

# Forensic Investigation

# Stolen Szechuan Sauce



By Kowsor, Esther & Trevor

# Table Contents:

Forensic Investigation	1
<b>Executive Summary</b>	<b>3</b>
<b>Process: Tools Used in the Investigation</b>	<b>3</b>
1. FTK Imager	3
2. Wireshark	4
3. VirusTotal	4
4. Registry Viewer/Registry Explorer	4
5. Window Event Viewer	4
1. What's the Operating System of the Server?	5
2. What's the operating system of the desktop?	6
3. What was the local time of the Server?	7
4. Was there a breach?	8
5. What was the initial entry vector (how did they get in)?	8
6. Was malware used? If so, what was it? If there was malware answer the following:	10
1. What process was malicious?	10
2. Identify the IP Address that delivered the payload.	11
3. What IP Address is the malware calling to?	11
4. Where is this malware on disk?	12
5. When did it first appear?	12
6. Did someone move it?	13
7. What were the capabilities of this malware?	13
8. Is this malware easily obtained?	13
9. Was this malware installed with persistence on any machine?	13
■ When?	13
■ Where?	13
7. What malicious IP Addresses were involved?	14
1. Were any IP Addresses from known adversary infrastructure?	14
2. Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?	15
8. Did the attacker access any other systems?	15
1. How?	15
2. When?	15
3. Did the attacker steal or access any data?	15
■ When?	16
9. What was the network layout of the victim network?	16
Optional Questions	19
Conclusion	19
References & Citations	21

## Executive Summary

Malware poses a significant and multifaceted threat to computer systems, with certain variants capable of inflicting immediate damage, while others may operate undetected for prolonged periods. Even highly skilled and advanced users can become victims of malware, as demonstrated by a recent incident involving Rick Sanchez and Morty Smith.

In this case, related to the Stolen Szechuan Sauce, a hacker successfully compromised their network by initiating a single ping request, followed by a brute force attack targeting the Remote Desktop Protocol (RDP). Using automated tools, the attacker guessed the password to gain unauthorized access to the server's administrator accounts. This breach enabled the hacker to escalate their privileges, granting them full administrative access to the system's files and resources.

Once inside, the hacker installed a malicious software program named "coreupdater.exe." Initially placed in the administrator's downloads folder, the malware was moved to the System32 directory to enhance its concealment. The attacker created a file labeled "loot.zip" on the desktop but deleted it before terminating the RDP session. Despite the session's closure, the malware remained active on the system, allowing it to monitor and potentially escalate its malicious activities.

This incident underscores the critical need for robust cybersecurity measures and emphasizes the importance of vigilance against the continuously evolving threat landscape.

## Process: Tools Used in the Investigation

For this investigation, we employed various specialized tools to analyze and extract digital evidence from storage devices, memory dumps, and network traffic.

### 1. FTK Imager

FTK Imager is a forensic imaging tool used to create exact copies of drives while preserving the original data. This tool was crucial for analyzing systems and devices without altering any evidence, allowing us to maintain the integrity of the investigation.

## **2. Wireshark**

Wireshark, a network protocol analyzer, was utilized to capture and analyze network traffic in real time. It enabled us to inspect data packets, troubleshoot network issues, and identify potential security threats. With Wireshark, we were able to determine who was communicating with the system, the nature of their communications, the system's responses, and whether any data transfers occurred.

## **3. VirusTotal**

We employed VirusTotal, a web-based service, to analyze files and URLs for malware and other malicious content. By aggregating results from multiple antivirus engines, VirusTotal provided comprehensive threat intelligence, helping us link malicious activities to specific patterns and threat groups.

## **4. Registry Viewer/Registry Explorer**

Registry Viewer, also known as Registry Explorer, was utilized to investigate Windows registry files and analyze registry hives. This tool enabled us to collect evidence and gain insights into system configurations by providing an organized and searchable repository of system data.

## **5. Window Event Viewer**

The built-in Windows Event Viewer was utilized to analyze event logs, containing information on system events, application activity, and security incidents. It provided a graphical interface for filtering events and generating reports, essential for troubleshooting and monitoring performance. This tool offered valuable insights into system health, aiding in diagnosing issues and maintaining stability.

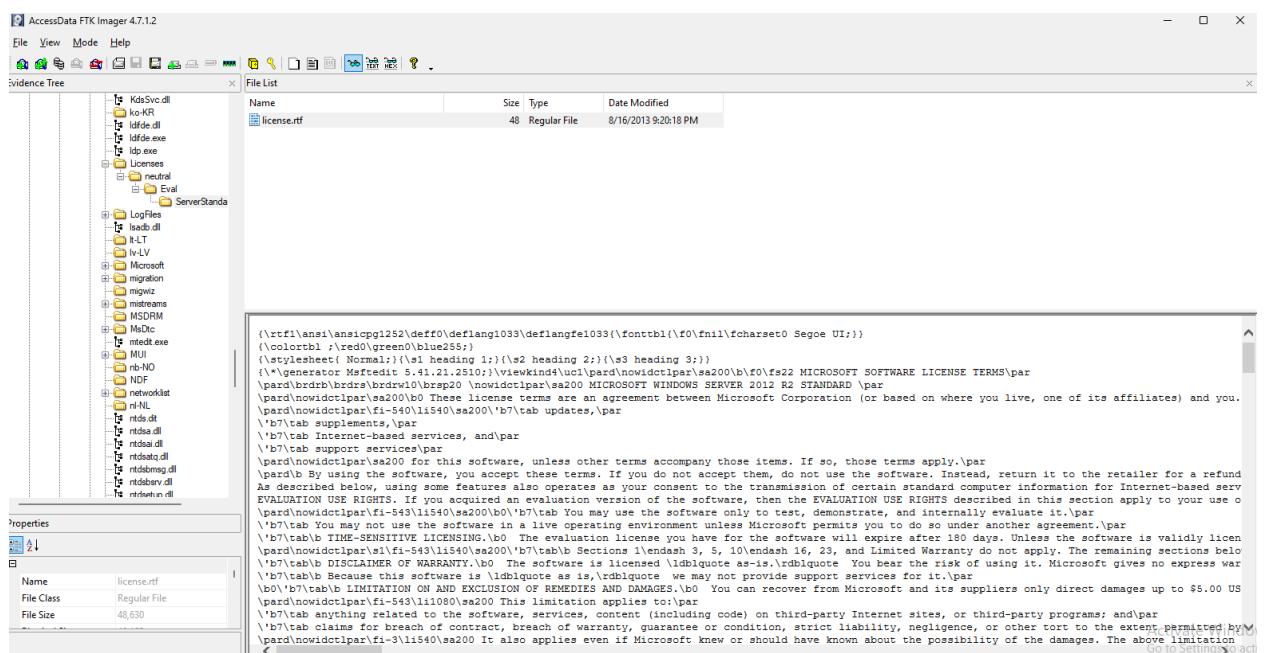
These tools played a vital role in our investigation, ensuring that we could extract and analyze digital evidence comprehensively and thoroughly. Their combined capabilities allowed us to effectively assess the security incident and gather the necessary evidence for further analysis.

This case highlights the importance of implementing fundamental cybersecurity measures to safeguard valuable digital assets. The attack, which exploited weaknesses in network access

controls and system monitoring, could have been mitigated through the adoption of basic security protocols. These include the use of multi-factor authentication for remote access, stronger password policies, encryption, and regular system backups. In addition, vigilant monitoring of network traffic could have detected and prevented the brute force attack. By adopting these preventive measures, the organization could have significantly reduced the risk of unauthorized access and the theft of sensitive information. This incident serves as a reminder that even advanced users and valuable assets are vulnerable to cyber threats, and robust cybersecurity practices are essential to protect against evolving risks.

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

Our team conducted a comprehensive analysis of the server's disk image using FTK Imager, a specialized forensic analysis tool. Our investigation confirmed that the server is operating on Windows Server 2012 R2 Standard, a commonly used server operating system. We verified this by locating the operating system license in the "C:\Windows\System32\licenses" folder.



*Figure 1: Screenshot showing the Operating System of the Server*

As part of our thorough investigation, we utilized FTK Imager, a specialized forensic analysis tool, to examine the server's disk image and identify its operating system. Our findings confirmed that the server was running Windows Server 2012 R2 Standard, a widely used and

reliable server operating system. We verified this by locating the operating system license in the "C:\Windows\System32\licenses" folder.

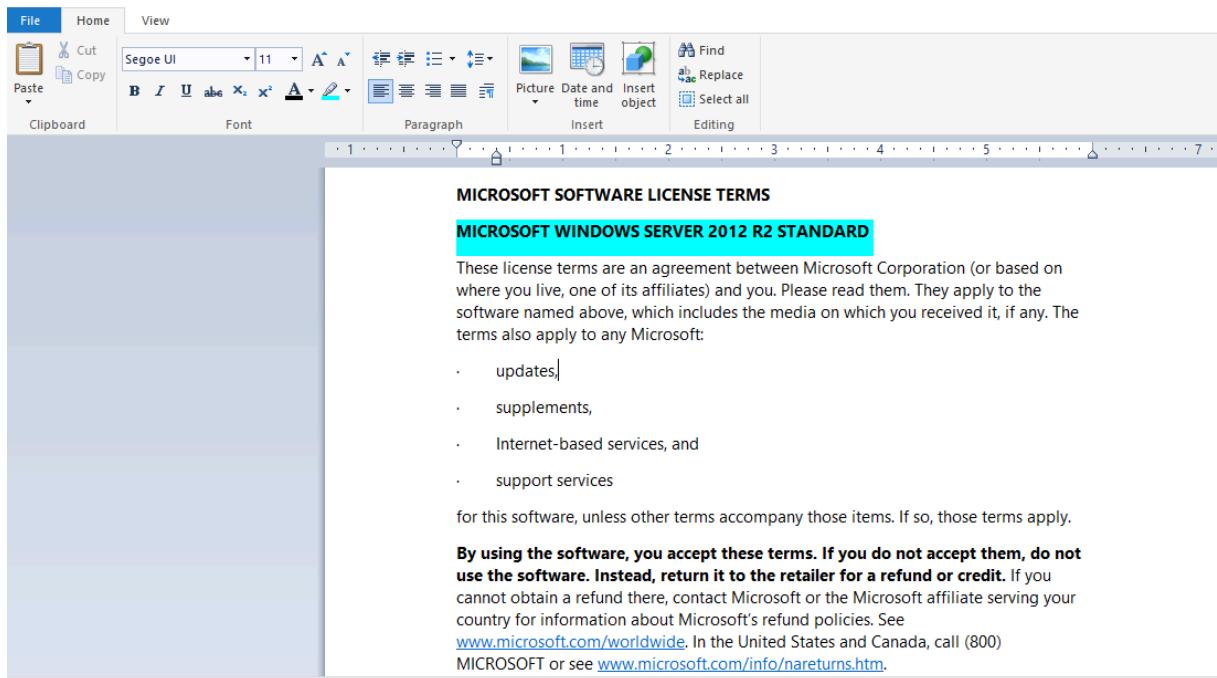


Figure 2: Screenshot Showing the Windows Operating System Licence

## 2. What's the operating system of the desktop?

The operating system of the desktop is Windows 10 Enterprise

Key name	Value Name	Value Type	Data
R\W\c	CurrentVersion	RegSz	6.3
WAB	EditionID	RegSz	EnterpriseEval
WBEM	EditionSubManufacturer	RegSz	
WIMMount	EditionSubstring	RegSz	
Windows	EditionSubVersion	RegSz	
Windows Desktop Se	InstallationType	RegSz	Client
Windows Mail	InstallDate	RegDword	0
Windows Media Devic	ProductName	RegSz	Windows 10 Enterprise
Windows Media Foun	ReleaseId	RegSz	2004
Windows Media Playe	SoftwareType	RegSz	System
Windows Messaging S	SystemRoot	RegSz	C:\Windows
Windows NT	UBR	RegDword	264
CurrentVersion	RegisteredOwner	RegSz	Admin
Windows Photo View	RegisteredOrganization	RegSz	
Windows Portable De			
Windows Script Host			

*Figure 3: Screenshot showing the Operating System of the Desktop*

3. What was the local time of the Server?

As can be seen in Figure 4 below, we could see the time was Pacific Standard Time.

*Figure 4: Screenshot Showing the Time Zone Information*

## 4. Was there a breach?

Our investigation confirmed a breach. We analyzed network traffic using Wireshark and uncovered evidence of unauthorized access and alterations, which we will present below.

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

Our investigation found that the attackers were able to gain unauthorized access to our system by using a technique called "RDP Brute Force" against the Domain Controller with the IP address 10.42.85.10. This technique involves repeatedly guessing login credentials until access is granted.

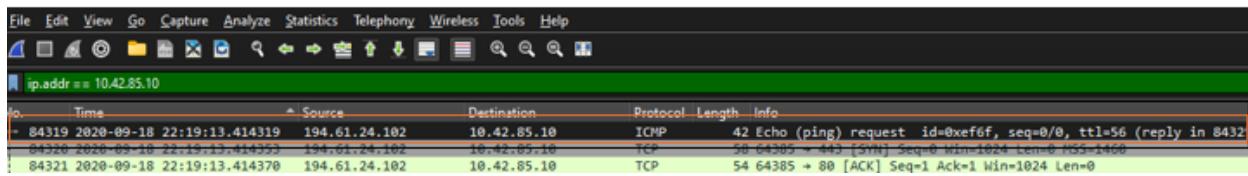


Figure 5: Screenshot Showing Initial Access of Malicious IP Address using Brute Force

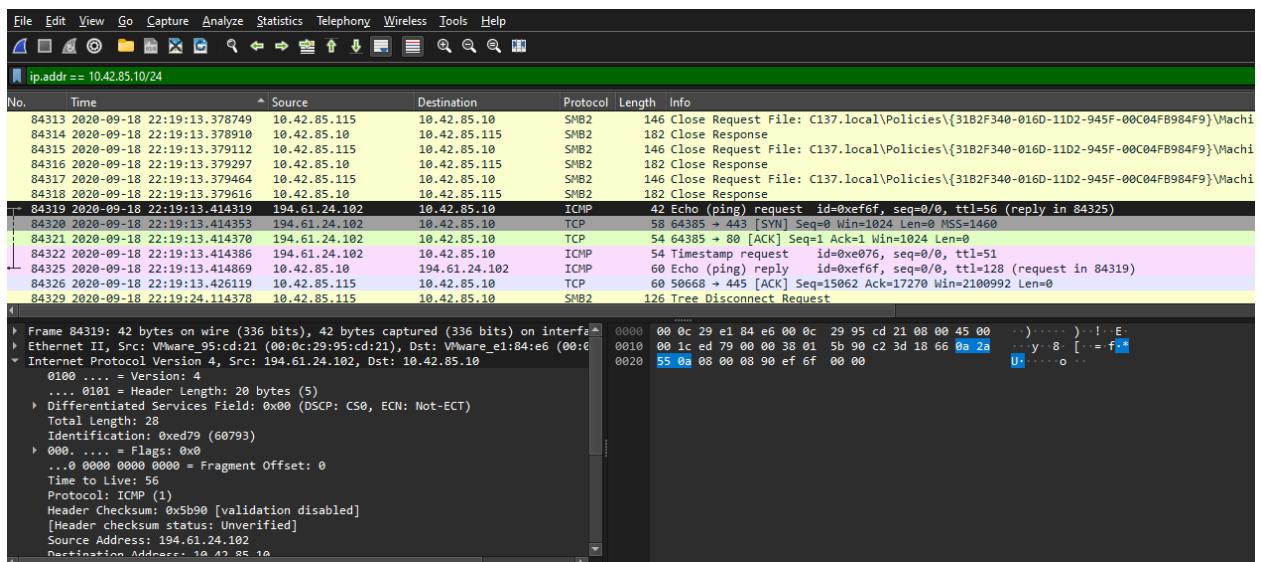
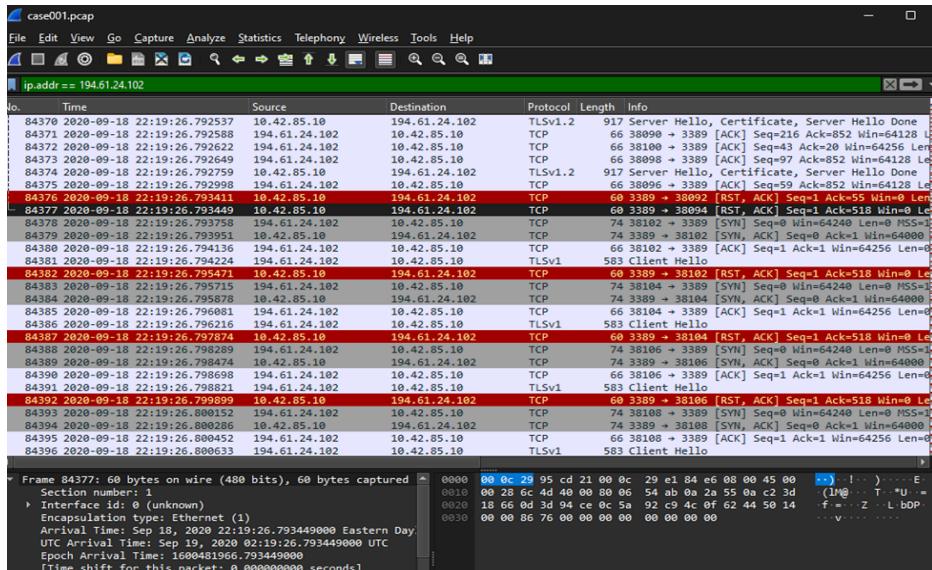


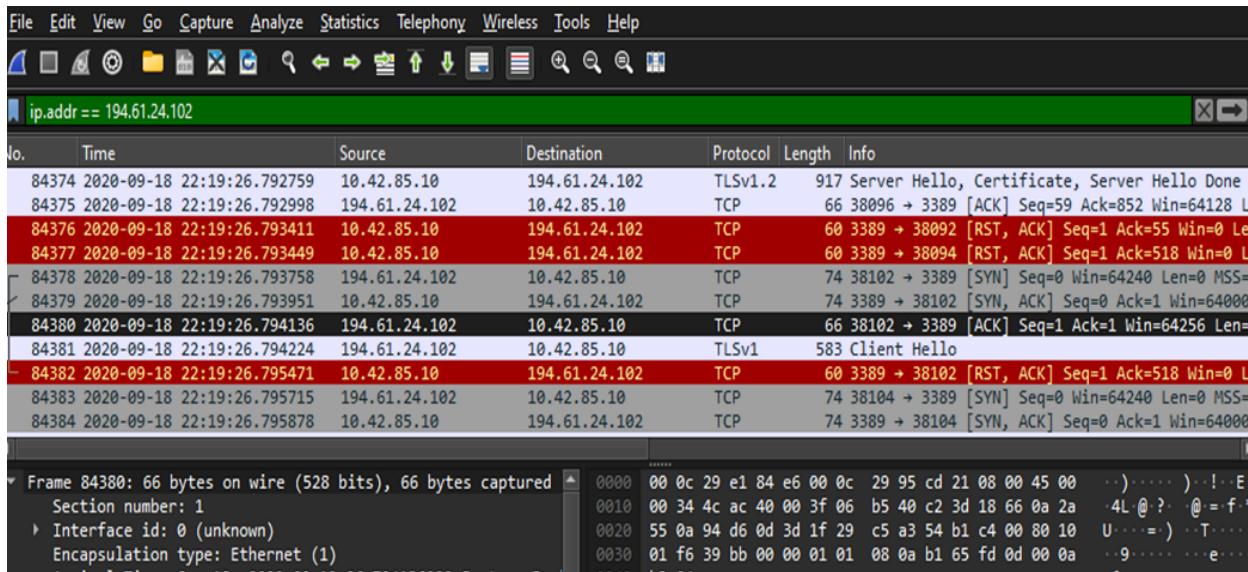
Figure 6: Screenshot from PCAP Capture Showing The Malicious IP Communication

We observed the hacker's network scanning activity using Wireshark. The hacker's source IP address, 194.61.24.102, sent a ping request (figure 5 above) to the server

and received a response. See the ping request above as well as figures 6,7, & 8 below for more information.



**Figure 7:** Screenshot from PCAP Capture Showing the Malicious IP Communication



*Figure 8: Screenshot from PCAP Capture Showing Brute Force*

We were able to determine this by analyzing network logs using a tool called Wireshark. This tool allows us to see the details of network traffic, which helped us identify the RDP Brute Force attack as the method of entry.

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

1. *What process was malicious?*

### COREUPDATER.EXE

To answer this question, we investigated the PCAP file using Wireshark. Since the desktop IP was connecting to a hacker's IP via HTTP, applied an HTTP filter to the Wireshark traffic. After that, the file was exported using 'export objects' for easier visualization. Packets 236791, 236809, and 238574 seem to have downloaded a file from favicon.ico.

Packet	Hostname	Content Type	Size	Filename
84048	tile-service.weather.microsoft.com	text/xml	4294 bytes	preinstall?region=US&appid=C98EA5B0842
84086	go.microsoft.com	text/xml	1668 bytes	?LinkId=252669&clcid=0x409
84103	dmd.metaspaces.microsoft.com	text/xml	1668 bytes	metadata.svc
84108	dmd.metaspaces.microsoft.com	text/xml	1734 bytes	metadata.svc
84144	ocsp.digicert.com	application/ocsp-response	471 bytes	MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ
236080	www.bing.com	image/x-icon	237 bytes	favicon.ico
236120	ocsp.digicert.com	application/ocsp-response	1507 bytes	MFEwTzBNMEswSTAJBgUrDgMCGgUABBE
236172	ocsp.digicert.com	application/ocsp-response	1507 bytes	MFEwTzBNMEswSTAJBgUrDgMCGgUABBTE
236679	go.microsoft.com	text/html	1212 bytes	browserconfig.xml
236791	194.61.24.102	text/html	228 bytes	\
236809	194.61.24.102	text/html	195 bytes	favicon.ico
238574	194.61.24.102	application/x-msdos-program	7168 bytes	coreupdater.exe
265840	go.microsoft.com	text/xml	1418 bytes	?LinkId=252669&clcid=0x409
265923	dmd.metaspaces.microsoft.com	text/xml	1418 bytes	metadata.svc
266312	dmd.metaspaces.microsoft.com	text/xml	1734 bytes	metadata.svc
266476	go.microsoft.com	text/xml	2058 bytes	?LinkId=252669&clcid=0x409
266516	dmd.metaspaces.microsoft.com	text/xml	2058 bytes	metadata.svc
266758	dmd.metaspaces.microsoft.com	text/xml	1734 bytes	metadata.svc
266770	go.microsoft.com	text/xml	1420 bytes	?LinkId=252669&clcid=0x409
266795	dmd.metaspaces.microsoft.com	text/xml	1420 bytes	metadata.svc
266938	dmd.metaspaces.microsoft.com	text/xml	1734 bytes	metadata.svc
266972	go.microsoft.com	text/xml	2058 bytes	?LinkId=252669&clcid=0x409
267024	dmd.metaspaces.microsoft.com	text/xml	2058 bytes	metadata.svc
267237	dmd.metaspaces.microsoft.com	text/xml	1734 bytes	metadata.svc
267268	go.microsoft.com	text/xml	1418 bytes	?LinkId=252669&clcid=0x409

Figure 9: Screenshot Showing Exporting the Malicious File

We exported the file and it was immediately quarantined by Windows Defender, confirming it as malware.

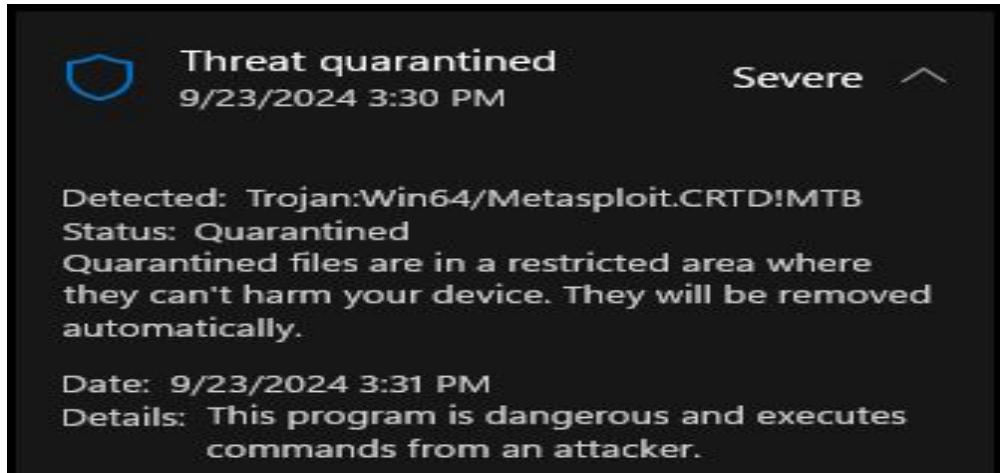


Figure 10: Screenshot Showing Windows Defender Confirming the Threat Quarantine

The file was exported from quarantine and the hash was extracted using Powershell, which was then used to verify the threat on Virus Total.

The screenshot displays the VirusTotal analysis interface. On the left, there's a circular progress bar with the number "63 / 72" and a "Community Score" of "12". The main panel shows the following details for the file "coreupdater.exe":  
SHA256 Hash: 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6  
Path: C:\Users\student\Desktop\Fore...  
Reanalyze Similar More  
63/72 security vendors flagged this file as malicious  
coreupdater.exe  
peexe idle direct-cpu-clock-access spreader assembly 64bits runtime-modules  
Size: 7.00 KB Last Analysis Date: 23 hours ago EXE

Figure 11: Screenshot from Virus Total Showing the Community Score of coreupdater.exe

2. Identify the IP Address that delivered the payload.

The payload was delivered by 194.61.24.102 - this was the IP it connected to via HTTP.

3. What IP Address is the malware calling to?

VirusTotal indicates that 203.78.103.109 is the most probable address.

20.99.185.48	1 / 94	8075	US
20.99.186.246	0 / 94	8075	US
203.78.103.109	6 / 94	18362	TH

Figure 12: Screenshot from Virus Total Showing Probable Malicious IP Address

- The address was confirmed using Wireshark.

ip.addr == 203.78.103.109						
No.	Time	Source	Destination	Protocol	Length Info	
2422	2020-09-18 22:25:18.565676	10.42.85.10	203.78.103.109	TCP	66 62414 → 443 [SYN, ECE, CWR] Seq=0 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM	

Figure 13: Screenshot from Wireshark Capture Confirming Malicious IP

- Address confirmed using Volatility workbench.

0x60182590	TCPv4	10.42.85.10	62613	203.78.103.109	443	ESTABLISHED	3644	coreupdater.exe	N/A	
0x601cda00	TCPv6	fe80::2dcf:e600:be73:d220	135	fe80::2dcf:e600:be73:d220		CLOSED	684	svchost.exe	N/A	
0x601fae50	TCPv4	0.0.0.0	62475	0.0.0.0	0	LISTENING	3724	spoolsv.exe	N/A	
0x601fae50	TCPv6	::	62475	::	0	LISTENING	3724	spoolsv.exe	N/A	

Figure 14: Screenshot Showing Established Connection Between CoreUpdater Using Volatility

#### 4. Where is this malware on disk?

- C:\Windows\System32\coreupdater.exe (via EZ Timeline Explorer)

Image Path	Version	Launch String
R[D]	R[D]	R[D]
c:\windows\system32\coreupdater.exe		C:\Windows\System32\coreupdater.exe

Figure 15: Screenshot from Registry Explorer Confirming the Location of Malware

#### 5. When did it first appear?

According to the packet data in Wireshark, the coreupdater.exe first appeared on 2020-09-19 at 2:24:06 UTC

Wireshark · Export · HTTP object list					
Text Filter: coreupdater					
Packet	Hostname	Content Type	Size	Filename	
2385...	194.61.24.102	application/x-msdos-program	7168 bytes	coreupdater.exe	
2658...	194.61.24.102	application/x-msdos-program	7168 bytes	coreupdater.exe	

Figure 16: Screenshot Showing Initial entry of Coreupdater.exe

#### 6. Did someone move it?

Yes, since it was downloaded, it was moved from the downloads folder to the System32 directory.

#### 7. What were the capabilities of this malware?

According to VirusTotal, coreupdater.exe is a trojan that uses Metasploit, which can inject processes.



Figure 17: Screenshot showing Virus Total identifying coreupdater.exe as a Trojan.

#### 8. Is this malware easily obtained?

Yes, it can be obtained from Metasploit - a popular penetration testing tool, free to download.

#### 9. Was this malware installed with persistence on any machine?

- When?
- ❖ 2020-09-19 at 2:24:06 UTC
- Where?
- ❖ Windows Registry, and as a service

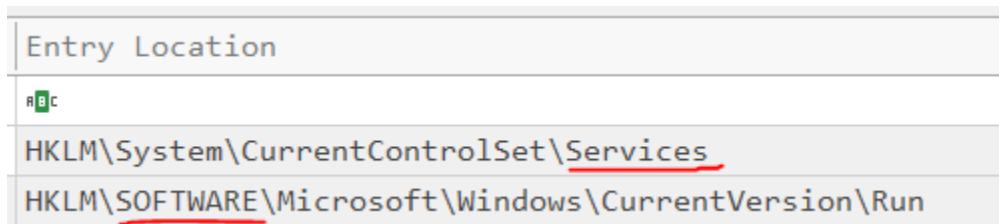


Figure 18: Screenshot of Registry showing the entry location

## 7. What malicious IP Addresses were involved?

194.61.24.102 and 203.78.103.109

### 1. Were any IP Addresses from known adversary infrastructure?

- Yes. Both IPs were reported/logged on dates before the disc image (first image: 194.61.24.0/24; second image 203.78.103.105)

A screenshot of a security analysis interface. On the left, there's a circular icon with a red '1' and a blue '94' inside, labeled 'Community Score'. In the center, a message says '1/94 security vendor flagged this IP address as malicious'. Below it, the IP address '194.61.24.102 (194.61.24.0/24)' and its AS number 'AS 41842 (LLC media Systems)' are shown. At the bottom, tabs for 'DETECTION', 'DETAILS', 'RELATIONS' (which is selected), and 'COMMUNITY' are visible. A green banner at the bottom encourages joining the community. A table titled 'Passive DNS Replication (3)' shows three entries with columns for Date resolved, Detections, Resolver, and Domain. The 'Date resolved' column has three entries: '2020-05-07', '2019-11-06', and '2019-11-05'. The 'Detections' column shows '0 / 94' for each. The 'Resolver' column lists 'VirusTotal' for all. The 'Domain' column lists 'blacklist-in.rbl.ipline.eu', 'klient055.online', and 'klient-293.xyz' respectively. The '2019-11-06' and '2019-11-05' entries are underlined in red.

Figure 19: Screenshot Showing Dates Malicious IP Address

2020-09-07	0 / 94	VirusTotal	ns1.happydoghappycat-th.com
2020-08-27	0 / 94	VirusTotal	ns1.pppethome.com
2020-08-27	0 / 94	VirusTotal	ns1.brownyepetworld.com
2020-08-27	0 / 94	VirusTotal	webmail.happydoghappycat-th.com
2020-08-27	0 / 94	VirusTotal	www.happydoghappycat-th.com
2020-08-27	0 / 94	VirusTotal	happydoghappycat-th.com
2020-08-25	0 / 94	VirusTotal	ns1.petmall1999.com
2020-08-23	0 / 94	VirusTotal	ns1.dogenjoypattaya.com

Figure 20: Virus Total Screenshot Showing Dates of Other Attacks

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

Yes (see above dates)

## 8. Did the attacker access any other systems?

1. *How?*

The Desktop-SDN1RPT was compromised by the 194... IP address via brute force attack. They were able to gain the password for the administrator account, which they used to access the DC via RDP

2. *When?*

Using the ‘rdp’ filter on Wireshark, we were able to identify the first time that the DC accessed the desktop, at 02:23:55 UTC

2652...	2020-09-19 02:35:55.291953	10.42.85.10	10.42.85.115	RDP	73 Negotiate Request
	2020-09-19 02:35:55.324188	10.42.85.10	194.61.24.102	TLSv1.2	151 Application Data

Figure 21: Screenshot from PCAP Capture Showing the First Access

3. *Did the attacker steal or access any data?*

Yes. The attacker accessed all the files contained within “secret” folder

Source Name	S	C	O	Path	Date Accessed	Data Source
Beth_Secret.lnk				C:\FileShare\Secret\Beth_Secret.txt	2020-09-18 23:35:07 EDT	20200918_0347_CDrive.E01
NoJerry.lnk				C:\FileShare\Secret\NoJerry.txt	2020-09-18 18:29:54 EDT	20200918_0347_CDrive.E01
PortalGunPlans.lnk				C:\FileShare\Secret\PortalGunPlans.txt	2020-09-18 18:34:02 EDT	20200918_0347_CDrive.E01
Secret.lnk				C:\FileShare\Secret	2020-09-18 18:29:54 EDT	20200918_0347_CDrive.E01
SECRET_beth.lnk				C:\FileShare\Secret\SECRET_beth.txt	2020-09-18 18:39:22 EDT	20200918_0347_CDrive.E01
Szechuan Sauce.lnk				C:\FileShare\Secret\Szechuan Sauce.txt	2020-09-18 18:35:59 EDT	20200918_0347_CDrive.E01
mstsc.exe.lnk				C:\Windows\System32\mstsc.exe	0000-00-00 00:00:00	20200918_0347_CDrive.E01
No preferred path found.lnk				No preferred path found	0000-00-00 00:00:00	20200918_0347_CDrive.E01
PortalGunPlans.txt.lnk				C:\FileShare\Secret\PortalGunPlans.txt	0000-00-00 00:00:00	20200918_0347_CDrive.E01
SECRET_beth.txt.lnk				C:\FileShare\Secret\SECRET_beth.txt	0000-00-00 00:00:00	20200918_0347_CDrive.E01
Beth_Secret.txt.lnk				C:\FileShare\Secret\Beth_Secret.txt	0000-00-00 00:00:00	20200918_0347_CDrive.E01
Szechuan Sauce.txt.lnk				C:\FileShare\Secret\Szechuan Sauce.txt	0000-00-00 00:00:00	20200918_0347_CDrive.E01
NoJerry.txt.lnk				C:\FileShare\Secret\NoJerry.txt	0000-00-00 00:00:00	20200918_0347_CDrive.E01
NTUSER.DAT				C:\Windows\system32\dsa.msc		20200918_0347_CDrive.E01
NTUSER.DAT				C:\Windows\system32\gpmc.msc		20200918_0347_CDrive.E01

Figure 22: Screenshot Showing Files Accessed by Malicious Player

- SECRET\_beth.txt was found in the recycle bin
- FTK image shows us that the SECRET\_beth.txt that was deleted contains a different message than the one in the secret folder.
- Looking in the webcache data using autopsy, several files were located, meaning, these files were exfiltrated.

WebCacheV01.dat		res:///C:\Windows\system32\mmcndmgr.dll\views.htm	2020-09-18 22:32:18 EDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		file:///C:/FileShare/Secret/PortalGunPlans.txt	2020-09-19 03:32:02 EDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		file:///C:/FileShare/Secret/Szechuan%20Sauce.txt	2020-09-19 03:32:21 EDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		file:///C:/FileShare/Secret/SECRET_beth.txt	2020-09-19 03:32:13 EDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		res:///iesetup.dll/HardAdmin.htm	2020-09-19 03:23:01 EDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat	0	http://194.61.24.102/	2020-09-19 03:23:41 EDT	Microsoft Edge Analyzer	194.61.24.102	Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat	0	http://194.61.24.102/favicon.ico	2020-09-19 03:23:41 EDT	Microsoft Edge Analyzer	194.61.24.102	Administrator	20200918_0347_CDrive.E01
WebCacheV01.dat		file:///C:/FileShare/Secret/Beth_Secret.txt	2020-09-19 03:35:07 EDT	Microsoft Edge Analyzer		Administrator	20200918_0347_CDrive.E01

Figure 23: Screenshot from Autopsy Showing Exfiltrated Files

### ■ When?

The files were accessed on 2020-09-18 between 18:35:59 - 23:35:07 EDT and exfiltrated at 3:23: UDT by the Administrator (see figure 25)

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

During our investigation, the network layout of the victim's network comprised a centralized data center (DC) and multiple endpoints.

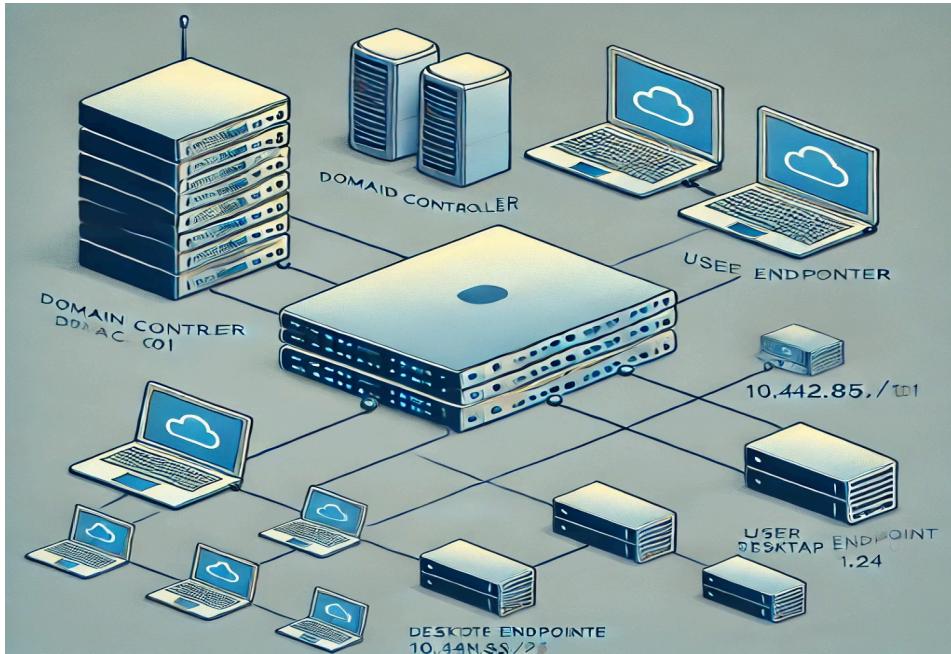


Figure 24: Screenshot Showing Network Layout

Wireshark - Endpoints - case001.pcap								
Endpoint Settings		Ethernet - 16	IPv4 - 258	IPv6 - 11	TCP - 15930	UDP - 1356		
		Address	Packets	Bytes	Tx Packets	Tx Bytes	Rx Packets	Rx Bytes
<input checked="" type="checkbox"/> Limit to display filter		8.240.65.254	437	458 kB	314	450 kB	123	8 kB
		8.240.169.252	164	157 kB	111	152 kB	53	4 kB
		8.252.107.126	11	2 kB	5	1 kB	6	781 bytes
		8.252.174.254	230	252 kB	171	247 kB	59	4 kB
		8.252.215.126	14	2 kB	7	1 kB	7	984 bytes
		8.252.220.254	68	7 kB	0	0 bytes	68	7 kB
		8.253.200.120	24	6 kB	12	5 kB	12	2 kB
		8.253.203.126	248	252 kB	169	246 kB	79	6 kB
		10.42.85.10	264,107	58 MB	115,627	21 MB	148,480	37 MB
		10.42.85.115	179,256	136 MB	65,547	14 MB	113,709	122 MB
		10.42.05.255	194	23 kB	0	0 bytes	194	23 kB
		10.90.90.90	4,579	964 kB	2,329	742 kB	2,250	223 kB
		13.35.126.20	93	54 kB	49	51 kB	44	4 kB
		13.74.179.117	80	15 kB	43	11 kB	37	4 kB
		13.78.149.173	29	9 kB	15	7 kB	14	2 kB
		13.88.23.8	26	12 kB	14	9 kB	12	3 kB
		13.88.28.53	32	14 kB	18	6 kB	14	9 kB
		13.89.202.241	21	7 kB	12	5 kB	9	2 kB
		13.107.3.254	70	22 kB	39	17 kB	31	4 kB
		13.107.4.254	65	20 kB	34	16 kB	31	4 kB

Figure 25: Screenshot from Wireshark Capture

## Optional Questions

1. What architectural changes should be made immediately?
  - The ability to connect via RDP should be disabled for external network connections since the initial breach was made using this pathway. There should also be a firewall put in place between the DC and the internet
2. Did the attacker steal the Szechuan sauce? If so, what time?
  - The attacker stole the Szechuan sauce at 3:23: EDT (see Figure 21)
3. Did the attacker steal or access any other sensitive files? If so, what times?
  - Yes, see figure 22
4. Finally, when was the last known contact with the adversary?
  - n/a.

## Conclusion

In conclusion, the recent case of the stolen Szechuan Sauce recipe could have been prevented if the organization had implemented a few basic security measures. These include practicing the principle of least privilege by requiring stronger authentication for network access, protecting sensitive information with multiple layers of defense, regularly backing up systems to detect file tampering, and implementing better monitoring methods for network traffic to identify vulnerabilities.

Had the organization required multi-factor authentication for remote access to the server and desktop, the attacker may have been deterred or prevented from gaining access. Additionally, the Szechuan Sauce recipe, which was a highly sensitive and valuable asset, could have been better protected with the use of encryption keys, multi-factor authentication, or stronger passwords.

Regular system backups would have provided a baseline comparison for forensic investigators to identify anomalies and potential malicious activity. This would also have protected the organization against ransomware attacks.

Finally, better monitoring of network traffic could have identified brute force attacks and vulnerabilities such as open ports, allowing the organization to take action to prevent the breach and the subsequent theft of the Szechuan Sauce recipe.

Overall, the implementation of these basic security measures could have significantly reduced the risk of a security breach and protected the organization's valuable assets, including the highly sought-after Szechuan Sauce recipe.

## References & Citations

James, M. (2021, March 25). *Case 001 - The stolen Szechuan sauce. DFIR Madness.* <https://dfirmadness.com/the-stolen-szechuan-sauce/>

Lighthouse Labs. (n.d.). *Project 14: DFIR - Digital forensics and incident response. Lighthouse Labs.*

<https://web.compass.lighthouselabs.ca/p/14/113e24e3-e31f-456f-920c-2162f914fb4e>

Rapid7. (n.d.). *Metasploit | Penetration testing software. Metasploit.* <https://www.metasploit.com/>

TryHackMe. (n.d.). Windows forensics 1. TryHackMe. <https://tryhackme.com/r/room/windowsforensics1>