The Stolen Szechuan Sauce

Sabah Diiriye and Raquel Bueno

October 23, 2023

Lighthouse Labs

Executive Summary

In the realm of increasingly complex cyber threats, our project investigates a simulated cyber incident called "The Stolen Szechuan Sauce," crafted by DFIR Madness to emulate real-world scenarios. Utilizing forensic tools such as Autopsy, FTK Imager, Volatility, and Wireshark, our team—comprising Sabah and Raquel—developed into disk images, packet captures, and memory dumps from two implicated systems: a Microsoft Windows Server 2012 and a Windows 10 desktop. Our investigation confirmed a security breach executed through RDP brute-force attacks, identifying the use of a Metasploit Trojan named Coreupdater.exe. We also pinpointed malicious IP addresses 194.61.24.102 and 203.78.103.109 as being involved in the attack. Intriguingly, files in a "Secret" folder were found to be accessed and modified, indicating data compromise. Both systems were part of the same network block 10.42.85.0/24. Conclusively, our findings offer a detailed forensic account, highlighting areas of vulnerability while recommending immediate containment and long-term security enhancements. The insights gained from this investigation not only resolve the questions posed by this particular case but also serve as educational material for future cybersecurity efforts.

Introduction

The landscape of cybersecurity is rife with complexities, requiring experts to not only thwart cyber threats but also to dig deep into the digital remnants left behind during security incidents. One such intricate case that necessitates thorough investigation is the case of "The Stolen Szechuan Sauce." Crafted as a hands-on exercise by DFIR Madness, this project offers a simulated environment that aims to imitate real-world cybersecurity issues. This report serves as a comprehensive account of our digital forensic investigation, delving into the various questions surrounding the cyber event in question.

The scenario involves two distinct computational systems: a server and a desktop each implicated in the cyber event under investigation. We have acquired multiple types of evidence files, ranging from disk images (E01) to packet capture files (PCAP) and memory dumps, to develop a holistic understanding of the incident. By leveraging a range of forensic tools and methodologies, this investigation endeavors to uncover the facts related to the cyber incident, from confirming a breach to identifying malware and tracing the adversary's steps.

Our investigation is framed by a series of questions aimed at driving the inquiry to achieve its intended goals. Each question will be addressed methodically, leveraging appropriate forensic tools and techniques. This report not only documents our findings but also substantiates them with necessary screenshots, logs, and other relevant artifacts.

Due to the extensive nature of the evidence files, this project has been undertaken collaboratively. Both team members have contributed actively to the investigative process, as detailed within the report.

Overview of Forensic Tools

First of all, to understand the analysis done, it is important to know a few key concepts.

According to Forensics College, “Autopsy, it is a digital forensics platform and graphical interface that forensic investigators use to understand what happened on a phone or computer.. Select modules in Autopsy can do timeline analysis, hash filtering, and keyword search. In addition, they can extract web artifacts, recover deleted files from unallocated space, and find indicators of compromise. All of this can be done relatively rapidly”.

According to the same source about FTK Imager, it is possible to learn that it is a “tool that analyzes images of a drive and preserves the original integrity of the evidence without affecting its original state”.

Another very important forensic tool according to Forensics College, “the Volatility Foundation focuses on volatile memory (RAM) forensics. This allows the preservation of evidence in memory that would otherwise be lost during a system shutdown”.

Wireshark is the world’s most-used network protocol analysis tool, that according to the same source “implemented by governments, private corporations, and academic institutions worldwide. Wireshark lets a user see what is happening on a network at the microscopic level. By capturing network traffic, users can then scan for malicious activity”.

Considerations

The project was written and analyzed by both students, Sabah and Raquel, together via google doc and zoom meetings, respectively.

Raquel was responsible to download the six first files while Sabah downloaded the Desktop files, as shown below:

DC01 Disk Image (EO1)

DC01 Memory and PageFile

DC01 Autoruns

DC01 Protected Files

Case001 PCAP

Desktop Disk Image (E01)

Desktop Memory and PageFile

Desktop Autoruns

Desktop Protected Files

To verify file integrity in Windows Powershell, from the Download Dir: Get-FileHash -Algorithm md5 *

To verify file integrity in Linux, from the Download Dir: md5sum *

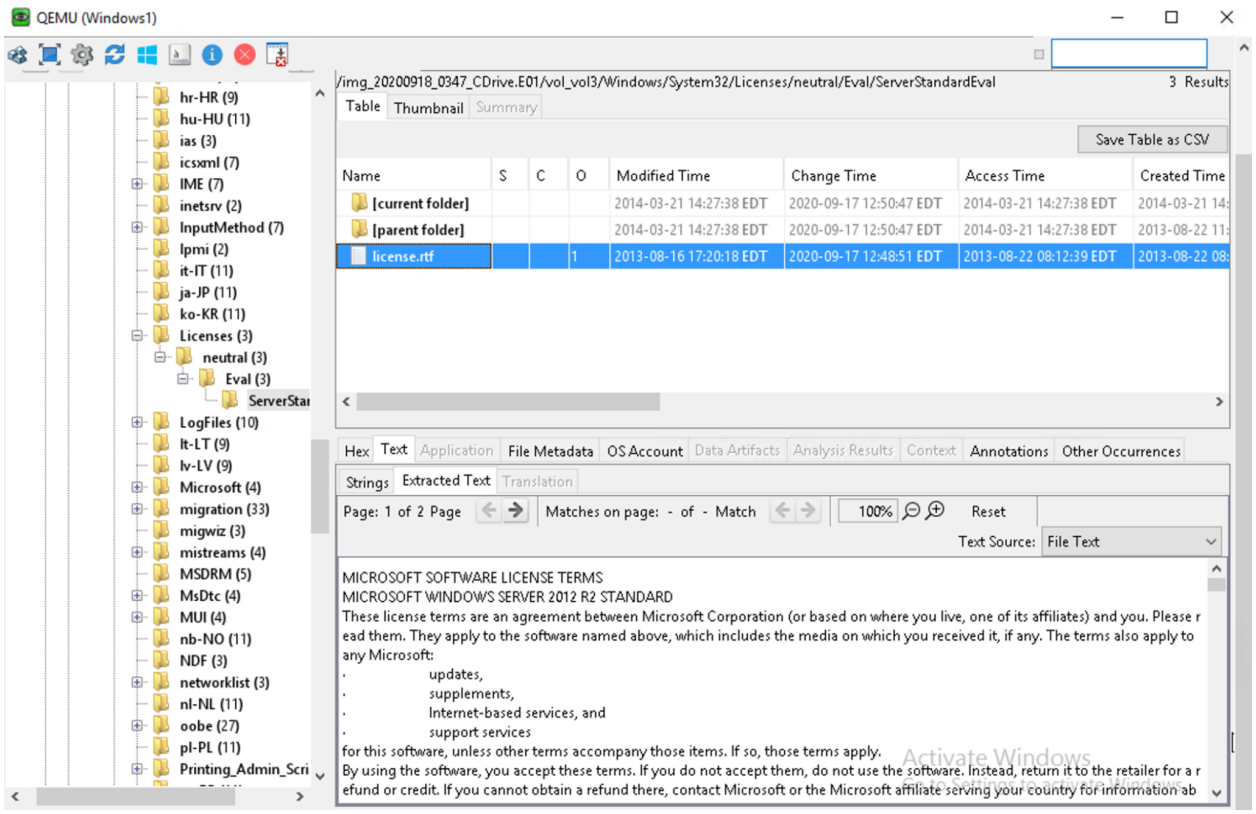
MD5 422046B753CF8A4DF49D2C4CE892DB16 case001-pcap.zip
MD5 964F2D710687D170C77C94947DA29E66 DC01-autorunsc.zip
MD5 E57FC636E833C5F1AB58DFACE873BBDE DC01-E01.zip
MD5 64A4E2CB47138084A5C2878066B2D7B1 DC01-memory.zip
MD5 964EEAF0009D08CC101DE4A83A4E5D23 DC01-pagefile.zip
MD5 AD29830A583EFE49C8C1C35FAFFD264F DC01-ProtectedFiles.zip
MD5 71C5C3509331F472ABCDF81EB6EFFF07 DESKTOP-E01.zip
MD5 3627DCAFA54E1365489A4EC0CC3D6A1C DESKTOP-SDN1RPT-autrunsc.zip
MD5 CF31E2635C77811AAA1BB04A92A721E2 DESKTOP-SDN1RPT-memory.zip
MD5 45C096F2688A0B5DE0346FB72391B245 Desktop-SDN1RPT-pagefile.zip
MD5 3E1A358D50003A9351AC2160AE6F0495 DESKTOP-SDN1RPT-Protected Files.zip

Question

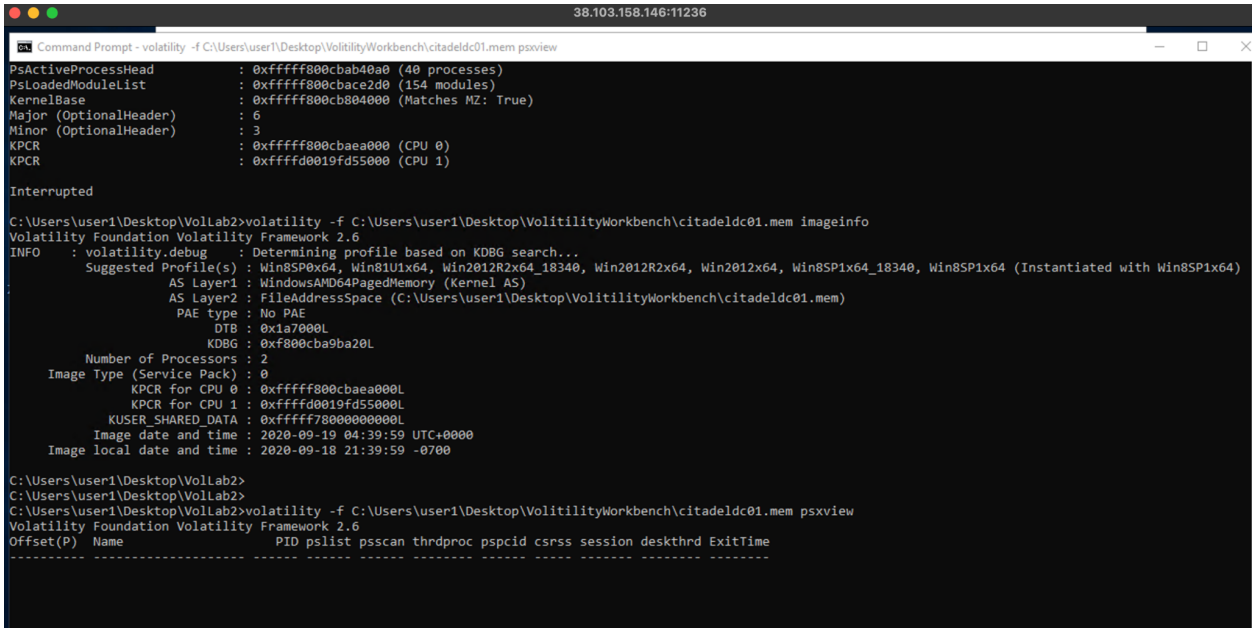
1. What's the Operating System of the Server?

The Operating System is Microsoft Windows Server 2012.

Using Autopsy, we were able to identify the OS in the file tree.

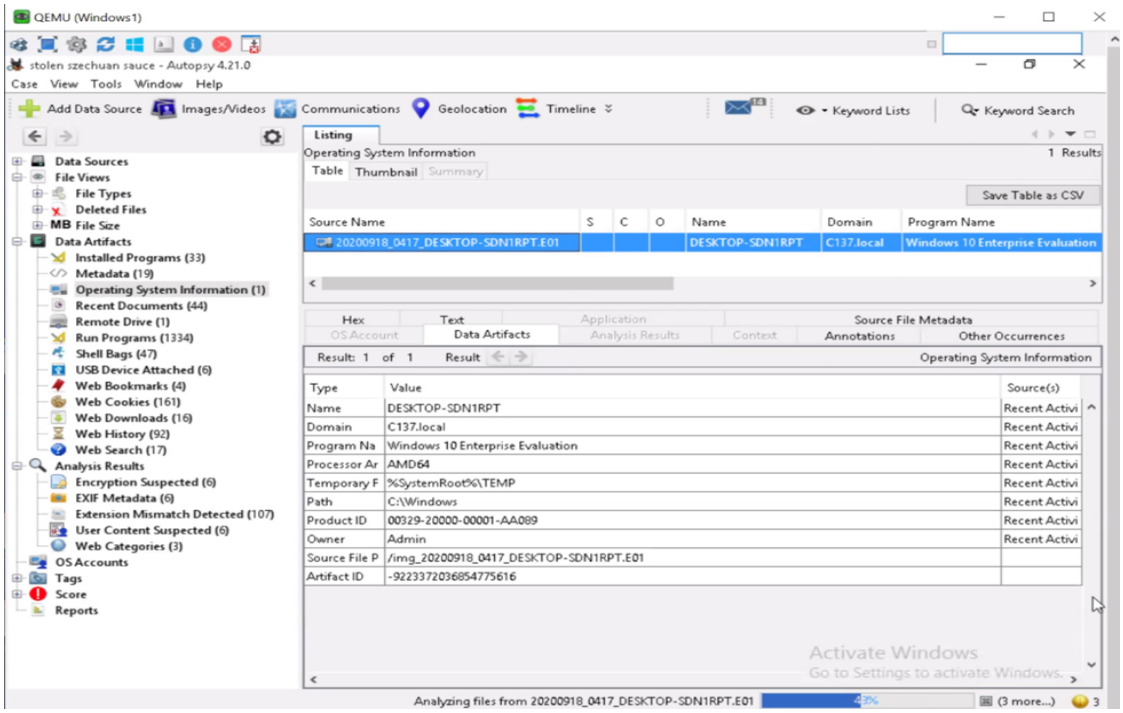


And also using Volatility, we were to prove that the server is Windows 2012, as shown in the image below.



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

The operating system of the desktop is Windows 10, and the way this was found using Autopsy.

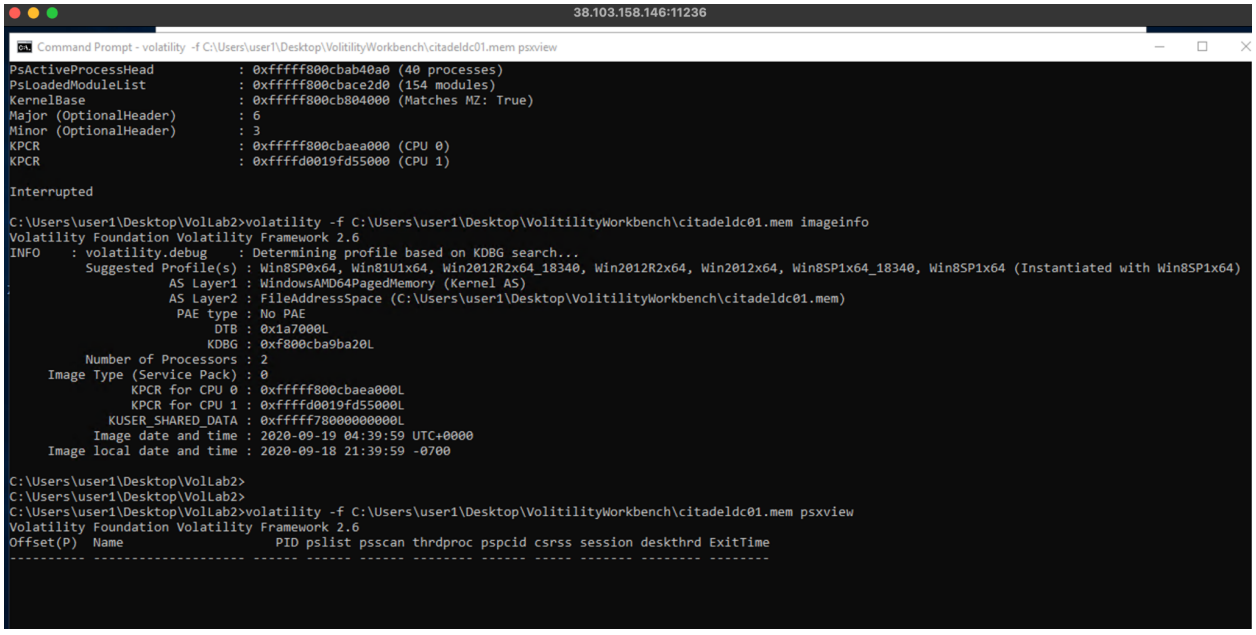


3. What was the local time of the Server?

According to dfirmadness.com, there is a note that says: ”Incident occurred at an organization located in Colorado in September. So, this places the incident at UTC-6”.

> **Note:** This incident occurred at an organization located in Colorado in September. So, this places the incident at UTC -6. Keep this in mind when looking at the output of various tools.

So, it is safe to say that it is talking about Mountain Standard Time (MST).



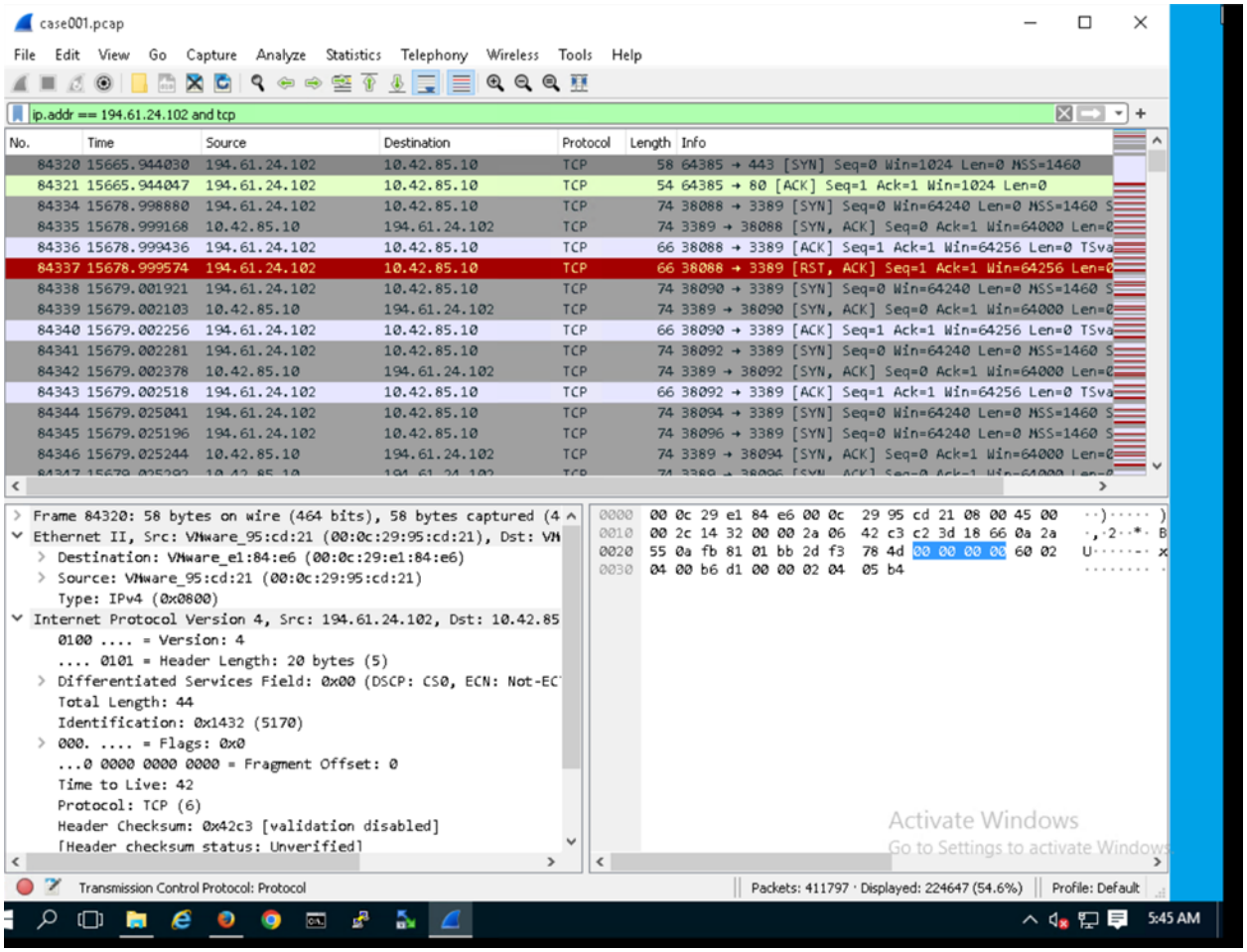
However, when we used Volatility to read the memory, we found that the image local time was 21:39:49 (UTC -0700).

4. Was there a breach?

Yes, it will be provided more information throughout this project.

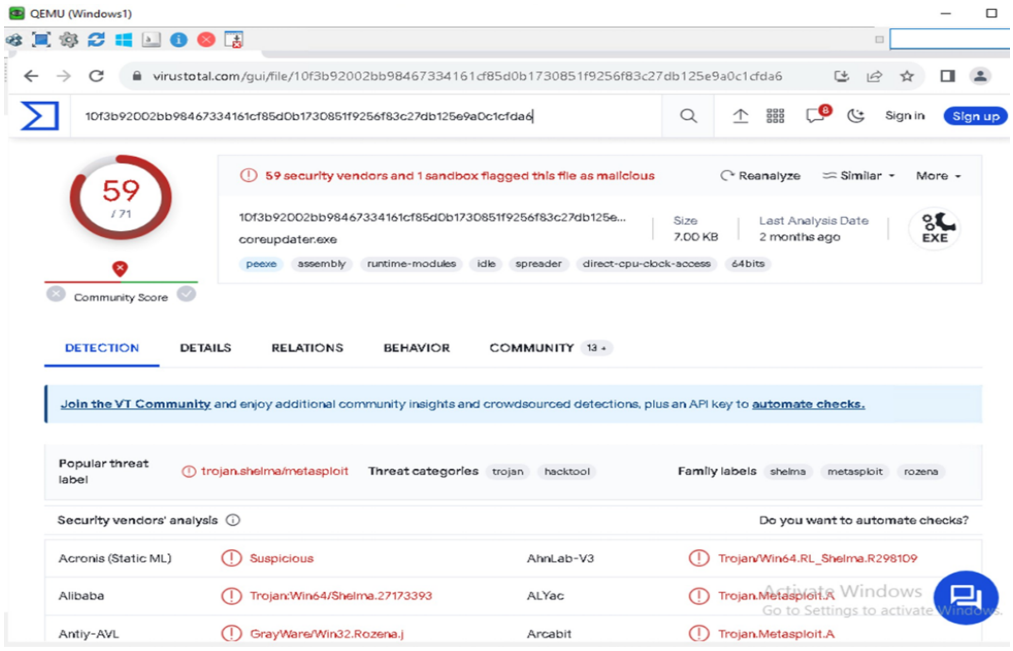
5. What was the initial entry vector (how did they get in)?

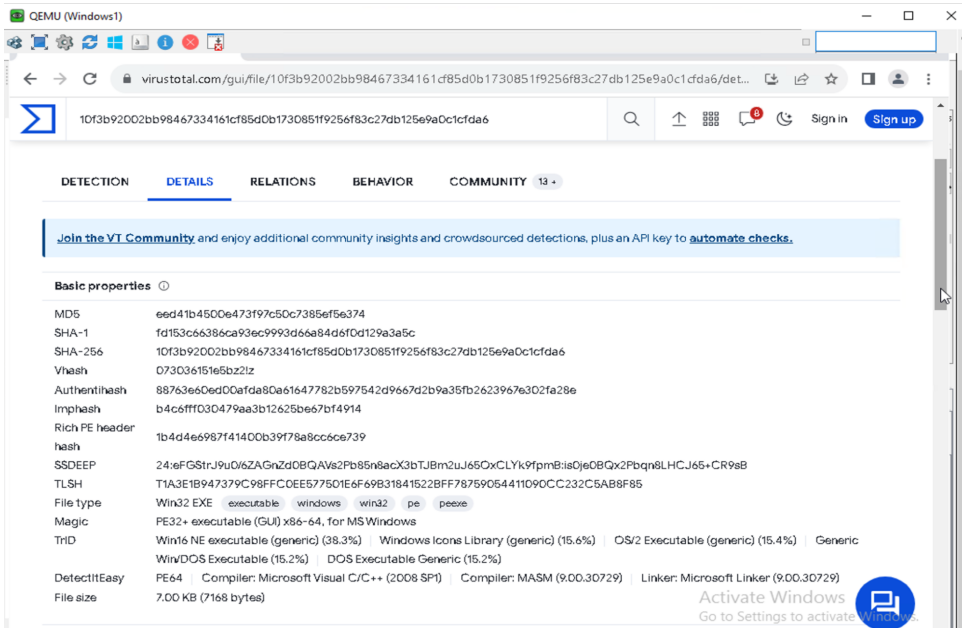
The initial attack vector was identified as RDP brute force, as evidenced by multiple SYN requests targeting the same destination port. This observation was made using the filter ip.addr==194.61.24.102 and tcp in the analysis of the case001.PCAP file.



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

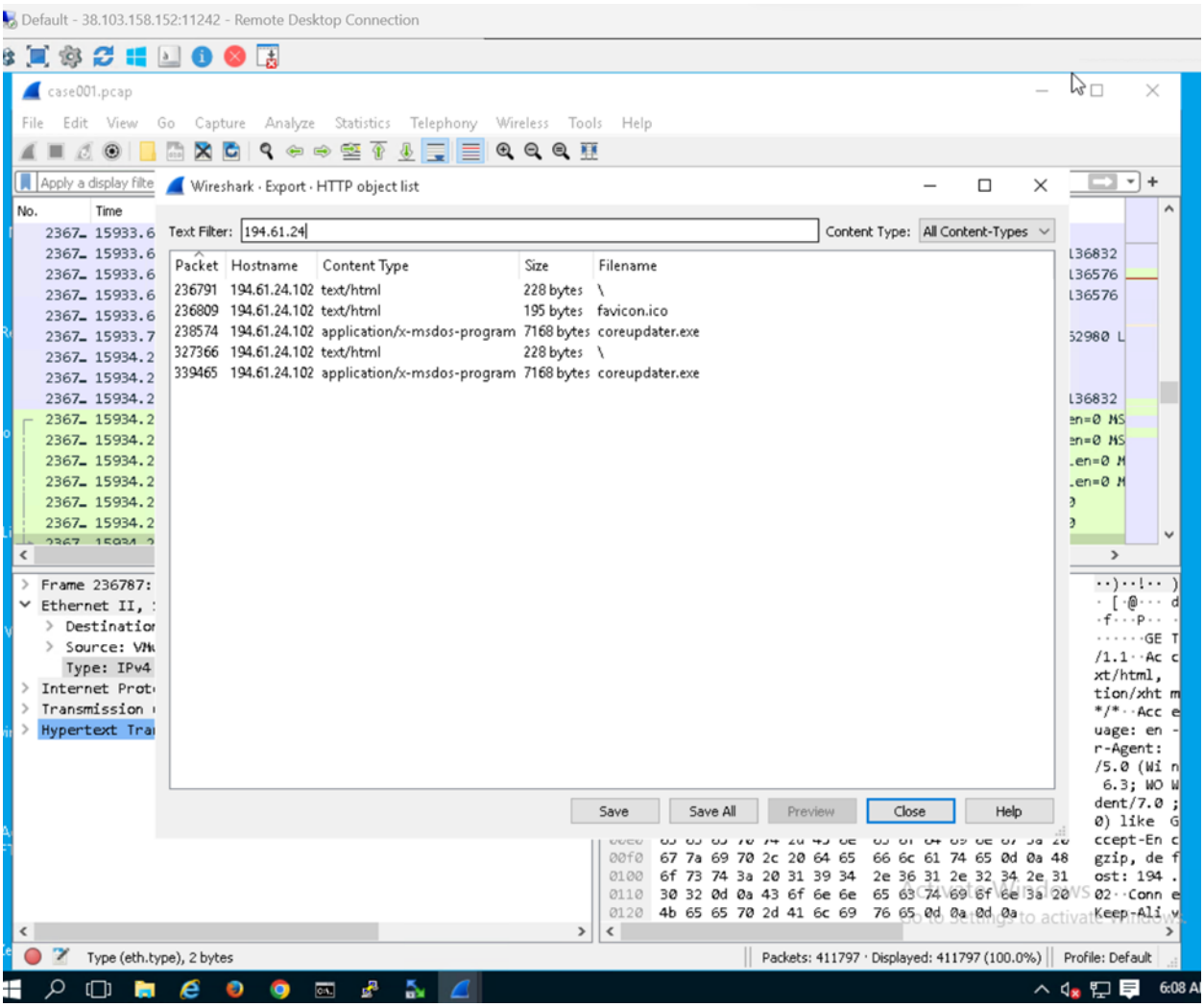
Malware was indeed employed in the form of a metasploit Trojan. To verify the malicious nature of the Coreupdater.exe process, it can be analyzed using threat detection platforms like VirusTotal.





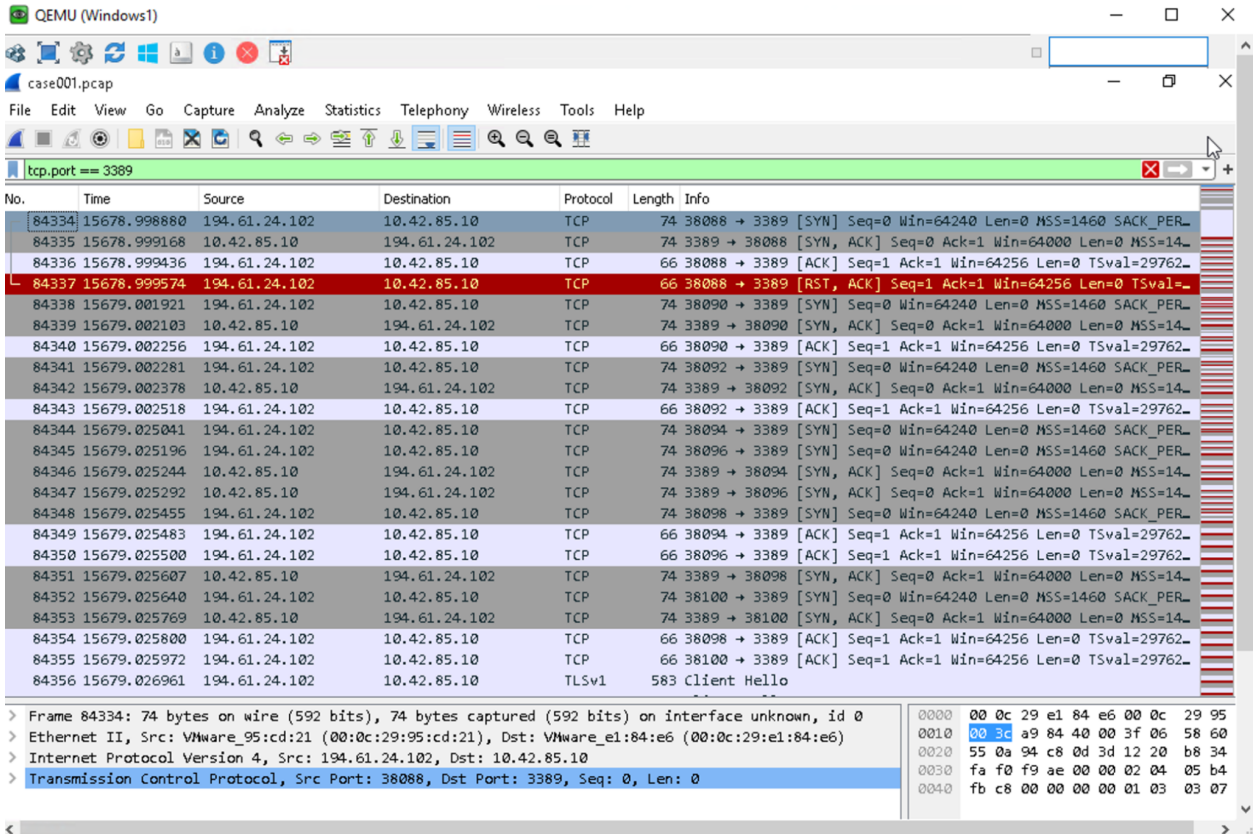
- **What process was malicious?**

The Malicious process identified during the investigation was Coreupdater.exe, which was recognized as a Metasploit Trojan. Further validation of its malicious nature was conducted by analyzing the file to examine it.



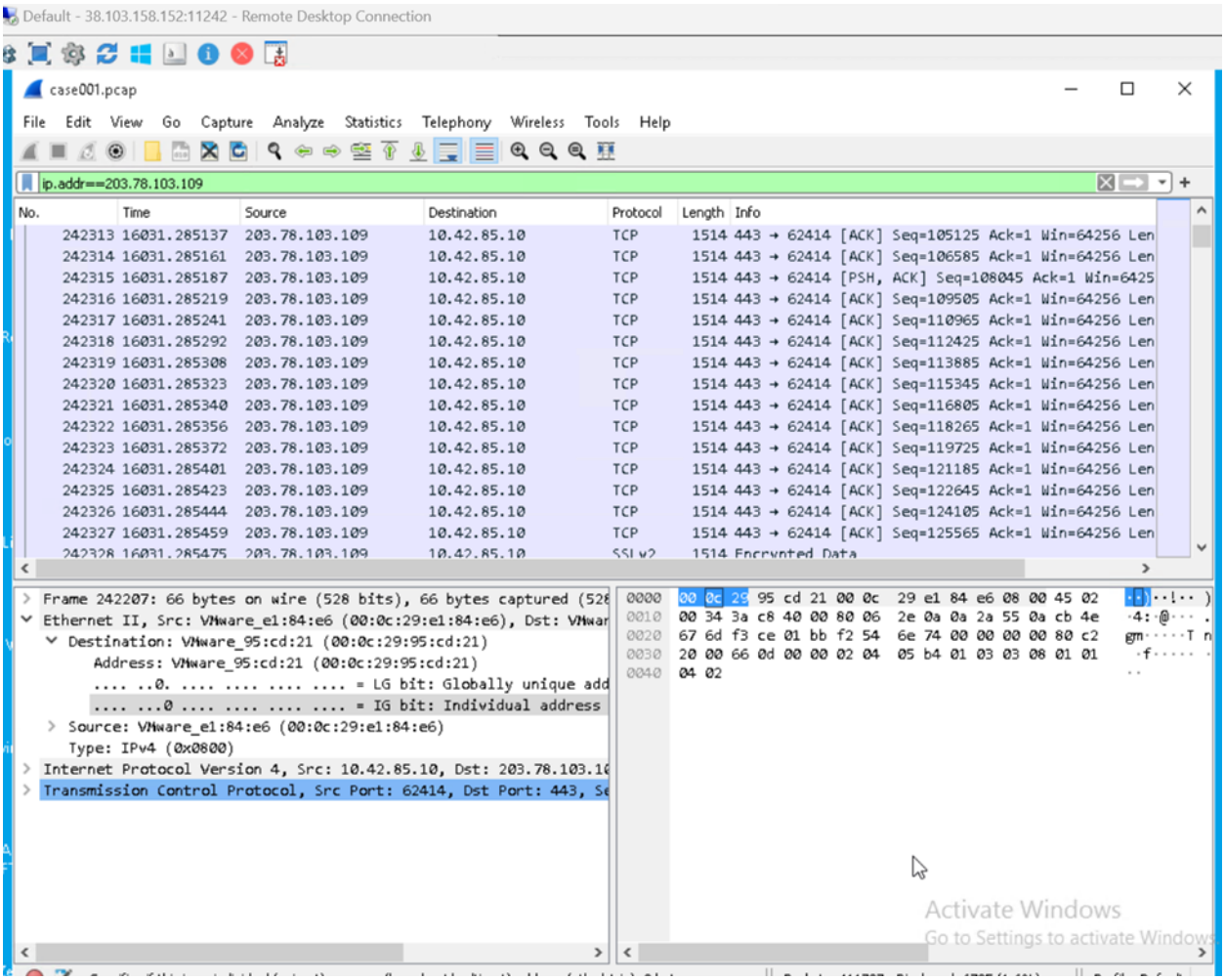
- **Identify the IP Address that delivered the payload?**

As observed in the packet capture data, the IP address 194.61.24.102 repeatedly initiated SYN requests targeted at the RDP port 3389, originating from a variety of source ports.



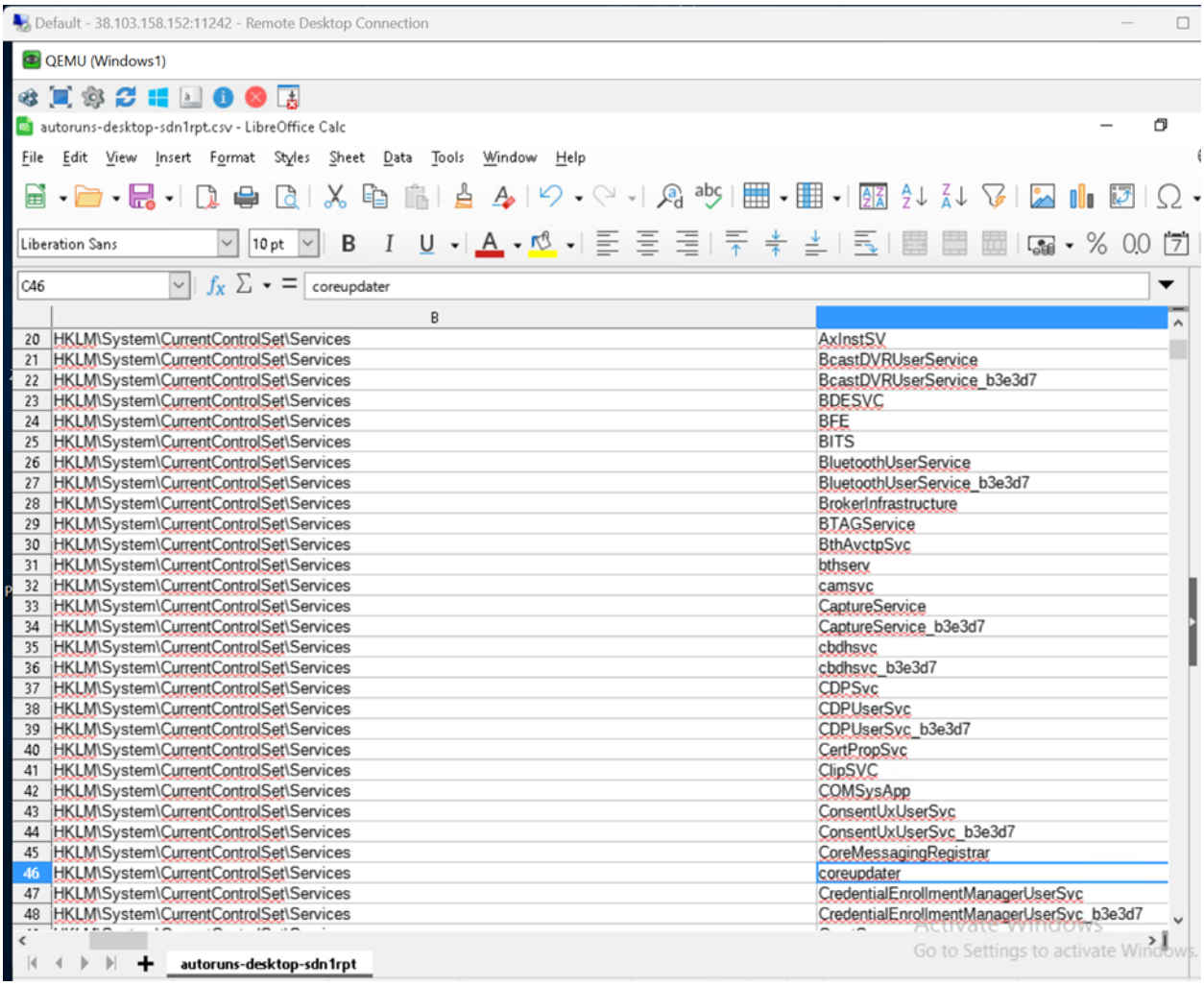
- **What IP Address is the malware calling to?**

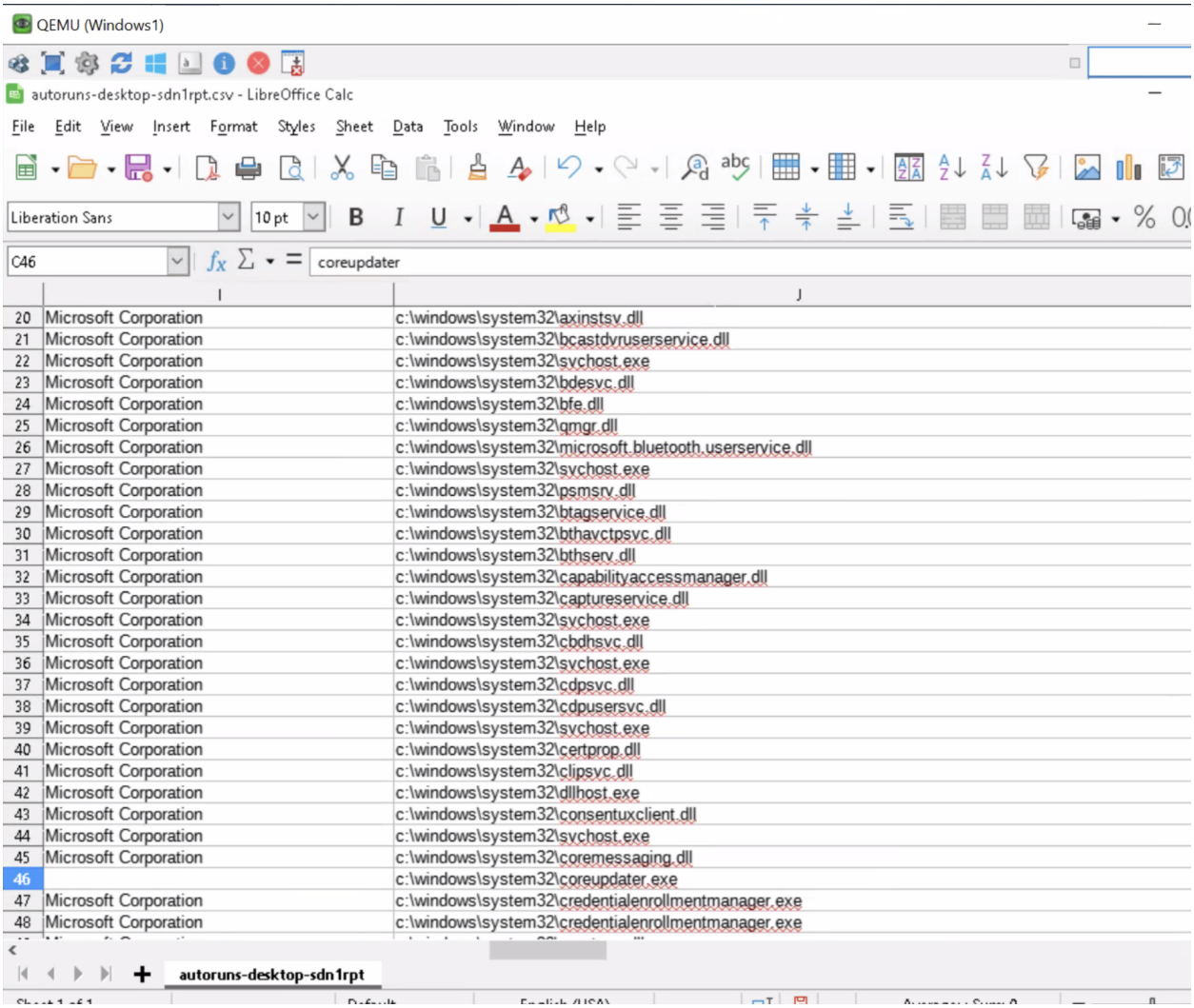
In the PCAP file analysis, we noticed that the malware is establishing outgoing connections to a specific address. The most frequently contacted IP in the dataset was 203.78.103.109.



- **Where is this malware on disk?**

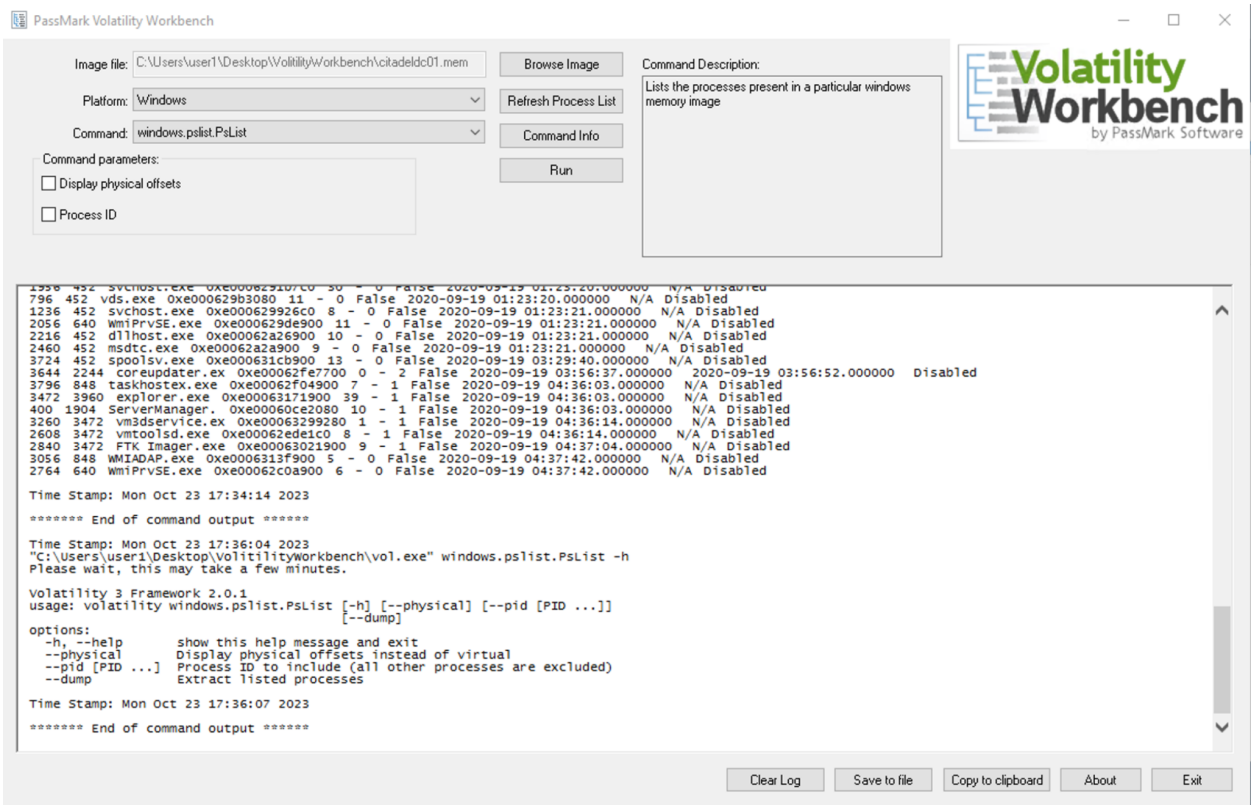
The malware is located on the disk at following file path `C:\Windows\System32\coreupdater.exe`.




QEMU (Windows1)
autoruns-desktop-sdn1rpt.csv - LibreOffice Calc
File Edit View Insert Format Styles Sheet Data Tools Window Help
Liberation Sans
10 pt
C46
coreupdater
I
J
20 Microsoft Corporation c:\windows\system32\axinstsv.dll
21 Microsoft Corporation c:\windows\system32\bcastdvruserservice.dll
22 Microsoft Corporation c:\windows\system32\svchost.exe
23 Microsoft Corporation c:\windows\system32\bdesvc.dll
24 Microsoft Corporation c:\windows\system32\bfe.dll
25 Microsoft Corporation c:\windows\system32\qmgr.dll
26 Microsoft Corporation c:\windows\system32\microsoft.bluetooth.userservice.dll
27 Microsoft Corporation c:\windows\system32\svchost.exe
28 Microsoft Corporation c:\windows\system32\psmsrv.dll
29 Microsoft Corporation c:\windows\system32\btagservice.dll
30 Microsoft Corporation c:\windows\system32\bthavctpsvc.dll
31 Microsoft Corporation c:\windows\system32\bthserv.dll
32 Microsoft Corporation c:\windows\system32\capabilityaccessmanager.dll
33 Microsoft Corporation c:\windows\system32\captureservice.dll
34 Microsoft Corporation c:\windows\system32\svchost.exe
35 Microsoft Corporation c:\windows\system32\cbdhsvc.dll
36 Microsoft Corporation c:\windows\system32\svchost.exe
37 Microsoft Corporation c:\windows\system32\cdpsvc.dll
38 Microsoft Corporation c:\windows\system32\cdpusersvc.dll
39 Microsoft Corporation c:\windows\system32\svchost.exe
40 Microsoft Corporation c:\windows\system32\certprop.dll
41 Microsoft Corporation c:\windows\system32\clipsvc.dll
42 Microsoft Corporation c:\windows\system32\dllhost.exe
43 Microsoft Corporation c:\windows\system32\consentuxclient.dll
44 Microsoft Corporation c:\windows\system32\svchost.exe
45 Microsoft Corporation c:\windows\system32\coremessaging.dll
46 c:\windows\system32\coreupdater.exe
47 Microsoft Corporation c:\windows\system32\credentialenrollmentmanager.exe
48 Microsoft Corporation c:\windows\system32\credentialenrollmentmanager.exe
autoruns-desktop-sdn1rpt

- **When did it first appear?**

According to Volatility Workbench, the malware (coreupdater.exe) first appeared on the disk on 202-09-19 03:56:37.



- **What were the capabilities of this malware?**

The malware possesses the following capabilities:

★ Data Exfiltration: It can steal confidential information such as passwords or trade secrets.
★ Remote Administration: It enables the intruder to remotely manage the compromised system through a backdoor.
★ Encryption and Ransom Requirement: Often seen in ransomware types, it can encode files and request payment for their release.
★ Lateral Movement: The malware can disseminate itself to other contacts or systems within the same network.
★ System Sabotage: In specific instances, the malware can deliberately disable or entirely wipe out your computing resources, resulting in substantial damage.

- **Is this malware easily obtained?**

The malicious software was detected relocating itself from the Administrator's Downloads folder to a critical system directory, namely C:\Windows\System32. Such behavior implies an attempt by the malware to conceal itself among key system files, potentially to establish long-term persistence and exert greater control over the system.

- **Was this malware installed with persistence on any machine?**

Yes, it was integrated both into the Windows registry and as a system service. Following a successful brute-force attack on the domain controller, the malware was laterally transferred into the system, embedding itself within the registry processes.

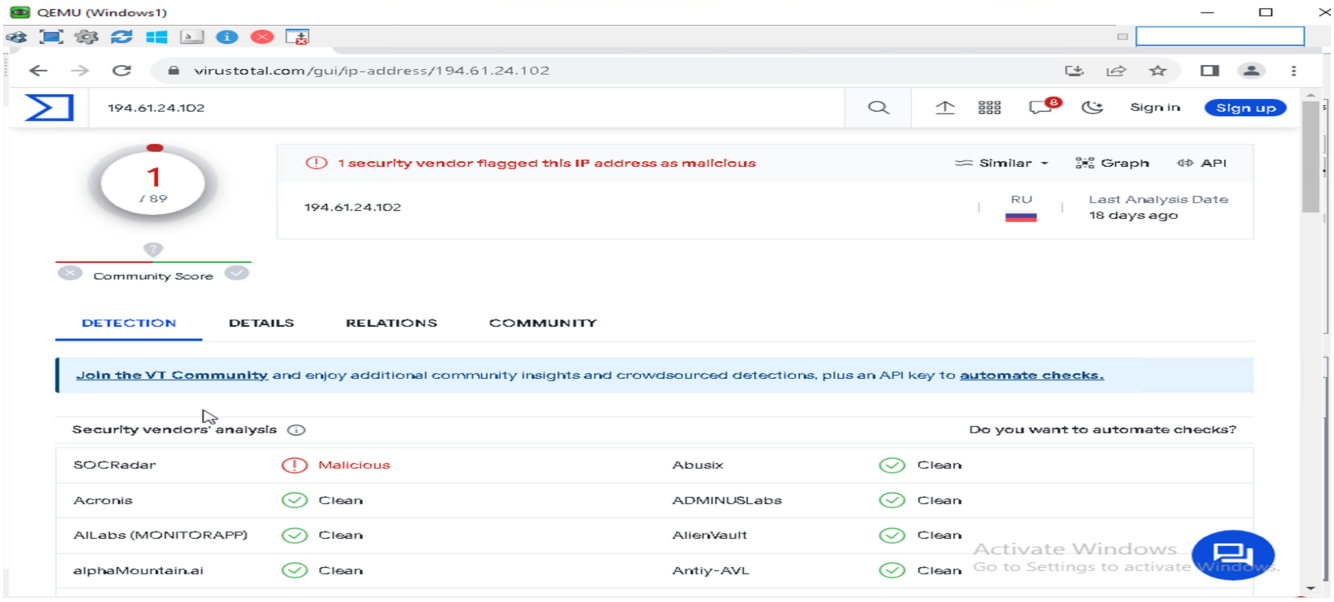
7. What malicious IP Addresses were involved?

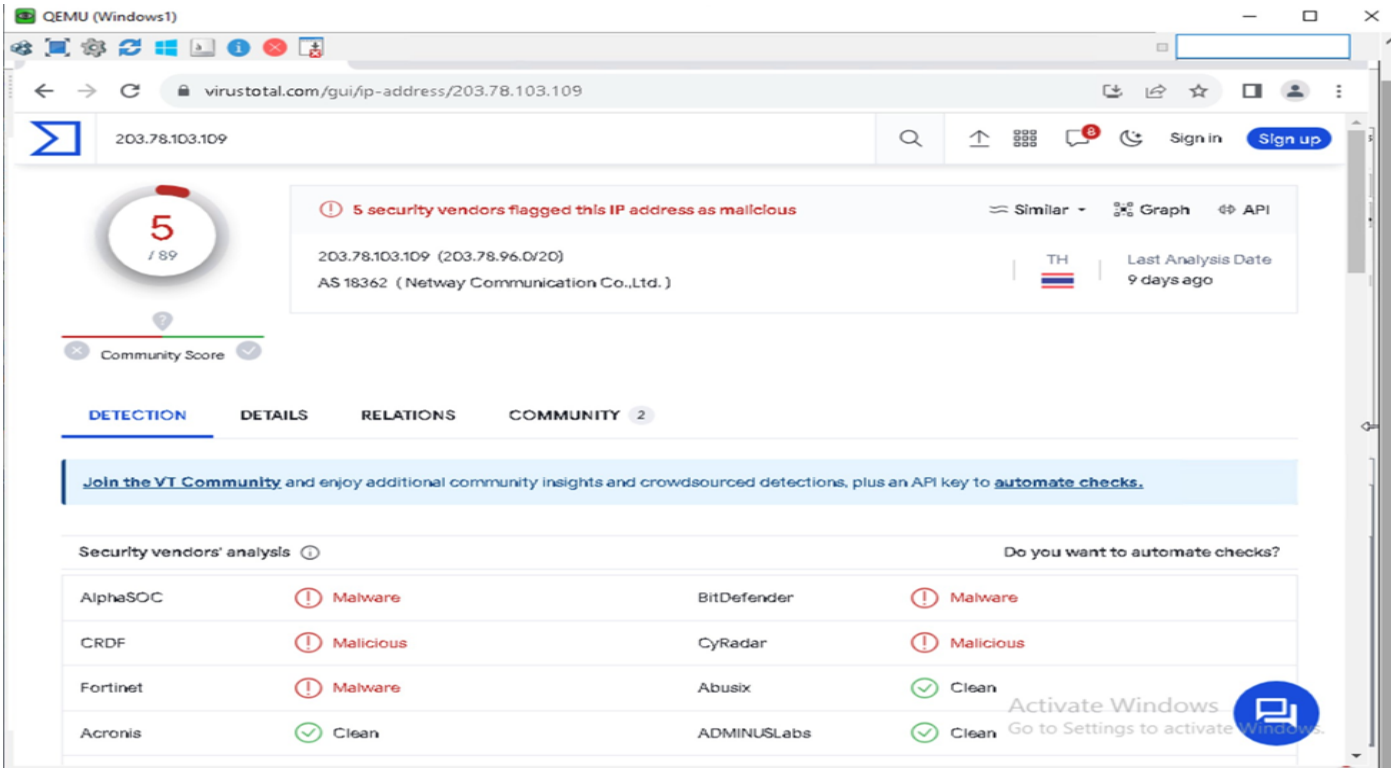
1. Were any IP Addresses from known adversary infrastructure?

The IP addresses identified as malicious in this case were 194.61.24.102 and 203.78.103.109. Prior to the incident, 194.61.24.102 was already flagged for involvement in RDP Brute Force attacks. Meanwhile, 203.78.103.109 had a brief association with the domain happydoghappycat-th.com, which is suspected of involvement with an Advanced Persistent Threat (APT). As shown in the pictures below.

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

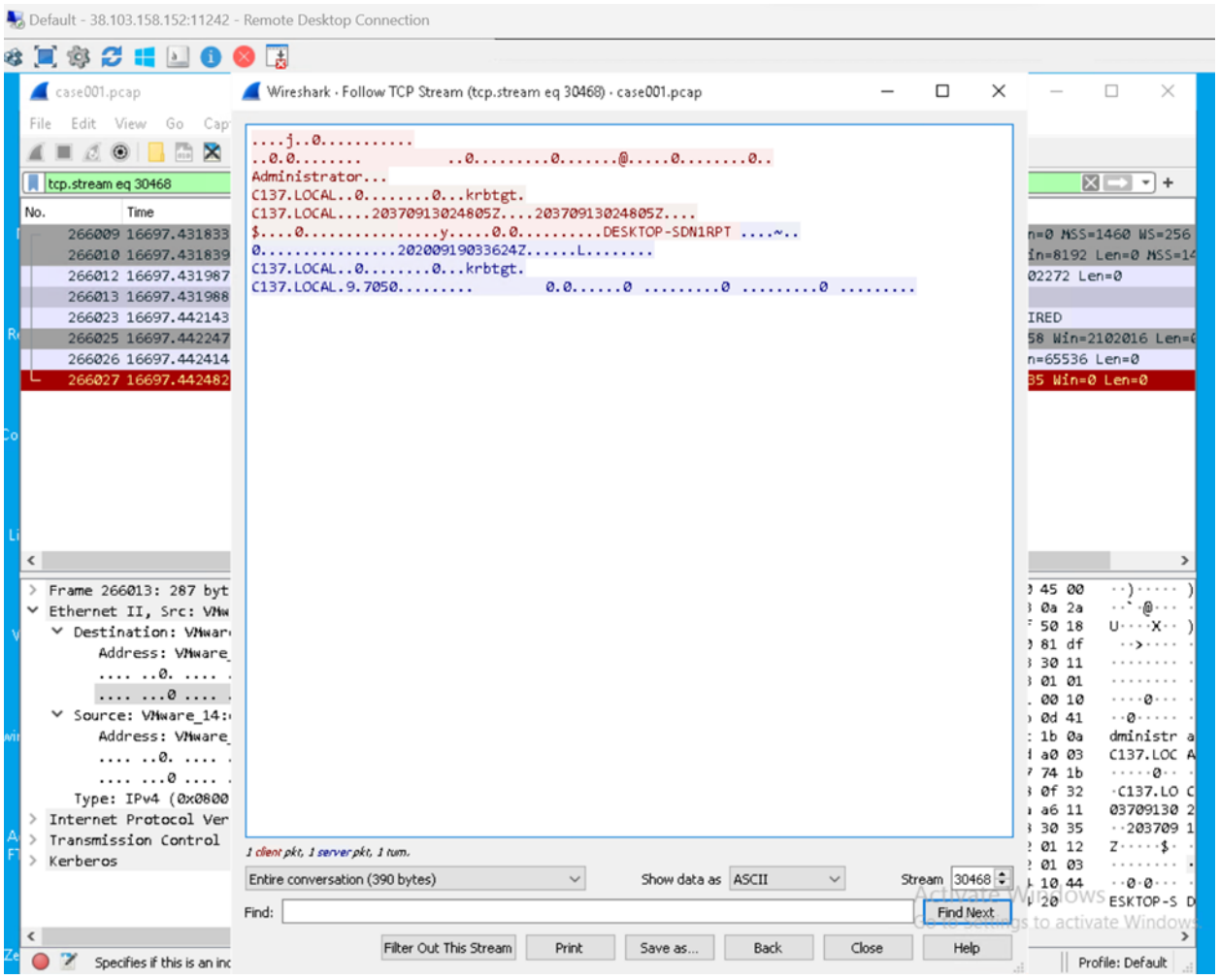
Only these two IP addresses participated in the attack. It is possible to see that in the pictures below.





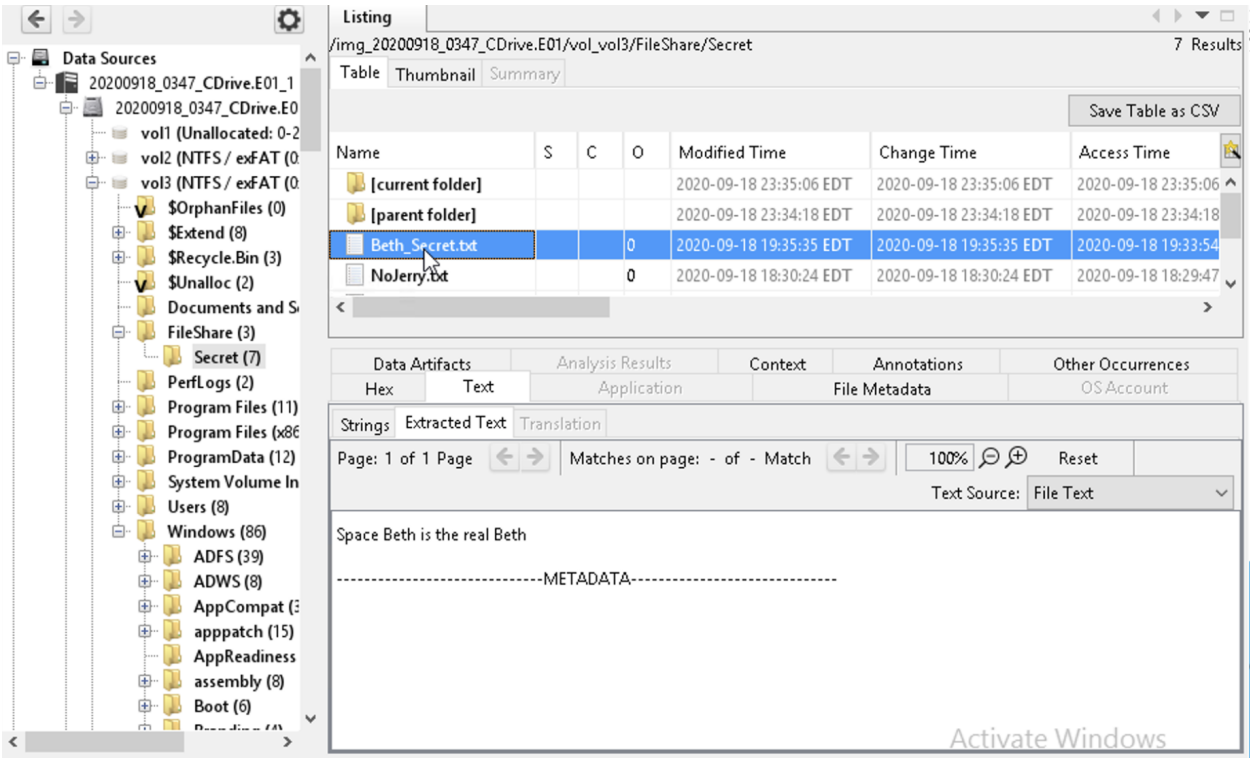
8. Did the attacker access any other systems?

The intrusion successfully gained access to C137\DESKTOP-SDN1RPT$ by leveraging Remote Desktop Protocol (RDP) from the Domain Controller (DC), utilizing the Administrator account. We discovered this behavior in the packet capture (pcap) file.

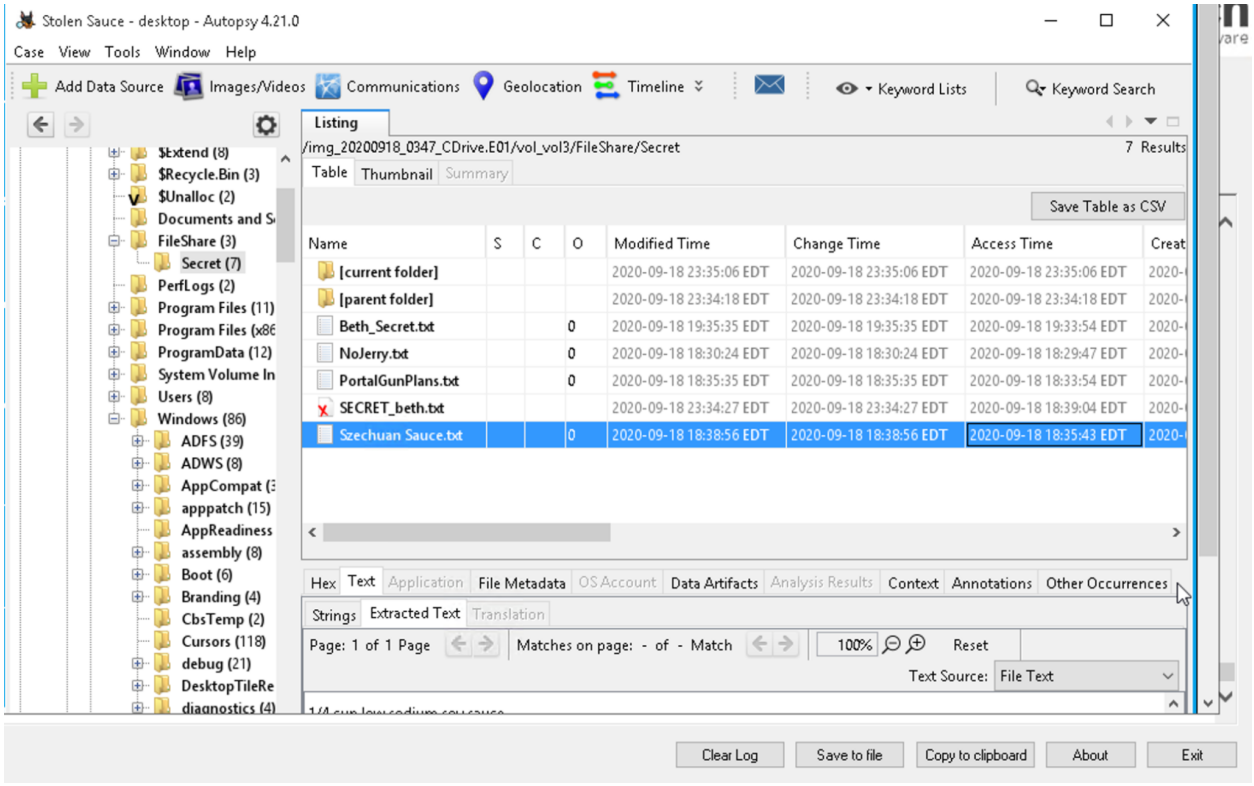

Default - 38.103.158.152:11242 - Remote Desktop Connection
case001.pcap
Wireshark · Follow TCP Stream (tcp.stream eq 30468) · case001.pcap
tcp.stream eq 30468
Administrator...
C137.LOCAL..0.....0...krbtgt.
C137.LOCAL....20370913024805Z....20370913024805Z....
DESKTOP-SDN1RPT
20200919033624Z
C137.LOCAL..0.....0...krbtgt.
C137.LOCAL.9.7050.....
1 client pkt, 1 server pkt, 1 turn.
Entire conversation (390 bytes)
Show data as ASCII
Stream 30468
Find:
Find Next
Filter Out This Stream
Print
Save as...
Back
Close
Help
Profile: Default

3. Did the attacker steal or access any data?

Using Autopsy, it becomes clear that the Administrator has recently engaged with every file in the "Secret" folder located in the shared file directory. It is possible to see that the file has been modified after being accessed by the attacker.



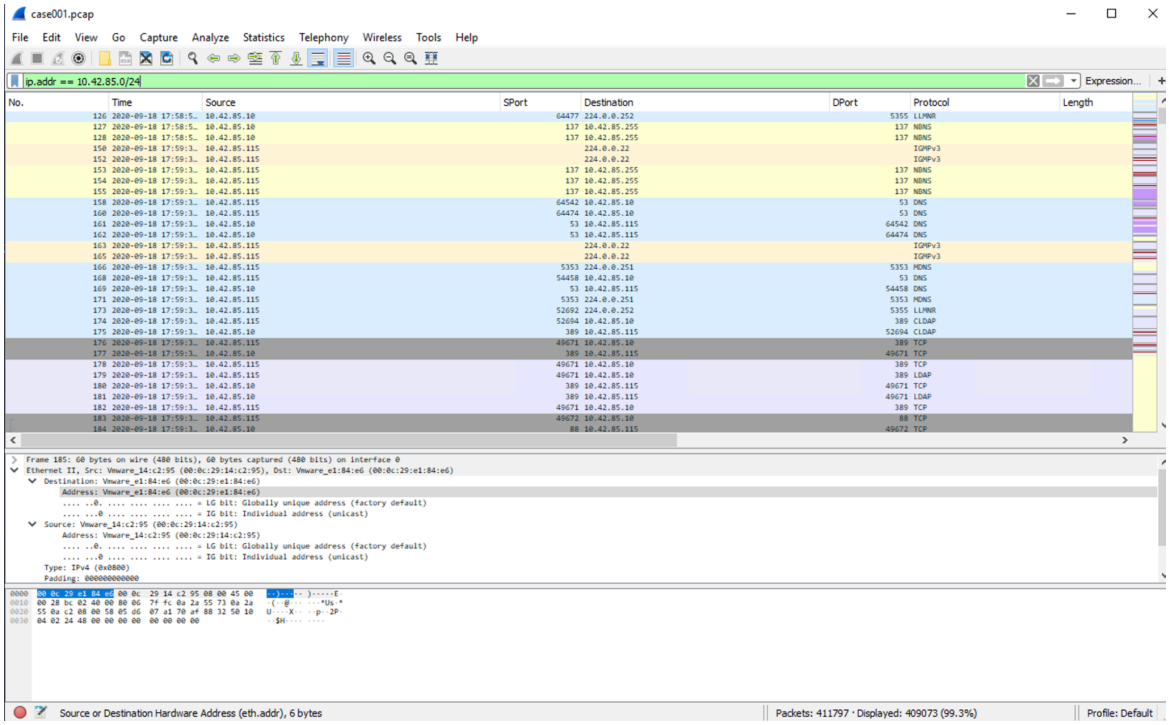
1. When?

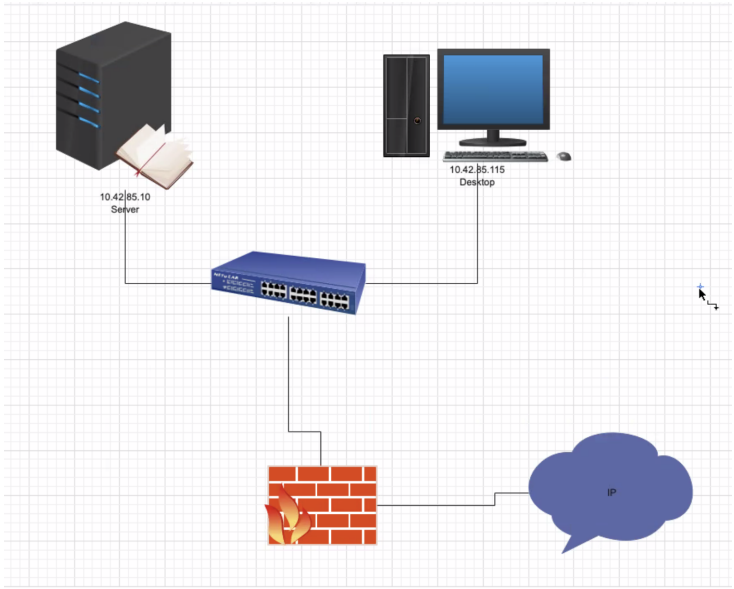


The picture captures the exact time that the file has been accessed and modified.

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

By this wireshark capture we can see the extensive communication between two ip addresses (server and desktop ones), and it is possible to conclude that they belong to the same network 10.42.85.0/24, as shown in the filter of the wireshark.





This diagram represents just an example of how they are connected.

Conclusion

In the face of rapidly evolving cyber threats, our investigation into the case of "The Stolen Szechuan Sauce" serves as an enlightening example of the complexities and challenges involved in digital forensic analysis. Utilizing a range of state-of-the-art forensic tools like Autopsy, FTK Imager, The Volatility Foundation, and Wireshark, we have conducted a comprehensive analysis of both a server and a desktop implicated in the cyber event under scrutiny.

Our methodical approach, framed by a series of guiding questions, allowed us to delve deep into multiple types of evidence files—disk images (E01), packet capture files (PCAP), and memory dumps. Through rigorous analysis, we confirmed a breach had occurred, identified malware and its capabilities, and traced the adversary's steps. These findings are supported by various artifacts including screenshots, logs, and network traffic data. Ensuring a robust and substantiated conclusion, this investigation underscores the vital role that thorough forensic analysis plays in demystifying complex cyber events and providing actionable intelligence for enhancing cybersecurity measures.

While our investigation has reached its intended goals, it's important to recognize that digital forensics is a continually evolving field. New methods and technologies are constantly emerging, offering both opportunities and challenges for future investigations. This project, undertaken collaboratively, not only serves as a testament to the capabilities of current forensic tools but also highlights the importance of teamwork and diverse skill sets in conducting successful cyber investigations. As cyber threats continue to advance in scale and sophistication, the lessons gleaned from this exercise will undoubtedly serve as valuable experience for tackling future cyber incide

References

James. (2021, March 25). *Case 001 - the stolen szechuan sauce*. DFIR Madness. https://dfirmadness.com/the-stolen-szechuan-sauce/

A guide to digital forensics and cybersecurity tools. Forensics Colleges. (2022, May 19). https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools

Wikimedia Foundation. (2023, October 15). *Windows NT*. Wikipedia. https://en.wikipedia.org/wiki/Windows_NT#:~:text=Windows%20NT%20is%20a%20proprietary,and%20multi%2Duser%20operating%20system.

Free Automated Malware Analysis Service - powered by Falcon Sandbox - viewing online file analysis results for “coreupdater.exe.” (n.d.). https://www.hybrid-analysis.com/sample/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6/5f7695f4a553eb21aa0cdfe1

VirusTotal. (n.d.). Www.virustotal.com. https://www.virustotal.com/gui/home/search