

Digital Forensics Report & Documentation: The Stolen Szechuan Sauce

By DFIR Madness

Prepared on April 28, 2025 by:

Ifeanyi Christian Edeh
Cybersecurity Specialist

<https://www.linkedin.com/in/ifeanyiedeh>

Toolbox:

MITRE ATT&CK, FTKImager, Autopsy, Wireshark, Volatility Workbench, Eric Zimmerman's Registry Explorer, OTX AlienVault LevelBlue, VMWare, Virus Total, NIST SP 800-53, NIST CSF

Table of Contents

**Forensics Report & Documentation:
The Stolen Szechuan Sauce
By DFIR Madness**

Table of Contents	1
Executive Summary	2
Solving the Case	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?	4
4. Was there a breach?	5
5. What was the initial entry vector?	5
6. Was malware used? If so, what was it? If there was malware answer the following:	5
7. What malicious IP Addresses were involved?	14
8. Did the attacker access any other systems?	19
9. What was the network layout of the victim network?	21
10. What architecture changes should be made immediately?	21
References	22

Executive Summary

Intro to Case - The Stolen Szechuan Sauce

The digital forensics investigation explores a security breach using advanced analytical techniques. Through detailed examination of network traffic and system artifacts, we identified key insights into the incident, including the timeline, points of entry, and nature of the malicious activities involved.

Key findings include:

- the breach's initial entry via RDP brute force,
- the presence of malware ("coreupdater.exe"), and
- the compromise of sensitive information.

This investigation highlights the importance of digital forensics in unraveling complex security incidents and strengthening cyber defenses. It also provides recommendations for architectural improvements and preventive measures to bolster security.

This report is the result of a collaborative effort by RM and Bernadette Chan. Richard focused on analyzing desktop artifacts, while I concentrated on server files. We both independently reviewed the PCAP file.

Key Cybersecurity Tools Used

- FTKImager
- Autopsy 4.21.0
- Wireshark
- Volatility Workbench V3.0 Build 1008
- EvtxeCmd V1.5.0.0
- Timeline Explorer V2.0.0.1
- Microsoft Windows Powershell V1.20.1178

Artifacts

- [DC01 Disk Image \(E01\)](#)
- [DC01 Memory file](#)
- [Case 001 PCAP](#)
- [Desktop Disk Image \(E01\)](#)
- [Desktop Memory file](#)

Solving the Case

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

Using FTKImager to view the server's disk image, we found the operating system of the server to be **Windows 2012 R2 standard**.

The screenshot shows the AccessData FTK Imager interface. The Evidence Tree pane on the left lists numerous system files and folders, including gpmgmt.dll, GPOAdmin.dll, GPOAdminCommon.dll, GPOAdminCustom.dll, gppref.dll, gpprefbr.dll, gpprefcn.dll, gpregistrybrowser.dll, GPRSO.dll, gptedit.msc, GroupPolicy, GroupPolicyUsers, he-IL, hr-HR, hu-HU, ias, icxml, IME, inetsrv, InputMethod, iplm, ismp.dll, ismserv.exe, it-IT, ja-JP, kdcpw.dll, kdcsvc.dll, KdsSvc.dll, ko-KR, lidle.dll, lidle.exe, ldp.exe, Licenses, neutral, Eval, and ServerStandardEval. The File List pane on the right shows a single file, license.rtf, with a size of 48 bytes, regular type, and a date modified of 2013-08-1... The right pane displays the contents of the 'license.rtf' file, which is a Microsoft Word document containing the Windows Server 2012 R2 Standard End-User License Agreement.

```
{\rtf1\ansi\ansicpg1252\deff0\deflang1033\deflangfe1033{\fonttbl{\fnil\fcharset0 Segoe UI;}}{\colortbl ;\red\green\blue255;}{\stylesheet{ Normal;}{\s1 heading 1;}{\s2 heading 2;}{\s3 heading 3;}}{\generator Msftedit 5.41.21.2510;}{\viewkind4}\pard\nowidctlpar\sa200\b\f0\fs22 MICROSOFT SOFTWARE \pard\b\brdrb\brdrw10\brsp20 \nowidctlpar\sa200 MICROSOFT WINDOWS SERVER 2012 R2 STANDARD \par\pard\nowidctlpar\sa200\b0 These license terms are an agreement between Microsoft Corporation (or based \pard\nowidctlpar\f1-540\li540\sa200\b7\tab updates,\par\b7\tab supplements,\par\b7\tab Internet-based services, and\par\b7\tab support services\par\pard\nowidctlpar\sa200 for this software, unless other terms accompany those items. If so, those terms \pard\b By using the software, you accept these terms. If you do not accept them, do not use the software As described below, using some features also operates as your consent to the transmission of certain sta
```

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

Using Autopsy 4.21.0 to view the desktop disk image, the operating system present on the host machine DESKTOP-SDN1RPT was **Microsoft Windows 10 Enterprise Evaluation**.

The screenshot shows the Autopsy 4.21.0 interface with the title "Case 001 - The Stolen Szechuan Sauce - Autopsy 4.21.0". The left sidebar contains a tree view of data sources, file types, deleted files, data artifacts, and analysis results. The main pane displays "Operating System Information" with two results listed:

Source Name	S	C	O	Name	Domain	Program Name	Processor Architecture	Temporary Files Directory	Path	Product ID
20200918_0417_DESKTOP-SDN1RPT.E01				DESKTOP-SDN1RPT	C137.local	Windows 10 Enterprise Evaluation	AMD64	%SystemRoot%\TEMP	C:\Windows	0033-3000-00001-AA089
20200918_0347_CDdrive.E01				CITADEL-DC01	C137.local	Windows Server 2012 R2 Standard Evaluation	AMD64	%SystemRoot%\TEMP	C:\Windows	0023-1000-00000-AA289

Below this, there is a detailed table for the first result:

Type	Value	Source(s)
Name	DESKTOP-SDN1RPT	Recent Activity
Domain	C137.local	Recent Activity
Program Name	Windows 10 Enterprise Evaluation	Recent Activity
Processor Architecture	AMD64	Recent Activity
Temporary Files Directory	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	0033-3000-00001-AA089	Recent Activity
Owner	Admin	Recent Activity

3. What was the local time of the Server?

Extracting the System32 > Config > System log files from FTKImager and importing into Eric Zimmerman's Registry Explorer, we found the local time of the server to be **Pacific Standard Time**.

The screenshot shows the Registry Explorer v2.0.0.0 interface with the title "Registry Explorer v2.0.0.0". The left pane shows the registry tree with the "System" key expanded, showing subkeys like ControlSet001, ControlSet002, and ControlSet003. The right pane shows a table of values for the "Control" subkey:

Value Name	Value Data
DaylightBias	-60
DaylightName	@tzres.dll,-211
StandardStart	Month 11, week of month
StandardBias	0
StandardName	@tzres.dll,-212
Bias	480
DaylightStart	Month 3, week of month 2
TimeZoneKeyName	Pacific Standard Time
ActiveTimeBias	420

4. Was there a breach?

Yes.

5. What was the initial entry vector?

According to the analysis of the PCAP file on Wireshark, a suspicious IP address 194.61.24.102 sent a Ping Request to our machine (10.42.85.10) with no response. It tried to start a 3-way handshake with port 443 (https), no response. It tried again to start a 3-way handshake with port 80 (http), and our server sent a Ping Reply. From then on, we see many back-and-forth pings to port 3389 (RDP = remote desktop protocol).

This is an indication of a **RDP bruteforce attack** - someone is trying to guess the password so that they can log on and control our machine remotely.

No.	Time	Source	Src Port	Destination	Dest Port	Protocol	Length	Info
84319	2020-09-19 02:19:..	194.61.24.102	10.42.85.10			ICMP	42	Echo (ping) request id=0xef6f, seq=0/0, ttl=56 (reply)
84320	2020-09-19 02:19:..	194.61.24.102	64385	10.42.85.10	443	TCP	58	64385 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
84321	2020-09-19 02:19:..	194.61.24.102	64385	10.42.85.10	80	TCP	54	64385 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
84322	2020-09-19 02:19:..	194.61.24.102	10.42.85.10			ICMP	54	Timestamp request id=0xe076, seq=0/0, ttl=51
84325	2020-09-19 02:19:..	10.42.85.10		194.61.24.102		ICMP	60	Echo (ping) reply id=0xef6f, seq=0/0, ttl=128 (request)
84334	2020-09-19 02:19:..	194.61.24.102	38088	10.42.85.10	3389	TCP	74	38088 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_0
84335	2020-09-19 02:19:..	10.42.85.10		194.61.24.102	38088	TCP	74	38088 → 38088 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
84336	2020-09-19 02:19:..	194.61.24.102	38088	10.42.85.10	3389	TCP	66	38088 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=25
84337	2020-09-19 02:19:..	194.61.24.102	38088	10.42.85.10	3389	TCP	66	38088 → 3389 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=25
84338	2020-09-19 02:19:..	194.61.24.102	38090	10.42.85.10	3389	TCP	74	38090 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_0
84339	2020-09-19 02:19:..	10.42.85.10		194.61.24.102	38090	TCP	74	38090 → 38090 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
84340	2020-09-19 02:19:..	194.61.24.102	38090	10.42.85.10	3389	TCP	66	38090 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=25
84341	2020-09-19 02:19:..	194.61.24.102	38092	10.42.85.10	3389	TCP	74	38092 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_0
84342	2020-09-19 02:19:..	10.42.85.10		194.61.24.102	38092	TCP	74	38092 → 38092 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
84343	2020-09-19 02:19:..	194.61.24.102	38092	10.42.85.10	3389	TCP	66	38092 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=25
84344	2020-09-19 02:19:..	194.61.24.102	38094	10.42.85.10	3389	TCP	74	38094 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_0
84345	2020-09-19 02:19:..	194.61.24.102	38096	10.42.85.10	3389	TCP	74	38096 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_0
84346	2020-09-19 02:19:..	10.42.85.10		194.61.24.102	38094	TCP	74	38094 → 38094 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
84347	2020-09-19 02:19:..	10.42.85.10		194.61.24.102	38096	TCP	74	38096 → 38096 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
84348	2020-09-19 02:19:..	194.61.24.102	38098	10.42.85.10	3389	TCP	74	38098 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_0
84349	2020-09-19 02:19:..	194.61.24.102	38094	10.42.85.10	3389	TCP	66	38094 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=25
84350	2020-09-19 02:19:..	194.61.24.102	38096	10.42.85.10	3389	TCP	66	38096 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=25
84351	2020-09-19 02:19:..	10.42.85.10		194.61.24.102	38098	TCP	74	38098 → 38098 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
84352	2020-09-19 02:19:..	194.61.24.102	38100	10.42.85.10	3389	TCP	74	38100 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_0
84353	2020-09-19 02:19:..	10.42.85.10		194.61.24.102	38100	TCP	74	38100 → 38100 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460
84354	2020-09-19 02:19:..	194.61.24.102	38098	10.42.85.10	3389	TCP	66	38098 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=25

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

What process was malicious?

Yes, malware was used.

We were able to verify that the file '**coreupdater.exe**' was the initial malicious process.

Searching for the hash of this file in Autopsy (hash value:

Fd153c66386ca93ec9993d66a84d6f0d129a3a5c), we put it in VirusTotal and received a

Community Source of 64/75, confirming that coreupdater.exe is indeed a malicious file.
Virustotal. (n.d.).

```
C:\> Users > student > Desktop > 1.csv
1 MD5,SHA1,FileNames
2 "eed41b4500e473f97c50c7385ef5e374","fd153c66386ca93ec9993d66a84d6f0d129a3a5c","20200918_0347_CDdrive.E01\Partition 2 [11168MB]\NONAME [NTFS]\[root]\Windows\System32\coreupdater.exe"
```

hash value

virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6
coreupdater.exe

peexe direct-cpu-clock-access assembly idle runtime-modules spreader 64bits

Community Score 64 / 75

Community Score -12

64/75 security vendors flagged this file as malicious

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

Security vendors' analysis

Acronis (Static ML) Suspicious AhnLab-V3

Identify the IP Address that delivered the payload.

While analyzing PCAP file on Wireshark, we see that the source IP address is **194.61.24.102** that navigated to the website on http (port 80) to download the coreupdate.exe file.

No.	Time	Source	Destination	Protocol	Length	Info
2367...	15934.261190	10.42.85.10	194.61.24.102	TCP	66	62408 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460
2367...	15934.261404	194.61.24.102	10.42.85.10	TCP	66	80 → 62408 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2367...	15934.261525	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
→ 2367...	15934.261595	10.42.85.10	194.61.24.102	HTTP	302	GET / HTTP/1.1
2367...	15934.261715	194.61.24.102	10.42.85.10	TCP	54	80 → 62408 [ACK] Seq=1 Ack=249 Win=64128 Len=0
• 2367...	15934.264111	194.61.24.102	10.42.85.10	TCP	71	80 → 62408 [PSH, ACK] Seq=1 Ack=249 Win=64128 Len=17 [TCP
2367...	15934.264322	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [ACK] Seq=249 Ack=18 Win=261888 Len=0
+ 2367...	15934.264353	194.61.24.102	10.42.85.10	HTTP	420	HTTP/1.0 200 OK (text/html)
2367...	15934.264453	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [ACK] Seq=249 Ack=385 Win=261632 Len=0
2367...	15934.264892	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [FIN, ACK] Seq=249 Ack=385 Win=261632 Len=0
2367...	15934.265089	194.61.24.102	10.42.85.10	TCP	54	80 → 62408 [ACK] Seq=385 Ack=250 Win=64128 Len=0

What IP Address is the malware calling to?

After searching the hash on virus total, we were able to find that the malware was calling to another suspicious IP address: **203.78.103.109** from Thailand. And we were also able to verify that this IP address was involved in breach as we analyzed the PCAP file on Wireshark.

The screenshot shows the VirusTotal analysis interface for the hash 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6. The 'RELATIONS' tab is selected. It displays a list of contacted domains and IP addresses. The IP address 203.78.103.109 is highlighted in blue and has a red border around it, indicating it is the target of interest.

Domain	Detections	Created	Registrar
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.

IP	Detections	Autonomous System	Country
192.168.0.30	0 / 94	-	-
192.168.0.34	0 / 94	-	-
192.168.0.38	0 / 94	-	-
192.229.211.108	0 / 94	15133	US
20.96.52.198	0 / 94	8075	US
20.99.132.105	0 / 94	8075	US
20.99.133.109	0 / 94	8075	US
20.99.184.37	0 / 94	8075	US
20.99.185.48	1 / 94	8075	US
20.99.186.246	0 / 94	8075	US
203.78.103.109	6 / 94	18362	TH

Where is this malware on disk?

While analyzing the Server's disk image using FTKImager, we found that the malware was downloaded to **C:\Windows\System32**

coreupdate.exe	7 Re...	2020-09-19 3:24:06 AM
CoreMmRes.dll	15 Re...	2013-08-22 11:45:01 AM
convert.exe	20 Re...	2013-08-22 11:32:31 AM
control.exe	113 Re...	2013-08-22 11:03:56 AM
console.dll	79 Re...	2013-08-22 11:17:25 AM
consent.exe	112 Re...	2013-08-22 12:44:43 PM
connectedsearch-zeroinput.searchco...	7 Re...	2014-03-21 6:49:19 PM

.E01/Partition 2 [11168MB]/NONAME [NTFS]/[root]/Windows/System32/coreupdate.exe

When did it first appear?

According to the PCAP file analyzed on Wireshark, the timestamp of the GET Request was **September 19, 2020 at 02:23:41 GMT**.

The screenshot shows a Wireshark interface with a list of network packets and a detailed view of a selected packet.

Packets List:

No.	Time	Source	Destination	Protocol	Length	Info
2367...	15934.261190	10.42.85.10	194.61.24.102	TCP	66	62408 → 80 [SYN, ECE, CWR] Seq=0 Win=65535 Len=0 MSS=1460
2367...	15934.261404	194.61.24.102	10.42.85.10	TCP	66	80 → 62408 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460
2367...	15934.261525	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [ACK] Seq=1 Ack=1 Win=262144 Len=0
→ 2367...	15934.261595	10.42.85.10	194.61.24.102	HTTP	302	GET / HTTP/1.1
2367...	15934.261715	194.61.24.102	10.42.85.10	TCP	54	80 → 62408 [ACK] Seq=1 Ack=249 Win=64128 Len=0
• 2367...	15934.264111	194.61.24.102	10.42.85.10	TCP	71	80 → 62408 [PSH, ACK] Seq=1 Ack=249 Win=64128 Len=17 [TCP]
2367...	15934.264322	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [ACK] Seq=249 Ack=18 Win=261888 Len=0
2367...	15934.264353	194.61.24.102	10.42.85.10	HTTP	420	HTTP/1.0 200 OK (text/html)
2367...	15934.264453	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [ACK] Seq=249 Ack=385 Win=261632 Len=0
2367...	15934.264892	10.42.85.10	194.61.24.102	TCP	60	62408 → 80 [FIN, ACK] Seq=249 Ack=385 Win=261632 Len=0
2367...	15934.265089	194.61.24.102	10.42.85.10	TCP	54	80 → 62408 [ACK] Seq=385 Ack=250 Win=64128 Len=0

Selected Packet Details:

```
GET / HTTP/1.1
Accept: text/html, application/xhtml+xml, */*
Accept-Language: en-US
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Accept-Encoding: gzip, deflate
Host: 194.61.24.102
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.18
Date: Sat, 19 Sep 2020 02:23:41 GMT
Content-type: text/html; charset=UTF-8
Content-Length: 228

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>Directory listing for /</title>
<body>
<h2>Directory listing for /</h2>
<hr>
<ul>
<li><a href="coreupdater.exe">coreupdater.exe</a>
</li>
<hr>
</ul>
</body>
</html>
```

Did someone move it?

Using Autopsy 4.21.0 and viewing the SYSTEM log file, we found the file was moved into **C:\Windows\System32\config\system** in the registry.

Name	Keyword Preview	Location
SRUtmp.log	Windows\System32\coreupdate.exe\Device\... /img_20200918_0417_DESKTOP-SDN1RPT.E01\vol_v06/C:\Windows\System32\coreupdate.exe=ObjectName... /img_20200918_0347_CDrive.E01\vol_v03\Windows\Sy...	
SYSTEM		

Analysis Results		
Metadata	Values	Annotations
Name: coreupdate Number of subkeys: 0 Number of values: 6 Modification Time: 2020-09-19 03:27:49 GMT+00:00	Name Type Value Type REG_DWORD 0x00000010 (16) Start REG_DWORD 0x00000002 (2) ErrorControl REG_DWORD 0x00000001 (1) ImagePath REG_EXPAND_SZ Windows\System32\coreupdate.exe ObjectName REG_SZ LocalSystem DelayedAutoStart REG_DWORD 0x00000001 (1)	

What were the capabilities of this malware?

According to VirusTotal, this malware has data manipulation capabilities, specifically with encoding data using XOR (Exclusive OR). XOR is a common technique used by malware to obfuscate its code and evade detection. (PCMag, n.d.)

Capabilities

- **Data-Manipulation**
- Encode data using XOR

Is this malware easily obtained?

Yes, this malware is easy to obtain as it's part of the free, open-source Metasploit Framework, which, unfortunately, is a widely used open-source penetration testing tool. This means it can be used by both ethical security professionals and malicious actors. While its primary purpose is to help organizations identify and address vulnerabilities, it can also be exploited by attackers to compromise systems. (Metasploit, n.d.)

Was this malware installed with persistence on any machine?

According to MITRE ATT&CK, “Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.” (MITRE ATT&CK, n.d.)

Based on this definition, yes, this malware was persistent. Coreupdater.exe was installed in the registry and as a service on the Server CITADEL-DC01 and the Desktop DESKTOP-SDN1RPT.

When?

Using Autopsy 4.21.0, we found “coreupdater.exe” installed on September 18th 2020 at 16:10:53 PDT on the Server and on September 18th 2020 18:08:37 PDT on the Desktop.

The screenshot shows the Autopsy 4.21.0 interface with the title "Case 001 - The Stolen Szechuan Sauce - Autopsy 4.21.0". The left sidebar shows a tree view of the file system, with the "System32" folder expanded to show numerous sub-files. The main pane displays a table titled "Listing" with 54 results, filtered by the path "/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config". The table columns are Name, S, C, O, Modified Time, Change Time, Access Time, and Create. The table shows several log files: netlogon.dnb, netlogon.dns, SAM, SAM.LOG1, SAM.LOG2, SECURITY, and SECURITY.LOG. The "Accessed" column for netlogon.dns and netlogon.dns shows the timestamp 2020-09-18 16:10:53 PDT. The bottom pane shows the "Metadata" tab for the selected file, displaying various file properties including Name, Type, MIME Type, Size, File Name Allocation, Metadata Allocation, Modified, Accessed, Created, Changed, and MD5.

Name	S	C	O	Modified Time	Change Time	Access Time	Create
netlogon.dnb	0			2020-09-18 18:28:22 PDT	2020-09-18 18:28:22 PDT	2020-09-17 10:57:54 PDT	2020-
netlogon.dns	0			2020-09-18 18:28:22 PDT	2020-09-18 18:28:22 PDT	2020-09-17 10:57:54 PDT	2020-
SAM	0			2020-09-17 22:02:29 PDT	2020-09-17 10:56:13 PDT	2020-09-18 16:10:53 PDT	201-
SAM.LOG1	0			2013-08-22 06:25:30 PDT	2020-09-17 10:56:13 PDT	2013-08-22 06:25:30 PDT	201-
SAM.LOG2	0			2013-08-22 06:25:30 PDT	2020-09-17 10:56:13 PDT	2013-08-22 06:25:30 PDT	201-
SECURITY	0			2020-09-18 16:10:53 PDT	2020-09-17 10:56:13 PDT	2020-09-18 16:10:53 PDT	201-
SECURITY.LOG	0			2013-08-22 06:25:30 PDT	2020-09-17 10:56:13 PDT	2013-08-22 06:25:30 PDT	201-

Metadata

Name: /img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/config/SYSTEM
Type: File System
MIME Type: application/x.windows-registry
Size: 12845056
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2020-09-18 16:10:53 PDT
Accessed: 2020-09-18 16:10:53 PDT
Created: 2013-08-22 06:25:30 PDT
Changed: 2020-09-17 10:56:13 PDT
MD5: 05cd86230d5bdbca0fd6da1d5313a4

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of the file system, with the 'System32 (4535)' folder expanded, showing sub-folders like '0409 (2)', 'AdvancedInstallers (3)', and 'am-et (4)'. The main pane shows a table of files under the 'Listing' tab. The table has columns for Name, S, C, O, Modified Time, Change Time, Access Time, and Create Time. The 'SYSTEM' file is listed with a modified time of 2020-09-18 18:08:37 PDT and a change time of 2020-09-17 23:37:39 PDT. Below the table, tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences are visible. A detailed view of the 'SYSTEM' file's metadata is shown at the bottom, including fields like Name, Type, MIME Type, Size, File Name Allocation, Metadata Allocation, Modified, Accessed, Created, Changed, and MDS.

Name	S	C	O	Modified Time	Change Time	Access Time	Create Time
SOFTWARE				2020-07-10 10:00:37 PDT			2015
SOFTWARE.LOG1			▼	1	2019-12-07 01:03:44 PST	2020-09-17 23:37:39 PDT	2019-12-07 01:03:44 PST
SOFTWARE.LOG2			▼	1	2019-12-07 01:03:44 PST	2020-09-17 23:37:41 PDT	2019-12-07 01:03:44 PST
SYSTEM			▼	1	2020-09-18 18:08:37 PDT	2020-09-17 23:37:39 PDT	2020-09-18 18:08:37 PDT
SYSTEM.LOG1			▼	1	2019-12-07 01:03:44 PST	2020-09-17 23:37:38 PDT	2019-12-07 01:03:44 PST
SYSTEM.LOG2			▼	1	2019-12-07 01:03:44 PST	2020-09-17 23:37:38 PDT	2019-12-07 01:03:44 PST
COMPONENTS.LOG1			✗		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00
DRIVERS.LOG1			✗		0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00

Metadata

Name:	/img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6/Windows/System32/config/SYSTEM
Type:	File System
MIME Type:	application/x-windows-registry
Size:	13369344
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-09-18 18:08:37 PDT
Accessed:	2020-09-18 18:08:37 PDT
Created:	2019-12-07 01:03:44 PST
Changed:	2020-09-17 23:37:39 PDT
MDS:	d49b01b56708a1ff6bc182ec7d3ca7dd

Where?

Using Autopsy 4.21.0, we found “coreupdater.exe” in the registry in C:/windows/System32 under ControlSet001 > Services > coreupdater on the Server and the Desktop.

The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of the file system, including System (3), System32 (3368), 0409 (3), ADDSDeployment_Internal (4), adprep (67), AdvancedInstallers (5), AppLocker (2), ar-SA (11), BestPractices (3), bg-BG (9), Boot (7), catroot (4), catroot2 (11), CodeIntegrity (4), Com (9), config (54), Journal (2), RegBack (7), systemprofile (9), TxR (9), Configuration (5), cs-CZ (11), da-DK (11), de-DE (11), Dism (25), dns (6), downlevel (103), drivers (317), DriverStore (5), DRVSTORE (6), dsc (5), el-GR (11). The main pane shows a listing of files under /img_20200918_0347_CDdrive.E01/vol_vob3/Windows/System32/config, including netlogon.dnb, netlogon.dns, SAM, SAM.LOG1, SAM.LOG2, SECURITY, and SECURITY.LOG. A table below lists these files with columns for Name, S, C, O, Modified Time, Change Time, Access Time, and Create. The right pane shows a detailed view of the coreupdate registry key, including its metadata (Name: coreupdate, Number of subkeys: 0, Number of values: 6, Modification Time: 2020-09-19 03:27:49 GMT+00:00) and its values (Type, Value, Start, ErrorControl, ImagePath, ObjectName, DelayedAutostart).

Name	S	C	O	Modified Time	Change Time	Access Time	Create
netlogon.dnb	0			2020-09-18 18:28:22 PDT	2020-09-18 18:28:22 PDT	2020-09-17 10:57:54 PDT	2021
netlogon.dns	0			2020-09-18 18:28:22 PDT	2020-09-18 18:28:22 PDT	2020-09-17 10:57:54 PDT	2021
SAM	0			2020-09-17 22:02:29 PDT	2020-09-17 10:56:13 PDT	2020-09-18 16:10:53 PDT	2021
SAM.LOG1	0			2013-08-22 06:25:30 PDT	2020-09-17 10:56:13 PDT	2013-08-22 06:25:30 PDT	2021
SAM.LOG2	0			2013-08-22 06:25:30 PDT	2020-09-17 10:56:13 PDT	2013-08-22 06:25:30 PDT	2021
SECURITY	0			2020-09-18 16:10:53 PDT	2020-09-17 10:56:13 PDT	2020-09-18 16:10:53 PDT	2021
SECURITY.LOG				2013-08-22 06:25:30 PDT	2020-09-17 10:56:13 PDT	2013-08-22 06:25:30 PDT	2021

Metadata		
Name:	coreupdate	
Number of subkeys:	0	
Number of values:	6	
Modification Time:	2020-09-19 03:27:49 GMT+00:00	
Values		
Type	Name	Type
Crypt_DWORD	coreupdate	Value
Start	crypt32	0x0000000010 (16)
ErrorControl	CryptSvc	0x00000002 (2)
ImagePath	DComLocator	0x0000000001 (1)
ObjectName	DcomLaunch	
DelayedAutostart	defragsvc	
	DeviceAssociationService	
	DeviceInstall	
	Dfs	

The screenshot shows the Autopsy Forensic Browser interface. The left pane displays a tree view of the file system, with the root node being 'System32 (4535)'. The right pane shows a detailed table of log files found in this directory. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, and Create. The table lists the following files:

Name	S	C	O	Modified Time	Change Time	Access Time	Create
SOFTWARE				2019-09-18 18:08:37 PDT	2019-09-17 23:37:39 PDT	2019-12-07 01:03:44 PST	2015
SOFTWARE.LOG1	▼	1		2019-12-07 01:03:44 PST	2020-09-17 23:37:41 PDT	2019-12-07 01:03:44 PST	2015
SOFTWARE.LOG2	▼	1		2019-12-07 01:03:44 PST	2020-09-17 23:37:41 PDT	2019-12-07 01:03:44 PST	2015
SYSTEM	▼	1		2020-09-18 18:08:37 PDT	2020-09-17 23:37:39 PDT	2020-09-18 18:08:37 PDT	2015
SYSTEM.LOG1	▼	1		2019-12-07 01:03:44 PST	2020-09-17 23:37:38 PDT	2019-12-07 01:03:44 PST	2015
SYSTEM.LOG2	▼	1		2019-12-07 01:03:44 PST	2020-09-17 23:37:38 PDT	2019-12-07 01:03:44 PST	2015
COMPONENTS.LOG1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000
DRIVERS.LOG1				0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000

Metadata

Name: /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_v06/Windows/System32/config/SYSTEM
Type: File System
MIME Type: application/x-windows-registry
Size: 13369344
File Name Allocation: Allocated
Metadata Allocation: Allocated
Modified: 2020-09-18 18:08:37 PDT
Accessed: 2020-09-18 18:08:37 PDT
Created: 2019-12-07 01:03:44 PST
Changed: 2020-09-17 23:37:39 PDT
MD5: d49b01b56708a1ff6bc182ec7d3ca7dd

7. What malicious IP Addresses were involved?

After inputting the suspicious IP address **194.61.24.102** into VirusTotal.com, it resulted in 1/94 security vendor flagging it as malicious from Criminal IP. This IP initiated the attack on CITADEL-DC01.

While searching the hash on VirusTotal, we were able to find another suspicious IP address: **203.78.103.109**. This one is from Thailand and has a community score of 6/94. Wireshark shows that this IP contacted our server after the RDP bruteforce was successful. Then 194.61.24.102 accessed DESKTOP-SDN1RPT.

The screenshot shows the VirusTotal interface for the IP address 194.61.24.102. The main header bar includes navigation icons, a search bar with the IP address, and the URL virustotal.com/gui/ip-address/194.61.24.102. Below the header, there's a large summary card with a 'Community Score' of 1/94, a red exclamation mark icon indicating 1/94 security vendors flagged it as malicious, and details about the IP address (194.61.24.102 / 194.61.24.0/24) and its AS number (AS 41842 - LLC media Systems). A 'Community' button is also present. Below this are tabs for DETECTION (which is active), DETAILS, RELATIONS, and COMMUNITY. A call-to-action box encourages users to join the community. Under the 'DETECTION' tab, there's a section for 'Security vendors' analysis' with a red exclamation mark icon and two status boxes: 'Criminal IP' and 'Malicious'.

Σ 194.61.24.102

! 1/94 security vendor flagged this IP address as malicious

194.61.24.102 (194.61.24.0/24)
AS 41842 (LLC media Systems)

Community Score

DETECTION DETAILS RELATIONS COMMUNITY

[Join our Community](#) and enjoy additional community insights and crowdsourced detections, plus an API!

Security vendors' analysis ⓘ

Criminal IP ⚠ Malicious

The screenshot shows a forensics report interface with a search bar at the top containing the hash value `10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6`. Below the search bar is a navigation menu with tabs: DETECTION, DETAILS, RELATIONS (which is currently selected), BEHAVIOR, and COMMUNITY (with a count of 14+). A call-to-action banner encourages users to "Join our Community" for additional insights. The main content area displays two sections: "Contacted Domains (1)" and "Contacted IP addresses (17)".

Contacted Domains (1)

Domain	Detections	Created	Registrar
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.

Contacted IP addresses (17)

IP	Detections	Autonomous System	Country
192.168.0.30	0 / 94	-	-
192.168.0.34	0 / 94	-	-
192.168.0.38	0 / 94	-	-
192.229.211.108	0 / 94	15133	US
20.96.52.198	0 / 94	8075	US
20.99.132.105	0 / 94	8075	US
20.99.133.109	0 / 94	8075	US
20.99.184.37	0 / 94	8075	US
20.99.185.48	1 / 94	8075	US
20.99.186.246	0 / 94	8075	US
203.78.103.109	6 / 94	18362	TH

Were any IP Addresses from known adversary infrastructure?

Yes, according to Level Blue/Labs, both IP addresses: 203.78.103.109 (Thailand) & 194.61.24.102 (Russia) are associated with various CVEs. (LevelBlue Open Threat Exchange, n.d.)

The screenshot shows the LevelBlue OTX analysis interface for the IP address 203.78.103.109. The top navigation bar includes links for 'LevelBlue/Labs', 'Browse', 'Scan Endpoints', and search filters for 'All' and '203.78.103.109'. Below the header, the IP is identified as 'IPv4 203.78.103.109'. Key statistics are displayed: 0 Pulses, 14 Passive DNS entries, 7 URLs, and 4 Files. The 'Analysis Overview' section provides detailed information:

Location	Thailand	Indicator Facts	IP mentioned on Twitter
ASN	AS18362 netway communication co. ltd.		14 domains resolved in all time
DNS Resolutions	14 Domains	Antivirus Detections	2 top-level domains
Top Level Domains	2 Unique TLDs		Trojan:Win64/Meterpreter.E, TrojanDropper:PowerShell/Ploty.C
Related Pulses	None	AV Detection Ratio	4 / 4
Related Tags	None	External Resources	Whois, VirusTotal

Pulses 31 **Passive DNS** 0 **URLs** 0 **Files** 0

Location	Russian Federation	Indicator Facts	Historical OTX telemetry IP mentioned on Twitter Running SSH
ASN	ASNone	Open Ports	2 Open Ports 22, 53
Related Pulses	OTX User-Created Pulses (31)	Exploited CVEs	All Time: 2017-9805, 2017-5638 2014-6271
Related Tags	9 Related Tags Nextray, cyber security, ioc, phishing, malicious More	External Resources	Whois, VirusTotal

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

Yes, according to Level Blue/Labs, 203.78.103.109 was involved in other attacks around the same time under hostname related to pets like: www.petmallthailand.com, www.happydoghappycat-th.com, or pppettohome.com

Passive DNS						
Show 25	entries	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN
Unknown	www.petmallthailand.com	A	203.78.103.109		2021-04-22 03:17	2021-06-21 03:17
Unknown	petmallthailand.com	A	203.78.103.109		2021-04-22 03:17	2022-02-16 03:18
Unknown	nipponpets.com	A	203.78.103.109		2021-04-16 11:14	2022-05-13 02:16
Unknown	www.happydoghappycat-th.com	A	203.78.103.109		2021-02-26 11:14	2022-04-22 11:52
Unknown	kugarden.com	A	203.78.103.109		2020-11-13 05:16	2022-05-08 11:51
Unknown	ns1.happydoghappycat-th.com	A	203.78.103.109		2020-10-26 06:16	2020-10-26 06:16
Unknown	ns2.happydoghappycat-th.com	A	203.78.103.109		2020-10-26 06:16	2020-10-26 06:16
Unknown	happydoghappycat-th.com	A	203.78.103.109		2020-08-27 03:01	2022-04-22 11:52
Unknown	pppettohome.com	A	203.78.103.109		2020-08-21 08:51	2022-02-22 09:17
Unknown	petmall1999.com	A	203.78.103.109		2020-08-21 08:50	2022-04-23 09:51
Unknown	dogenjoypattaya.com	A	203.78.103.109		2020-08-21 08:38	2022-04-23 11:16
Unknown	browniepetworld.com	A	203.78.103.109		2020-08-21 08:33	2022-02-22 09:17
Unknown	happydog-happycat.com	A	203.78.103.109		2020-08-16 08:08	2021-01-08 04:19
Unknown	203-78-103-109.plesk.page	A	203.78.103.109		2020-07-19 10:30	2022-03-11 10:17

8. Did the attacker access any other systems?

Yes, the attacker accessed the desktop (named DESKTOP-SDN1RPT at IP address 10.42.85.115) and the Server (named CITADEL-DC01 at IP address 10.42.85.10).

How? When?

The attacker performed a RDP bruteforce attack on the Server. Once successful, they moved to the Desktop. This happened on **September 18 2020 between 15:38:56 PDT and 20:34:18 PDT**, as evident by a few files being accessed as seen on Autopsy.

Did the attacker steal or access any data? When?

Yes, the attacker accessed and stole data on both server and desktop. Two files were created and exfiltrated called “**Loot.zip**” and “**Secret.zip**.”

Case 001 - The Stolen Szechuan Sauce - Autopsy 4.21.0

Case 001 - The Stolen Szechuan Sauce - Autopsy 4.21.0

Case 001 - The Stolen Szechuan Sauce - Autopsy 4.21.0

Forensics Report

April 28, 2025

The attacker stole data from the **Server CITADEL-DC01** on **September 18 2020 at 15:38:56 PDT** from the “Secret” folder in “FileShare” by archiving the “Secret” folder to Secret.zip. We believe the Secret Szechuan Sauce recipe was inside the file.

The screenshot shows the EnCase Forensic software interface with the following details:

- Case Name:** Case 001 - The Stolen Szechuan Sauce - Autopsy 4.21.0
- File List:** The current view is "File List" under the "Discovery" tab.
- Selected Item:** The file "SECRET_bath.txt" is selected, highlighted with a red border.
- File Details:**
 - Name: SECRET_bath.txt
 - Size: 28
 - Type: Unallocated
 - Location: /img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
 - Modified Time: 2020-09-18 20:34:57 PDT
 - Access Time: 2020-09-18 15:39:04 PDT
 - Created Time: 2020-09-18 15:39:04 PDT
 - Flags(Dir): Unallocated
 - Flags(Meta): Unallocated
 - Known: unknown
 - Location: /img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
- File List Content:**

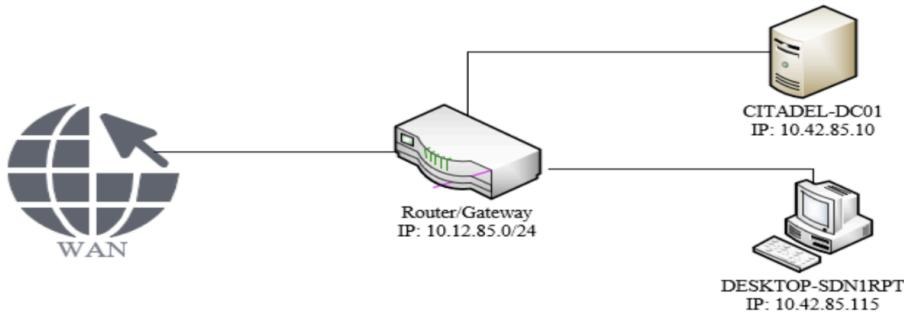
Name	S	C	O	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
[current folder]				2020-09-18 20:35:06 PDT	2020-09-18 20:35:06 PDT	2020-09-18 15:29:34 PDT	2020-09-18 15:29:34 PDT	56	Allocated	Allocated	unknown	/img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
[parent folder]				2020-09-18 20:34:18 PDT	2020-09-18 20:34:18 PDT	2020-09-18 20:34:18 PDT	2020-09-18 21:48:11 PDT	144	Allocated	Allocated	unknown	/img_20200918_0347_CDrive.ED1/vol_vol3/fileShare
Beth_Secret.txt	o			2020-09-18 16:35:53 PDT	2020-09-18 16:35:53 PDT	2020-09-18 16:35:54 PDT	2020-09-18 16:35:54 PDT	27	Allocated	Allocated	unknown	/img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
NoJerry.txt	o			2020-09-18 15:30:24 PDT	2020-09-18 15:30:24 PDT	2020-09-18 15:29:47 PDT	2020-09-18 15:29:47 PDT	25	Allocated	Allocated	unknown	/img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
PortalGunPlans.txt	o			2020-09-18 15:35:15 PDT	2020-09-18 15:35:15 PDT	2020-09-18 15:35:14 PDT	2020-09-18 15:35:14 PDT	143	Allocated	Allocated	unknown	/img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
SECRET_bath.txt	SECRET			2020-09-18 20:34:57 PDT	2020-09-18 20:34:57 PDT	2020-09-18 15:39:04 PDT	2020-09-18 15:39:04 PDT	28	Unallocated	Unallocated	unknown	/img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
Szechuan Sauce.txt	o			2020-09-18 15:38:56 PDT	2020-09-18 15:38:56 PDT	2020-09-18 15:35:43 PDT	2020-09-18 15:35:43 PDT	478	Allocated	Allocated	unknown	/img_20200918_0347_CDrive.ED1/vol_vol3/fileShare/Secret
- File List Summary:** Shows 1 of 1 page, 100% completion, and a search bar for "Matches on page: - of - Match".
- Bottom Navigation:** Includes tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, Other Occurrences, and METADATA.

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

Gateway: C137 (10.42.85.0/24)

Desktop: DESKTOP-SDN1RPT (10.42.85.115)

Server: CITADEL-DC01 (10.42.85.10)



10. What architecture changes should be made immediately?

Given the attacker's successful RDP brute force access to CITADEL-DC01, it's imperative to bolster RDP security. Here are specific recommendations as per NIST Cybersecurity Framework (NIST, 2020)

- **Patch Management:** Ensure operating systems and applications are updated with the latest security patches to address known vulnerabilities.
- **Multi-Factor Authentication (MFA):** Implement MFA as a mandatory requirement for all RDP connections, adding an extra layer of protection beyond passwords.
- **Privileged Access Management (PAM):** Enforce strict controls on privileged access, granting only necessary permissions to authorized users.
- **Password Hygiene:** Mandate strong, unique passwords for RDP accounts and enforce regular password changes.
- **Stored Password Elimination:** Avoid storing passwords locally. Consider using password vaults or single sign-on (SSO) solutions.
- **RDP Connection History:** Regularly clean RDP connection history to minimize the risk of unauthorized access.
- **Network Level Authentication (NLA):** Require NLA for all RDP sessions to verify user credentials before allowing a connection.
- **Firewall Restrictions:** Configure firewalls to strictly allow only authorized IP addresses to connect to RDP.
- **RDP Gateways:** Deploy RDP gateways to centralize and manage RDP connections, providing additional security measures.
- **Port Number Change:** Modify the default RDP port to make it less discoverable by attackers.

By implementing these security measures, you can significantly reduce the risk of future RDP-based attacks and protect your systems from unauthorized access.

References

- Definition of XOR.* PCMag. (n.d.). <https://www.pcmag.com/encyclopedia/term/xor>
- Force, J. T. (2020, December 10). *Security and Privacy Controls for Information Systems and organizations*. CSRC. <https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final>
- James. (2021, January 15). *Answers to the case of the stolen szechuan sauce (CASE001)*. DFIR Madness. <https://dfirmadness.com/answers-to-szechuan-case-001/>
- LevelBlue - Open Threat Exchange.* LevelBlue Open Threat Exchange. (n.d.). <https://otx.alienvault.com/indicator/ip/203.78.103.109>
- Pearson, A. (2021, May 10). *Volatility 3 CheatSheet*. onfvp. <https://blog.onfvp.com/post/volatility-cheatsheet/>
- Penetration testing software, PEN testing security.* Metasploit. (n.d.). <https://www.metasploit.com/>
- Persistence.* Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®. (n.d.). <https://attack.mitre.org/tactics/TA0003/>
- Shah, P. (2022, December 27). *How to change the time zone settings on windows*. MUO. <https://www.makeuseof.com/windows-change-time-zone/#:~:text=In%20the%20Registry%20Editor%20window,to%20use%20and%20click%20OK>
- Virustotal. (n.d.). <https://www.virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6/behavior>