

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”.

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol2 (NTFS / exFAT (0x07): 2048-718847)	2	2048	716800	NTFS / exFAT (0x07)	Allocated
vol3 (NTFS / exFAT (0x07): 718848-23590911)	3	718848	22872064	NTFS / exFAT (0x07)	Allocated
vol4 (Unallocated: 23590912-23592959)	4	23590912	2048	Unallocated	Unallocated

Type	Value	Source(s)
Name	CITADEL-DC01	Recent Activity
Domain	C137.local	Recent Activity
Program Name	Windows Server 2012 R2 Standard Evaluation	Recent Activity
Processor Archit	AMD64	Recent Activity
Temporary Files	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00252-10000-0000-AA228	Recent Activity
Owner	Windows User	Recent Activity

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”.

The screenshot shows the Autopsy 4.21.0 forensic analysis interface. The left sidebar displays a tree view of data sources, including 'Data Sources' (20200918_0417_DESKTOP-SDN1RPT.E01) and various file types like 'File Views', 'File Types', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Recent Documents', 'Remote Drive', 'Run Programs', 'Shell Bags', 'USB Device Attached', 'Web Bookmarks', 'Web Cookies', 'Web Downloads', 'Web History', 'Web Search', 'Analysis Results', and 'OS Accounts'. The main pane shows a 'Listing' of disk partitions for the selected source. The table includes columns for Name, ID, Starting Sector, Length in Sectors, Description, and Flags. The table contains 9 entries:

Name	ID	Starting Sector	Length in Sectors	Description	Flags
vol1 (Unallocated: 0-2047)	1	0	2048	Unallocated	Unallocated
vol4 (EFI system partition: 2048-206847)	4	2048	204800	EFI system partition	Allocated
vol5 (Microsoft reserved partition: 206848-239616)	5	206848	32768	Microsoft reserved partition	Allocated
vol7 (Unallocated: 30417013-30418943)	6	239616	30177397	Basic data partition	Allocated
vol8 (Unknown: 30418944-31453183)	7	30417013	1931	Unallocated	Unallocated
vol8 (Unknown: 30418944-31453183)	8	30418944	1034240	Unknown	Allocated
vol9 (Unallocated: 31453184-31457279)	9	31453184	4096	Unallocated	Unallocated

Below the table, there are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Data Artifacts' tab is selected, showing 'Operating System Information' details:

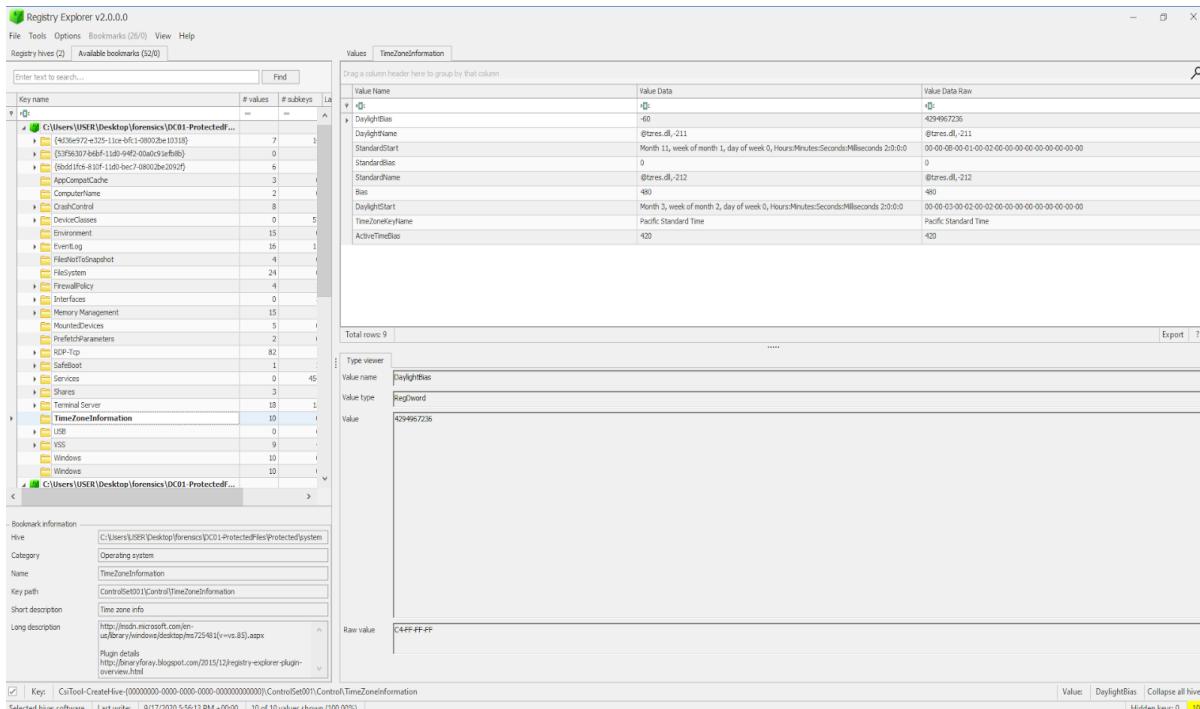
Type	Value	Source(s)
Name	DESKTOP-SDN1RPT	Recent Activity
Domain	C137.local	Recent Activity
Program Name	Windows 10 Enterprise Evaluation	Recent Activity
Processor Archit	AMD64	Recent Activity
Temporary Files	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00329-20000-00001-AA089	Recent Activity
Owner	Admin	Recent Activity

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

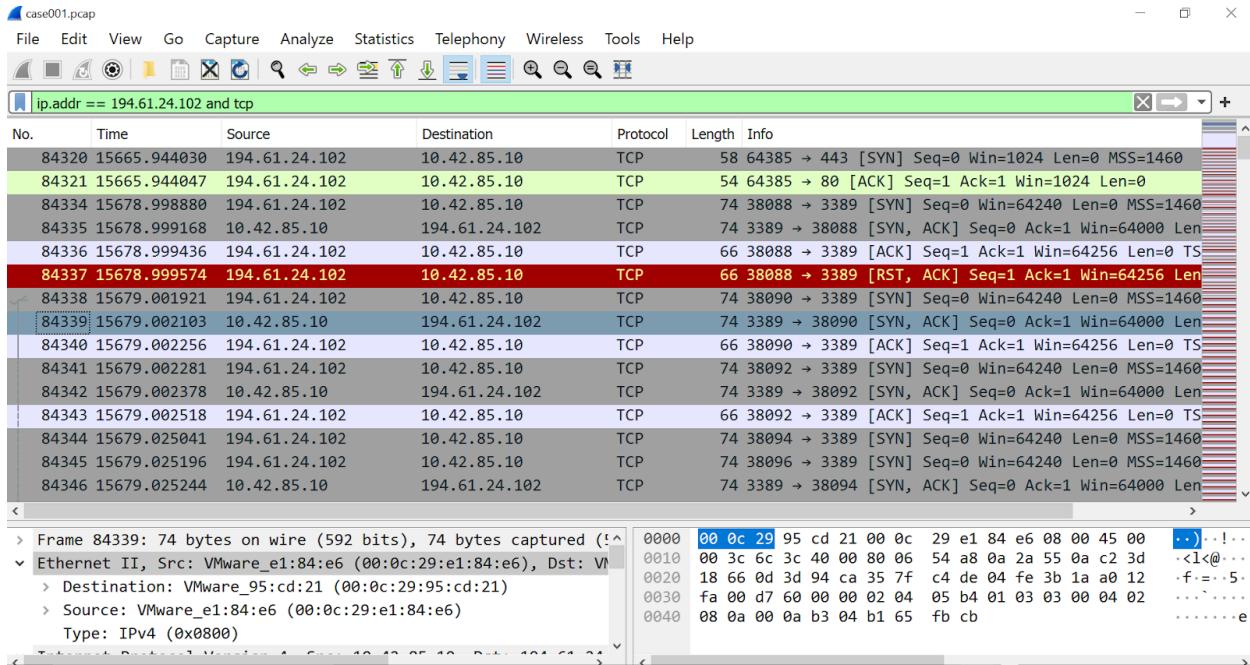
- There was a breach, as indicated by all aspects of this analysis, as further explanation will be provided through the answers to the following questions as well as providing additional insights into the nature and extent of the breach .

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.

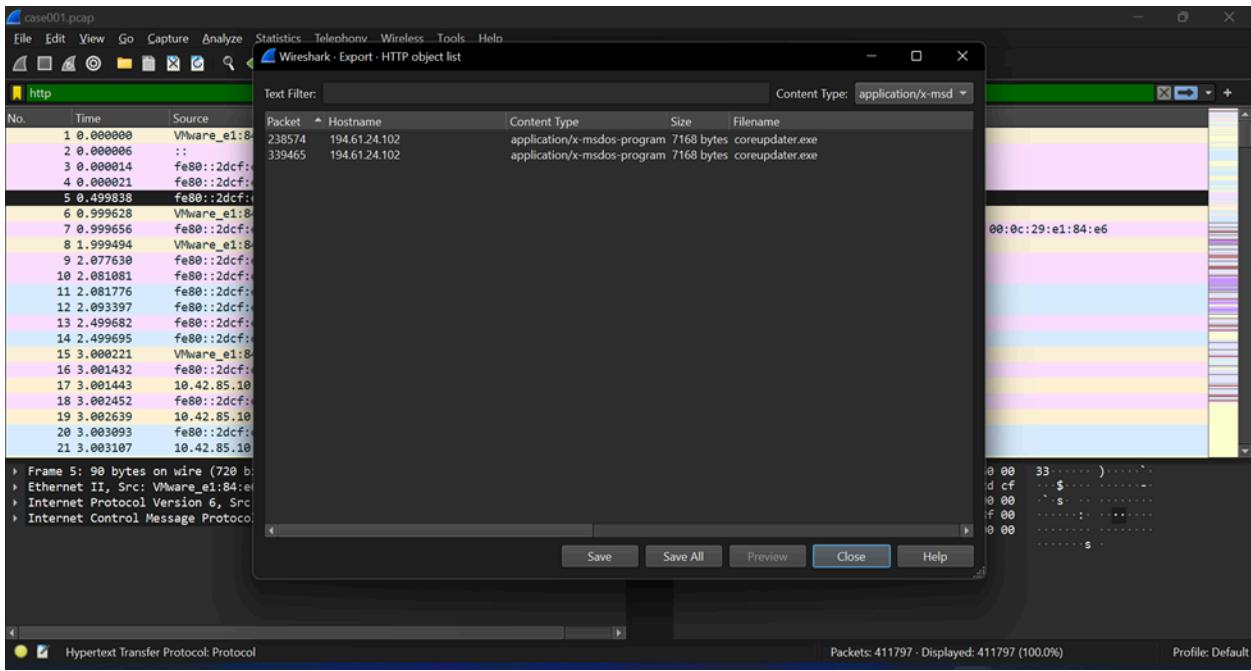
-This filters out the attacking IP address which is 194.61.24.102 and the protocol which is tcp showing the numerous SYN requests which indicate a brute force.



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

Data Sources

- 20200918_0347_CDrive.E01_1 Host
- File Views
- File Types
- Deleted Files
- MB 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

Keyword search

Listing | Keyword search 2 - coreupdater | Keyword search 3 - coreupdater.exe... | Keyword Search

Table Thumbnail Summary

Save Table as CSV

Name	Keyword Pr...	Location	Modified Time	Chang...
Unalloc_225312_471711744_11245039616	coreupdater...	/img_20200918_0347_CDrive.E01/vol_vo3/\$Unalloc/Unalloc_225312_47...	0000-00-00 00:00:00	0000-
coreupdater.exe	coreupdater...	/img_20200918_0347_CDrive.E01/vol_vo3/Windows/System32/coreupa...	2020-09-19 06:24:06 EAT	2020
coreupdater.exe-slack	<coreupdat...	/img_20200918_0347_CDrive.E01/vol_vo3/Windows/System32/coreupa...	2020-09-19 06:24:06 EAT	2020
WebCacheV01.dat	http://194.6...	/img_20200918_0347_CDrive.E01/vol_vo3/Users/Administrator/AppData...	2020-09-19 07:37:05 EAT	2020
SYSTEM	C:\Windows...	/img_20200918_0347_CDrive.E01/vol_vo3/Windows\System32/config/S...	2020-09-19 02:10:53 EAT	2020
SYSTEM.LOG1	C:\Windows...	/img_20200918_0347_CDrive.E01/vol_vo3/Windows\System32/config/S...	2013-08-22 16:25:30 EAT	2020
pagefile.sys	F\$imyndow...	/img_20200918_0347_CDrive.E01/vol_vo3/pagefile.sys	2020-09-19 04:22:39 EAT	2020
SYSTEM.LOG2	C:\Windows...	/img_20200918_0347_CDrive.E01/vol_vo3/Windows\System32/config/S...	2013-08-22 16:25:30 EAT	2020
NTUSER.DAT	coreupdater...	/img_20200918_0347_CDrive.E01/vol_vo3/Users/Administrator/NTUSER...	2020-09-19 06:57:40 EAT	2020
\$UsnJnl:\$	<container.d...	/img_20200918_0347_CDrive.E01/vol_vo3/\$Extend/\$UsnJnl:\$	2020-09-17 18:51:42 EAT	2020
V01.log	61.24.102/...	/img_20200918_0347_CDrive.E01/vol_vo3/Users/Administrator/AppData...	2020-09-19 06:52:46 EAT	2020

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

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

Σ 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

64 / 75 security vendors flagged this file as malicious

coreupdater.exe

Community Score: 75

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: Acronis (Static ML) Suspicious AhnLab-V3 Trojan/Win64.RL_Shelma.R298109

Do you want to automate checks?

The screenshot shows the VirusTotal analysis interface for the file 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6. The top navigation bar includes 'Sign in' and 'Sign up'. Below the search bar, there are sections for 'Activity Summary', 'Download Artifacts', 'Full Reports', and 'Help'. The 'Activity Summary' section shows 2 Detections (2 MALWARE, 1 TROJAN), 5 Mitre Signatures (INFO), 0 IDS Rules (NOT FOUND), 0 Sigma Rules (NOT FOUND), 122 Dropped Files (1 DNS, 20 IP), and 0 Network comms (1 DNS, 20 IP). The 'Behavior Tags' section lists 'direct-cpu-clock-access', 'idle', and 'runtime-modules'. The 'Dynamic Analysis Sandbox Detections' section shows two warnings: 'The sandbox Lastline flags this file as: MALWARE TROJAN' and 'The sandbox CAPE Sandbox flags this file as: MALWARE'. The 'MITRE ATT&CK Tactics and Techniques' section lists three categories: Defense Evasion (TA0005), Discovery (TA0007), and Command and Control (TA0011). A blue circular icon with a white speech bubble is visible on the right.

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

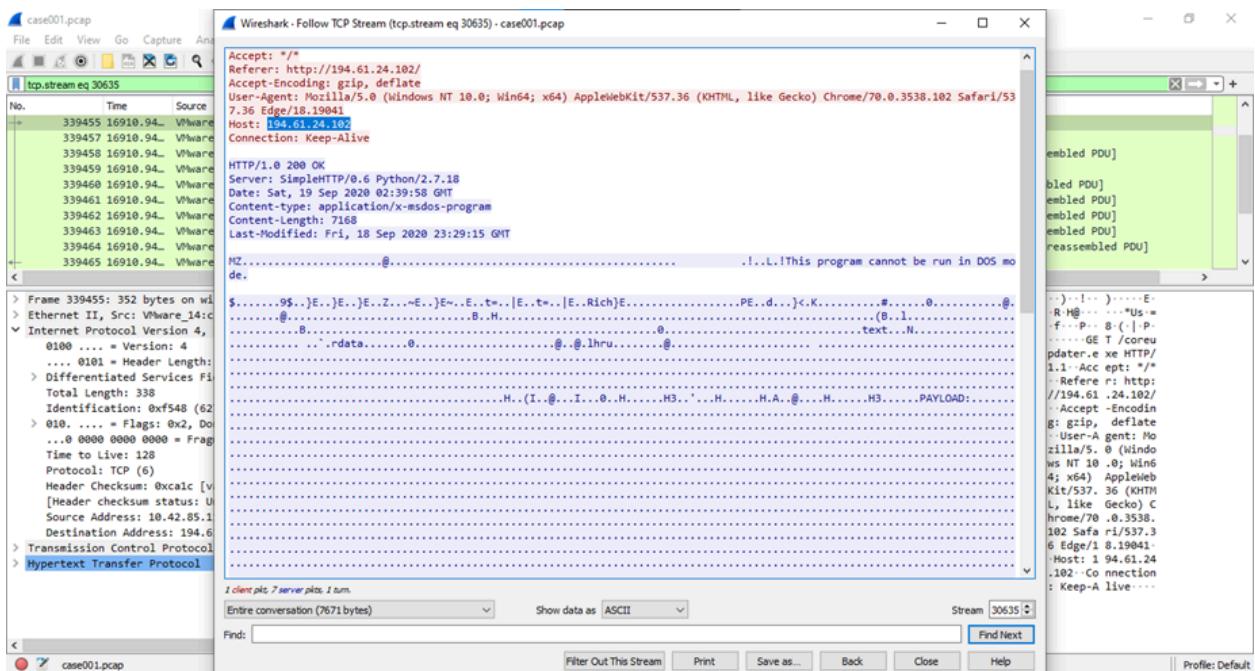
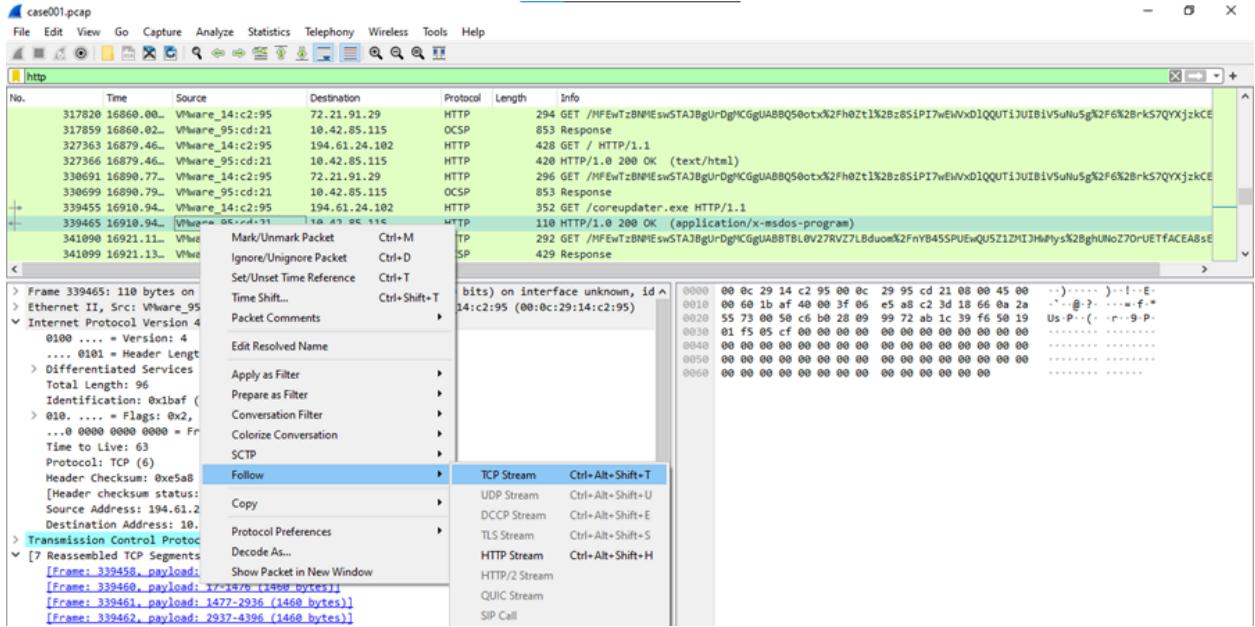
192.61.24.102

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

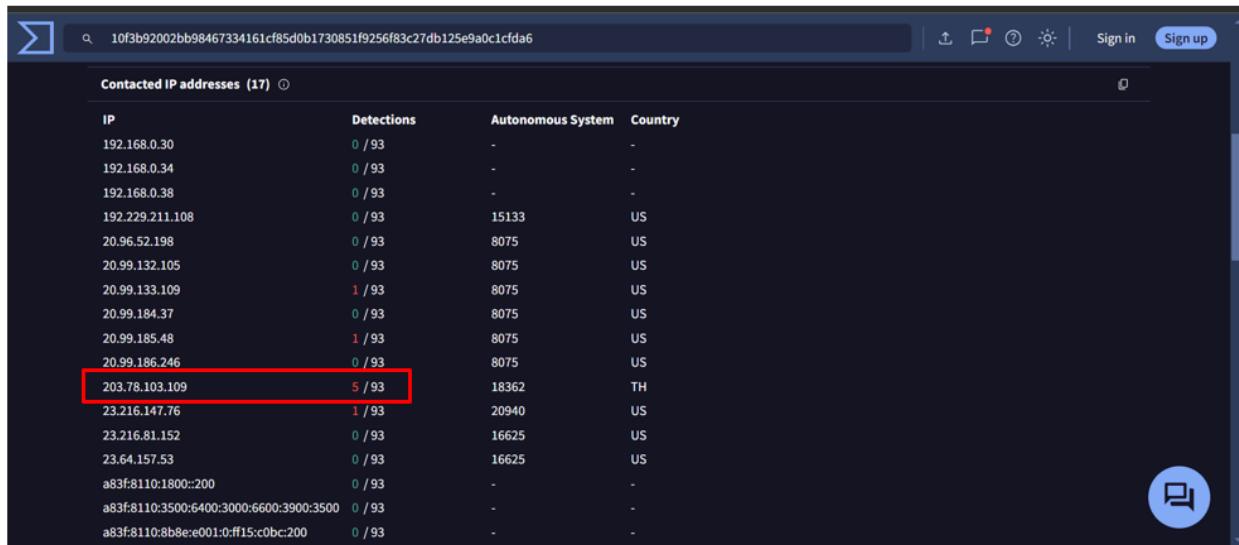
From the results we can get to see the host



(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 file hash value as shown below



Contacted IP addresses (17)			
IP	Detections	Autonomous System	Country
192.168.0.30	0 / 93	-	-
192.168.0.34	0 / 93	-	-
192.168.0.38	0 / 93	-	-
192.229.211.108	0 / 93	15133	US
20.96.52.198	0 / 93	8075	US
20.99.132.105	0 / 93	8075	US
20.99.133.109	1 / 93	8075	US
20.99.184.37	0 / 93	8075	US
20.99.185.48	1 / 93	8075	US
20.99.186.246	0 / 93	8075	US
203.78.103.109	5 / 93	18362	TH
23.216.147.76	1 / 93	20940	US
23.216.81.152	0 / 93	16625	US
23.64.157.53	0 / 93	16625	US
a83f:8110:1800::200	0 / 93	-	-
a83f:8110:3500:6400:3000:6600:3900:3500	0 / 93	-	-
a83f:8110:8b8:e001:0:ff15:c0bc:200	0 / 93	-	-

(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?

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
SOFTWARE	0			2020-09-19 02:10:53 EAT	2020-09-17 20:56:13 EAT	2020-09-19 02:10:53 EAT	2013-08-22 16:25:30 EAT
SOFTWARE.LOG				2013-08-22 16:25:30 EAT	2020-09-17 20:56:13 EAT	2013-08-22 16:25:30 EAT	2013-08-22
SOFTWARE.LOG1	0			2013-08-22 16:25:30 EAT	2020-09-17 20:56:13 EAT	2013-08-22 16:25:30 EAT	2013-08-22
SOFTWARE.LOG2	0			2013-08-22 16:25:30 EAT	2020-09-17 20:56:13 EAT	2013-08-22 16:25:30 EAT	2013-08-22
SYSTEM	0			2020-09-19 02:10:53 EAT	2020-09-17 20:56:13 EAT	2020-09-19 02:10:53 EAT	2013-08-22
SYSTEM.LOG				2013-08-22 16:25:30 EAT	2020-09-17 20:56:13 EAT	2013-08-22 16:25:30 EAT	2013-08-22
SYSTEM.LOG1	0			2013-08-22 16:25:30 EAT	2020-09-17 20:56:13 EAT	2013-08-22 16:25:30 EAT	2013-08-22
SYSTEM.LOG2	0			2013-08-22 16:25:30 EAT	2020-09-17 20:56:13 EAT	2013-08-22 16:25:30 EAT	2013-08-22

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

When?

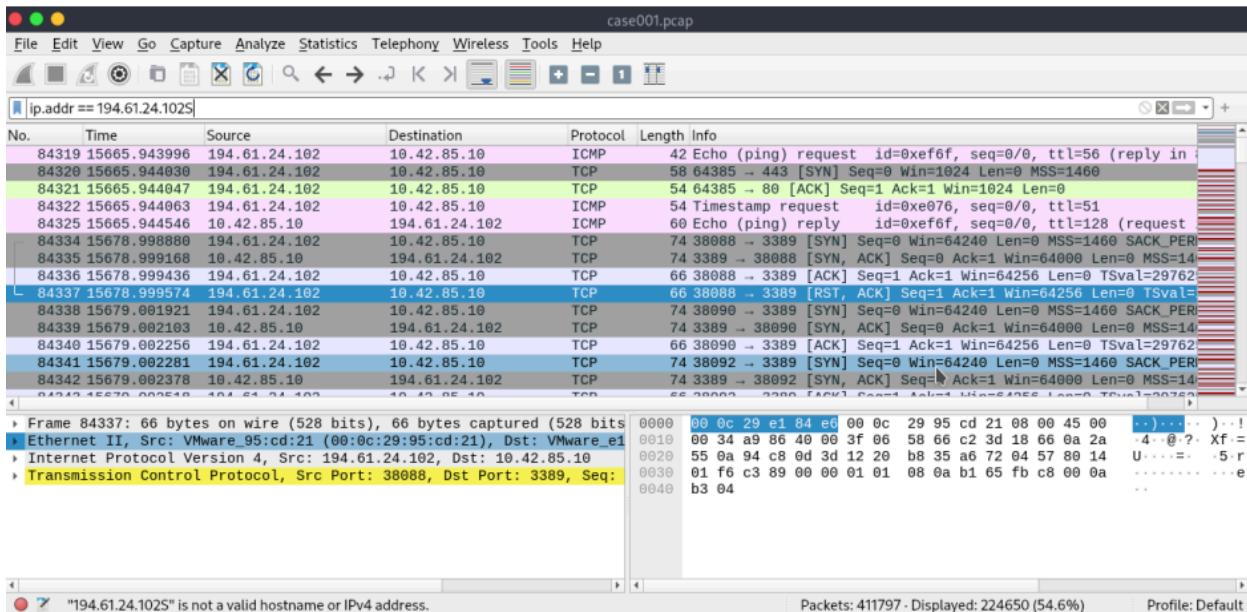
2020-09-19 03:27:49 GMT+00:00

Where?

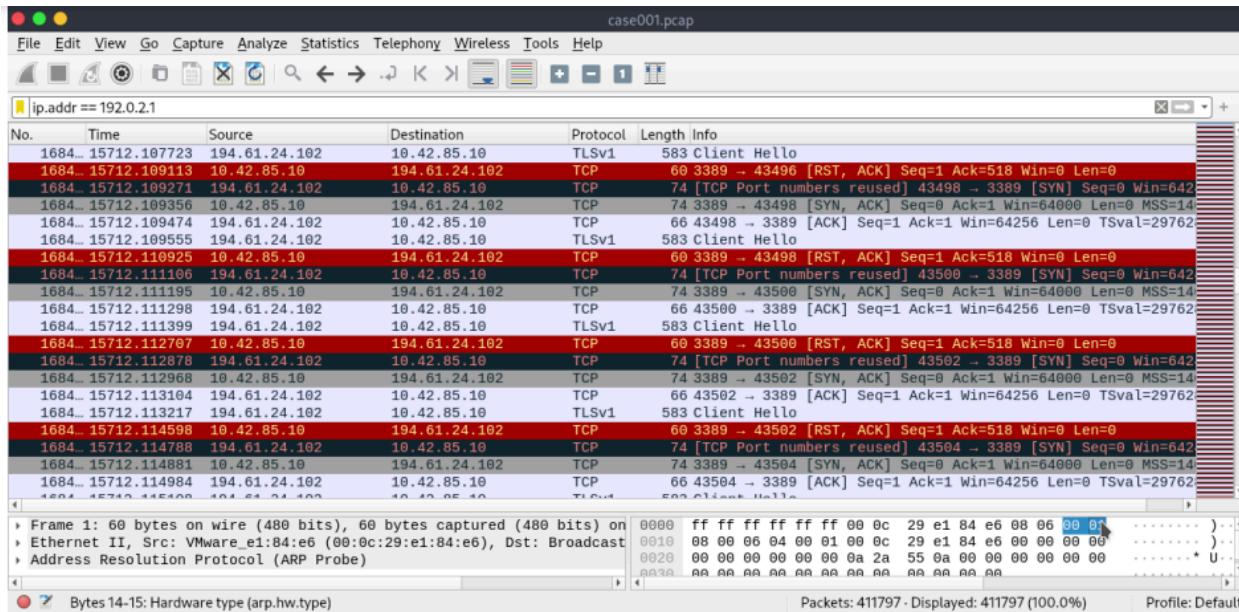
C:\Windows\System32\coreupdater.exe

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 is 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. These flags show that the IP address 194.61.24.102 was trying to initiate communication with 10.42.85.10 without success and terminated forcefully. This suggests a brute-force attack. The attacker was trying to use different passwords and usernames.



From AbuseIPDB this ip address has been reported.

IP Abuse Reports for 194.61.24.102:

This IP address has been reported a total of **1** time from 1 distinct source. It was most recently reported **6 months ago**.

Old Reports: The most recent abuse report for this IP address is from **6 months ago**. It is possible that this IP is no longer involved in abusive activities.

Reporter	IoA Timestamp in UTC	Comment	Categories
✓ BlueWire Hosting	2024-01-04 21:12:59 (6 months ago)	Probing for Wordpress vulnerabilities	Bad Web Bot Web App Attack

Showing 1 to 1 of 1 reports

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.

About 72 results (0.16 seconds) Sort by: Relevance

Answers to the Case of the Stolen Szechuan Sauce (Case001)
dfirmadness.com
14 Oct 2020 ... 194.61.24.102 via Internet Explorer download when the attacker was RDP'd into the victim. What IP Address is the malware calling to? 203.78.

IP 194.61.24.102 spam report. Blacklists & IP abuse DB - CleanTalk
cleantalk.org
IP 194.61.24.102 has spam activity on 110 websites, history spam attacks. AS41842 spam rate 0.00%. IP Address spam activity, Whois Details, IP abuse report.

Case of the stolen Szechuan sauce | by Tanvi Latwani - Medium
medium.com
23 Aug 2023 ... addr == 194.61.24.102 and tcp in the case001.pcap. Question: Was malware used? If so ...

WHOIS 194.61.24.102 | Optima Communications LLC - AbuseIPDB
www.abuseipdb.com
194.61.24.102 IP Address Information. ISP, Optima Communications LLC, Usage Type, Fixed Line ISP, Hostname, nsa2.medi-a.ru, Domain Name, optimacoms.ru, Country.

CyberDefenders: Szechuan Sauce CTF Writeup | by Ellis S - Medium
ellisstannard.medium.com
3 Nov 2022 ... Note that Type 3 is sometimes shown as NLA is an authentication from Remote Desktop Protocol. Furthermore that remote IP address, 194.61.24.102 ...

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.

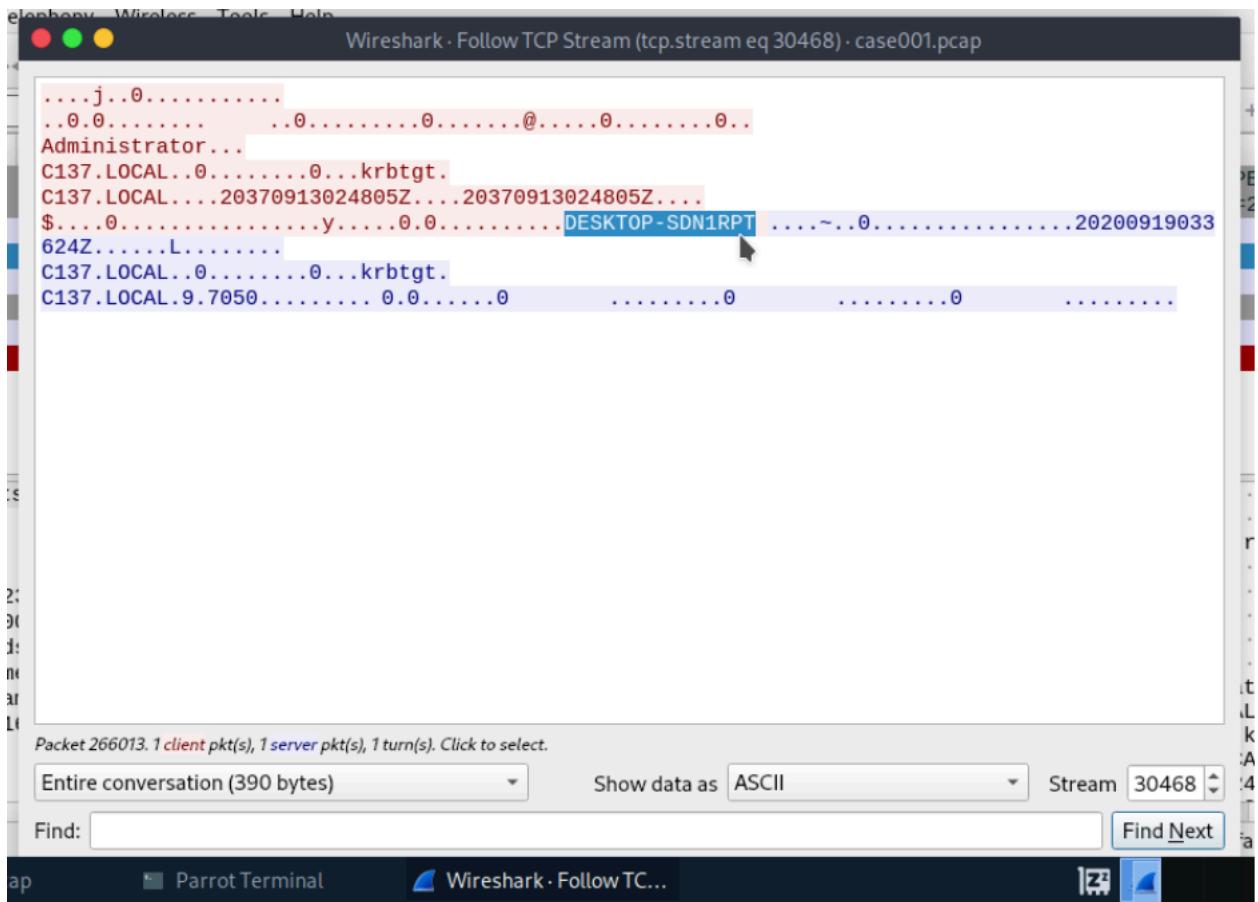
Files Referring (53)

Scanned	Detections	Type	Name
2024-04-21	2 / 59	Network capture	ia473final2024.pcap
2024-02-29	2 / 57	Network capture	case001.pcap
2022-12-06	2 / 60	Network capture	Case002.pcap
2022-06-08	2 / 56	Network capture	1.pcapng
2022-03-17	2 / 55	Network capture	case001.17C232E6.pcap
2021-12-16	2 / 56	Network capture	New.pcap
2023-12-14	2 / 59	unknown	3724.dmp
2020-12-10	2 / 60	Text	pham_mothersql
2020-04-22	1 / 58	Text	winnipeg_newhcadb.sql
2020-04-22	1 / 59	Text	winnipeg_newhcadb.sql

Historical Whois Lookups (8)

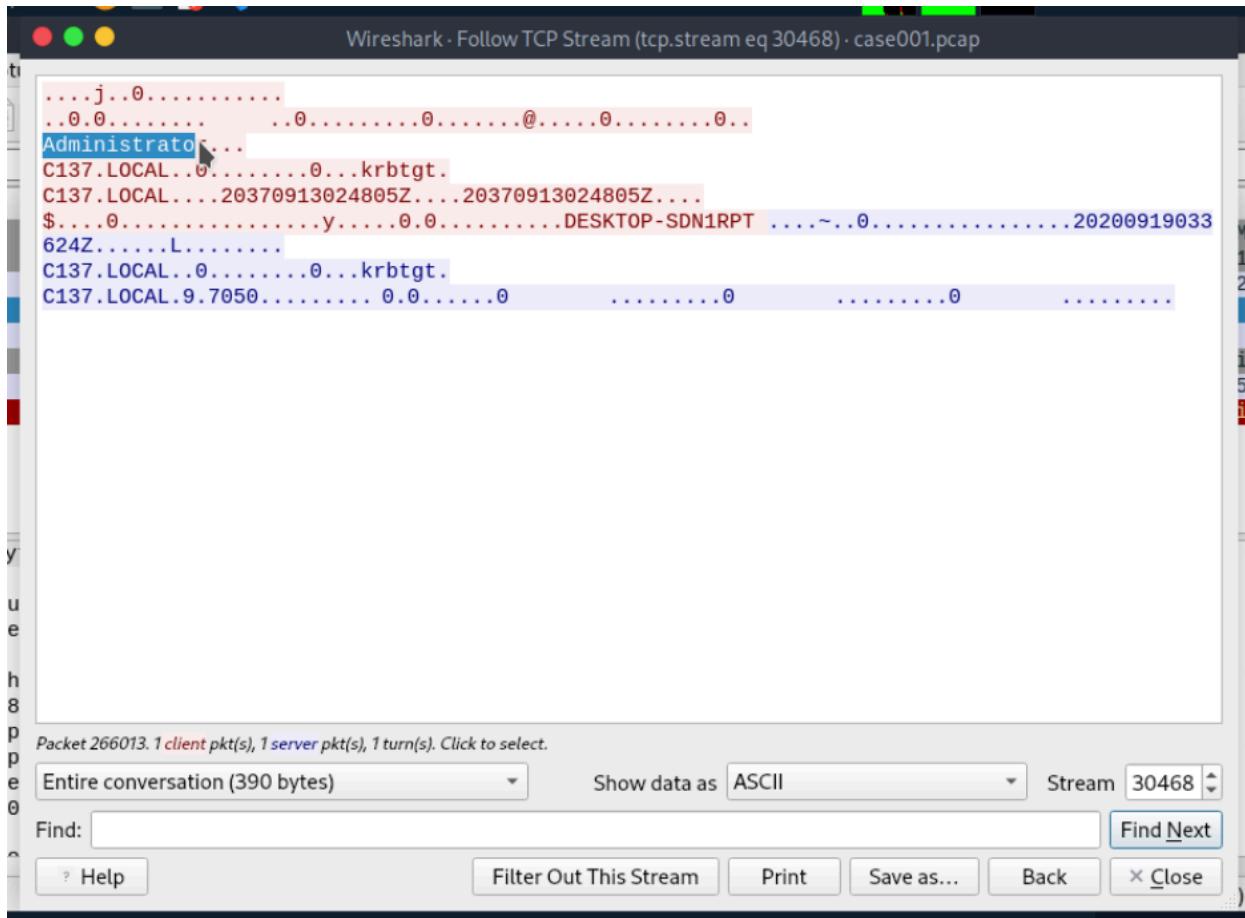
Last Updated	Organization	Email
+ 2023-11-13	RIPE Network Coordination Centre	abuse@ripe.net
+ 2023-09-11	RIPE Network Coordination Centre	abuse@ripe.net
+ 2023-03-11		
+ 2022-06-07		
+ 2021-02-08	RIPE Network Coordination Centre	abuse@ripe.net
+ 2020-05-08	RIPE Network Coordination Centre	abuse@ripe.net

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

No.	Time	Source	Destination	Protocol	Length	Info
2660...	16697.431833	10.42.85.115	10.42.85.10	TCP	66	56694 → 88 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PEE...
2660...	16697.431839	10.42.85.10	10.42.85.115	TCP	66	88 → 50694 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=2...
2660...	16697.431987	10.42.85.115	10.42.85.10	TCP	60	56694 → 88 [ACK] Seq=1 Ack=1 Win=2102272 Len=0
2660...	16697.431988	10.42.85.115	10.42.85.10	KRB5	287	AS-REQ
2660...	16697.442143	10.42.85.10	10.42.85.115	KRB5	211	KRB Error: KRB5KDC_ERR_PREAMUTH_REQUIRED
2660...	16697.442247	10.42.85.115	10.42.85.10	TCP	60	56694 → 88 [FIN, ACK] Seq=234 Ack=158 Win=2102016 Len=0
2660...	16697.442414	10.42.85.10	10.42.85.115	TCP	60	88 → 50694 [ACK] Seq=158 Ack=235 Win=65536 Len=0
2660...	16697.442482	10.42.85.10	10.42.85.115	TCP	60	88 → 50694 [RST, ACK] Seq=158 Ack=235 Win=0 Len=0

Frame 266027: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface 0 (unknown) at Sep 19, 2020 02:36:24.912805000 UTC [Time shift for this packet: 0.000000000 seconds] Epoch Time: 1600482984.912805000 seconds [Time delta from previous captured frame: 0.000068000 seconds] [Time delta from previous displayed frame: 0.000068000 seconds] [Time since reference or first frame: 16697.442482000 seconds] Frame Number: 266027 Frame Length: 60 bytes (480 bits)

Absolute time when this frame was captured (frame.time): 00:00:28.734500000

Packets: 411797 - Displayed: 8 (0.0%) Profile: Default

i. Did the attacker steal or access any data?

This is a screenshot showing recently accessed file using administrator account

The screenshot shows the Autopsy 4.21.0 forensic analysis tool interface. The left sidebar contains navigation links such as Data Sources, File Views, File Types, Deleted Files, MB File Size, Data Artifacts, Recent Documents, Analysis Results, and more. The main pane displays a table titled "Recent Documents" with columns for Source Name, Path, Date Accessed, and Data Source. The table lists several files, including "Secret.link" which is highlighted. Below the table, there is a detailed analysis view for "Secret.link" with tabs for Hex, Text, Application, Source File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The "Data Artifacts" tab is selected, showing details like Type, Value, Path, Path ID, Date Access, Source File Path, and Artifact ID.

Source Name	Path	Date Accessed	Data Source
Beth_Secret.link	C:\FileShare\Secret\Beth_Secret.txt	2020-09-19 06:35:07 EAT	20200918_0347_CDr
NoJerry.link	C:\FileShare\Secret\NoJerry.txt	2020-09-19 01:29:54 EAT	20200918_0347_CDr
PortalGunPlans.link	C:\FileShare\Secret\PortalGunPlans.txt	2020-09-19 01:34:02 EAT	20200918_0347_CDr
Secret.link	C:\FileShare\Secret	2020-09-19 01:29:54 EAT	20200918_0347_CDr
SECRET_beth.link	C:\FileShare\Secret\SECRET_beth.txt	2020-09-19 01:39:22 EAT	20200918_0347_CDr
Szechuan Sauce.link	C:\FileShare\Secret\Szechuan Sauce.txt	2020-09-19 01:35:59 EAT	20200918_0347_CDr
meter.exe link	C:\Windows\System32\meter.exe	nnnn:nn nn:nn:nn	20200918_0347_CDr

Type	Value	Source(s)
Path	C:\FileShare\Secret	RecentActivit
Path ID	3284	RecentActivit
Date Access	2020-09-19 01:29:54 EAT	RecentActivit
Source File Path	/img_20200918_0347_CDrive.E01/vol_vol3/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/Secret.link	
Artifact ID	-922337203685477599	

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.

cyberG - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Keyword Lists Keyword Search

Listing
/img_20200918_0347_CDrive.E01/vol_v013/FileShare/Secret
Table Thumbnail Summary

Name	Modified Time	Change Time	Access Time	Created Time
[parent folder]	2020-09-19 06:34:18 EAT	2020-09-19 06:34:18 EAT	2020-09-19 06:34:18 EAT	2020-09-18 07:48:11
Beth_Secret.txt	2020-09-19 02:35:35 EAT	2020-09-19 02:35:35 EAT	2020-09-19 02:35:35 EAT	2020-09-19 02:35:35
NoJery.txt	2020-09-19 01:30:24 EAT	2020-09-19 01:30:24 EAT	2020-09-19 01:30:24 EAT	2020-09-19 01:30:24
PortalGunPlans.txt	2020-09-19 01:35:35 EAT	2020-09-19 01:35:35 EAT	2020-09-19 01:35:35 EAT	2020-09-19 01:35:35
SECRET_beth.txt	2020-09-19 06:34:27 EAT	2020-09-19 06:34:27 EAT	2020-09-19 01:39:04 EAT	2020-09-19 01:39:04
SECRET_beth.txt	2020-09-19 06:34:27 EAT	2020-09-19 06:34:27 EAT	2020-09-19 01:39:04 EAT	2020-09-19 01:39:04
Szechuan Sauce.txt	2020-09-19 01:38:56 EAT	2020-09-19 01:38:56 EAT	2020-09-19 01:38:56 EAT	2020-09-19 01:38:56

Save Table as CSV

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: of Result

File Views File Types By Extension By MIME Type Deleted Files MB File Size Data Artifacts Installed Programs (29)

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

cyberG - Autopsy 4.21.0

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Keyword Lists Keyword Search

Listing
/img_20200918_0347_CDrive.E01/vol_v013/FileShare
Table Thumbnail Summary

Name	Modified Time	Change Time	Access Time	Created Time
[current folder]	2020-09-19 06:34:18 EAT	2020-09-19 06:34:18 EAT	2020-09-19 06:34:18 EAT	2020-09-18 07:48:11 EAT
[parent folder]		2020-09-18 07:48:22 EAT	2020-09-18 07:48:22 EAT	2020-09-18 07:48:22 EAT
Secret	2020-09-19 06:35:06 EAT	2020-09-19 06:35:06 EAT	2020-09-19 06:35:06 EAT	2020-09-19 01:29:34 EAT

Save Table as CSV

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

File Name Allocation: Allocated
 Metadata Allocation: Allocated
 Modified: 2020-09-19 06:35:06 EAT
Accessed: 2020-09-19 06:35:06 EAT
 Created: 2020-09-19 01:29:34 EAT
 Changed: 2020-09-19 06:35:06 EAT
 MD5: Not calculated
 SHA-256: Not calculated
 Hash Lookup Results: UNKNOWN
 Internal ID: 3284

From The Sleuth Kit istat Tool:

(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.

The screenshot shows the Autopsy 4.15.0 interface with the following details:

- File List:** Shows a tree view of files under "vol1 (Allocated: 0-2047)".
- Table View:** A detailed table of file metadata for "img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret".
- Details View:** A table showing specific artifacts found in the file.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flag(Dr)	Flag(Meta)	Known	Location
[current folder]				2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT	2020-09-18 23:35:04 EDT	56	Allocated	Allocated	unknown	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret
[parent folder]				2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT	2020-09-18 00:40:11 EDT	144	Allocated	Allocated	unknown	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret
Beth_Secret.txt	1			2020-09-18 19:35:35 EDT	2020-09-18 19:35:35 EDT	2020-09-18 19:35:35 EDT	2020-09-18 19:35:54 EDT	27	Allocated	Allocated	unknown	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret
NoJerry.txt				2020-09-18 10:26:24 EDT	2020-09-18 10:30:24 EDT	2020-09-18 10:29:47 EDT	2020-09-18 10:29:47 EDT	25	Allocated	Allocated	unknown	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret
PortaGunPlans.txt	1			2020-09-18 10:26:35 EDT	2020-09-18 10:35:35 EDT	2020-09-18 10:33:54 EDT	2020-09-18 10:33:54 EDT	143	Allocated	Allocated	unknown	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret
SECRET_beth.txt				2020-09-18 23:34:27 EDT	2020-09-18 23:34:27 EDT	2020-09-18 10:39:04 EDT	2020-09-18 10:39:04 EDT	29	Unallocated	Unallocated	unknown	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret
Szechuan Sauce.txt		1		2020-09-18 10:36:56 EDT	2020-09-18 10:36:56 EDT	2020-09-18 10:36:56 EDT	2020-09-18 10:36:43 EDT	479	Allocated	Allocated	unknown	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret

Type	Value	Source(s)
Associated Artifact	#92337203684775229	
Source File Path	img_20200918_0347_CDrive.E01/vol1/vol3/FileShare/Secret/Szechuan Sauce.txt	
Artifact ID	-92337203684775228	

(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/vol1/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

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	2020-09-19 05:30:14 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 02:08:53 WAT	2020-09-18 06:4
State.evtx				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

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: 46 6C 66 46 69 6C 65 00 00 00 00 00 00 00 00 00 ElFile:.....  
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 1E 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 8/5/2024 8:15 PM

Event Viewer

Action View Help

Event Viewer (Local) 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 3:14:44 AM	Microsoft Windows security auditing.	4634	Logoff
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.	4634	Logon
Information	9/18/2020 3:14:59 AM	Microsoft Windows security auditing.	4624	Logoff
Information	9/18/2020 3:15:16 AM	Microsoft Windows security auditing.	4624	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.	4634	Logon

85°F 75°F

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>