Forensic Investigation
Stolen Szechuan Sauce

By Kowsor, Esther & Trevor

Table Contents:

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.

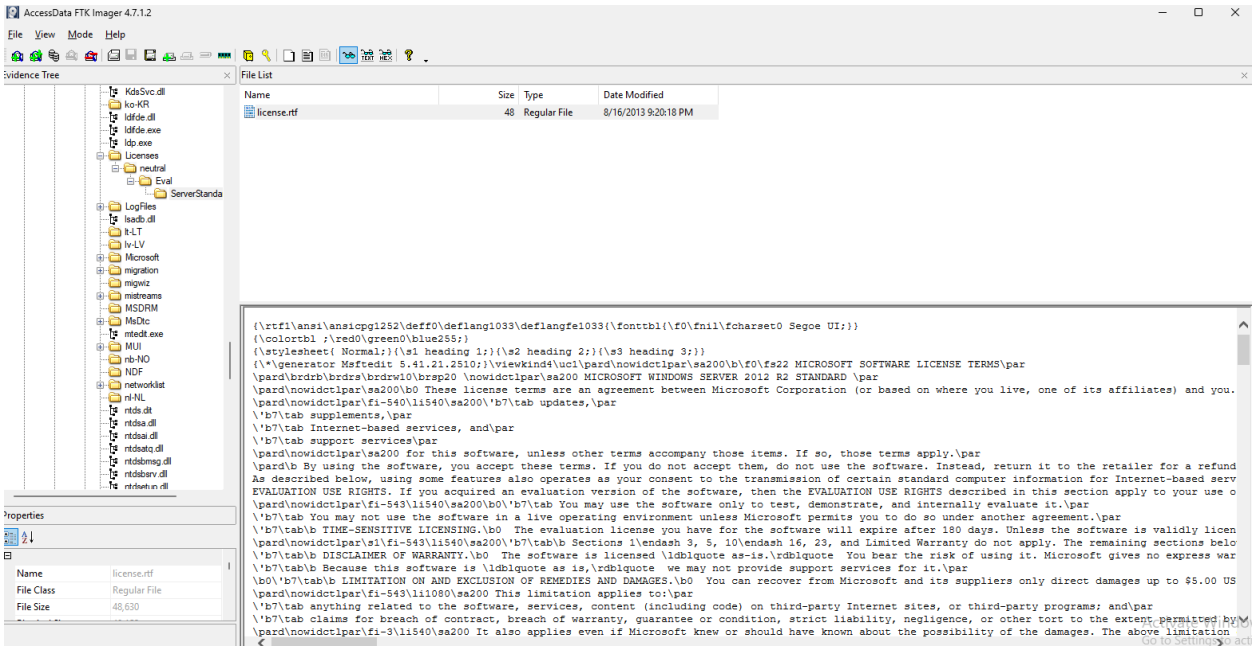


Figure 1: Screenshot showing the Operating System of the Server

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.

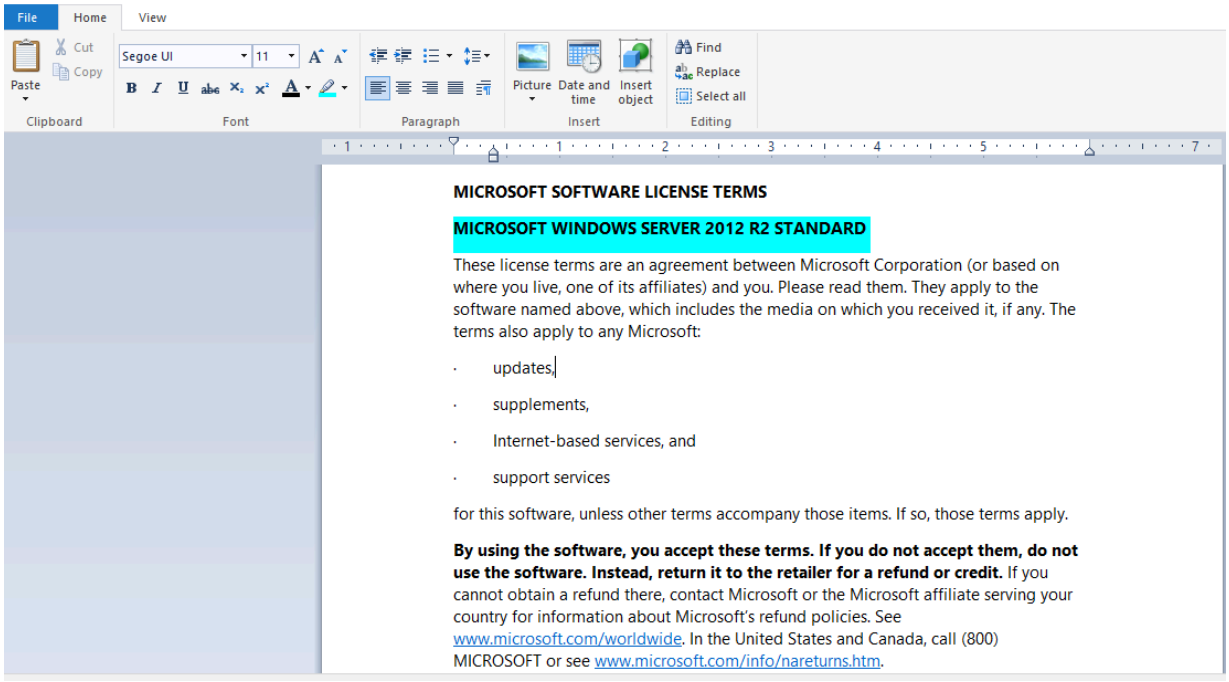


Figure 2: Screenshot Showing the Windows Operating System Licence

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

The operating system of the desktop is Windows 10 Enterprise

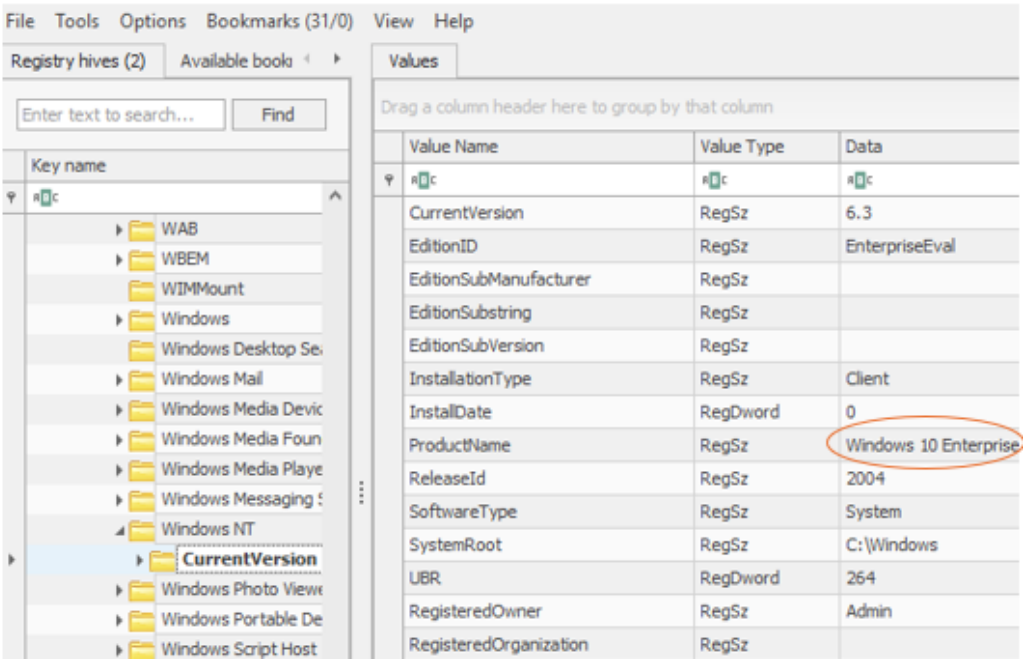


Figure 3: Screenshot showing the Operating System of the Desktop

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.

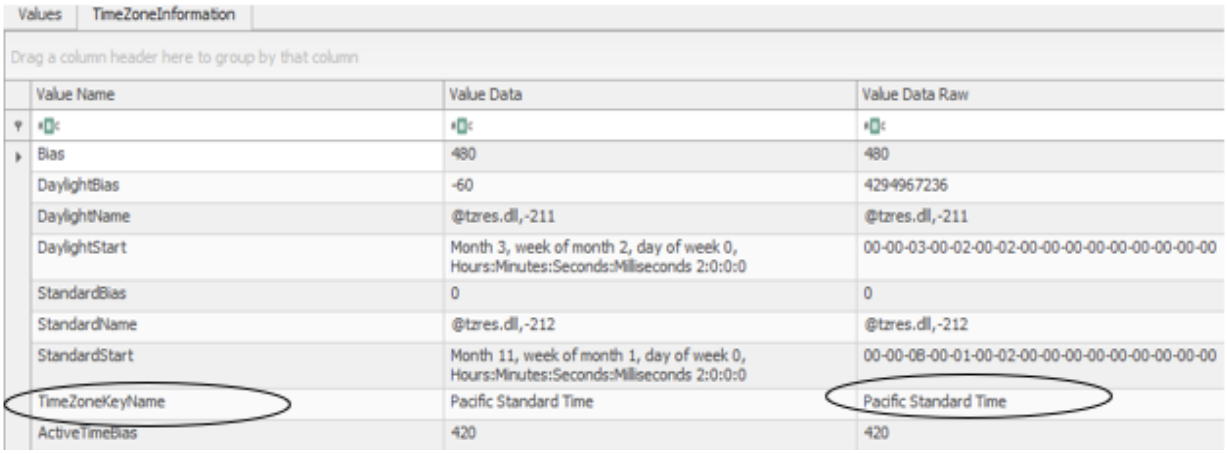


Figure 4: Screenshot Showing the Time Zone Information

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.

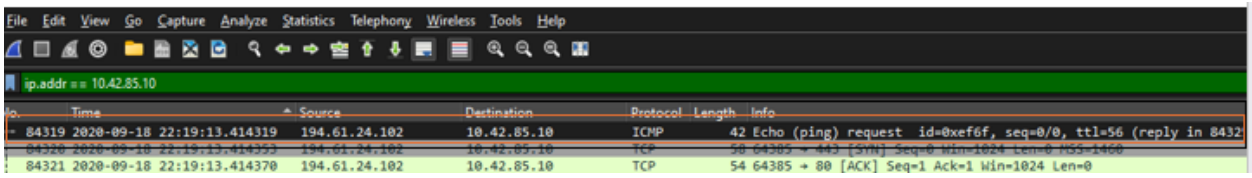


Figure 5: Screenshot Showing Initial Access of Malicious IP Address using Brute Force

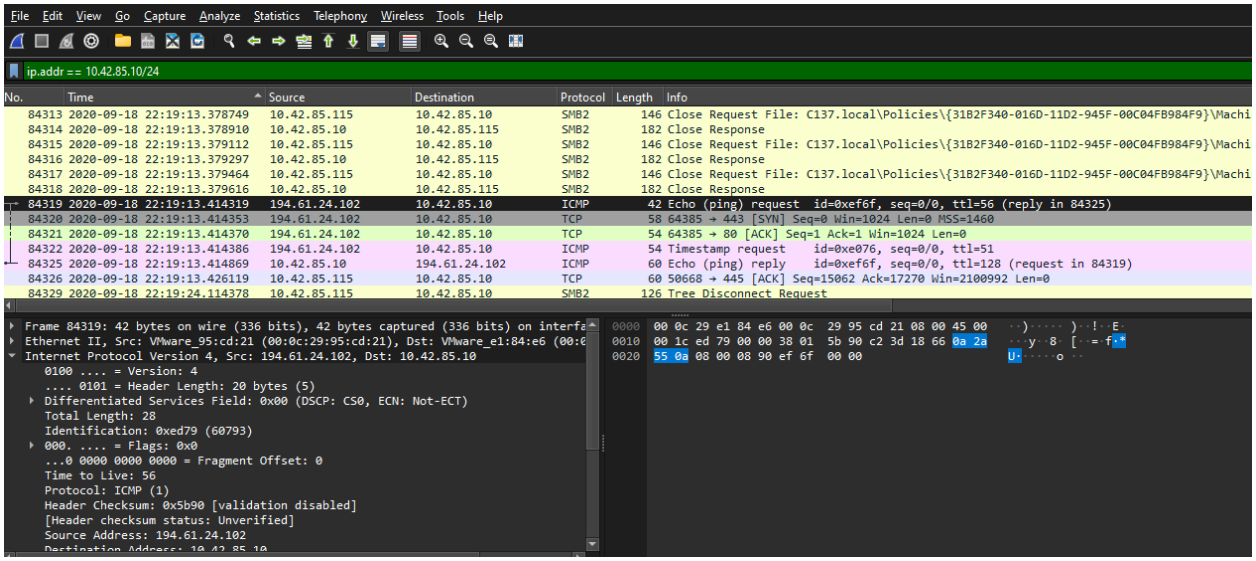


Figure 6: Screenshot from PCAP Capture Showing The Malicious IP Communication

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.

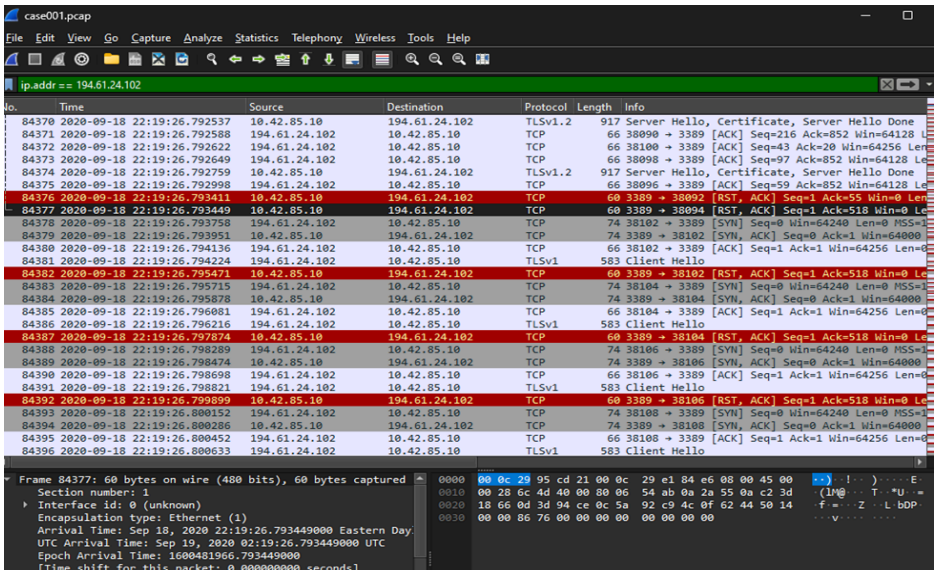


Figure 7: Screenshot from PCAP Capture Showing the Malicious IP Communication

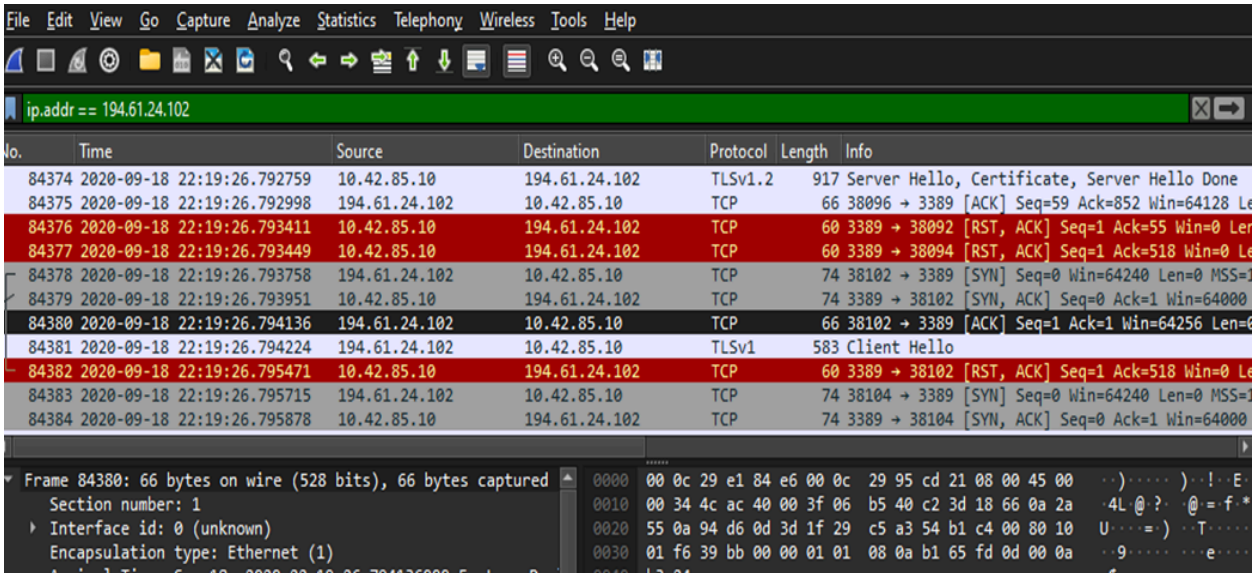


Figure 8: Screenshot from PCAP Capture Showing Brute Force

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.

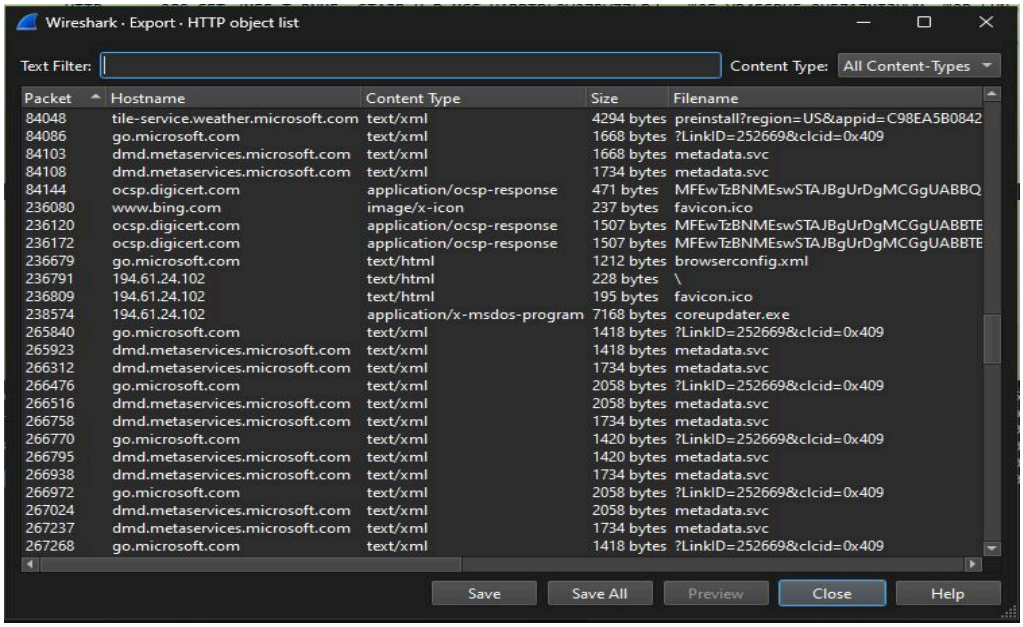


Figure 9: Screenshot Showing Exporting the Malicious File

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

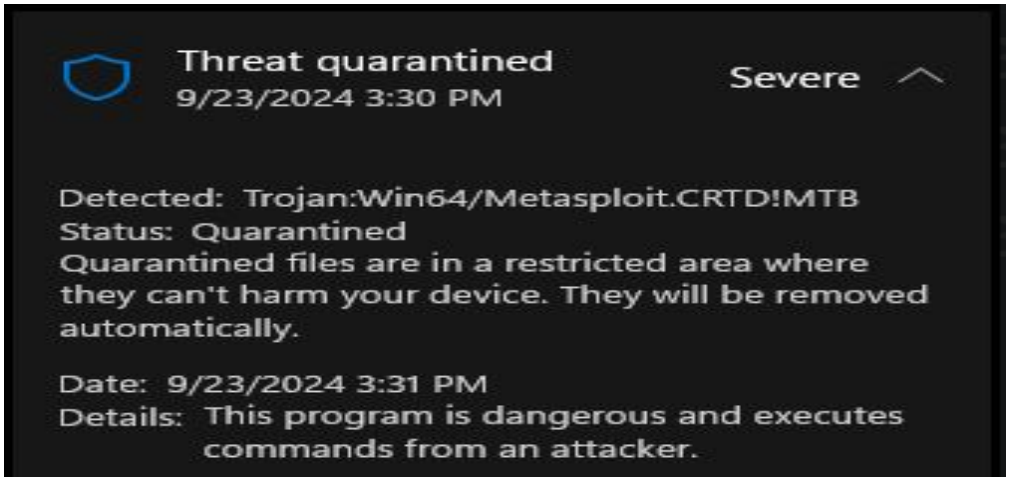
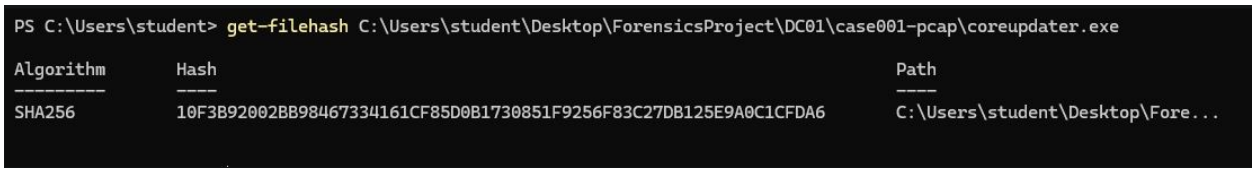


Figure 10: Screenshot Showing Windows Defender Confirming the Threat Quarantine

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



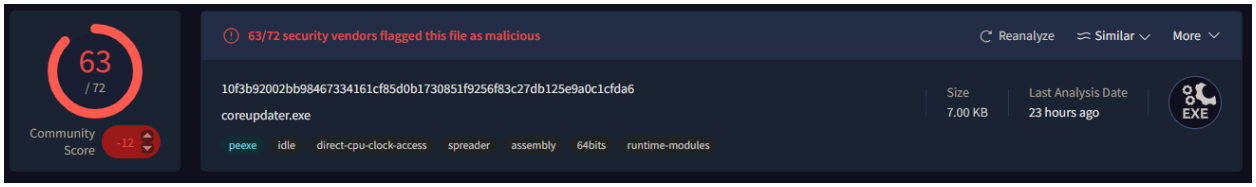


Figure 11: Screenshot from Virus Total Showing the Community Score of coreupdater.exe

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.

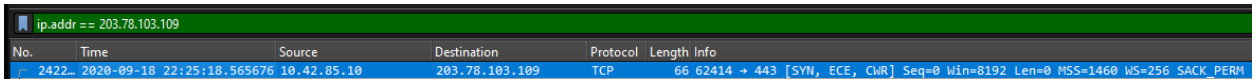


Figure 13: Screenshot from Wireshark Capture Confirming Malicious IP

- Address confirmed using Volatility workbench.

```
0x60182590      TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0x601cda00      TCPv6   fe80::2dcf:e660:be73:d220       135     fe80::2dcf:e660:be73:d220       62779   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)*

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

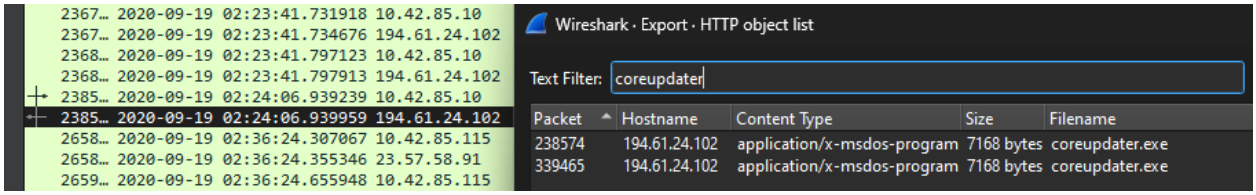


Figure 16: Screenshot Showing Initial entry of Coreupdater.exe

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.

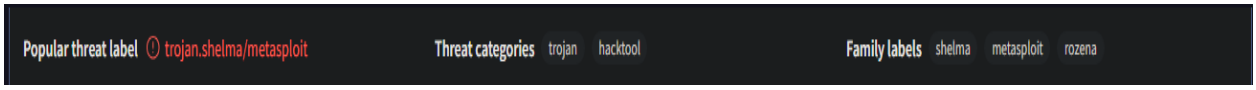


Figure 17: Screenshot showing Virus Total identifying coreupdater.exe as a Trojan.

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

Entry Location
ABC
HKLM\System\CurrentControlSet\Services
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

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)

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.browneypetworld.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

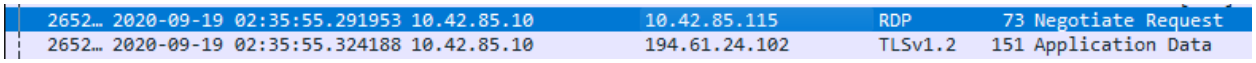


Figure 21: Screenshot from PCAP Capture Showing the First Access

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.

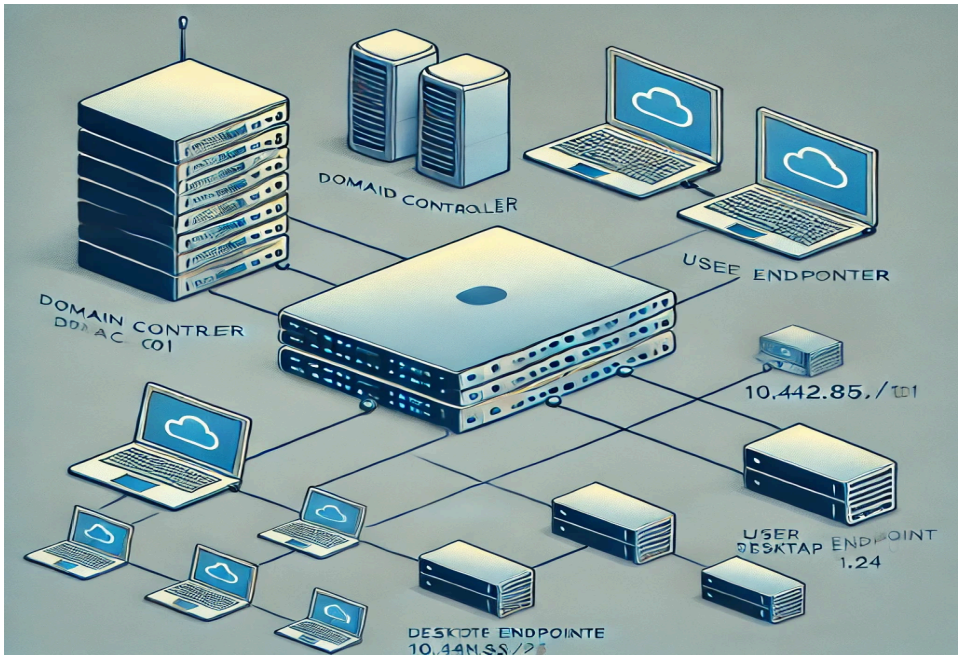


Figure 24: Screenshot Showing Network Layout

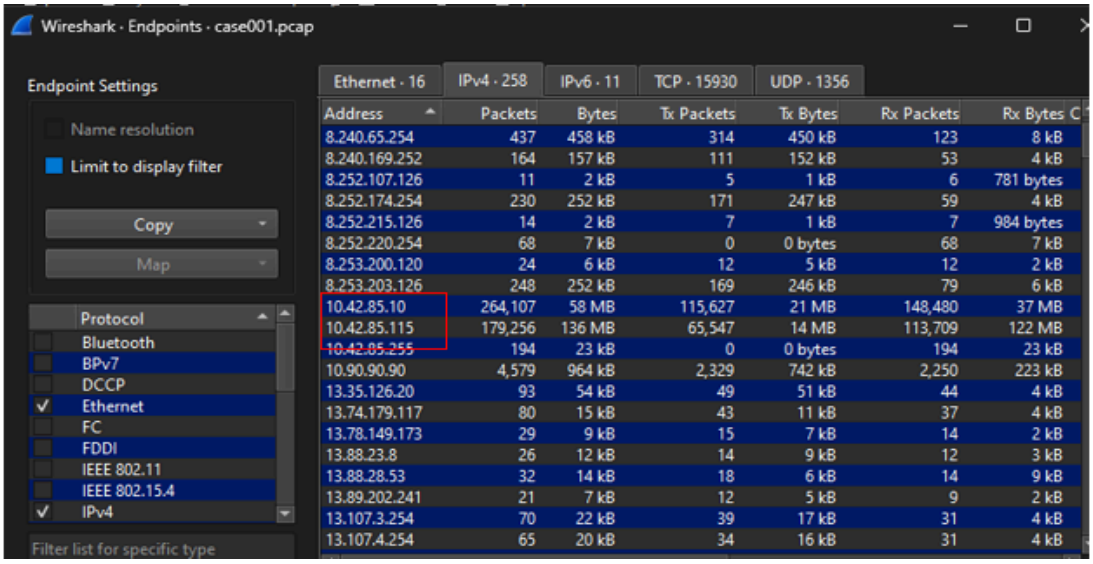


Figure 25: Screenshot from Wireshark Capture

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