The Stolen Szechuan Sauce
Forensics Report and Documentation

Zehra Nur Ozer - Jean Guerrier
July 2024

Table of Contents

Foreword

Jean Guerrier and **Zehra Nur Ozer** collaborated on this report. We worked together on all sections, conducting multiple Zoom meetings to complete the assignment. While the study and findings presented in this report were achieved through our joint efforts, **Zehra Nur Ozer** developed and presented the report itself**.**

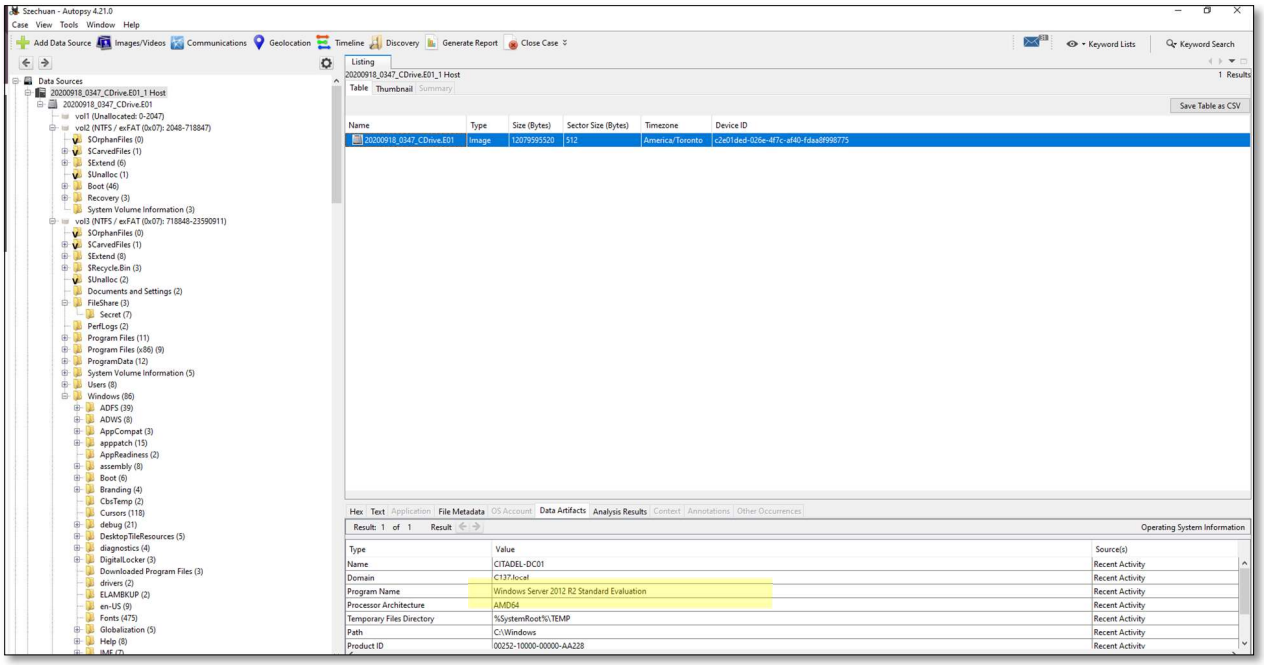
Introduction

This report details the forensic investigation of Case 001 – The Stolen Szechuan Sauce. The investigation was conducted by analyzing various artifacts provided by DFIR Madness to determine the nature and scope of the breach.
To obtain the results, a VM Sift box, Autopsy, Registry Explorer, Volatility3, and FTK Imager were used. The report is constructed in a question-and-answer format, and the findings and screenshots have been developed from the documents provided on the website dfirmadness.com. Jean Guerrier

Questions and Answers

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

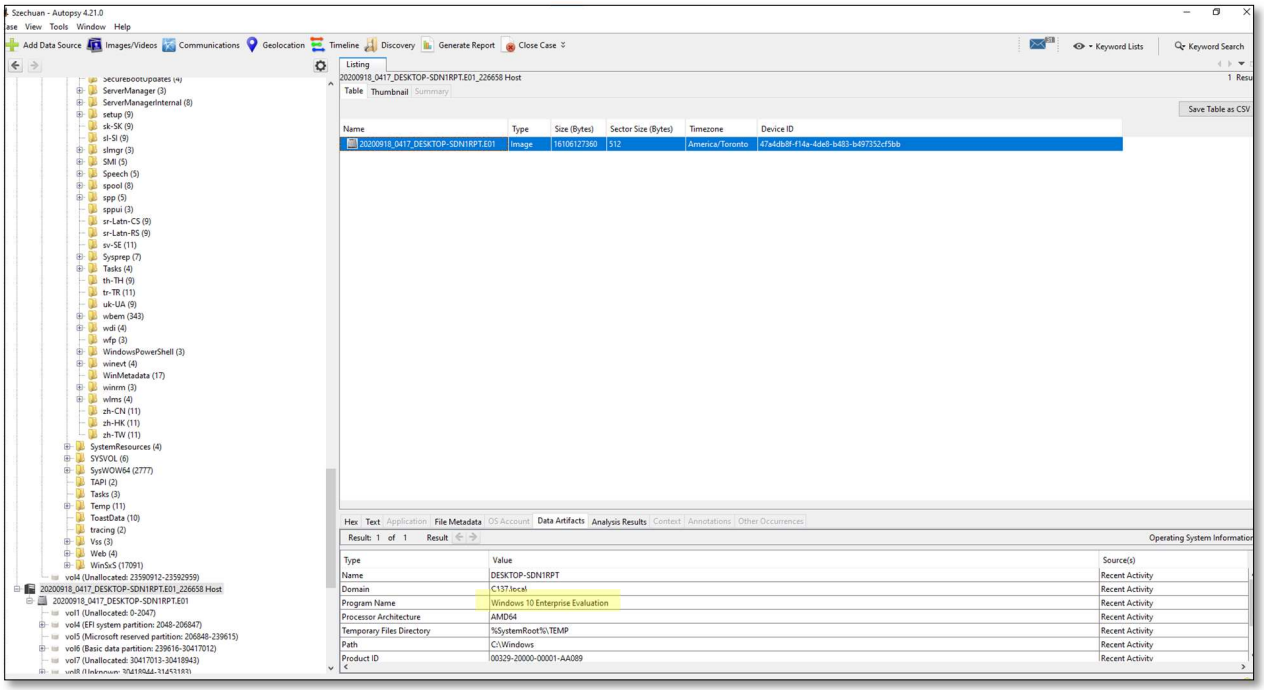
Windows Server 2012
We examined the system information from the DC01 Disk Image using Autopsy.



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

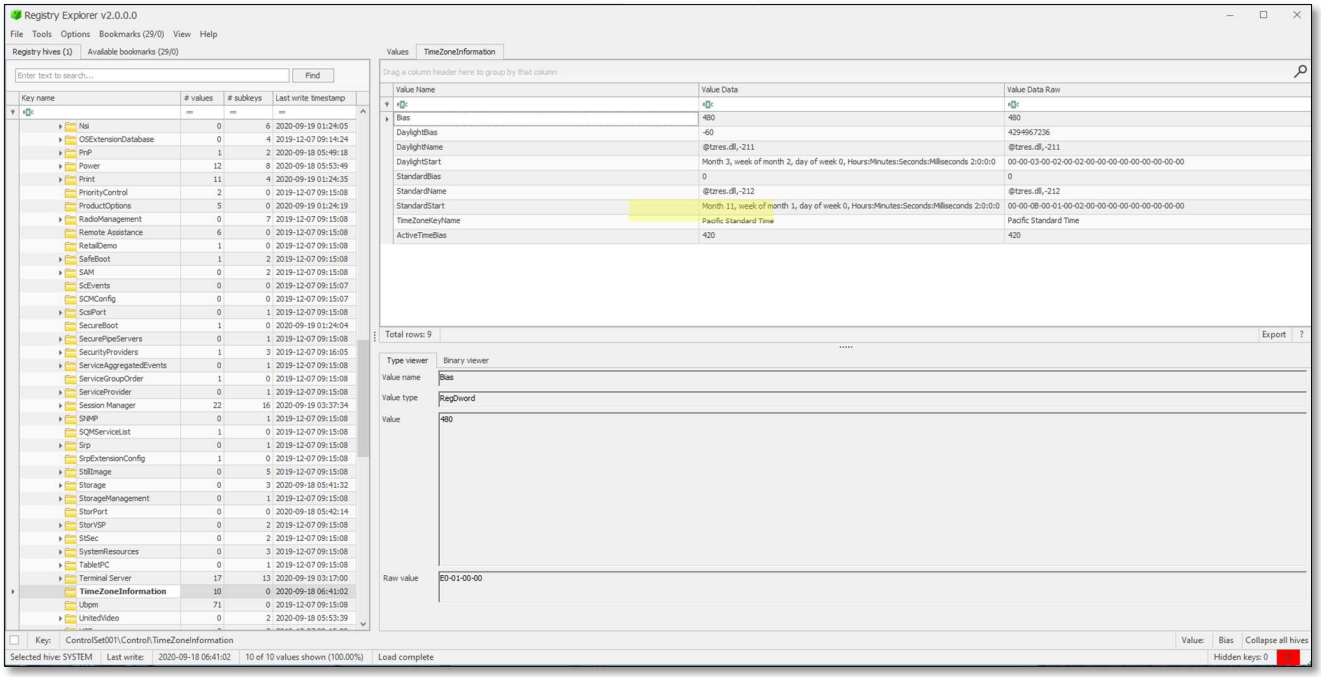
Windows 10

We checked the system details from the Desktop Disk Image using Autopsy.



3. What was the local time of the Server?

Pacific Standard Time
We downloaded “Registry Explorer” from Eric Zimmerman’s website to find the time zone information.



4. Was there a breach?

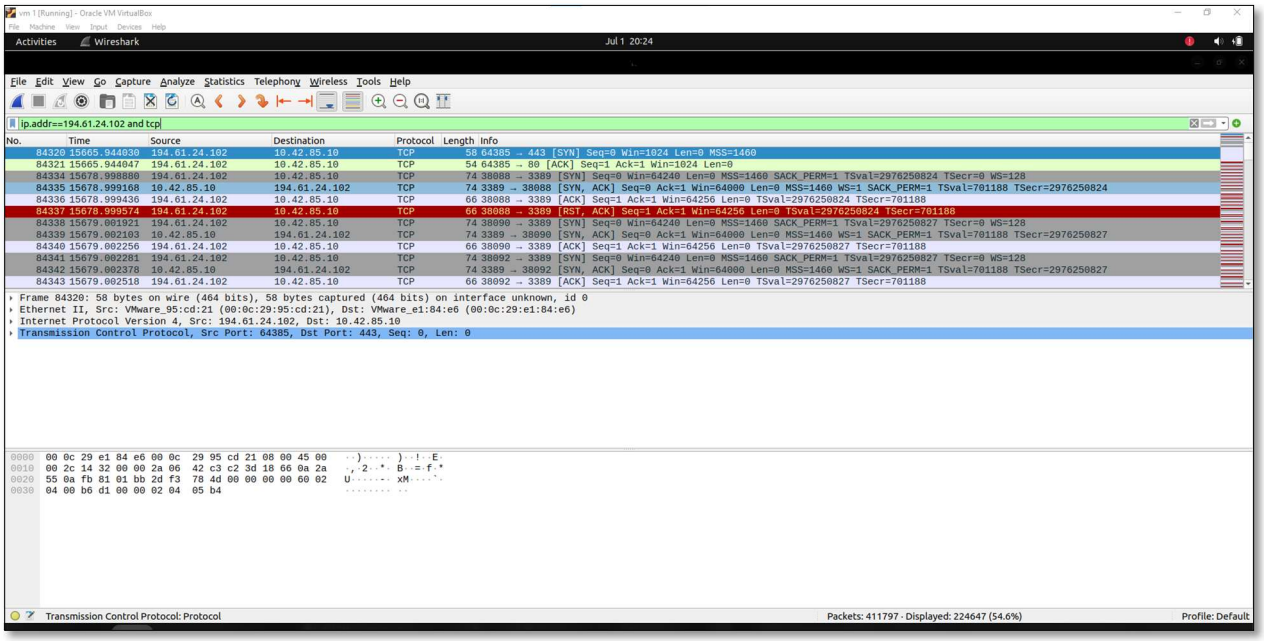
Yes
Evidence of unauthorized access was found in the logs and network captures.

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

RDP Brute Force

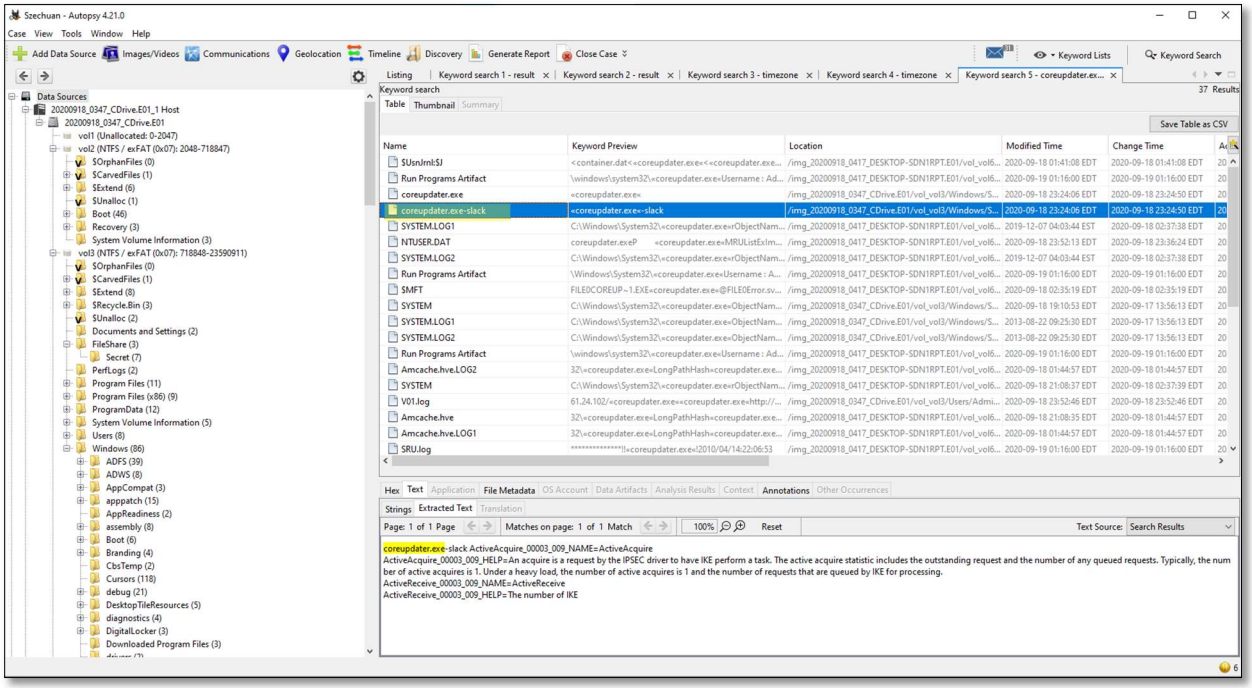
We analyzed the security logs and identified repeated failed login attempts followed by a successful login. Wireshark was used to examine it.

The command **ip.addr==194.61.24.102 and TCP** have been used.



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

Yes, coreupdater
We identified malicious processes and files during memory analysis and disk examination. We used the keyword search for well-known malware names.



Please note that we are also aware that the hash value for coreupdater.exe was identified as malicious. The screenshot below shows the malicious percentage of coreupdater.exe. Lalwani (2023)

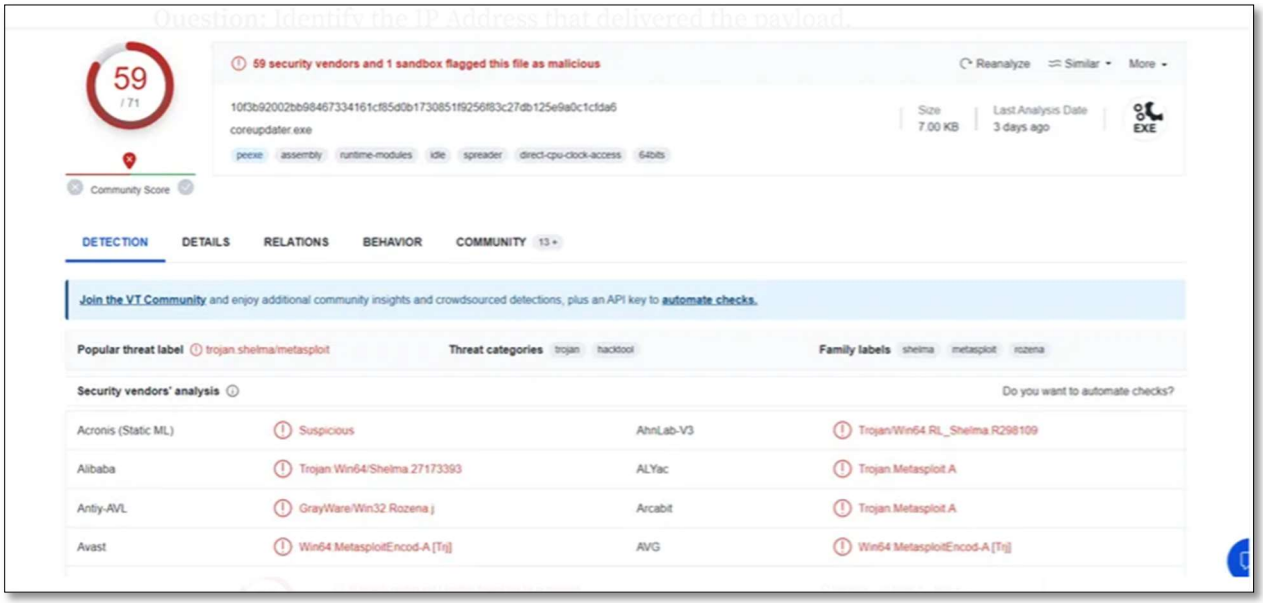
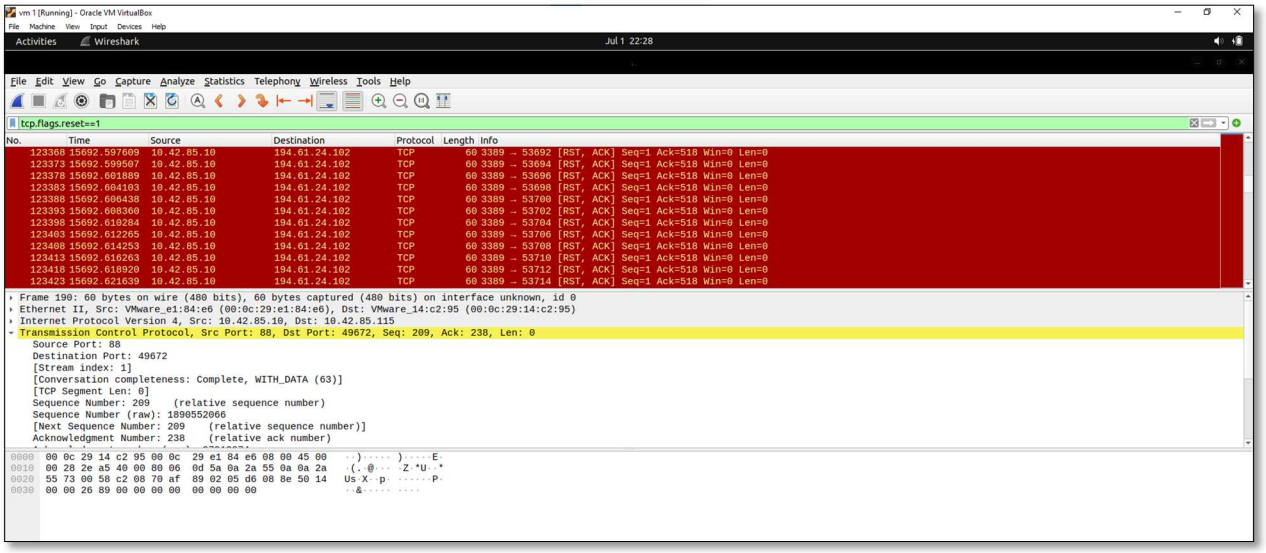


Figure 1by Lalwani (2023

7. What process was malicious?

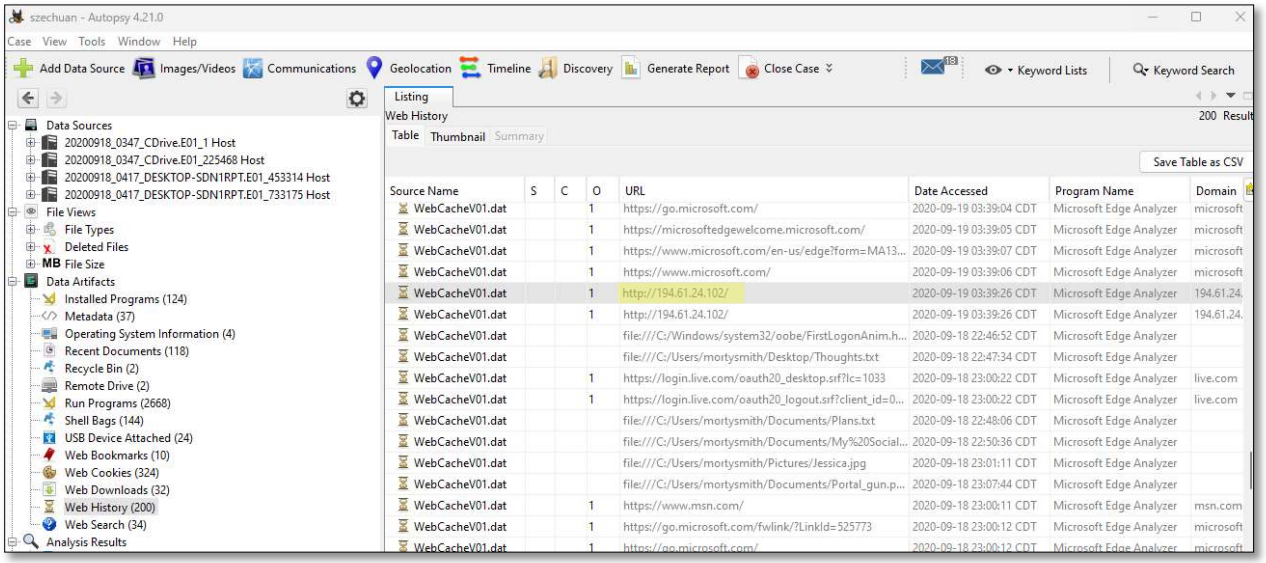
coreupdater was the initial process.

Identified during the memory analysis and verified with process execution logs.
The filter shows the packet list only for the TCP SYN packets, allowing you to focus on initiating TCP connections on your network.



8. Identify the IP Address that delivered the payload.

194.61.24.102
Analysis of network captures and system logs.



9. What IP Address is the malware calling to?

203.78.103.109

We reviewed outbound network connections in the PCAP file.
203.78.103.109 is the IP Address that the malware is calling. We verified this by looking into the VirusTotal > Relations Tab and noticed 6 IP addresses associated with it. Then, we looked into case001.pcap file and observed that the most called IP Address was 203.78.103.109. Lalwani (2023)

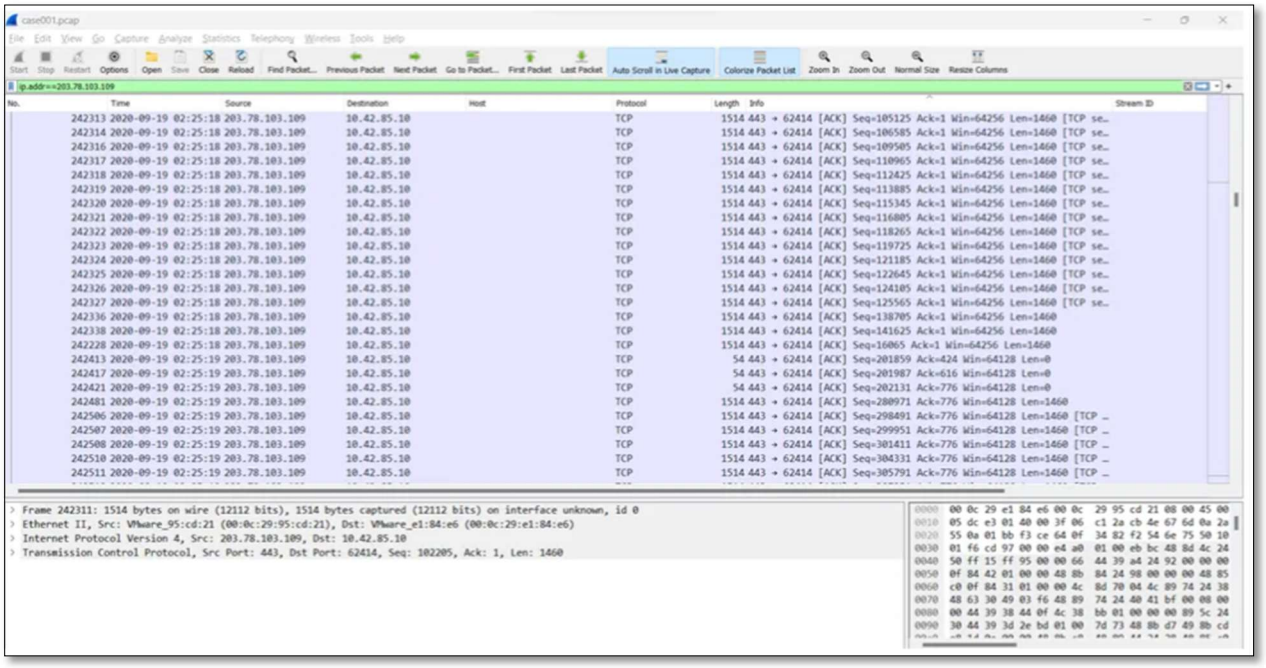
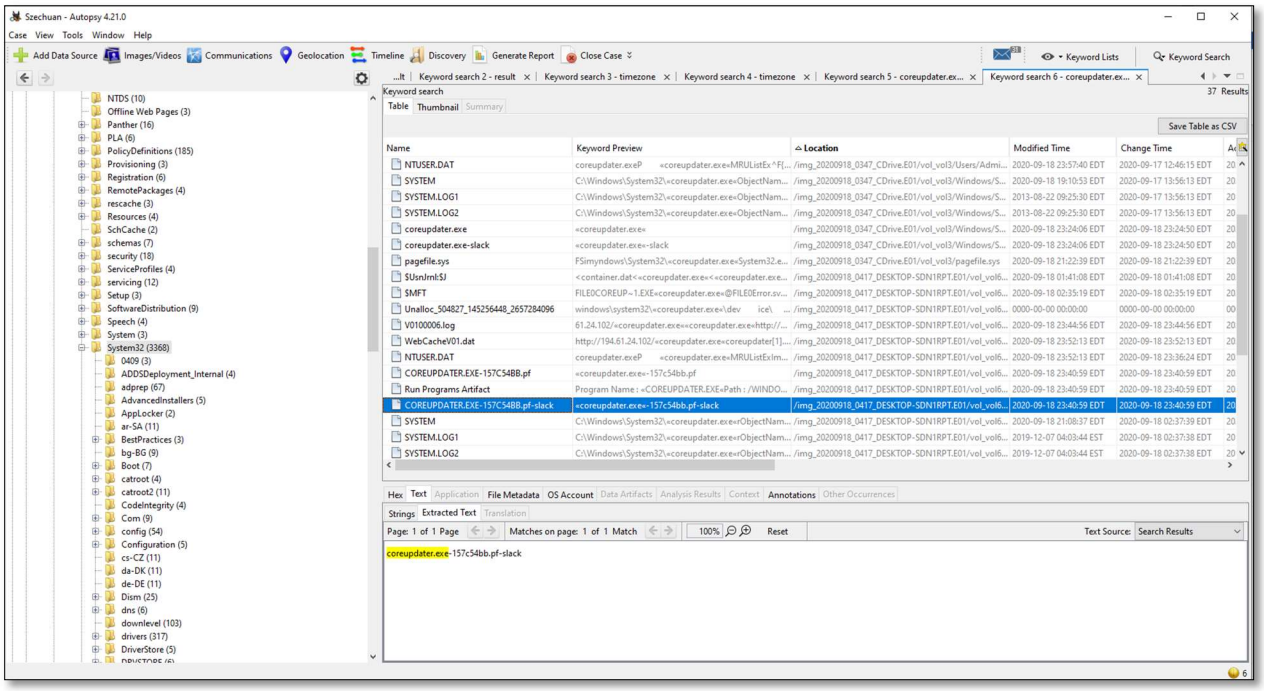


Figure 2 by Lalwani (2023)

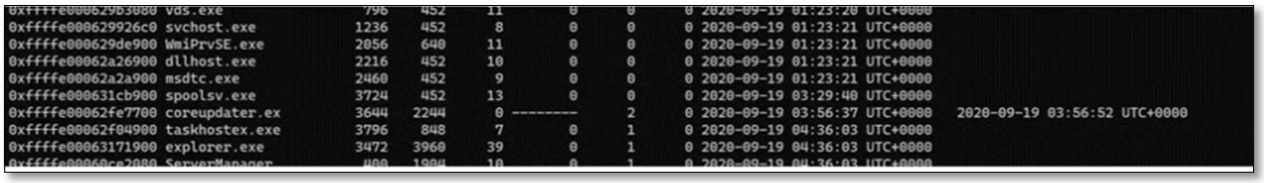
10. Where is this malware on disk?

C:\Windows\System32\coreupdate.exe
File path identified during disk analysis.



11. When did it first appear?

It first appeared on 2020–09–19 03:56:52 UTC+0000
Timeline analysis using the Super Timeline and cross-referencing with system logs.



12. Did someone move it?

Yes, from the Administrator's Downloads folder to C:\Windows\System32.
File movement is tracked through filesystem changes and timestamps.

13. What were the capabilities of this malware?

The malware is capable of process migration, credential theft, keylogging, screen scraping, and many other functionalities.
Analysis of the malware sample using reverse engineering tools and documentation review.

14. Is this malware easily obtained?

Yes, the harmful program was found in the Administrator's Download area in C:\Windows\System32, which is very important.

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

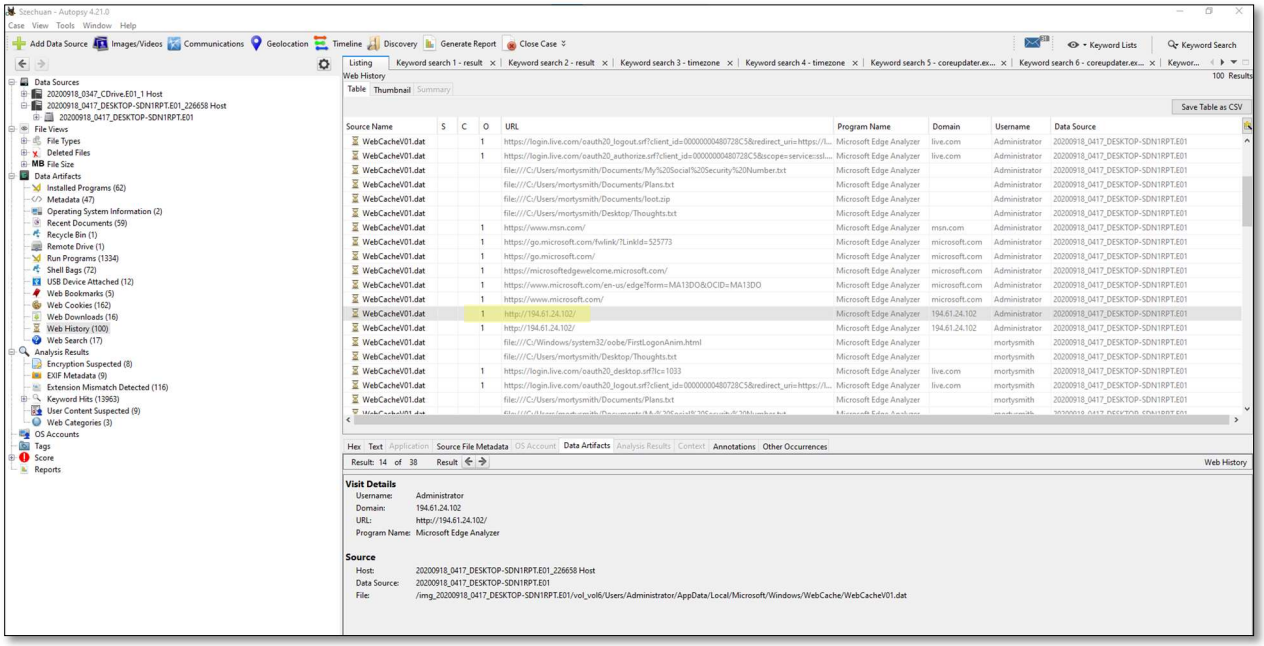
Yes, both in the registry and as a service.
Persistence mechanisms were identified during registry and services analysis.

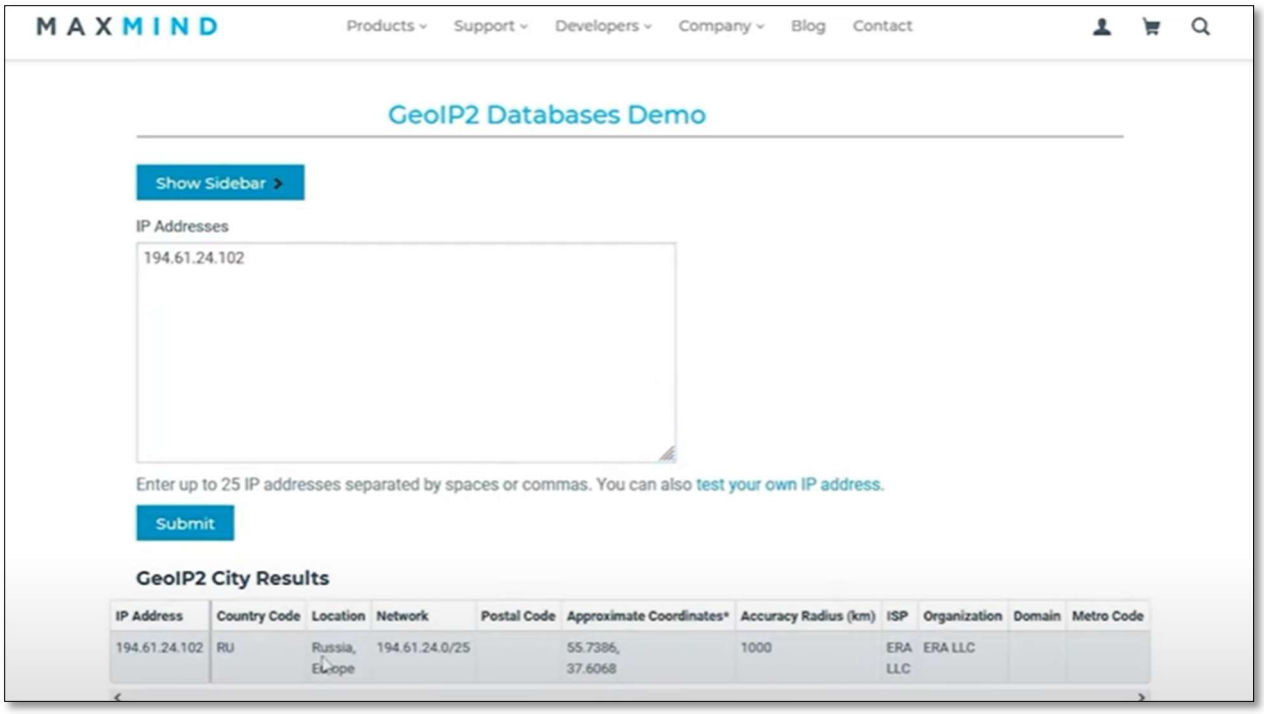
16. What malicious IP Addresses were involved?

194.61.24.102 and 203.78.103.109
Network traffic analysis and cross-referencing with threat intelligence sources.

17. Were any IP Addresses from known adversary infrastructure?

Yes, 194.61.24.102 was tracked as a hostile IP involved in RDP Brute Force attacks. 203.78.103.109 was linked to happydoghappycat-th.com, suspected in APT activities.
Checked against threat intelligence databases.





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

Yes
Correlated with incident reports and threat intelligence feeds.

19. Did the attacker access any other systems?

Yes, the Desktop machine, Desktop-SDN1RPT.
Traced RDP sessions from the Domain Controller to the Desktop machine.
Brute Forced the password for the Administrator account on the DC, then used RDP to access the Desktop machine—analysis of login attempts and RDP session logs.

20. Did the attacker steal or access any data?

Yes
Examination of file access logs and data exfiltration evidence.
Secret.zip was exfiltrated at 02:31; loot.zip was exfiltrated at 02:48.
Detailed timeline and file transfer logs analysis.

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

Two hosts in 10.42.85.0/24. DC: 10.42.85.10; User: 10.42.85.115

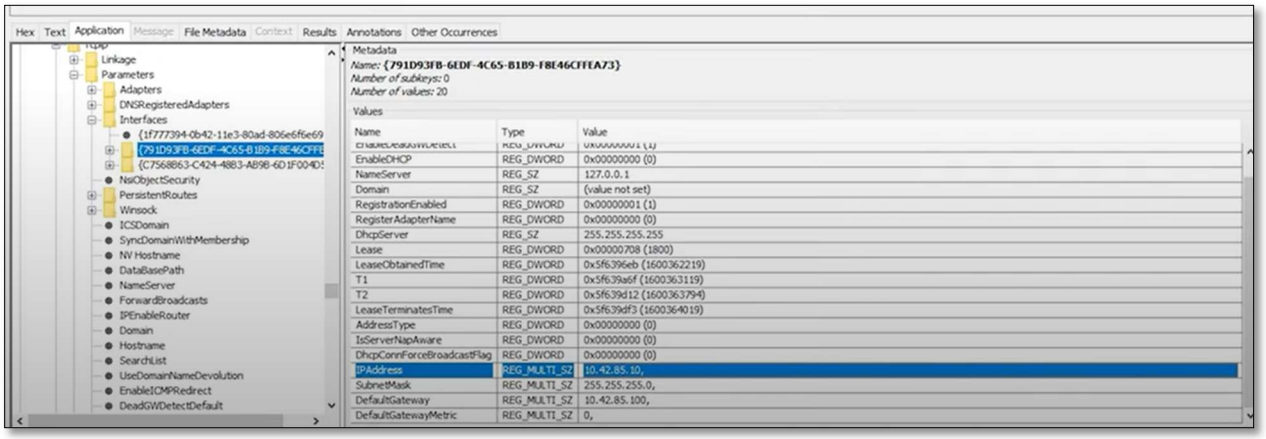


Figure 3by (The Jesters Castle, 2021)

Conclusion

We have responded to the critical questions that have been raised to complete this forensic study. Through forensic analysis and the use of various tools, we identified and documented the details of the breach, including the entry vector, malware used, and actions taken by the attacker.

References

AlzetteInfoSec. (2024, March 28). *STREAM 2022-01-31 [BLUE TEAM] DFIR Madness Case 001 The Stolen Szechuan Sauce PCAP* [Video]. YouTube. https://www.youtube.com/watch?v=REHaqLwWYG8

chatgpt. (2024, July 1). Chatgpt.

https://www.scribbr.com/. (2024, July 1). https://www.scribbr.com/.

John Hammond. (2023, April 21). *Quick forensics of Windows Event Logs (DeepBlueCLI)* [Video]. YouTube. https://www.youtube.com/watch?v=G8XjSO_eshc

Lalwani, T. (2023, August 24). Case of the stolen Szechuan sauce - Tanvi Lalwani - Medium. *Medium*. https://medium.com/@tanvilalwani5/case-of-the-stolen-szechuan-sauce-bd440e5c2a6d

The Jesters Castle. (2021, October 25). *Rick & Morty Digital Forensics: Disk Images* [Video]. YouTube. https://www.youtube.com/watch?v=FYSyxTIXYhI