

The Stolen Szechuan Sauce
Forensics Report and Documentation

Zehra Nur Ozer - Jean Guerrier
July 2024

Table of Contents

Foreword	3
Introduction	3
Questions and Answers	3
1. What's the Operating System of the Server?	3
2. What's the Operating System of the Desktop?	4
3. What was the local time of the Server?	5
4. Was there a breach?	5
5. What was the initial entry vector (how did they get in)?	6
6. Was malware used? If so, what was it?	7
7. What process was malicious?	8
8. Identify the IP Address that delivered the payload.	8
9. What IP Address is the malware calling to?	9
10. Where is this malware on disk?	10
11. When did it first appear?	10
12. Did someone move it?	10
13. What were the capabilities of this malware?	10
14. Is this malware easily obtained?	11
15. Was this malware installed with persistence on any machine?	11
16. What malicious IP Addresses were involved?	11
17. Were any IP Addresses from known adversary infrastructure?	11
18. Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?	12
19. Did the attacker access any other systems?	12
20. Did the attacker steal or access any data?	12
21. What was the network layout of the victim network?	13
Conclusion	13
References	14

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.

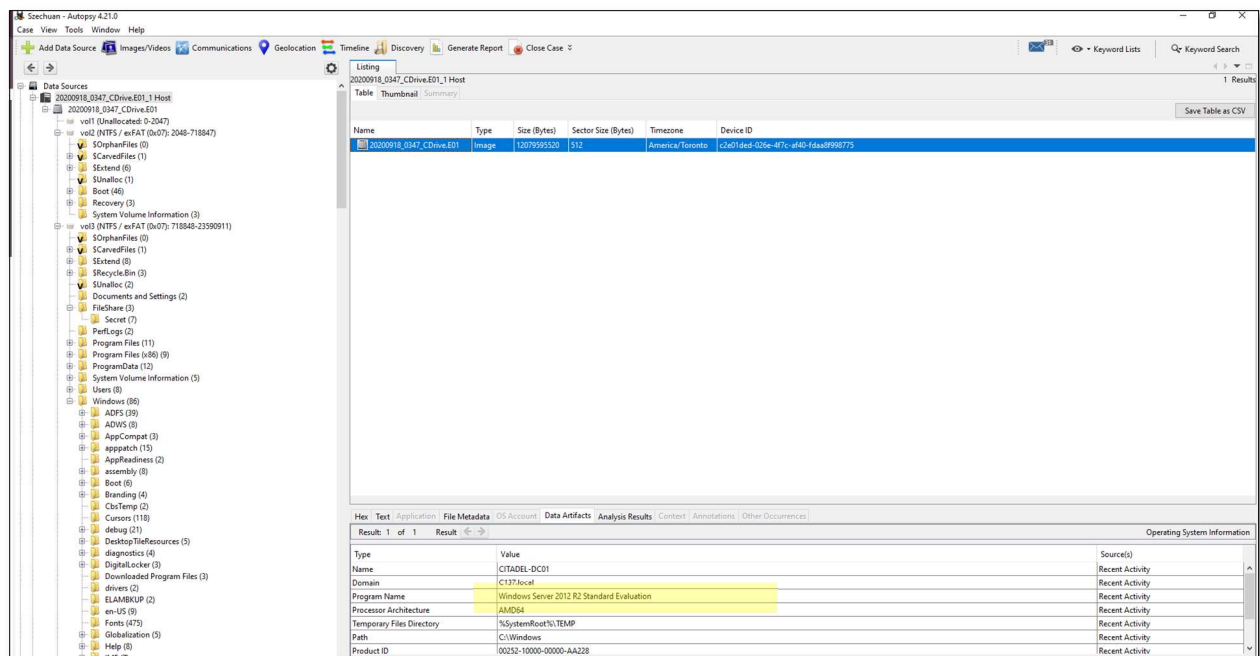
To obtain the results, a VM Sift box, Autopsy, Registry Explorer, Volatility3, and FTK Imager were used. The report is constructed in a question-and-answer format, and the findings and screenshots have been developed from the documents provided on the website dfirmadness.com. Jean Guerrier

Questions and Answers

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

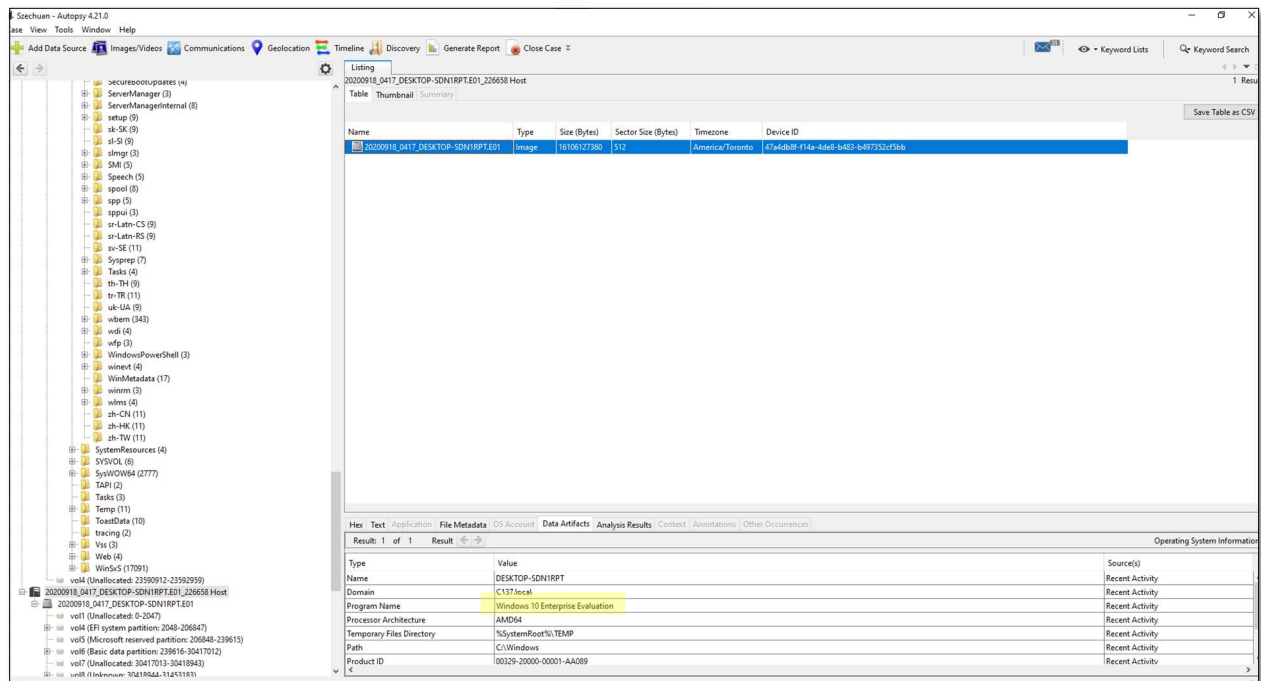
Windows Server 2012

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



Windows 10

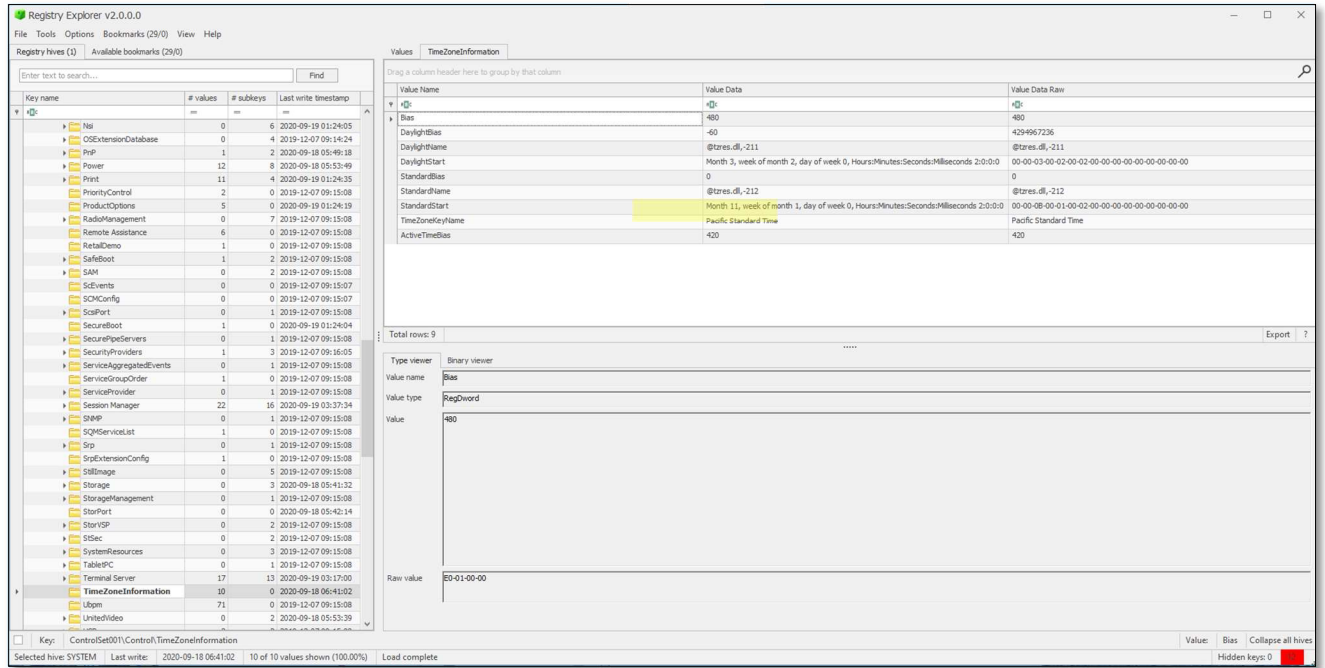
We checked the system details from the Desktop Disk Image using Autopsy.



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

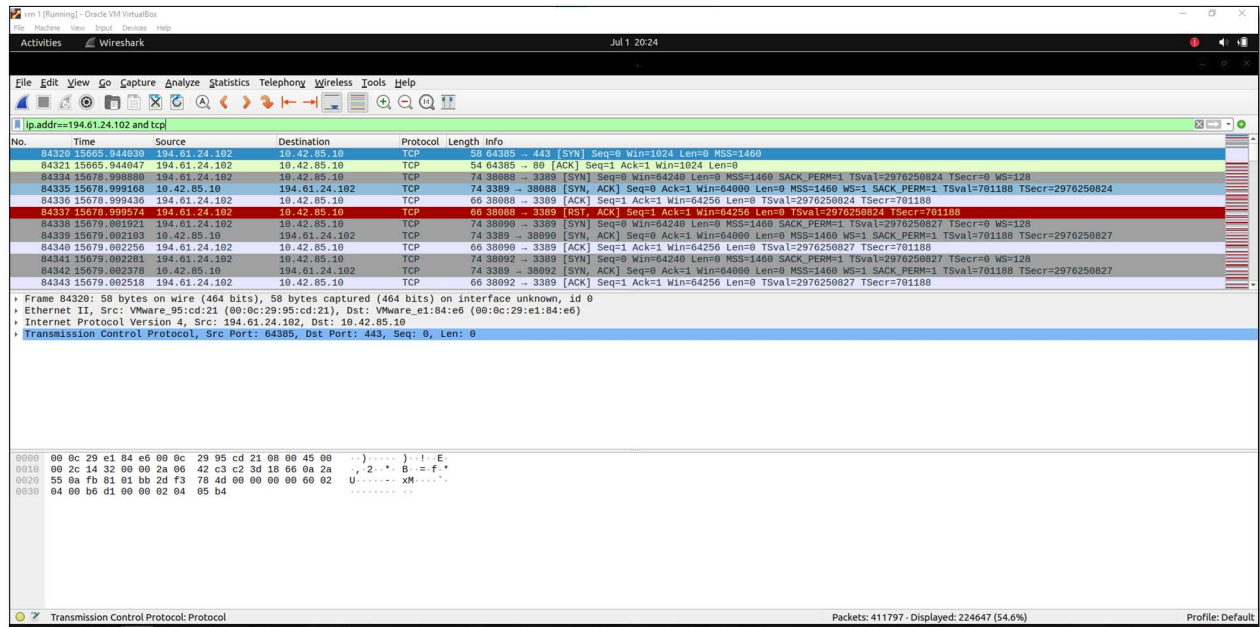
Evidence of unauthorized access was found in the logs and network captures.

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.

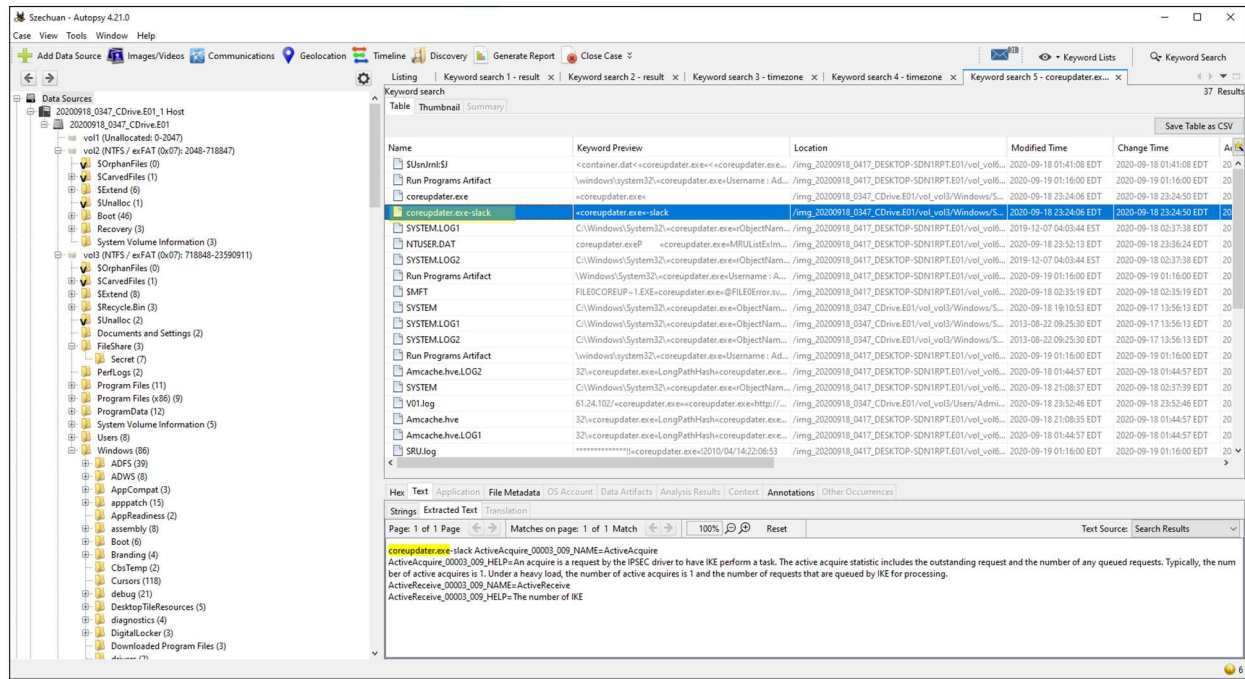
The command **ip.addr==194.61.24.102 and tcp** have been used.



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)

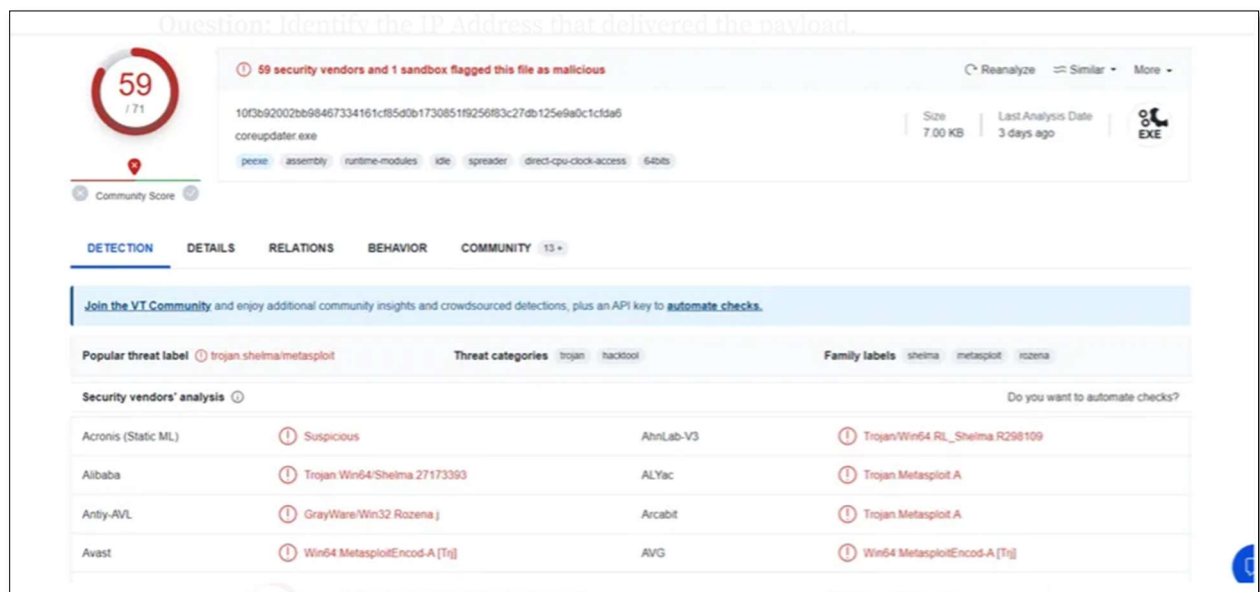


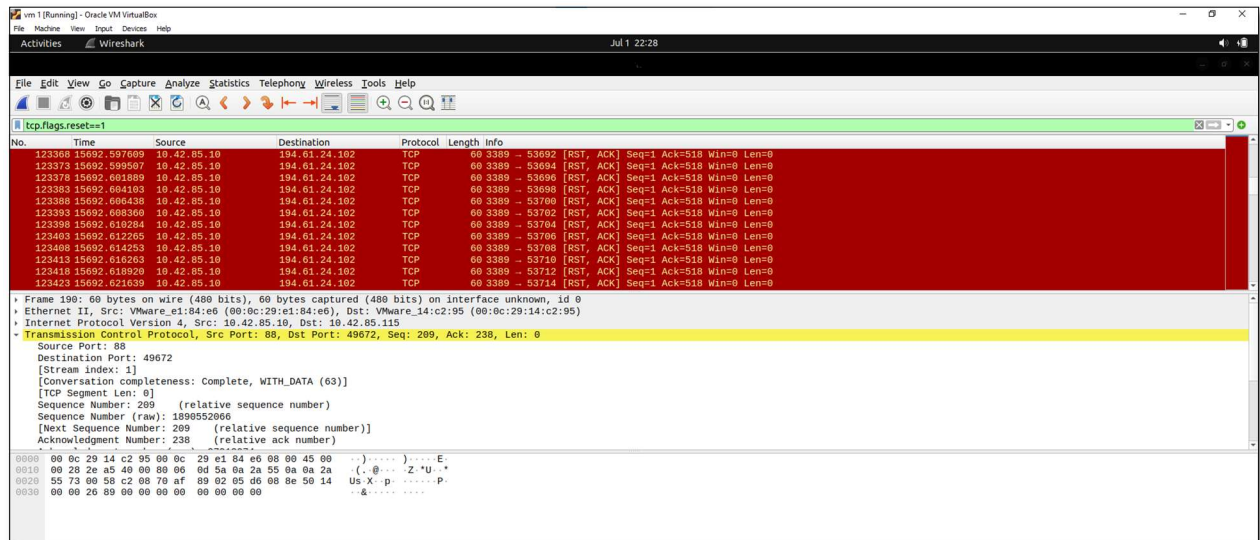
Figure 1 by Lalwani (2023)

7. What process was malicious?

coreupdater was the initial process.

Identified during the memory analysis and verified with process execution logs.

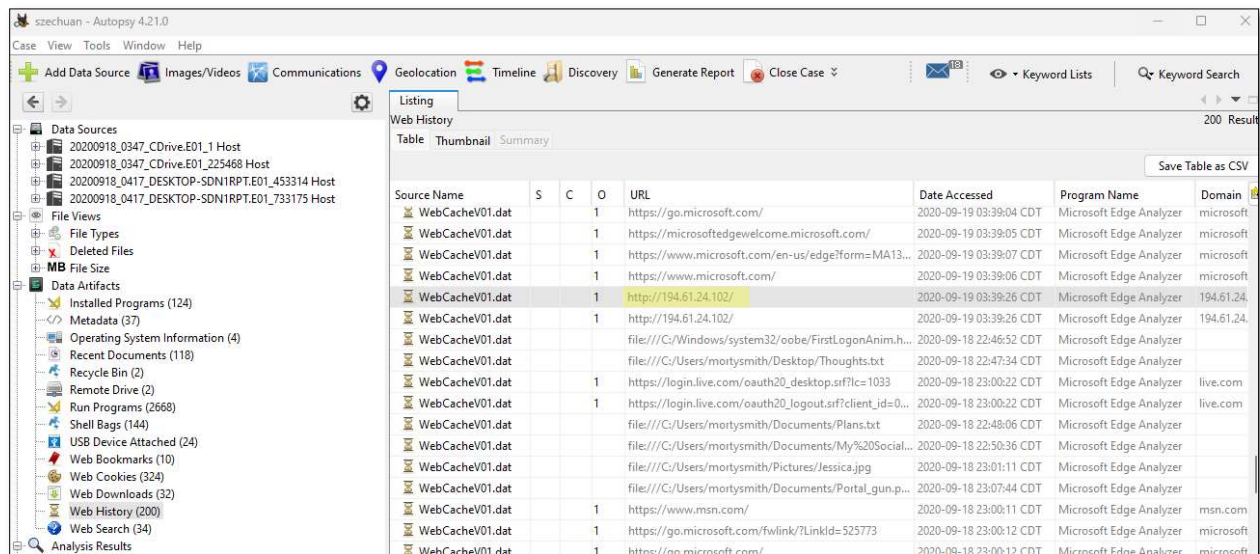
The filter shows the packet list only for the TCP SYN packets, allowing you to focus on initiating TCP connections on your network.



8. Identify the IP Address that delivered the payload.

194.61.24.102

Analysis of network captures and system logs.

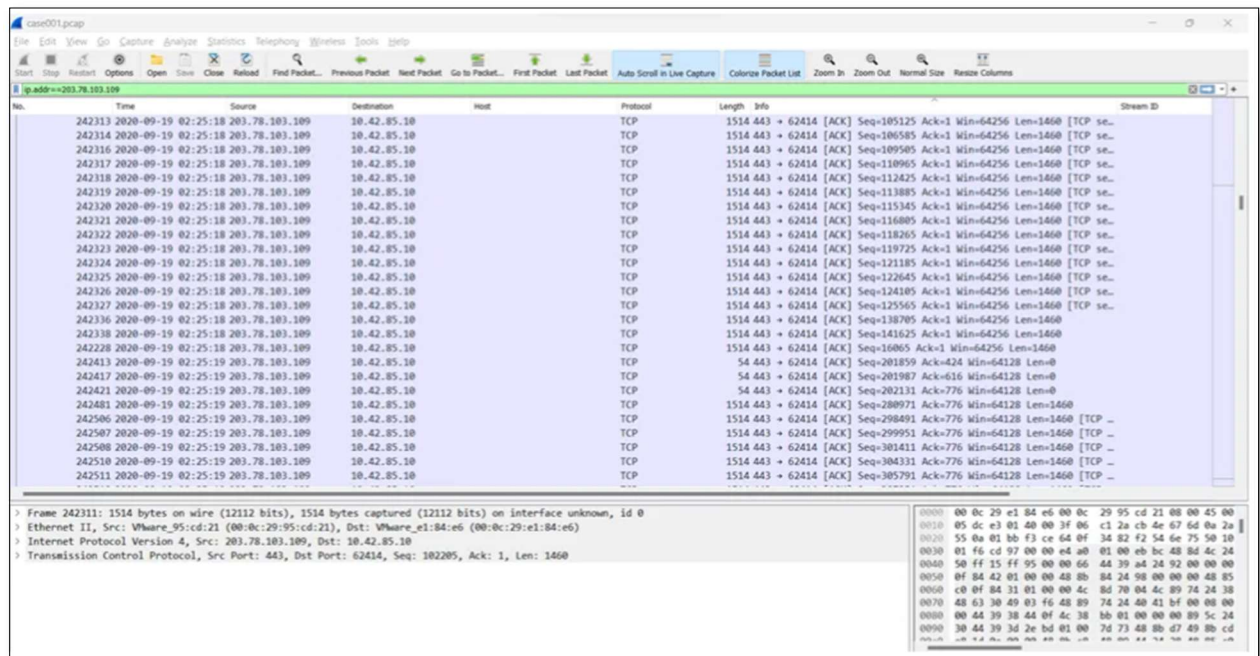


9. What IP Address is the malware calling to?

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)



The screenshot shows the Wireshark interface with a packet list table. The table has columns: No., Time, Source, Destination, Host, Protocol, Length, Info, and Stream ID. The filter bar at the top is set to 'ip.addr == 203.78.103.109'. The packet list shows multiple TCP connections from 203.78.103.109 to 10.42.85.10. The selected packet (No. 242311) is expanded, showing the raw packet data in hexadecimal and ASCII.

No.	Time	Source	Destination	Host	Protocol	Length	Info	Stream ID
242311	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=105125 Ack=1 Win=64256 Len=1460 [TCP se..	
242314	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=106585 Ack=1 Win=64256 Len=1460 [TCP se..	
242316	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=109505 Ack=1 Win=64256 Len=1460 [TCP se..	
242317	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=110905 Ack=1 Win=64256 Len=1460 [TCP se..	
242318	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=112425 Ack=1 Win=64256 Len=1460 [TCP se..	
242319	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=113805 Ack=1 Win=64256 Len=1460 [TCP se..	
242320	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=115345 Ack=1 Win=64256 Len=1460 [TCP se..	
242321	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=116805 Ack=1 Win=64256 Len=1460 [TCP se..	
242322	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=118205 Ack=1 Win=64256 Len=1460 [TCP se..	
242323	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=119725 Ack=1 Win=64256 Len=1460 [TCP se..	
242324	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=121185 Ack=1 Win=64256 Len=1460 [TCP se..	
242325	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=122645 Ack=1 Win=64256 Len=1460 [TCP se..	
242326	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=124105 Ack=1 Win=64256 Len=1460 [TCP se..	
242327	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=125565 Ack=1 Win=64256 Len=1460 [TCP se..	
242336	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=138705 Ack=1 Win=64256 Len=1460 [TCP se..	
242338	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=141625 Ack=1 Win=64256 Len=1460 [TCP se..	
242228	2020-09-19 02:25:18	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=16065 Ack=1 Win=64256 Len=1460 [TCP se..	
242413	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	54	443 → 62414 [ACK] Seq=201859 Ack=424 Win=64128 Len=0 [TCP se..	
242417	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	54	443 → 62414 [ACK] Seq=201987 Ack=616 Win=64128 Len=0 [TCP se..	
242421	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	54	443 → 62414 [ACK] Seq=202131 Ack=776 Win=64128 Len=0 [TCP se..	
242481	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=288971 Ack=776 Win=64128 Len=1460 [TCP se..	
242506	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=298491 Ack=776 Win=64128 Len=1460 [TCP se..	
242507	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=299951 Ack=776 Win=64128 Len=1460 [TCP se..	
242508	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=301411 Ack=776 Win=64128 Len=1460 [TCP se..	
242510	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=304331 Ack=776 Win=64128 Len=1460 [TCP se..	
242511	2020-09-19 02:25:19	203.78.103.109	10.42.85.10	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=305791 Ack=776 Win=64128 Len=1460 [TCP se..	

Frame 242311: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface unknown, id 0
Ethernet II, Src: VMware_95:cd:21 (00:0c:29:95:cd:21), Dst: VMware_e1:84:e6 (00:0c:29:e1:84:e6)
Internet Protocol Version 4, Src: 203.78.103.109, Dst: 10.42.85.10
Transmission Control Protocol, Src Port: 443, Dst Port: 62414, Seq: 102205, Ack: 1, Len: 1460

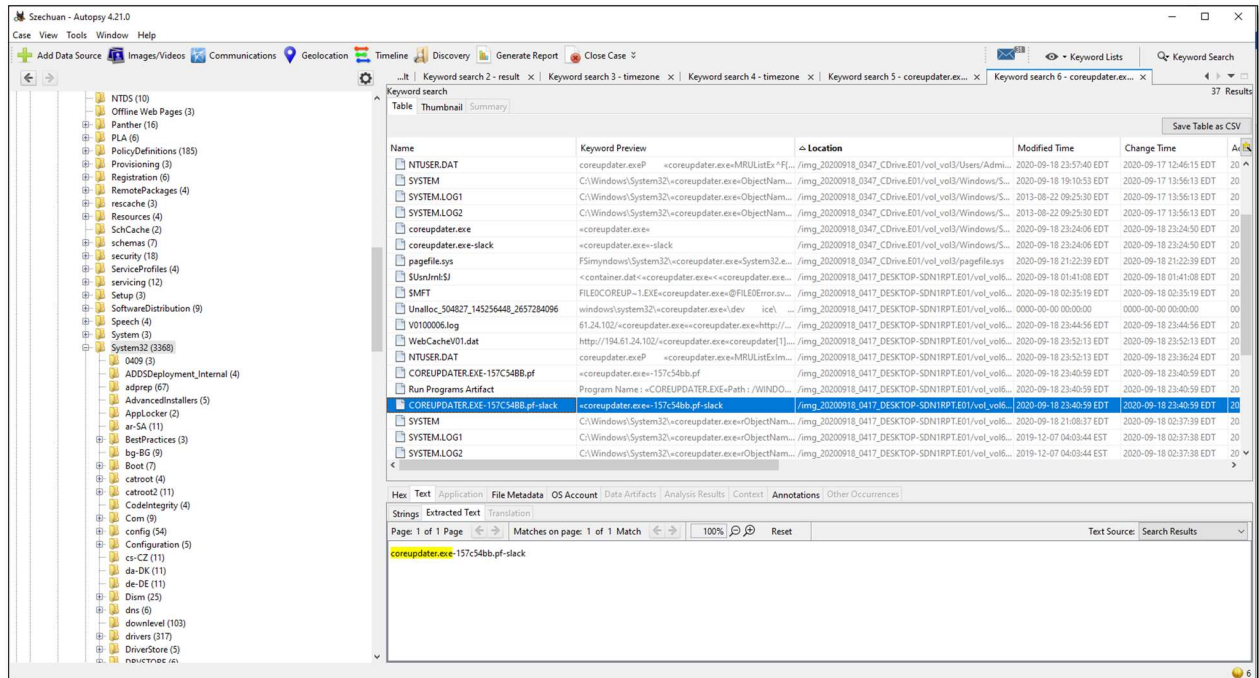
0000 00 0c 29 e1 84 e6 00 0c 29 95 cd 21 00 00 45 00
0010 05 dc e3 01 40 00 3f 06 c1 2a cb de 67 6d 0a 2a
0020 55 0a 01 bb f3 ce 64 0f 34 82 f2 54 6e 75 50 10
0030 01 f6 cd 97 00 00 e4 a0 01 00 eb bc 48 8d 4c 24
0040 50 ff 15 ff 95 00 00 66 44 39 a4 24 92 00 00 00
0050 0f 84 42 01 00 00 48 8b 84 24 98 00 00 00 48 85
0060 c0 0f 84 11 01 00 00 4c 8d 70 04 4c 89 74 24 38
0070 48 63 30 49 03 f6 48 89 74 24 40 41 bf 00 00 00
0080 00 44 39 38 44 0f 4c 38 bb 01 00 00 00 89 5c 24
0090 30 44 39 3d 2e bd 01 00 7d 73 48 8b d7 49 8b cd
00a0

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.

0x0000000000000000 vds.exe	796	452	11	0	0	0	2020-09-19 01:23:20 UTC+0000	
0xffffffff00000000 svchost.exe	1236	452	8	0	0	0	2020-09-19 01:23:21 UTC+0000	
0xffffffff00000000 WmiPrvSE.exe	2056	640	11	0	0	0	2020-09-19 01:23:21 UTC+0000	
0xffffffff00000000 dllhost.exe	2216	452	10	0	0	0	2020-09-19 01:23:21 UTC+0000	
0xffffffff00000000 msdtc.exe	2460	452	9	0	0	0	2020-09-19 01:23:21 UTC+0000	
0xffffffff00000000 spoolsv.exe	3724	452	13	0	0	0	2020-09-19 03:29:40 UTC+0000	
0xffffffff00000000 coreupdate.exe	3644	2244	0	-----	2	0	2020-09-19 03:56:37 UTC+0000	2020-09-19 03:56:52 UTC+0000
0xffffffff00000000 taskhost.exe	3796	848	7	0	1	0	2020-09-19 04:36:03 UTC+0000	
0xffffffff00000000 explorer.exe	3472	3960	39	0	1	0	2020-09-19 04:36:03 UTC+0000	
0xffffffff00000000 System32\cmd.exe	1488	1804	10	0	1	0	2020-09-19 04:36:03 UTC+0000	

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.

The screenshot displays the Autopsy 4.21.0 interface. The left sidebar shows the file system tree with 'Web History (100)' selected. The main pane shows a table of web history entries. The table has columns: Source Name, S, C, O, URL, Program Name, Domain, Username, and Data Source. The entry for 'WebCacheV01.dat' with URL 'http://194.61.24.102/' is highlighted. Below the table, the 'Visit Details' section shows the following information:

Field	Value
Username	Administrator
Domain	194.61.24.102
URL	http://194.61.24.102/
Program Name	Microsoft Edge Analyzer

The 'Source' section shows the following information:

Field	Value
Host	20200918_0417_DESKTOP-SDN1RPT.E01
Data Source	20200918_0417_DESKTOP-SDN1RPT.E01
File	/img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_v06/Users/Administrator/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat

MAXMIND Products ▾ Support ▾ Developers ▾ Company ▾ Blog Contact

GeolIP2 Databases Demo

Show Sidebar >

IP Addresses

194.61.24.102

Enter up to 25 IP addresses separated by spaces or commas. You can also [test your own IP address](#).

Submit

GeolIP2 City Results

IP Address	Country Code	Location	Network	Postal Code	Approximate Coordinates*	Accuracy Radius (km)	ISP	Organization	Domain	Metro Code
194.61.24.102	RU	Russia, Elope	194.61.24.0/25		55.7386, 37.6068	1000	ERA LLC	ERA LLC		

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.

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

[illegible]

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-](https://medium.com/@tanvilalwani5/case-of-the-stolen-szechuan-sauce-bd440e5c2a6d)

[bd440e5c2a6d](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>