHED 1392 lsass.exe N/A
```

Fig 11: IP address malware is calling to

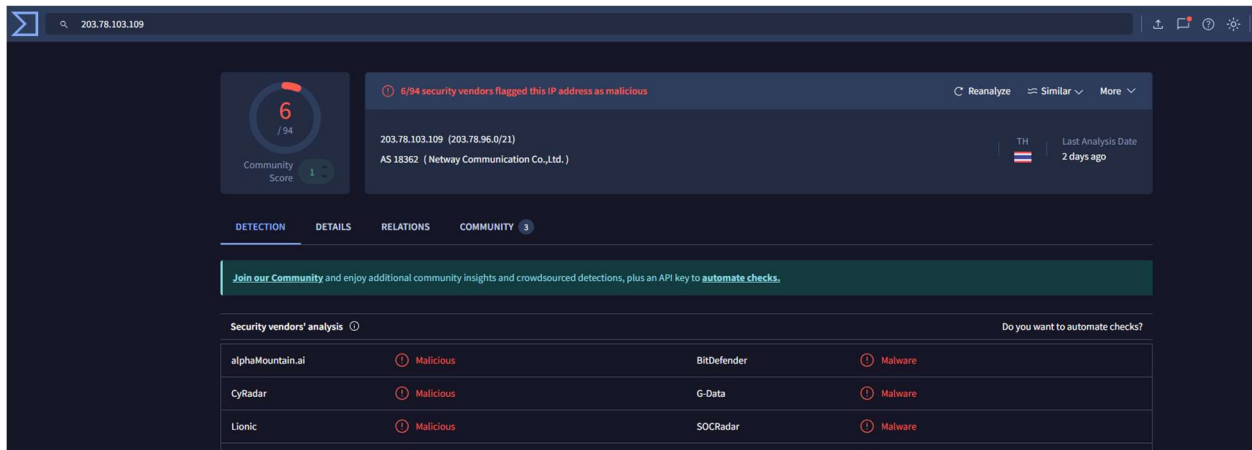


Fig 12: VirusTotal confirms IP is malicious

- Location of the malware on the disk.

Ans: C:\Root\Windows\System32\coreupdate.exe

Process: Loaded the C Drive E01 on FTK and searched through the second partition to the root folder, windows folder and system32 folder.

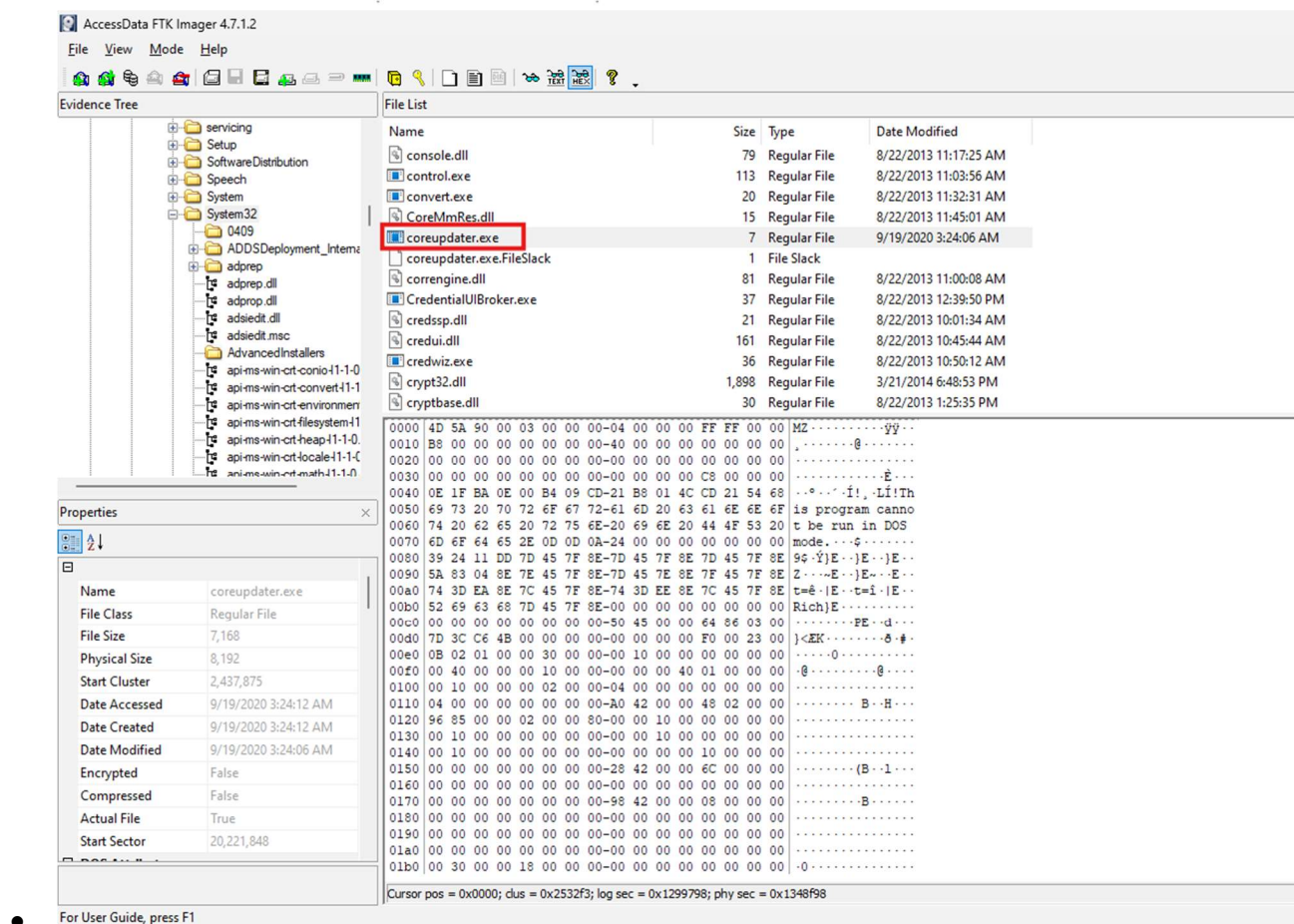


Fig 13: Location of malicious process.

- When did it first appear?

Ans: It first appear on 2020/09/19 03:40:49 UTC as revealed and highlighted in fig 5

- Did someone move it?

Ans: Yes, to C:\Windows\System32 as shown in Fig 13.

- The capabilities of the malware

Process: plugged in the hash of the malicious process and clicked on the behavior tab. According to MITRE ATT&CK tactics and techniques, this malware is capable of defence evasion, file obfuscation, and encodes data. VirusTotal. (2025, Jan 30)

The screenshot displays the VirusTotal Malware Behavior analysis page for the file hash `10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6`. The interface is dark-themed and includes a search bar at the top.

Activity Summary

⚠️ The Sandbox CAPE Sandbox tags this file as: MALWARE

MITRE ATT&CK Tactics and Techniques

- **Defense Evasion** (TA0005)
 - ⚙️ **Obfuscated Files or Information** (T1027)
 - encode data using XOR
- **Discovery** (TA0007)
 - 🔍 **System Information Discovery** (T1082)
 - Reads software policies
- **Command and Control** (TA0011)
 - 🌐 **Application Layer Protocol** (T1071)
 - Uses HTTPS
 - Adversaries may communicate using application layer protocols to avoid detection/network filtering by blending in with existing traffic.
 - 🔒 **Encrypted Channel** (T1573)
 - Uses HTTPS
 - Uses HTTPS for network communication, use the SSL MITM Proxy cookbook for further analysis

Malware Behavior Catalog Tree

- **Anti-Static Analysis** (OB0002)
 - ⚙️ **Obfuscated Files or Information** (E1027)
 - Encoding - Standard Algorithm (E1027.m02)
- **Defense Evasion** (OB0006)
 - ⚙️ **Obfuscated Files or Information** (E1027)
 - Encoding - Standard Algorithm (E1027.m02)
- **Data** (OC0004)
 - ⚙️ **Encode Data** (C0026)
 - XOR (C0026.002)
- **Communication** (OC0006)
 - 🌐 **HTTP Communication** (C0002)

Fig 14: VirusTotal – Malware Behavior

- Is this malware easily obtained?

Ans: Yes, it is a widely available threat as it has been reported by many vendors

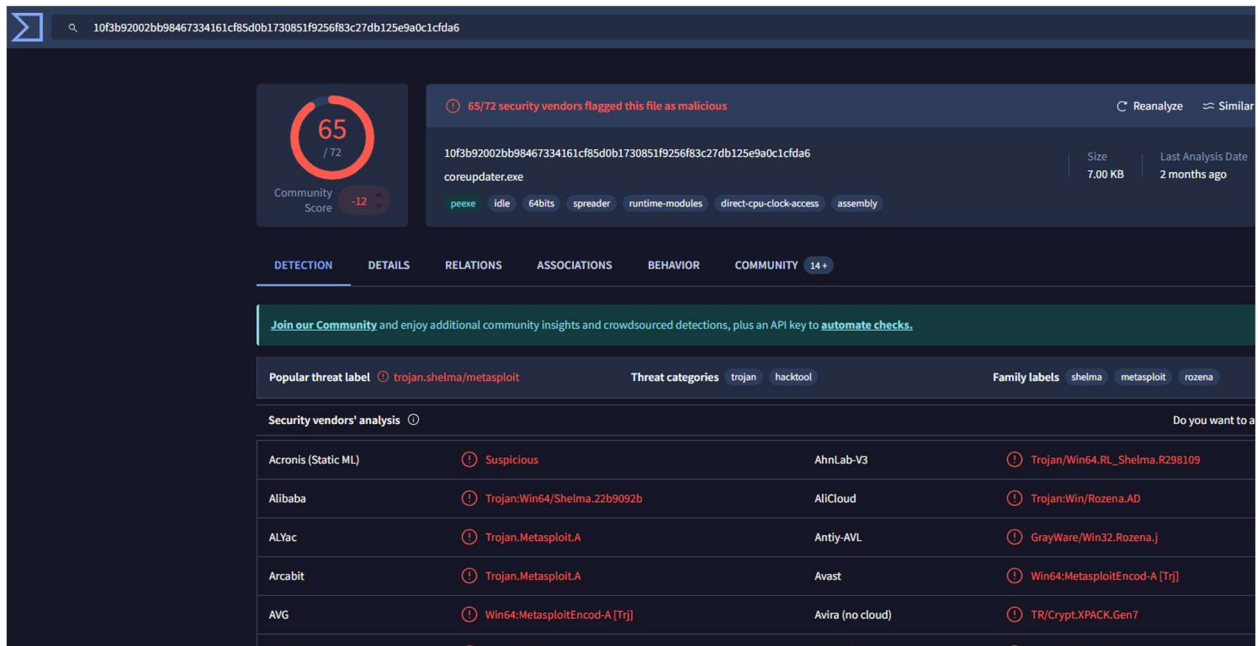


Fig15: Reports of Malicious file

- Was this malware installed with persistence on any machine?

Answer: Yes, it was installed on the server

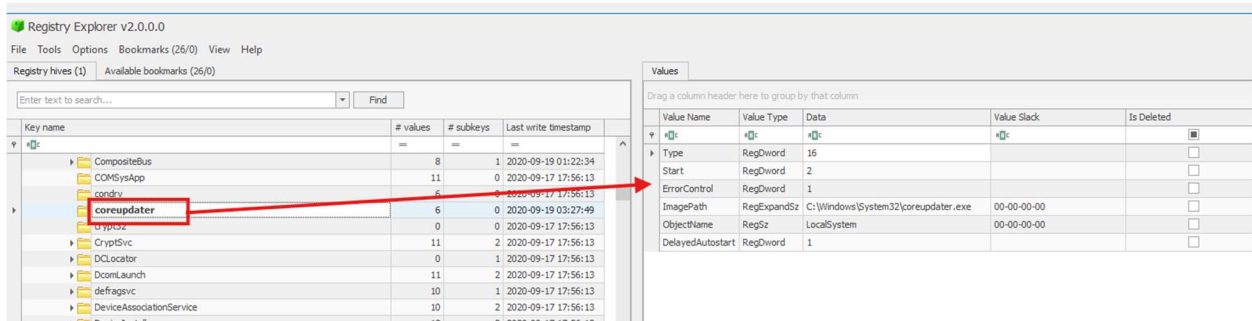


Fig 16 Persistent Malware Location.

7. Malicious IP addresses involved

Ans: IP address that delivered the payload (194.61.24.102) and IP address the malware was calling to (203.78.103.109) as confirmed by Fig 8 & 11.

- IP address (203.78.103.109) is from known adversary infrastructure
Process: Plugged in the IP address into VirusTotal and clicked the details tab and it shows the network is from Netway Communication Co., Ltd in Thailand.

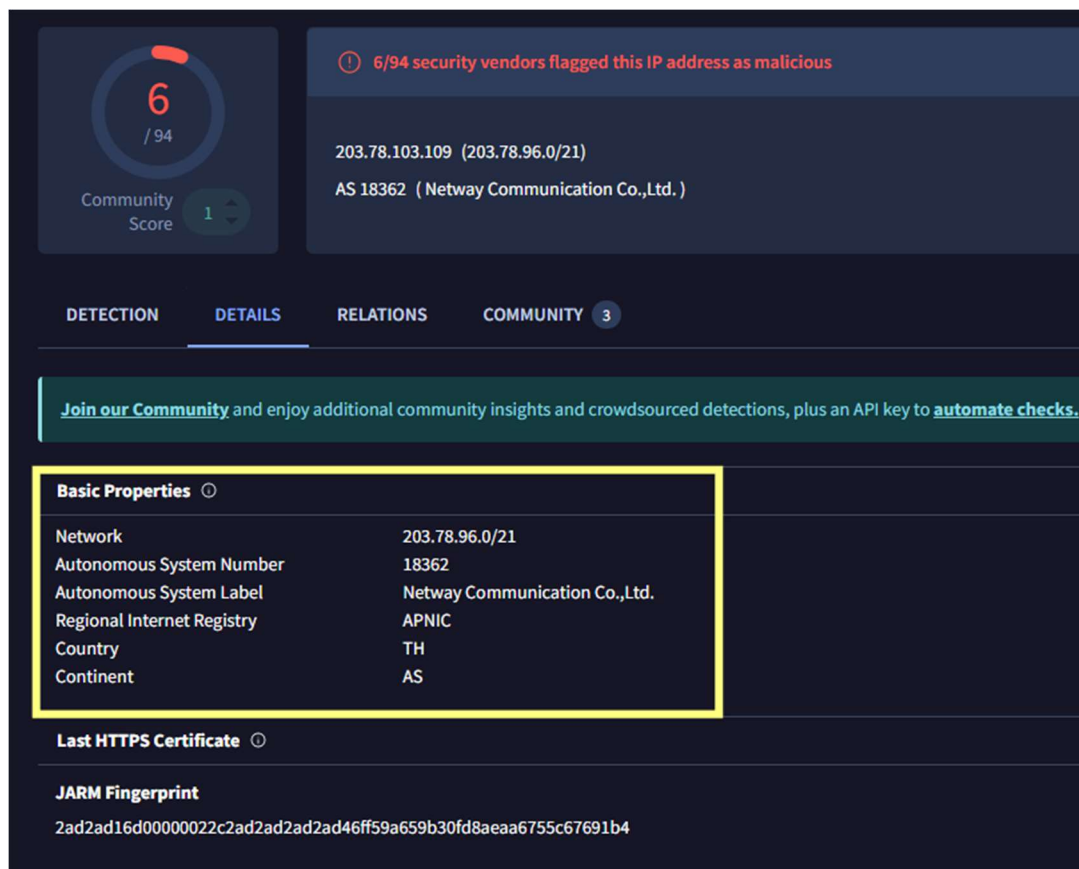


Fig 17: Known adversary structure

- It can not be confirmed the attacker carried out another attack at the same time as this
8. Did the attacker access any other systems?
- Ans: Yes, the attacker access another system (10.42.85.115)
- Process: Loaded PCAP file in Wireshark and filter rdp as that is the protocol the initial attack was done through.

case001.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

rdp

No.	Time	Source	Destination	Protocol	Length	Info
232...	15818.5773...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15818.5791...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15818.8037...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15818.8055...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15819.0297...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15819.0315...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15819.2555...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15819.2573...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15819.4830...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15819.4847...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15819.6965...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15819.6984...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15840.8419...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15840.8432...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15869.1946...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
232...	15869.1964...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
265...	16667.8216...	10.42.85.10	10.42.85.115	RDP	73	Negotiate Request
265...	16667.8943...	10.42.85.115	10.42.85.10	RDP	73	Negotiate Response
387...	17876.0689...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Administrator, Negotiate Request
387...	17876.0721...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response

Source: VMware_e1:84:e6 (00:0c:29:e1:84:e6)

... ..0 = IG bit: Individual address (unicast)

... ..0 = LG bit: Globally unique address (factory default)

... ..0 = IG bit: Individual address (unicast)

Fig 18: Other System Attacked

- How?

Ans: A connection request was done through open port 3389 which reveals it was through remote desktop protocol which the other system acknowledged.

232...	15840.8432...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
232...	15869.1946...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Admini
232...	15869.1964...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response
265...	16667.8216...	10.42.85.10	10.42.85.115	RDP	73	Negotiate Request
265...	16667.8943...	10.42.85.115	10.42.85.10	RDP	73	Negotiate Response
387...	17876.0689...	194.61.24.102	10.42.85.10	RDP	117	Cookie: msthash=Admini
387...	17876.0721...	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response

Destination Address: 10.42.85.115
[Stream index: 6]

Transmission Control Protocol, Src Port: 62514, Dst Port: 3389, Seq: 1, Ack: 1, Len: 19

TPKT, Version: 3, Length: 19

ISO 8073/X.224 COTP Connection-Oriented Transport Protocol

Remote Desktop Protocol

Type: RDP Negotiation Request (0x01)

Flags: 0x00

... ..0 = Restricted admin mode required: False

... ..0 = Redirected Authentication required: False

... 0... = Correlation info present: False

Length: 8

requestedProtocols: 0x0000000b, TLS security supported, CredSSP supported, CredSSP with

Fig 19: Attack Route

- When?

Ans: Sept 19, 2020 2:35:55 UTC

252...	15805.1704...	10.42.85.10	194.61.24.102	RDP	85 Negotiate Response
265...	16667.8216...	10.42.85.10	10.42.85.115	RDP	73 Negotiate Request
265...	16667.8943...	10.42.85.115	10.42.85.10	RDP	73 Negotiate Response
387...	17876.0689...	194.61.24.102	10.42.85.10	RDP	117 Cookie: msthash=Administrator,
387...	17876.0721...	10.42.85.10	194.61.24.102	RDP	85 Negotiate Response


```

Frame 265214: 73 bytes on wire (584 bits), 73 bytes captured (584 bits) on interface unknown, id 0
  Section number: 1
  ▾ Interface id: 0 (unknown)
    Interface name: unknown
    Encapsulation type: Ethernet (1)
    Arrival Time: Sep 18, 2020 22:35:55.291953000 Eastern Daylight Time
    UTC Arrival Time: Sep 19, 2020 02:35:55.291953000 UTC
    Epoch Arrival Time: 1600482955.291953000
    [Time shift for this packet: 0.000000000 seconds]
    [Time delta from previous captured frame: 0.000609000 seconds]
    [Time delta from previous displayed frame: 798.625191000 seconds]
    [Time since reference or first frame: 16667.821630000 seconds]
    Frame Number: 265214
    Frame Length: 73 bytes (584 bits)
    Capture Length: 73 bytes (584 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
  
```

Fig 20. Time of Attack

- Was data exfiltrated or accessed?

Ans: Yes, it was

Process: Loaded PCAP file on Wireshark and filtered ip.addr==203.78.103.109

&& tcp.port==443 at Sept 19, 2020 02:25:18 UTC

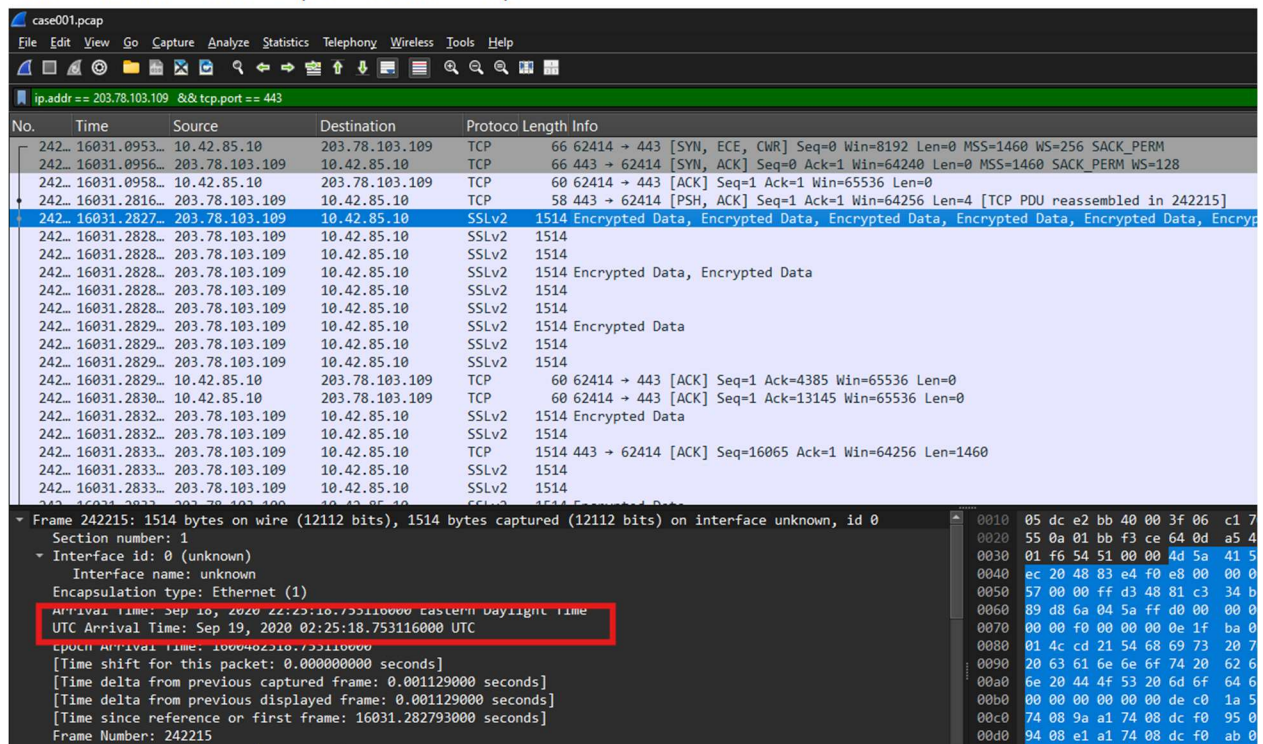


Fig 21: Data access and time

9. Network Layout

Ans: Network --Desktop (10.42.85.10) -----Server (10.42.85.115)

Process: The IP addresses were found in the registry path

(ControlSet001>Services>Tcpip>Parameters>Interfaces) which was from the imported hives of the server (C:\Users\student\Desktop\ForensicsProject\DC01\DC01-ProtectedFiles\Protected\system), and desktop

(C:\Users\student\Desktop\ForensicsProject\Desktop\DESKTOP-SDN1RPTProtectedFiles\Protected Files\system)

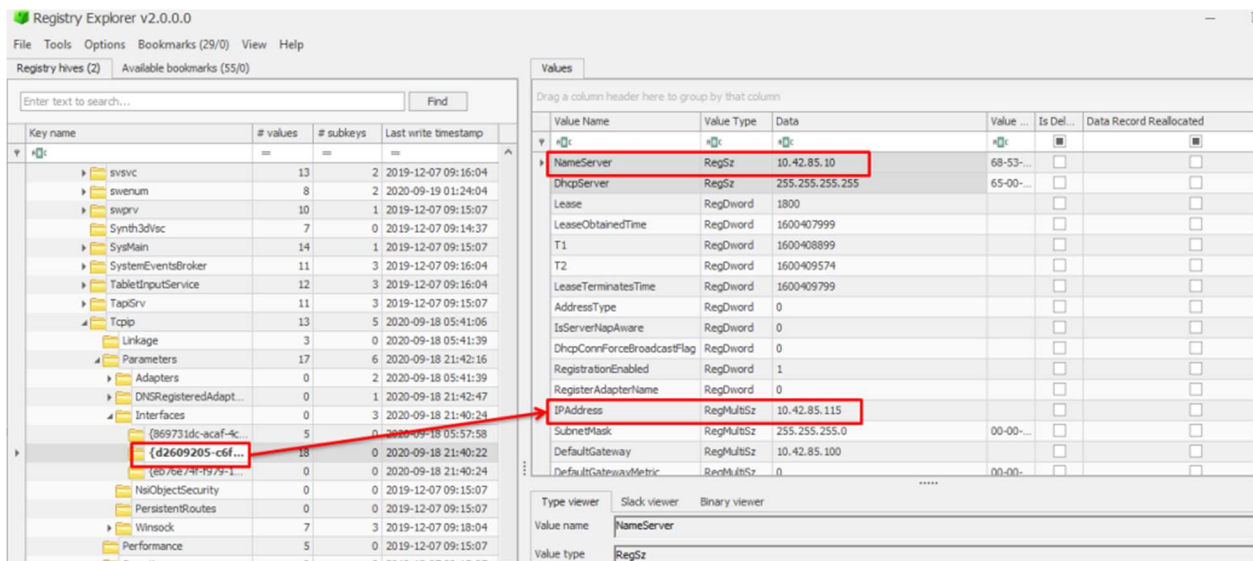


Fig 15: Server IP address

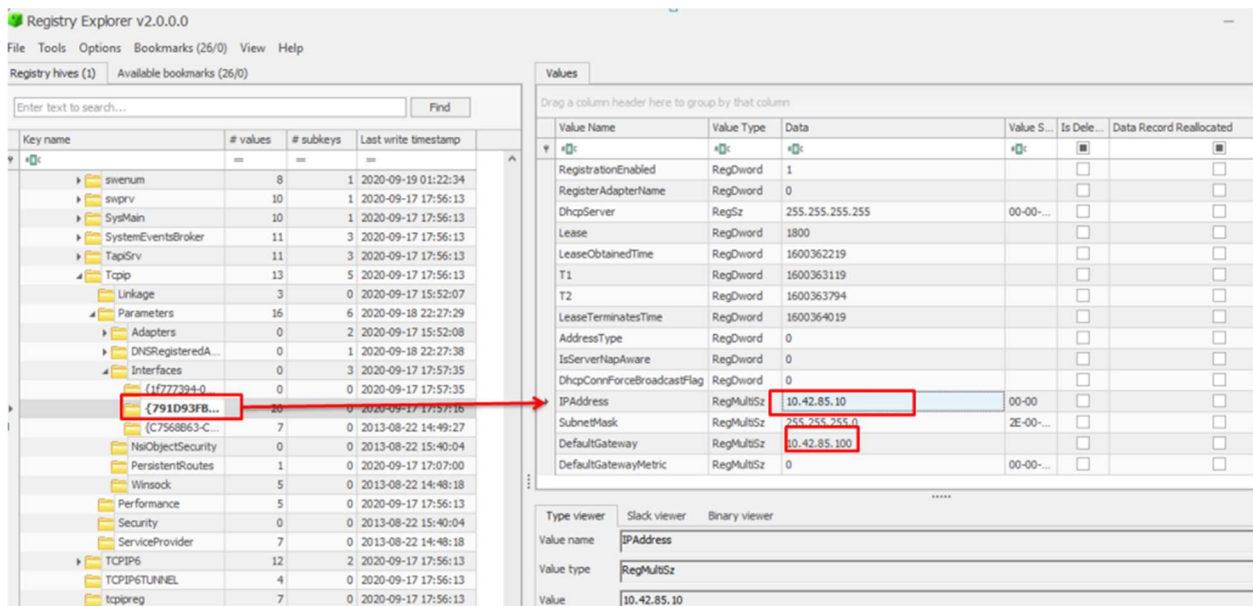


Fig 16: Desktop IP address.

Recommendation

- Require multi-factor authentication (MFA) for all Remote Desktop Protocol (RDP) access points.
- Restrict RDP access from external networks unless absolutely necessary and rely on VPNs for secure remote access.
- Deploy endpoint detection and response (EDR) tools, such as antivirus software, to monitor for unusual activities and potential malware infections.
- Regularly update and patch systems to fix vulnerabilities that could be exploited for unauthorized access.
- Revise incident response procedures to include comprehensive steps for detecting and addressing RDP-related attacks.
- Educate employees to identify and report phishing attempts and other social engineering tactics used to gain unauthorized access.

Reference

JoeSandbox. (2025). *Analysis report of 398583*. JoeSandbox.

<https://www.joesandbox.com/analysis/398583/0/html>

VirusTotal. (2025, January 30).

10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6. Retrieved from

<https://www.virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6/behavior>

The stolen Szechuan sauce. (2025, January 30). Dfirmadness.

<https://dfirmadness.com/the-stolen-szechuan-sauce/How>

Y. T. (2025). *Volatility* (Version 3.5.2) [Software]. Volatility Foundation.

<https://www.volatilityfoundation.org/>

AccessData. (2025). *FTK (Forensic Toolkit)* (Version 7.0) [Software]. AccessData.

<https://www.accessdata.com/product-download>

The Wireshark Team. (2025). *Wireshark* (Version 4.0) [Software]. Wireshark Foundation.

<https://www.wireshark.org/>