Report

on

Forensic Autopsy

(Case: The Stolen Szechuan Sauce)

INTRODUCTION

This forensic analysis was carried out to “Analyze a Suspect's Computer Image using Autopsy on the disk image provided on https://dfirmadness.com/case001/DC01 - E01.zip. This report examines a cybersecurity incident (Stolen Szechuan Sauce). The main aim is to determine how a secret Szechuan sauce recipe belonging to the CITADEL company ended up on a dark website . The company requested a forensic analysis of its Domain Controller and the network host to identify malicious applications installed on the system and determine place and time of software installation.

The report will cover the following main analysis points;

1.Timing the breach incident happened.

2.Attacker details(location , IP and networking details)

3.The initial entry vector the attackers used to get access to the system

4.List of Servers/systems details that got compromised

5.List of data , files , assets that were stolen , changed and deleted

6.Security controls that enable preventing future breaches

7.Recommended improvements to prevent similar attacks

8.Recommended policy control for securing the environment

Tools used:

1. wireshark: analyze the network traffic.
2. autopsy: analyze the artifacts.
3. virusTotal/AbuseIPDB: check report of the IP addresses

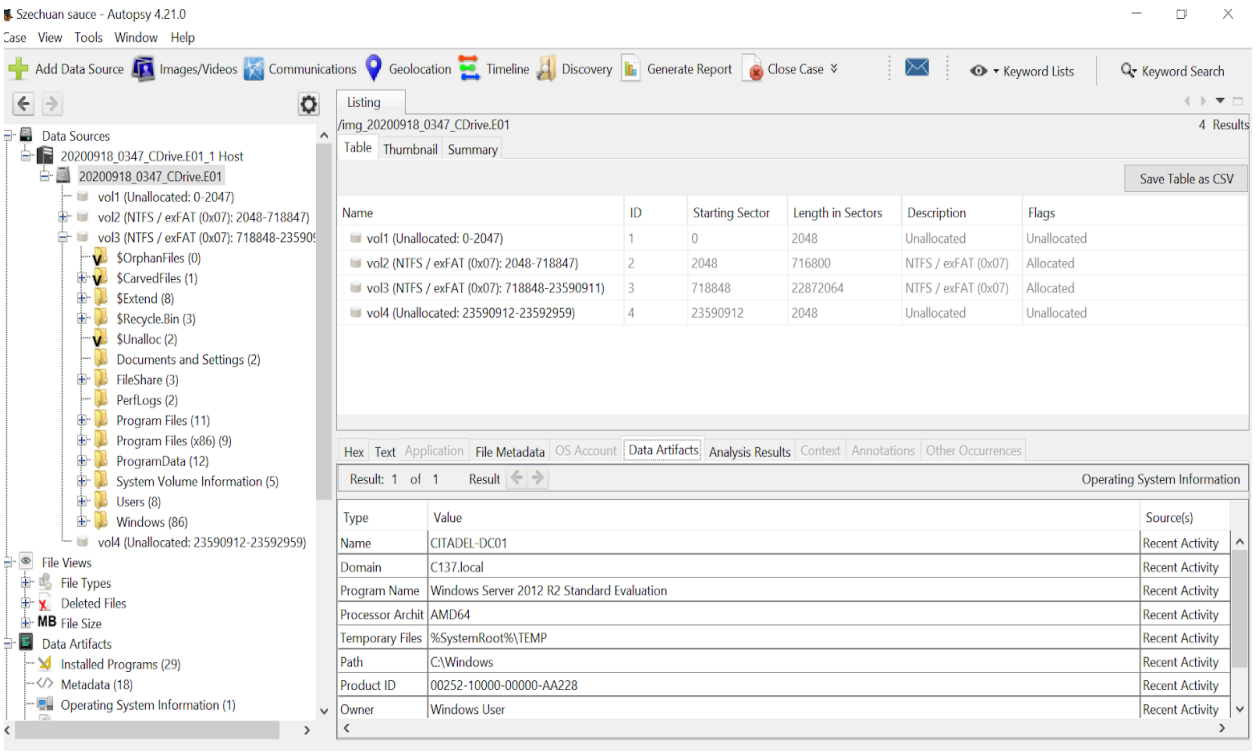
TECHNICAL FINDINGS:

a. What ’s the Operating System of the Server?

-Windows server 2012 R2 Standard Evaluation

-Using the Autopsy analysis tool for the DC01-EC01 data folder which is the disk image of the server , the data source- “20200918_0347_CDrive.E01” is identified as the data source to be analyzed.

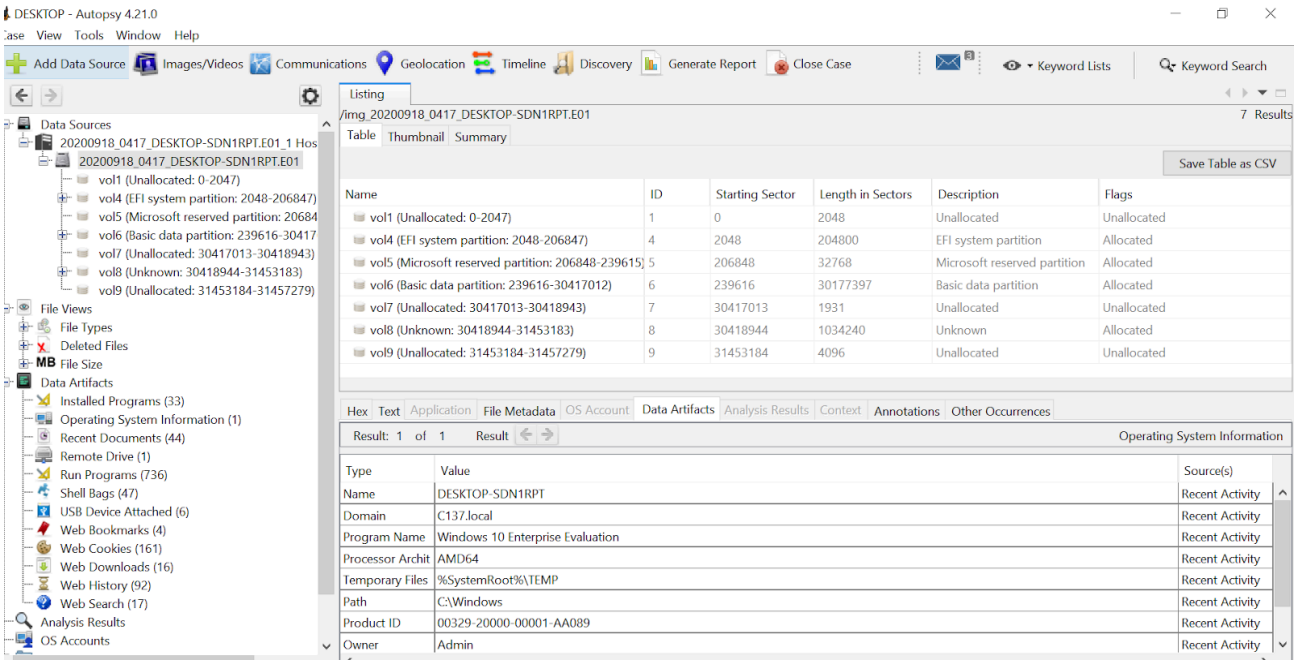
-The relevant Operating system information is found in vol3 under the data artifacts section in the top menu where the Program name is indicated as “Windows Server 2012 R2 Standard Evaluation”.



b. What ’s the Operating System of the Desktop?

-Windows 10 Enterprise

- Using the Autopsy analysis tool for the DESKTOP-E01 data folder which is the disk image of the desktop , in the left panel under the Operating System Information the Operating System of the desktop is obtained from the data artifacts section where the program name is indicated as “Windows 10 Enterprise”.

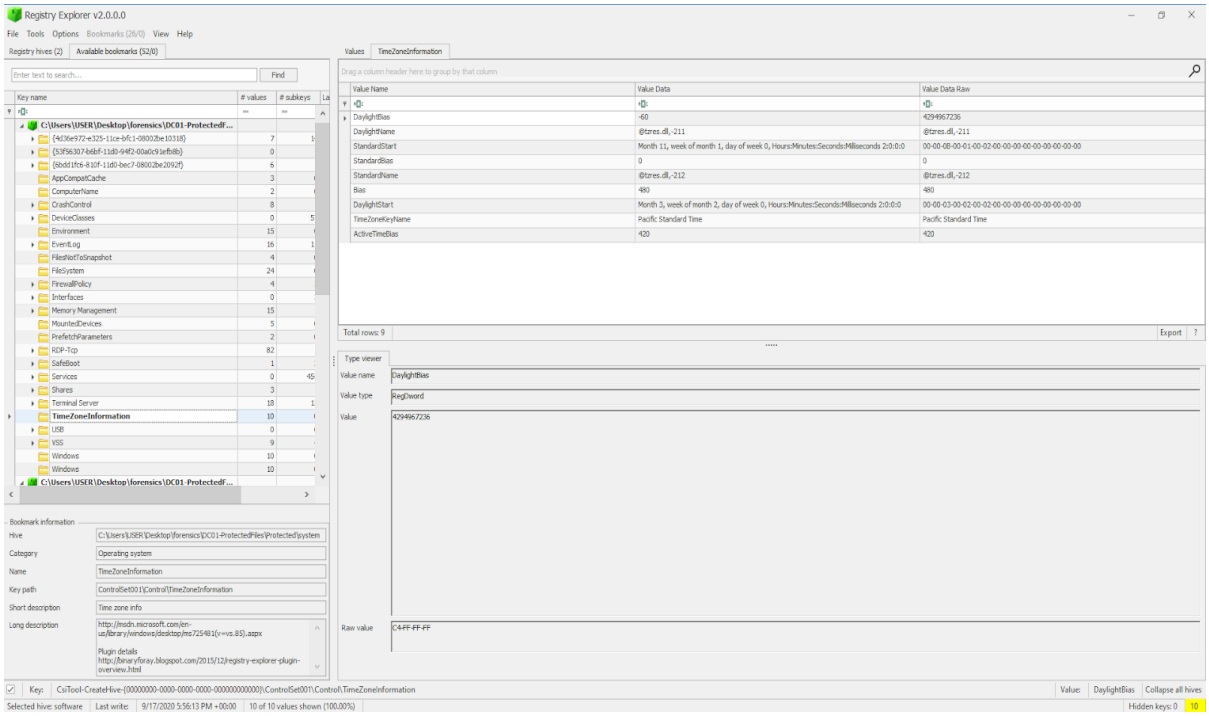


c. What was the local time of the Server?

-Pacific Standard Time (PST)

-To find the local time , registry explorer is used .It is a forensic tool used to view and analyze windows registry files allowing users to navigate registry hives and examine keys and values.

-By loading the relevant registry hives from DCO1-Protected file provided , as indicated in the hive path-“C:\Users\USER\Desktop\forensics\DC01-ProtectedFiles\ProtectedSystem” followed by navigating to the specific key -ControlSet001\Control\TimeZoneInformation where the time zone information is stored. The right panel will display the key values where the TimeZoneKeyName indicates the local time which is the Pacific Standard Time.



d. Was there a breach?

-Yes

- There was a breach, as indicated by all aspects of this analysis, as further explanation will be provided through the answers to the following questions as well as providing additional

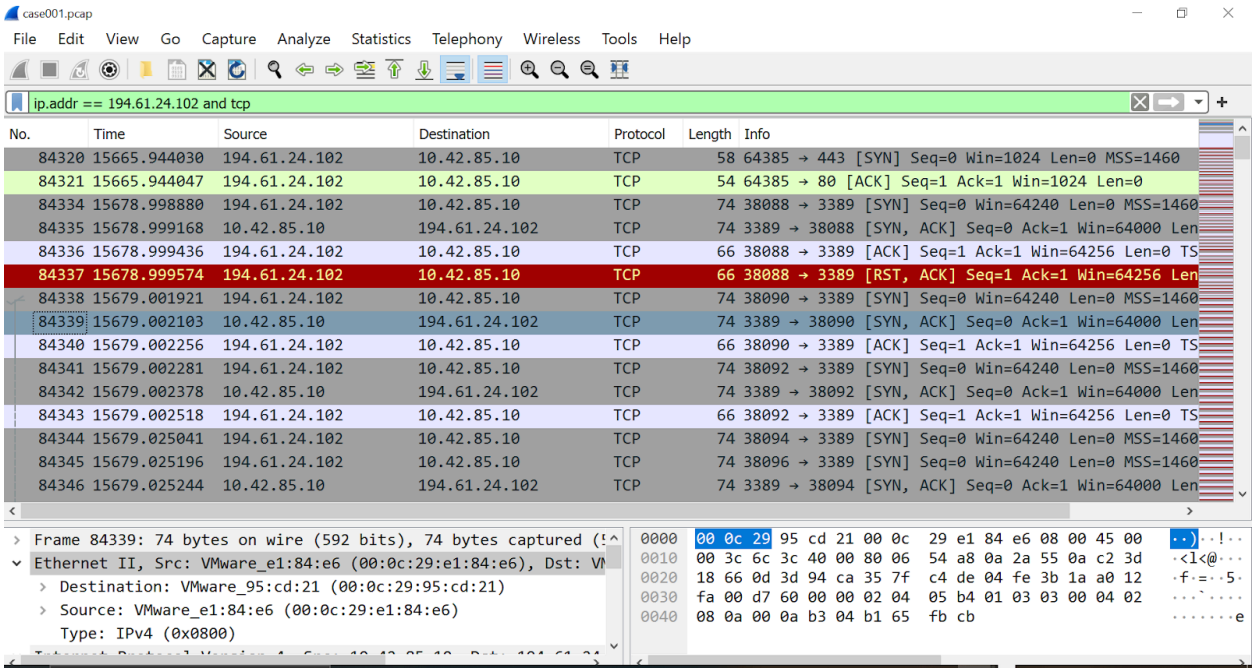
insights into the nature and extent of the breach .

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

-Brute Force was employed as the initial process.

-Due to the numerous SYN requests directed at the same destination port as found using wireshark with the filter "**ip.addr == 194.61.24.102 and tcp**" in the case001.pcap.

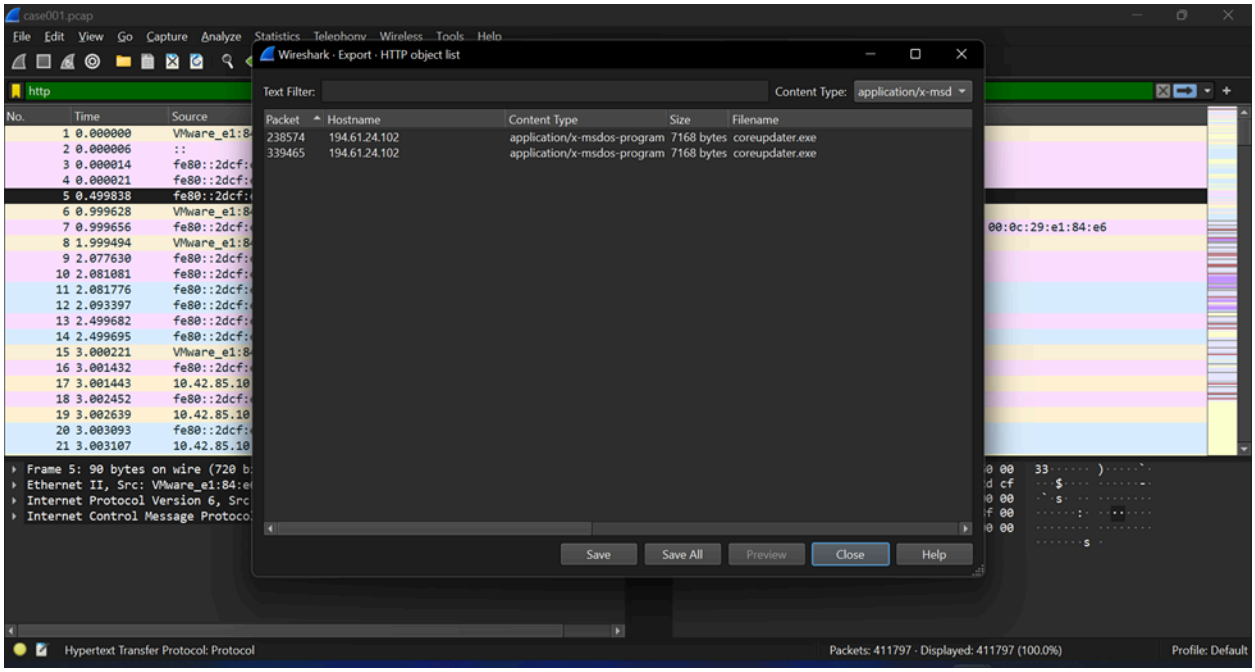
-This filters out the attacking IP address which is 194.61.24.102 and the protocol which is tcp showing the numerous SYN requests which indicate a brute force.



f) Was malware used? If so, what was it? If there was malware answer the Following:

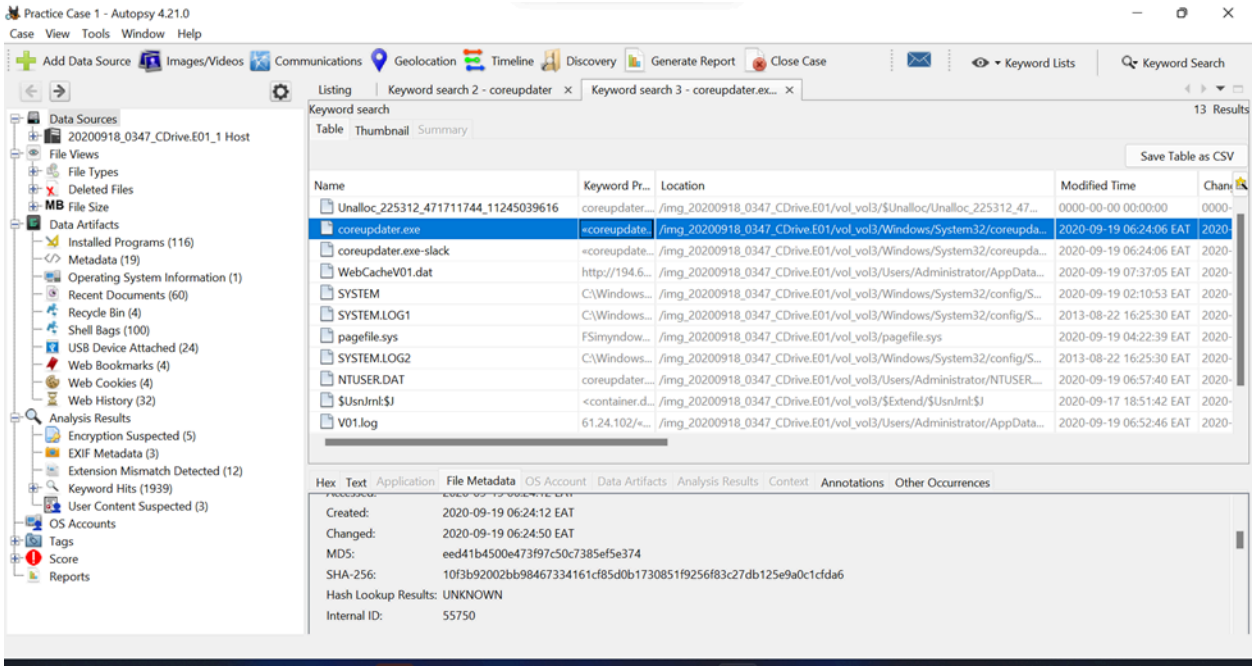
Yes, Trojan

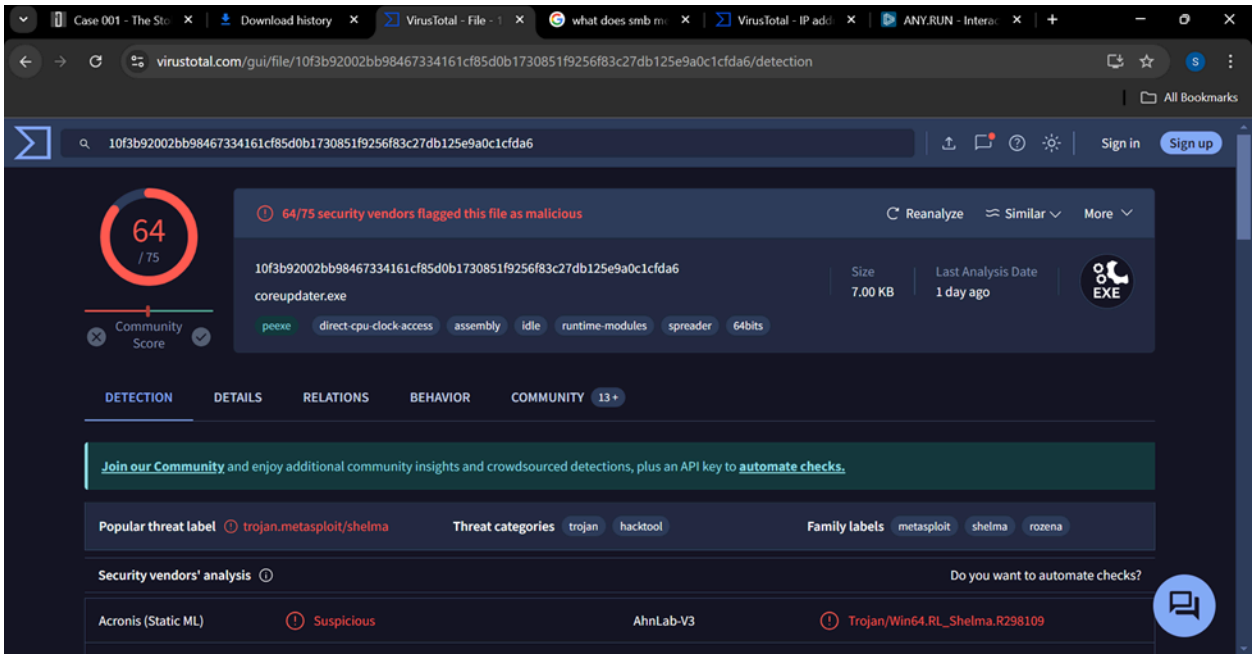
- First answer the question of how is malware delivered to a computer? In what form?
- A user might unknowingly download malware by clicking on a link, opening an attachment in an email, or visiting a compromised website. The malware could be hidden in an executable file (.exe), a script (.bat, .ps1), or other types of files that can run code on the computer as these are typically executable and script files that can be used to deliver malware.
- In wireshark there is a feature that allows us to view files that were transmitted within the file capture and also allows us to download them. Once we get there we check the usual suspects, .exe, .bat, .ps1, .cmd etc.
- Go to the PCAP file, choose option export objects, then choose HTTP, then filter by content type *(Application/x-msd)* – represents the executables *(.exe)*

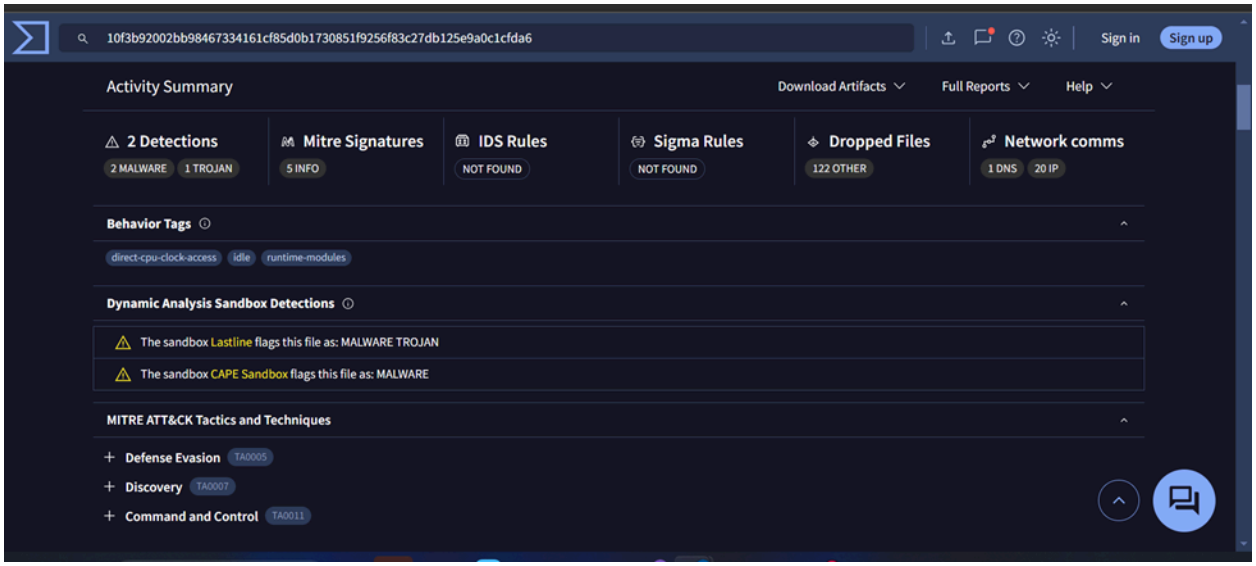


From the above results, we check if the downloaded file made it to the server or might have been blocked by an antivirus:

- Go to Autopsy, search coreupdater.exe
- From the results, we choose the second one which matched with the file found in the packet capture
- Navigate to coreupdater.exe metadata
- Copy the MD5 hash value
- Crosscheck it on go to virus total


Practice Case 1 - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing Keyword search 2 - coreupdater Keyword search 3 - coreupdater.ex...
Keyword search 13 Results
Table Thumbnail Summary
Save Table as CSV
Name Keyword Pr... Location Modified Time
Unalloc_225312_471711744_11245039616 coreupdater... /img_20200918_0347_CDrive.E01/vol_vol3/$Unalloc/Unalloc_225312_47... 0000-00-00 00:00:00
coreupdater.exe «coreupdate.. /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/coreupda... 2020-09-19 06:24:06 EAT
coreupdater.exe-slack «coreupdate... /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/coreupda... 2020-09-19 06:24:06 EAT
WebCacheV01.dat http://194.6... /img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/AppData... 2020-09-19 07:37:05 EAT
SYSTEM C:\Windows... /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config/S... 2020-09-19 02:10:53 EAT
SYSTEM.LOG1 C:\Windows... /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config/S... 2013-08-22 16:25:30 EAT
pagefile.sys FSimyndow... /img_20200918_0347_CDrive.E01/vol_vol3/pagefile.sys 2020-09-19 04:22:39 EAT
SYSTEM.LOG2 C:\Windows... /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config/S... 2013-08-22 16:25:30 EAT
NTUSER.DAT coreupdater... /img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/NTUSER... 2020-09-19 06:57:40 EAT
$UsnJrnl:$J <container.d... /img_20200918_0347_CDrive.E01/vol_vol3/$Extend/$UsnJrnl:$J 2020-09-17 18:51:42 EAT
V01.log 61.24.102/«... /img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/AppData... 2020-09-19 06:52:46 EAT
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Created: 2020-09-19 06:24:12 EAT
Changed: 2020-09-19 06:24:50 EAT
MD5: eed41b4500e473f97c50c7385ef5e374
SHA-256: 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6
Hash Lookup Results: UNKNOWN
Internal ID: 55750
Data Sources
20200918_0347_CDrive.E01_1 Host
File Views
File Types
Deleted Files
File Size
Data Artifacts
Installed Programs (116)
Metadata (19)
Operating System Information (1)
Recent Documents (60)
Recycle Bin (4)
Shell Bags (100)
USB Device Attached (24)
Web Bookmarks (4)
Web Cookies (4)
Web History (32)
Analysis Results
Encryption Suspected (5)
EXIF Metadata (3)
Extension Mismatch Detected (12)
Keyword Hits (1939)
User Content Suspected (3)
OS Accounts
Tags
Score
Reports


Case 001 - The Sto
Download history
VirusTotal - File - 1
what does smb m
VirusTotal - IP add
ANY.RUN - Interac
virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6/detection
All Bookmarks
10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6
Sign in
Sign up
64
/ 75
Community Score
64/75 security vendors flagged this file as malicious
Reanalyze
Similar
More
10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6
coreupdater.exe
Size
7.00 KB
Last Analysis Date
1 day ago
EXE
peexe
direct-cpu-clock-access
assembly
idle
runtime-modules
spreader
64bits
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 13+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Popular threat label
trojan.metasploit/shelma
Threat categories
trojan
hacktool
Family labels
metasploit
shelma
rozena
Security vendors' analysis
Do you want to automate checks?
Acronis (Static ML)
Suspicious
AhnLab-V3
Trojan/Win64.RL_Shelma.R298109



Using the VirusTotal results, the sandbox analysis results in the image provide insights into the behavior of a file when it is executed in a controlled environment, which helps in identifying whether the file is malicious. In this case, the lastline security engine has classified the file as **Trojan Malware.**

(i) What process was malicious?

The file download of Coreupdater.exe

(ii) Identify the IP Address that delivered the payload

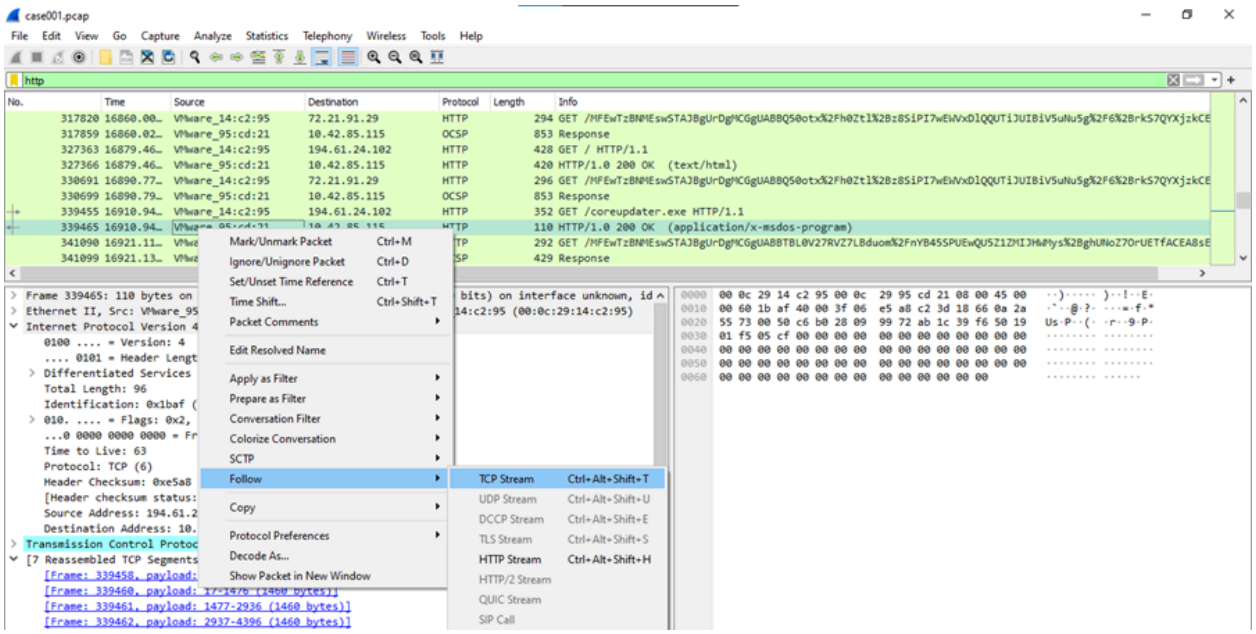
192.61.24.102

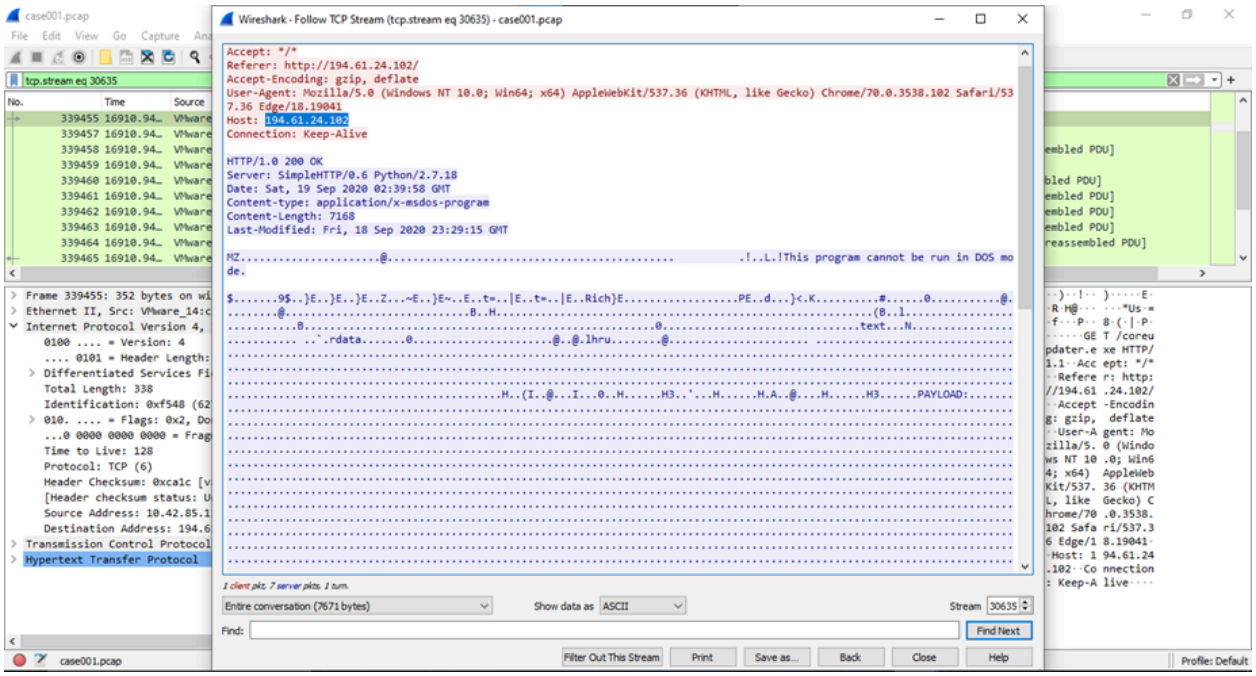
We head back to the packet capture to find the Ip address. From the file filtering in *figure 2*, we can head to the packet number 339465 which shows the packet when the file was downloaded.

Select the packet containing the coreupdater.exe

Right click on it and follow TCP stream

From the results we can get to see the host

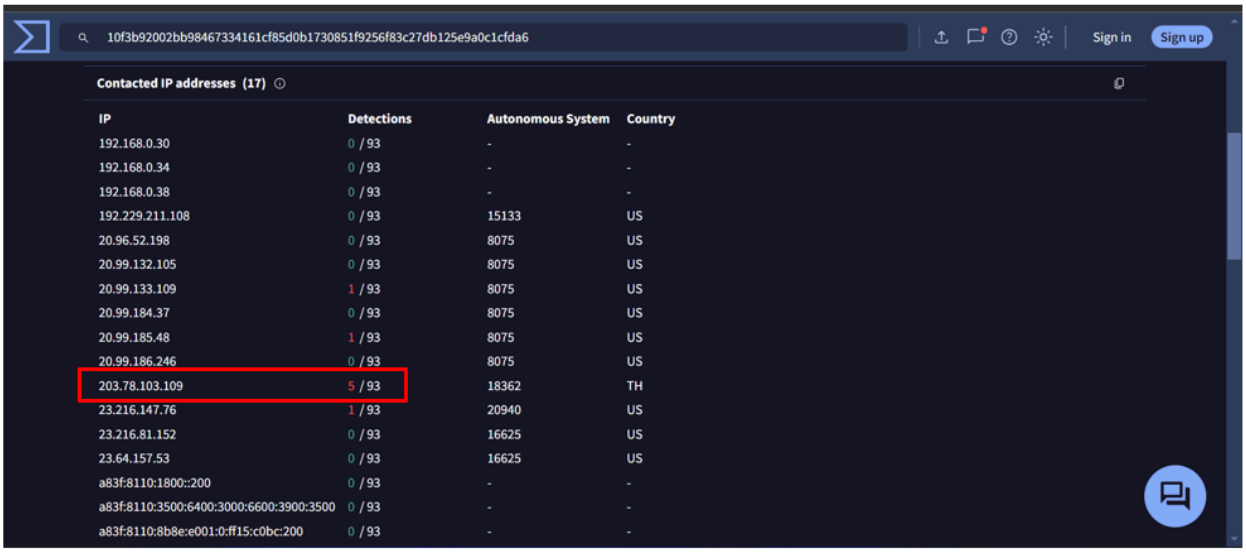




(iii) What IP Address is the malware calling to?

203.78.103.109 – VirusTotal

On VirusTotal, this IP address is the one that reacted most to the the file hash value as shown below



(iv) Where is this malware on disk?

/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/coreupdater.exe

(v) When did it first appear?

2020-09-19 06:24:12.093253200 (EAT)

(vi) Did someone move it?

Yes. From downloads to system32

(vii) What were the capabilities of this malware?

- The hash scan results showed that the malware was a trojan. A trojan has the following capabilities:

  Breach data: Trojans can steal sensitive data from your computer, such as login credentials, credit card details, and personal files.

  Botnet recruitment: Some Trojan horses are designed to convert infected computers and pull them into a botnet that cybercriminals can control remotely.

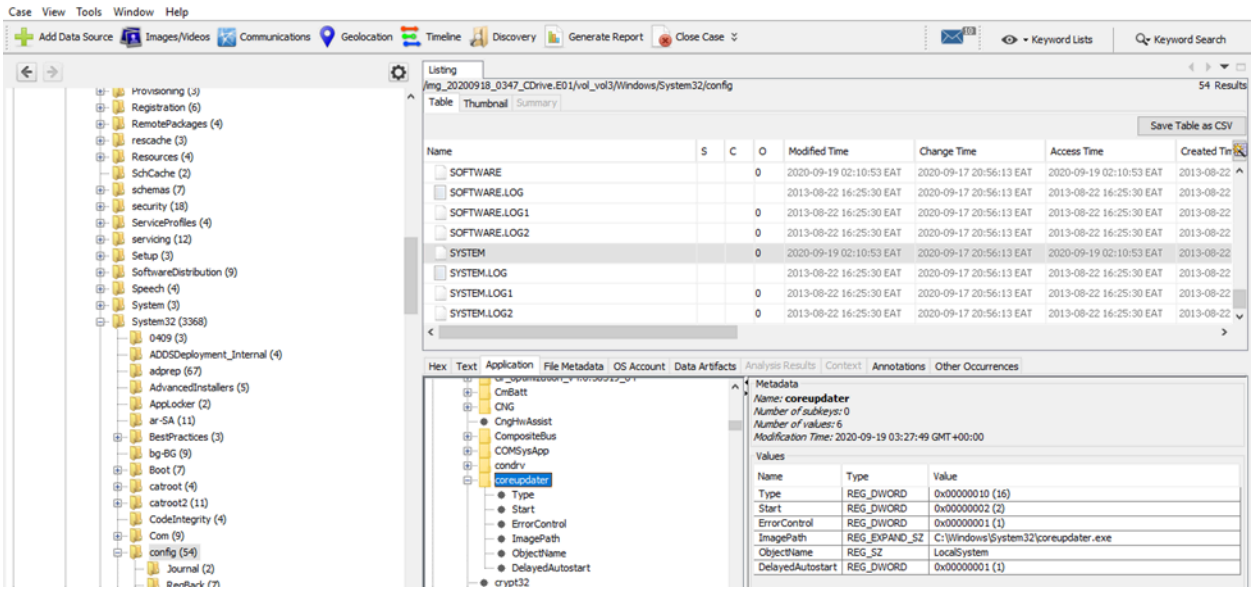
Data destruction: Certain Trojans may be programmed to delete files, corrupt data, or even reformat entire hard drives.

Espionage: Trojan horses can be used to monitor a user's activities, capture screenshots, and record keystrokes to gather sensitive information covertly.

(viii) Is this malware easily obtained?

Yes, it's easily available on a public website

(ix) Was this malware installed with persistence on any machine?



To check for persistence we check the registry files under which the application was installed.

When?

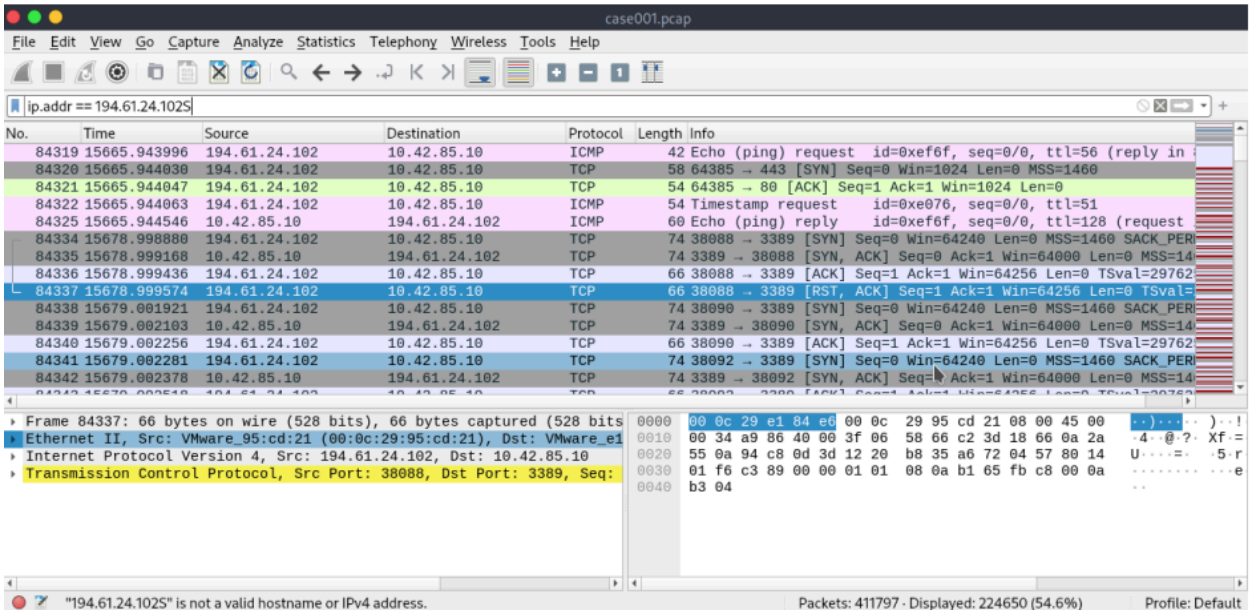
2020-09-19 03:27:49 GMT+00:00

Where?

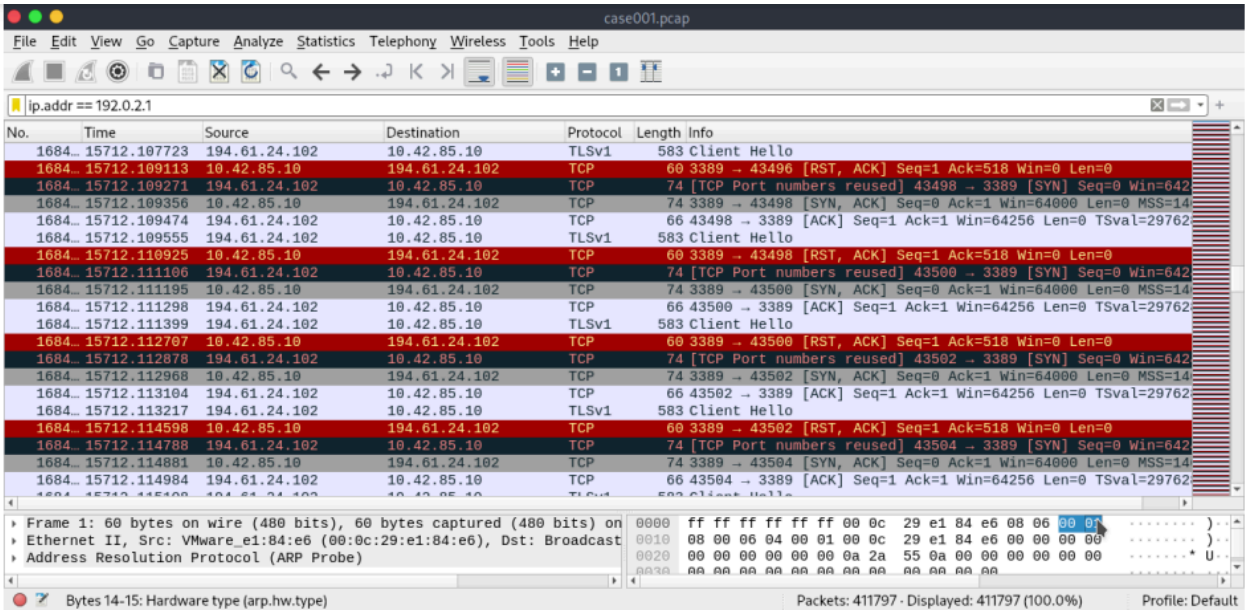
C:\Windows\System32\coreupdater.exe

g. What malicious IP Addresses were involved?: 194.61.24.102

192.61.24.102 is the IP address that initiated the connection as shown below. It does so repeatedly as shown - on opening the pcap file you will notice the IP 192.61.24.102 trying to initiate a connection.

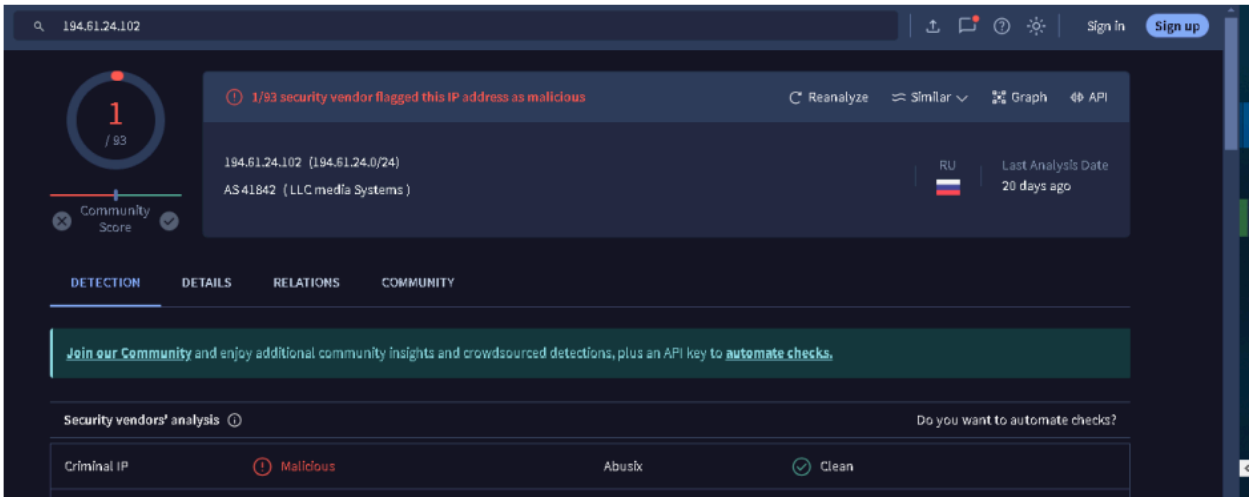


This a screenshot of the pcap file of the network traffic, it shows a lot of SYN,ACK,RST between 194.61.24.102 and 10.42.85.10.This flags show that the IP address 194.61.24.102 was trying to initiate communication with 10.42.85.10 without success and terminations forcefully. This suggests a bruteforce attack. Attacker was trying to use different passwords and usernames.



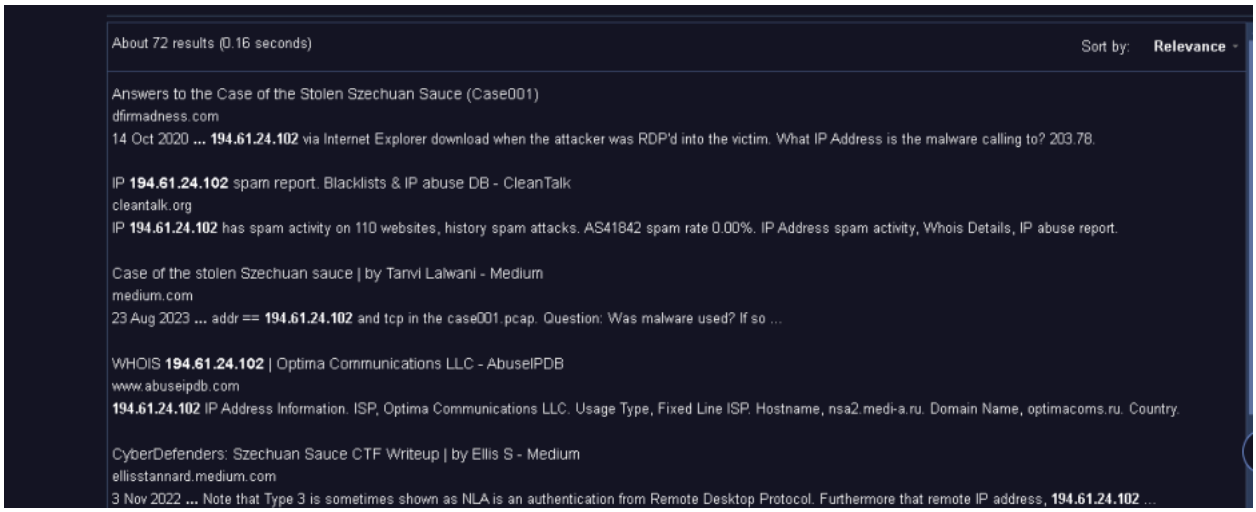
From AbuseIPDB this ip address has been reported.

Result from VirusTotal:

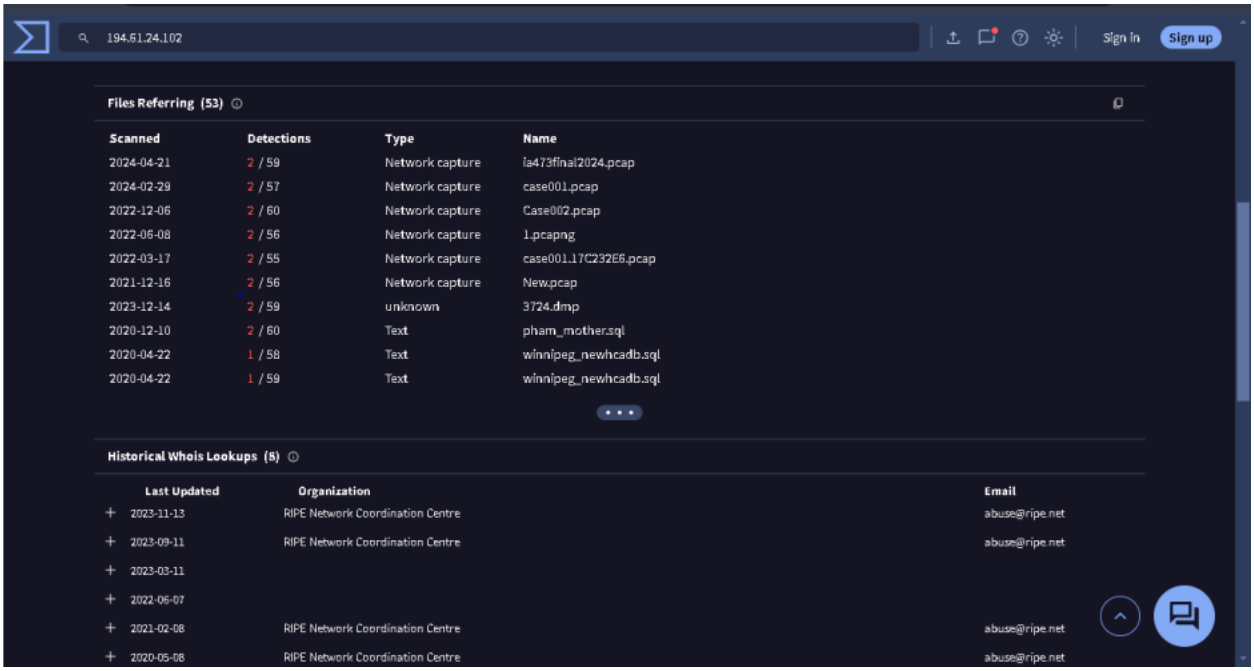


Additional Open source Information from VirusTotal which was important : using this information you can open the links to see what the result contains.

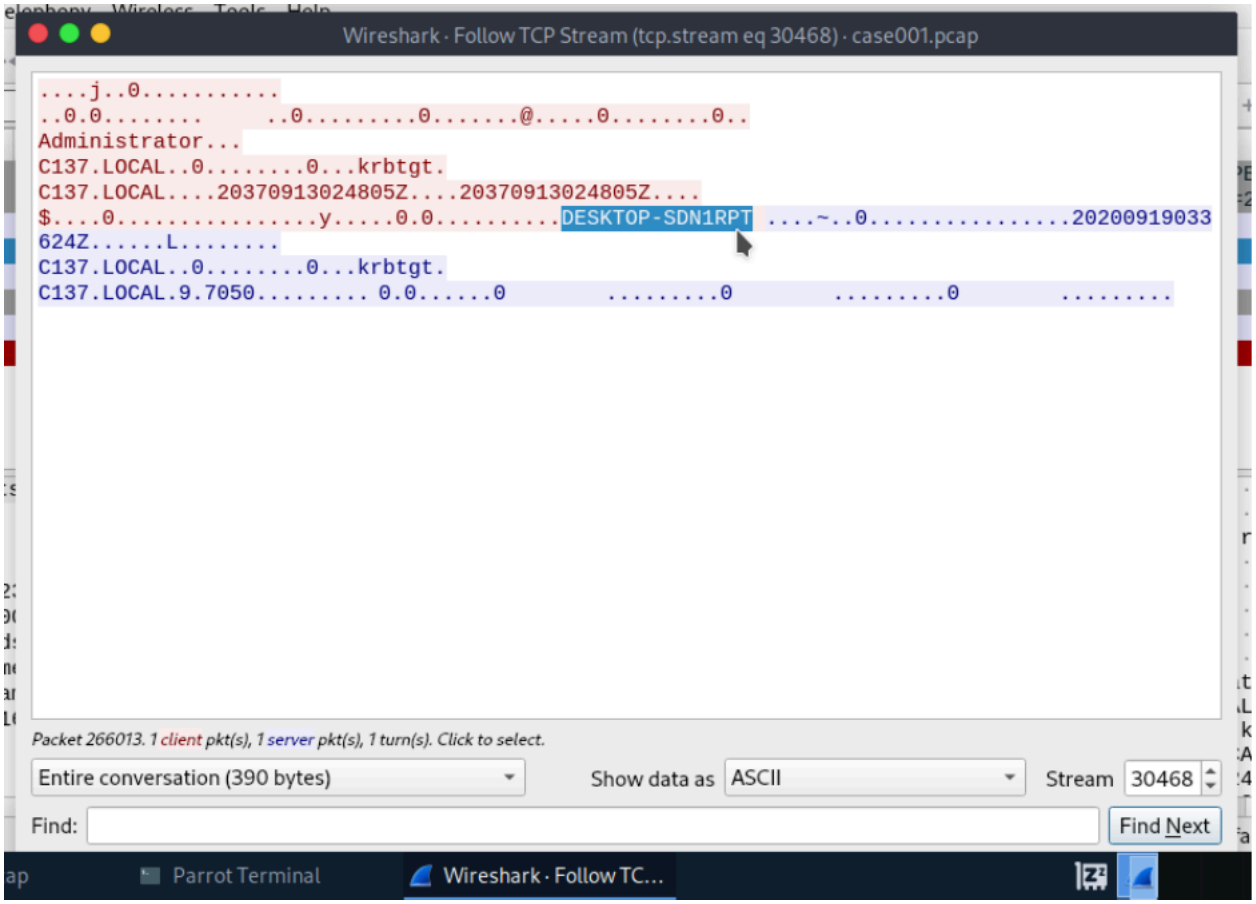
i. Were any IP Addresses from known adversary infrastructure? Yes, the IP address 194.61.24.102 is associated with known adversary infrastructure, based on its appearance in blacklists and its involvement in reported cyber incidents and case studies.



ii. Are these pieces of adversary infrastructure involved in other attacks around the time of the attack? Yes. This a report from virusTotal on different time and years the IP was detected malicious.

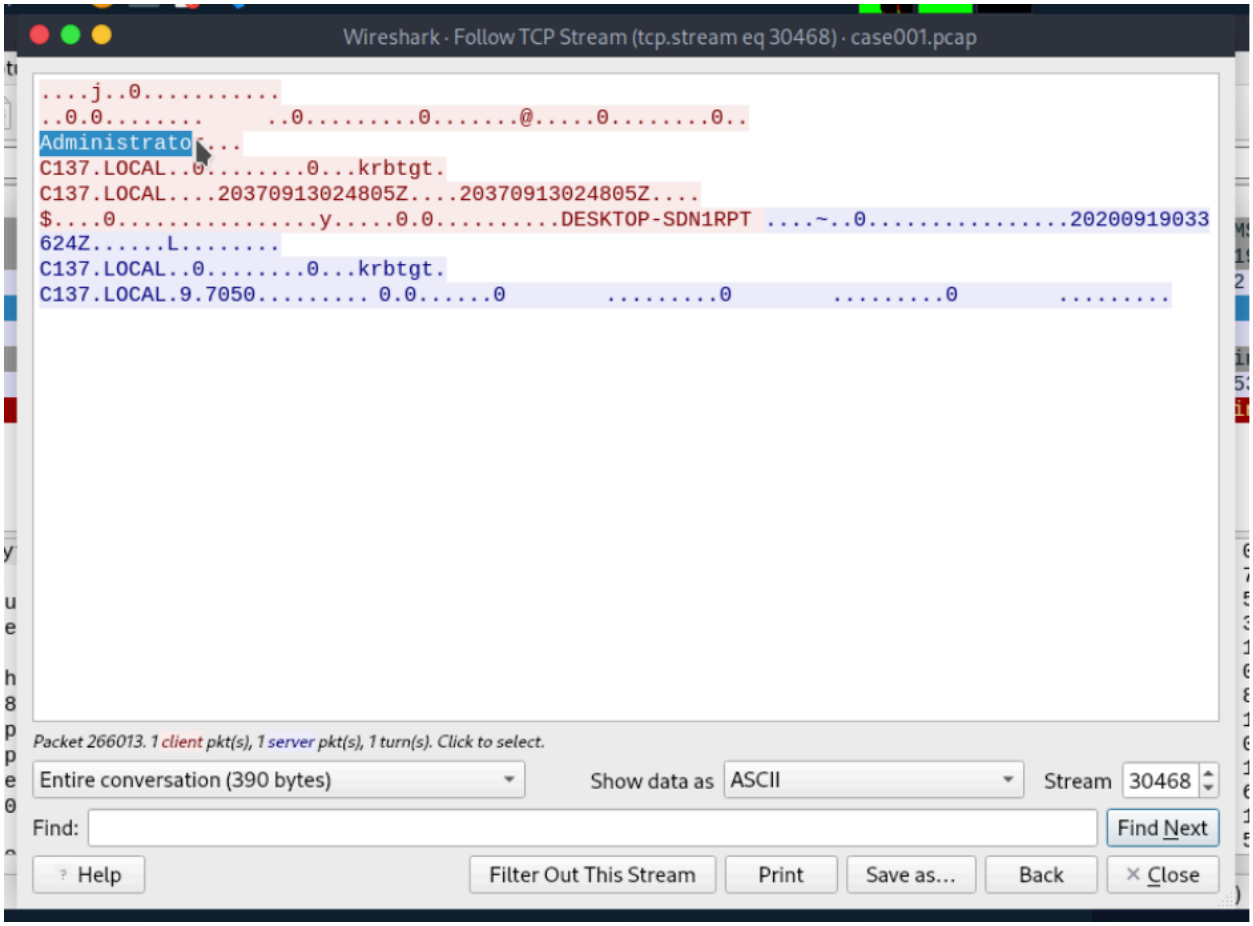


h. Did the attacker access any other systems? Yes.

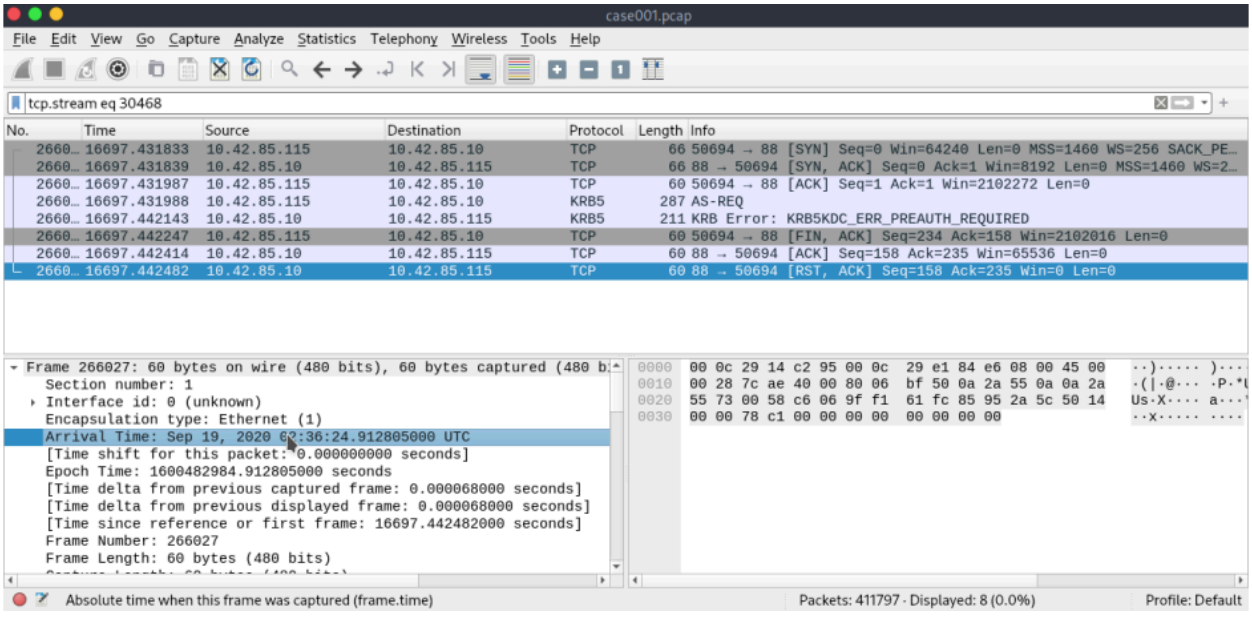


i. How? The attack used Remote Desktop Protocol (RDP) from the Domain Controller (DC) (after compromising the first target he used the target(DC) to navigate to the other) while using the Administrator account.

Administrator account: this is shown by:

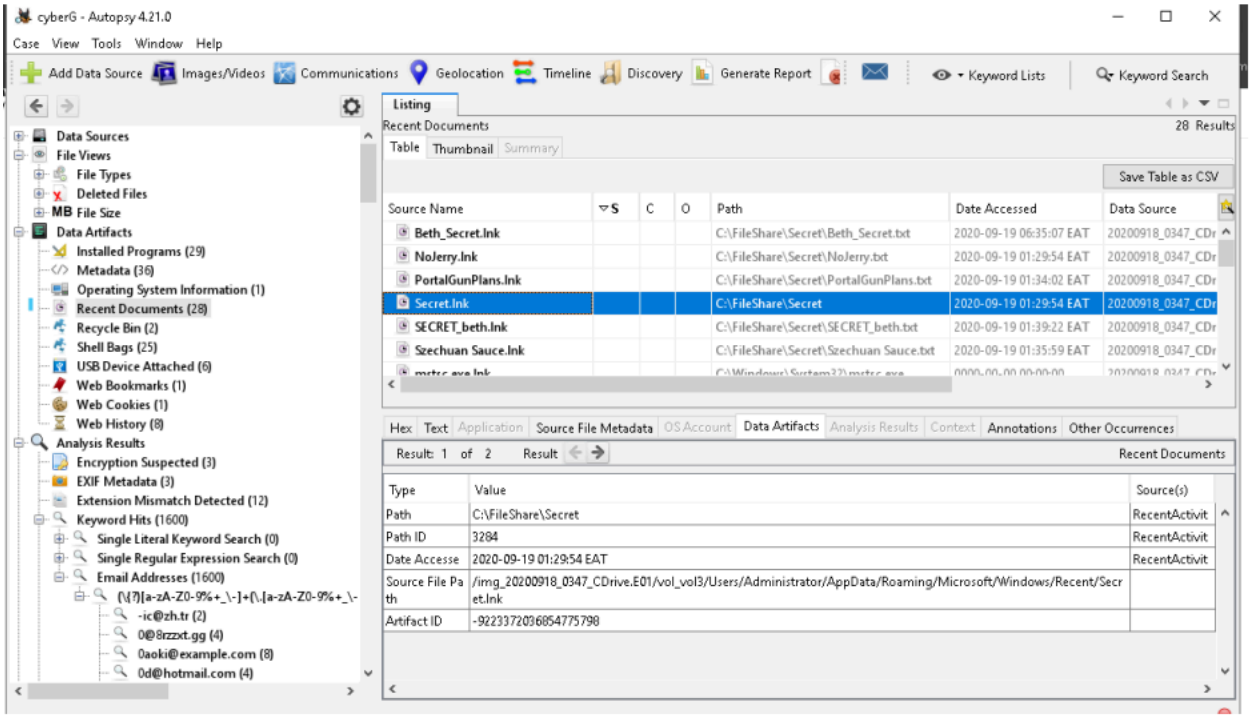


ii. When?: Sep 19, 2020 02:36:24.912805000 UTC

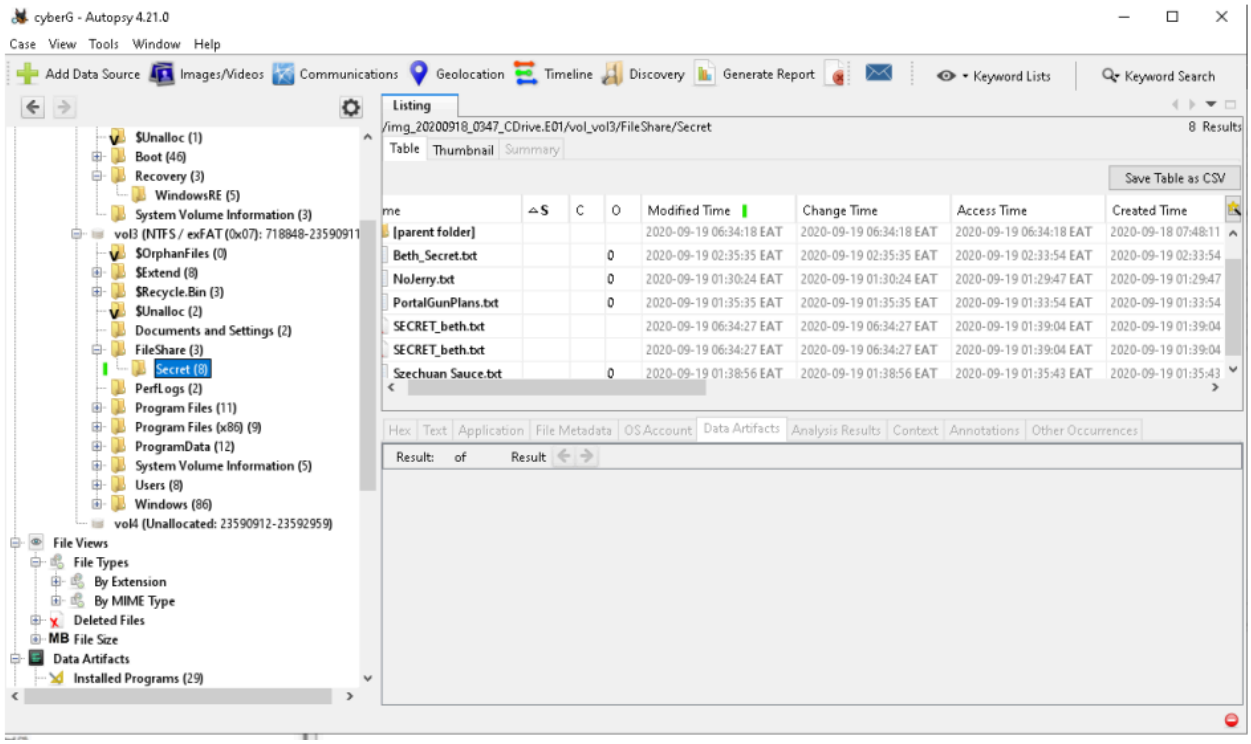


i. Did the attacker steal or access any data?

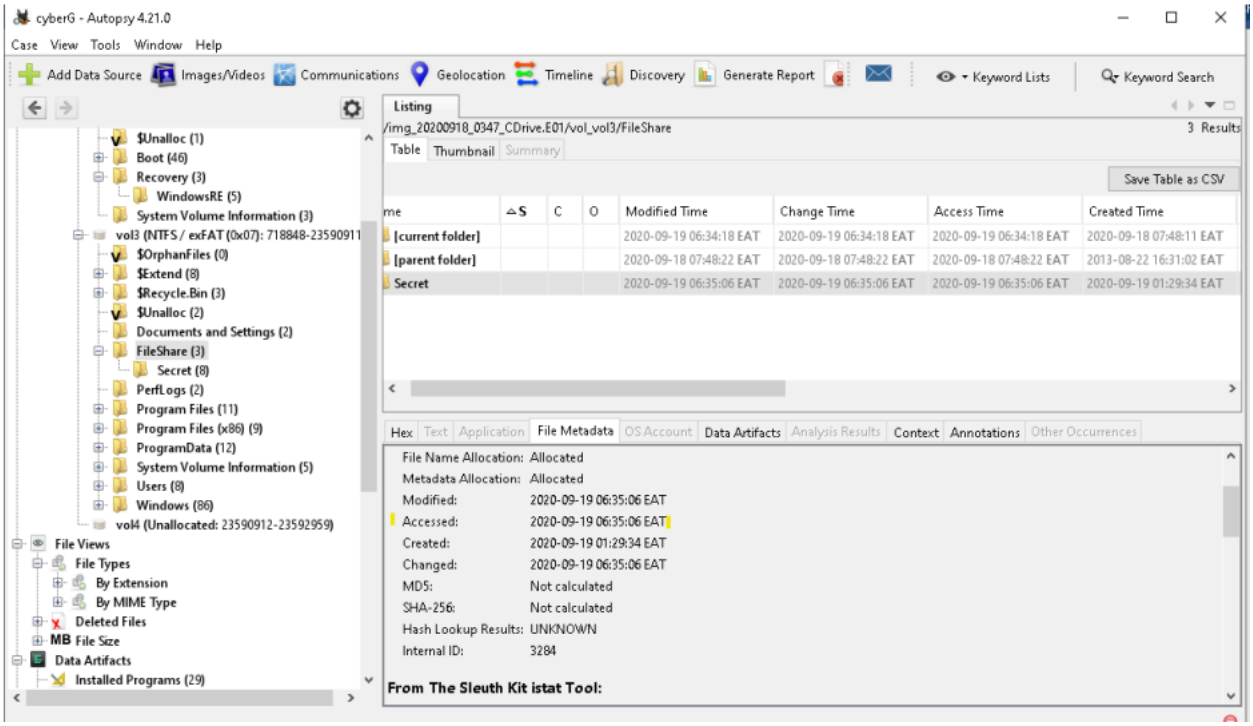
This is a screenshot showing recently accessed file using administrator account



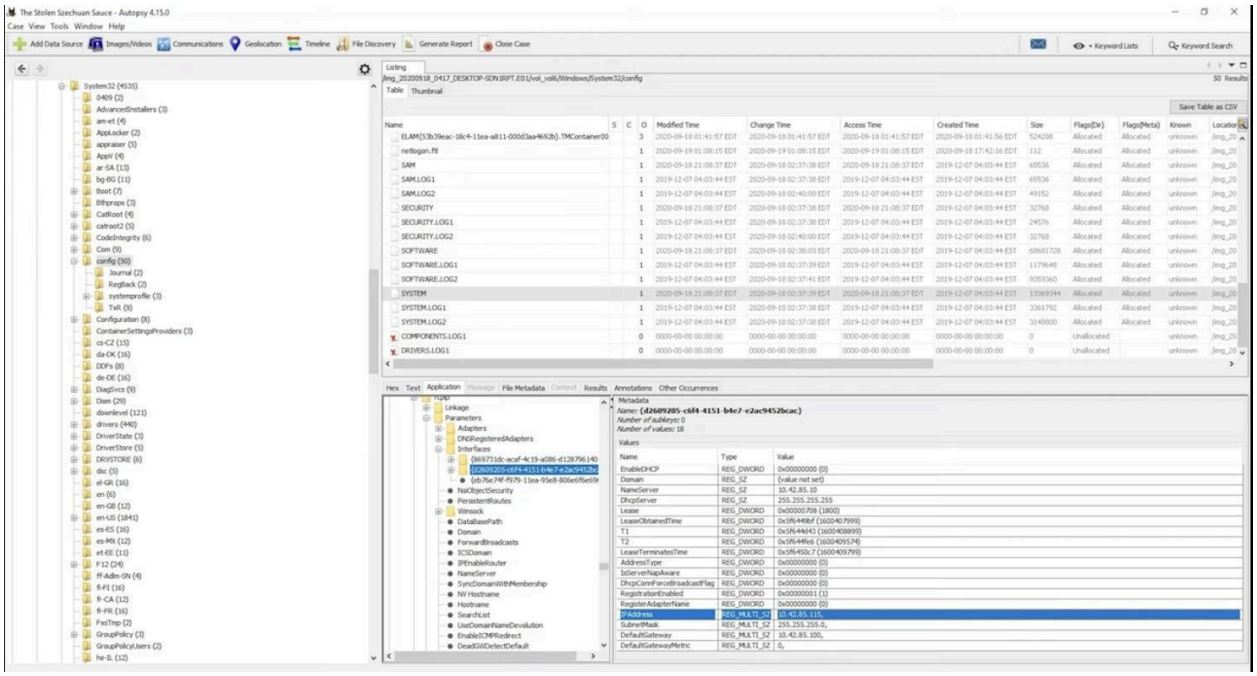
Did attacker steal any data? From the server in the file share folder we can see the attacker accessed the folder named secret and shared its content.



i. When? Accessed: 2020-09-19 06:35:06 EAT



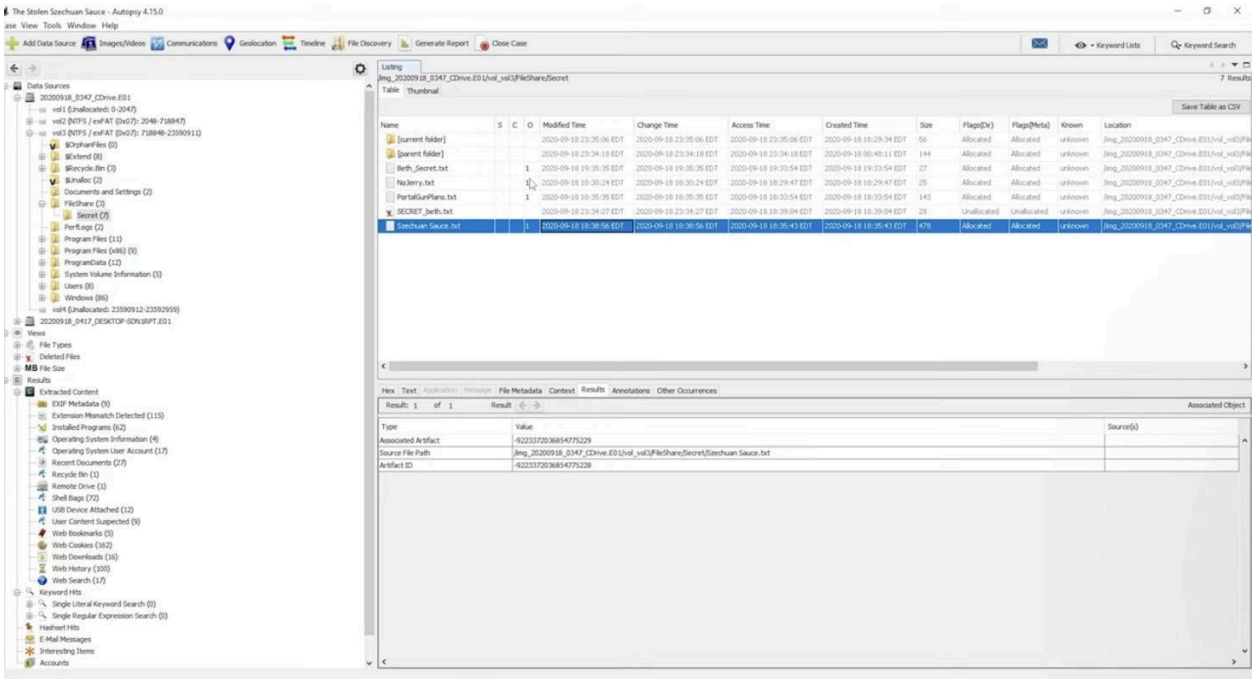
(j)The network layer of the victim network(10.42.85.0/24) has two devices: a Domain Controller with the IP address 10.42.85.10 and a desktop computer with the IP address 10.42.85.115. To see the this, you navigate to the following paths /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config and /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6/Windows/System32/config



(k)What architecture changes should be made immediately?
-Since the initial access was gained through an RDP brute-force attack on the DC, RDP access to the DC should be immediately blocked for external connections. Only devices within the same local network should be allowed to use RDP to connect to the DC

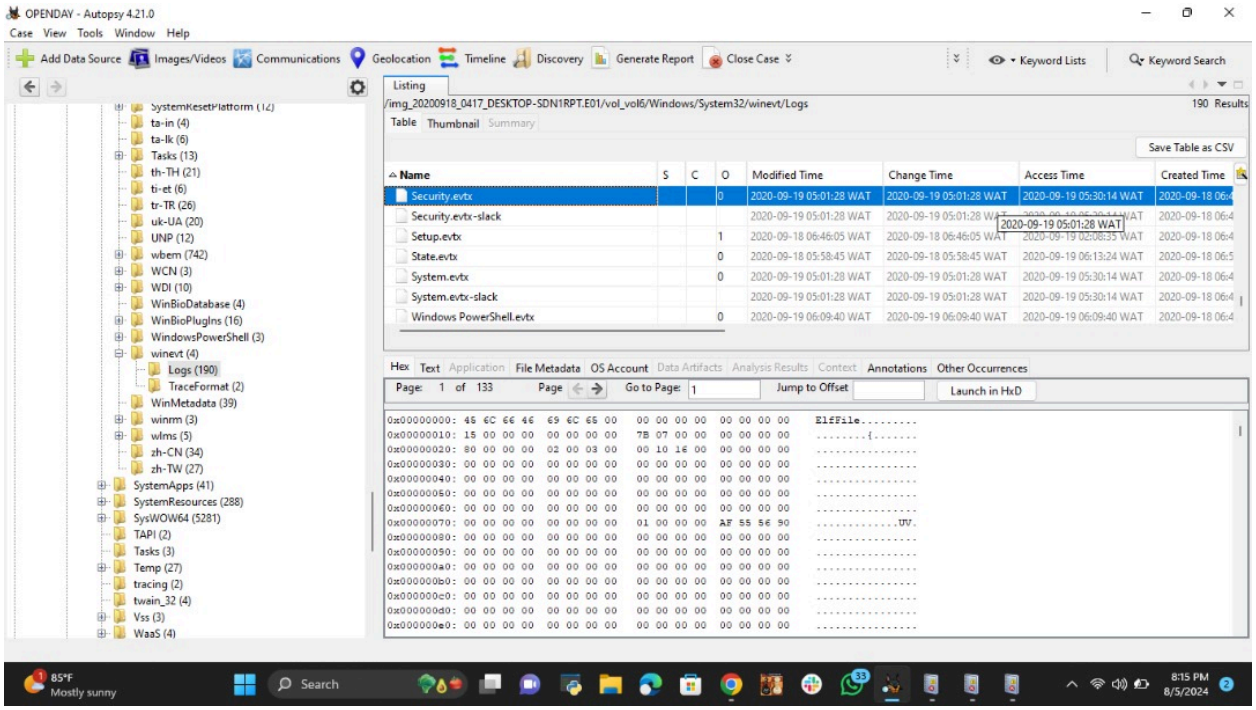
(l) Did the attacker steal the Szechuan sauce? If so, what time? Yes, the attacker did access the Szechuan sauce at around 18:38:56 on 2020-09-18, you can use this path

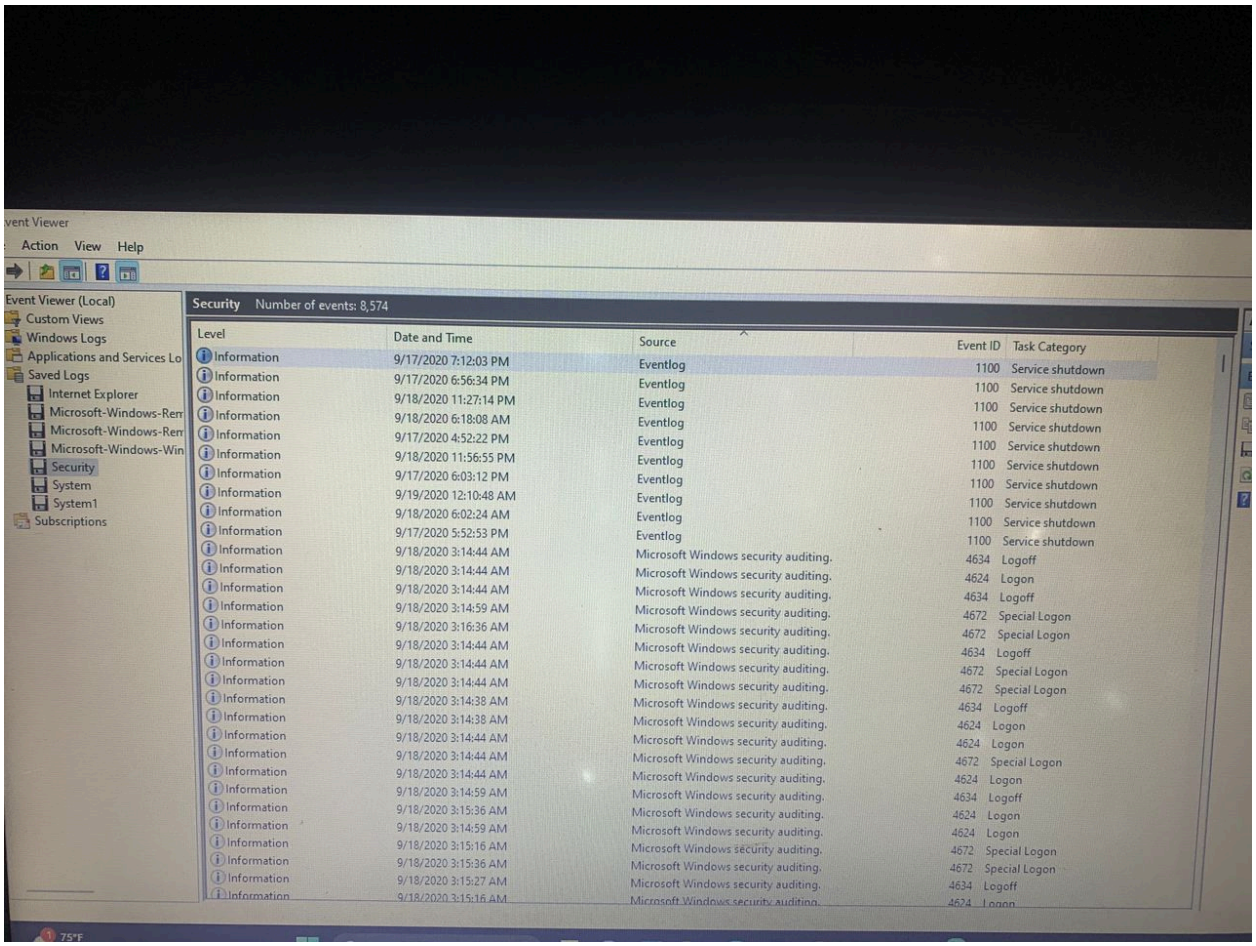
/img_20200918_0347_CDrive.E01/vol_vol3/FileShare/Secret to confirm that.



(m)Did the attacker steal or access any other sensitive files? If so, what times? Yes, it was observed that the attacker accessed the Beth secret file by 23:34:27 on 2020-09-18, this is confirmed via this path
/img_20200918_0347_Drive. E01/vol_vol3/FileShare/Secret

(n)Finally, when was the last known contact with the adversary? The last contact was on 2020-09-19 by 6pm. This can be seen when you right click the security.extx file as seen below and view it via external viewer to see the event logs.


OPENDAY - Autopsy 4.21.0
Case View Tools Window Help
Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case
Keyword Lists Keyword Search
Listing
/img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6/Windows/System32/winevt/Logs
190 Results
Table Thumbnail Summary
Save Table as CSV
Name S C O Modified Time Change Time Access Time Created Time
Security.evtx 0 2020-09-19 05:01:28 WAT 2020-09-19 05:01:28 WAT 2020-09-19 05:30:14 WAT 2020-09-18 06:4
Security.evtx-slack 2020-09-19 05:01:28 WAT 2020-09-19 05:01:28 WAT 2020-09-18 06:4
Setup.evtx 1 2020-09-18 06:46:05 WAT 2020-09-18 06:46:05 WAT 2020-09-19 02:08:35 WAT 2020-09-18 06:4
State.evtx 0 2020-09-18 05:58:45 WAT 2020-09-18 05:58:45 WAT 2020-09-19 06:13:24 WAT 2020-09-18 06:5
System.evtx 0 2020-09-19 05:01:28 WAT 2020-09-19 05:01:28 WAT 2020-09-19 05:30:14 WAT 2020-09-18 06:4
System.evtx-slack 2020-09-19 05:01:28 WAT 2020-09-19 05:01:28 WAT 2020-09-19 05:30:14 WAT 2020-09-18 06:4
Windows PowerShell.evtx 0 2020-09-19 06:09:40 WAT 2020-09-19 06:09:40 WAT 2020-09-19 06:09:40 WAT 2020-09-18 06:4
2020-09-19 05:01:28 WAT
Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences
Page: 1 of 133 Page Go to Page: 1 Jump to Offset Launch in HxD
0x00000000: 45 6C 66 46 69 6C 65 00 00 00 00 00 00 00 00 00 ElfFile.....
0x00000010: 15 00 00 00 00 00 00 00 7B 07 00 00 00 00 00 00 ....{.....
0x00000020: 80 00 00 00 02 00 03 00 00 10 16 00 00 00 00 00 ....
0x00000030: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000040: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000050: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000060: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000070: 00 00 00 00 00 00 00 00 01 00 00 00 AF 55 56 90 ....UV.
0x00000080: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x00000090: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000a0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000b0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000c0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000d0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
0x000000e0: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ....
85°F Mostly sunny
Search
8:15 PM 8/5/2024


vent Viewer
Action View Help
Event Viewer (Local)
Custom Views
Windows Logs
Applications and Services Lo
Saved Logs
Internet Explorer
Microsoft-Windows-Rem
Microsoft-Windows-Rem
Microsoft-Windows-Win
Security
System
System1
Subscriptions
Security Number of events: 8,574
Level Date and Time Source Event ID Task Category
Information 9/17/2020 7:12:03 PM Eventlog 1100 Service shutdown
Information 9/17/2020 6:56:34 PM Eventlog 1100 Service shutdown
Information 9/18/2020 11:27:14 PM Eventlog 1100 Service shutdown
Information 9/18/2020 6:18:08 AM Eventlog 1100 Service shutdown
Information 9/17/2020 4:52:22 PM Eventlog 1100 Service shutdown
Information 9/18/2020 11:56:55 PM Eventlog 1100 Service shutdown
Information 9/17/2020 6:03:12 PM Eventlog 1100 Service shutdown
Information 9/19/2020 12:10:48 AM Eventlog 1100 Service shutdown
Information 9/18/2020 6:02:24 AM Eventlog 1100 Service shutdown
Information 9/17/2020 5:52:53 PM Eventlog 1100 Service shutdown
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4634 Logoff
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4624 Logon
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4634 Logoff
Information 9/18/2020 3:14:59 AM Microsoft Windows security auditing. 4672 Special Logon
Information 9/18/2020 3:16:36 AM Microsoft Windows security auditing. 4672 Special Logon
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4634 Logoff
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4672 Special Logon
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4672 Special Logon
Information 9/18/2020 3:14:38 AM Microsoft Windows security auditing. 4634 Logoff
Information 9/18/2020 3:14:38 AM Microsoft Windows security auditing. 4624 Logon
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4624 Logon
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4672 Special Logon
Information 9/18/2020 3:14:44 AM Microsoft Windows security auditing. 4624 Logon
Information 9/18/2020 3:14:59 AM Microsoft Windows security auditing. 4634 Logoff
Information 9/18/2020 3:15:36 AM Microsoft Windows security auditing. 4624 Logon
Information 9/18/2020 3:14:59 AM Microsoft Windows security auditing. 4624 Logon
Information 9/18/2020 3:15:16 AM Microsoft Windows security auditing. 4672 Special Logon
Information 9/18/2020 3:15:36 AM Microsoft Windows security auditing. 4672 Special Logon
Information 9/18/2020 3:15:27 AM Microsoft Windows security auditing. 4634 Logoff
Information 9/18/2020 3:15:16 AM Microsoft Windows security auditing. 4624 Logon

CONCLUSION.

The investigation determined that the breach occurred on 19th September 2020, originating from an IP address 194.61.24.102 , which is the IP address that delivered the payload additionally , it has multiple reports as an adversary infrastructure. The attackers gained access through a trojan (coreupdater.exe) , compromising several key servers and systems within the network.

The attackers managed to alter a number of important files in addition to gaining access to private information, including the secret sauce recipe. A lack of strong security measures, such as weak access control, inadequate monitoring, and out-of-date software, made the intrusion easier to achieve.

To prevent future breaches, we recommend implementing enhanced security controls, including multi-factor authentication, regular software updates, and continuous network monitoring.To further secure the environment and protect against similar risks in the future, stringent access controls, frequent personnel training, and the implementation of a thorough security strategy are all necessary.

This incident serves as a reminder of the value of proactive cybersecurity measures and the necessity of constant vigilance to protect sensitive assets from sophisticated cyber threats.

REFERENCES:

Autopsy download. *Autopsy (Version 4.21.0)*. https://www.autopsy.com/

PCAP Analysis file. https://dfirmadness.com/case-001-pcap-analysis/

Autopsy user guide documentation. https://sleuthkit.org/autopsy/docs/user-docs/4.21.0/

Loughran, C. (2022, June 9). *Virustotal API: A powerful tool for security automation*. Tines. https://www.tines.com/blog/virustotal-api-security-automation

Disk analysis with Autopsy. https://youtu.be/o6boK9dG-Lc

Fortinet. *Malware analysis*. https://www.fortinet.com/resources/cyberglossary/malware-analysis

https://dfirmadness.com/case-001-autoruns-analysis/

https://dfirmadness.com/case-001-memory-analysis/

Lalwani, T. (2023, June 28). *Case of the stolen Szechuan sauce*. Medium. https://medium.com/@tanvilalwani5/case-of-the-stolen-szechuan-sauce-bd440e5c2a6d