

# The Stolen Szechuan Sauce



Table of Contents

EXECUTIVE SUMMARY ..... 1

CASE OVERVIEW ..... 1

TOOLS USED..... 1

QUESTIONS..... 1-10

REFERENCES ..... 11

By : Madhuri Chamarthi

## Executive Summary:

The “Case of the Stolen Szechuan Sauce” digital forensics project focuses on analyzing a breach by employing advanced tools and methodologies. Through careful examination of network traffic and system artifacts, the project uncovers critical information about the breach, including the breach timeline, attack vectors, and malicious activities. Key findings include the identification of the breach, initial entry vector through RDP brute force, presence of malware (“coreupdater.exe”), and the compromise of sensitive data. The project also recommends architectural improvements, policy enhancements, and preventive measures to fortify the security posture. Ultimately, the project underscores the significance of digital forensics in unraveling complex security incidents and strengthening cyber defenses.

## Case Overview:

“Your bedroom door bursts open, shattering your pleasant dreams. Your mad scientist of a boss begins dragging you out of bed by the ankle. He simultaneously explains between belches that the FBI contacted him. They found his recently developed Szechuan sauce recipe on the dark web. As you careen past the door frame you are able to grab your incident response “Go-Bag”. Inside is your trusty incident thumb drive and laptop...”

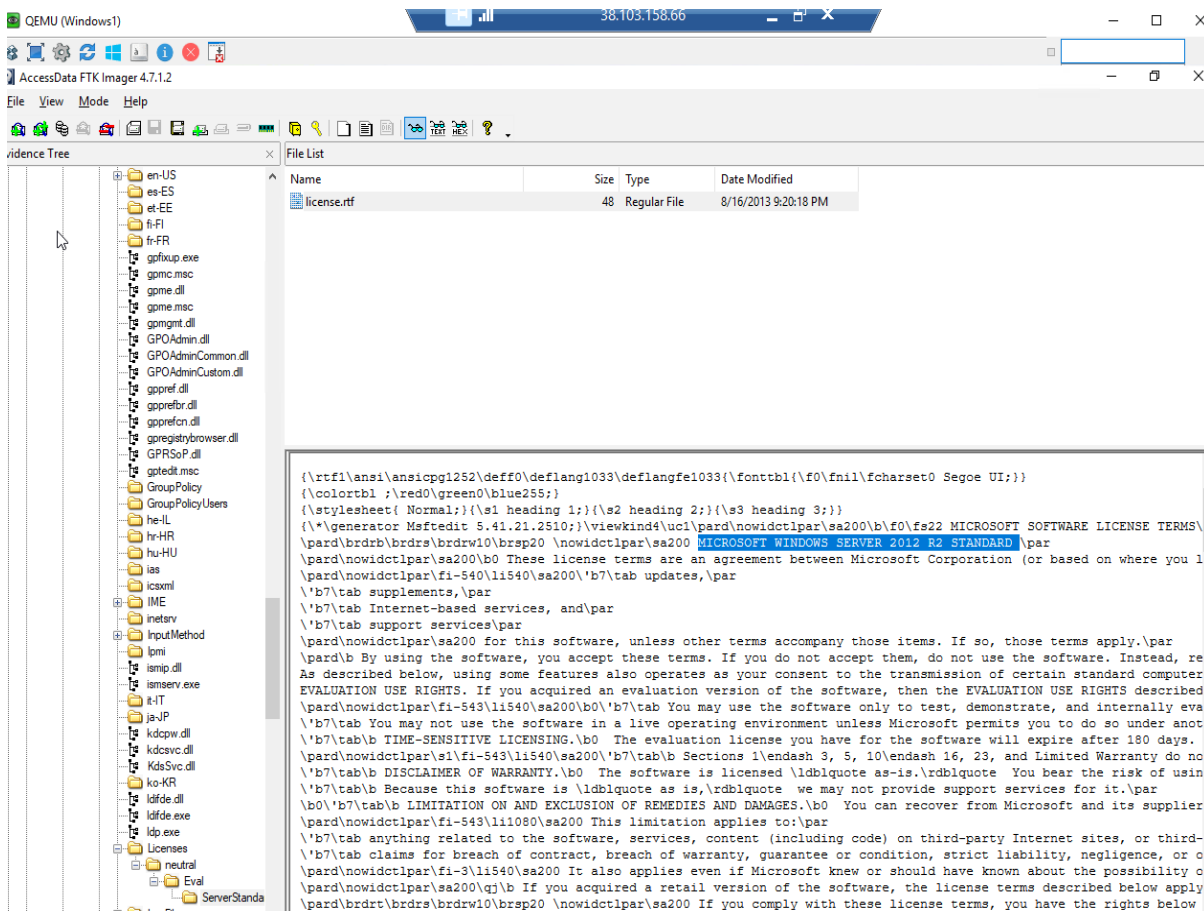
## Tools used:

- FTK Imager
- Registry editor
- Wireshark
- Access data Registry viewer

## Questions:

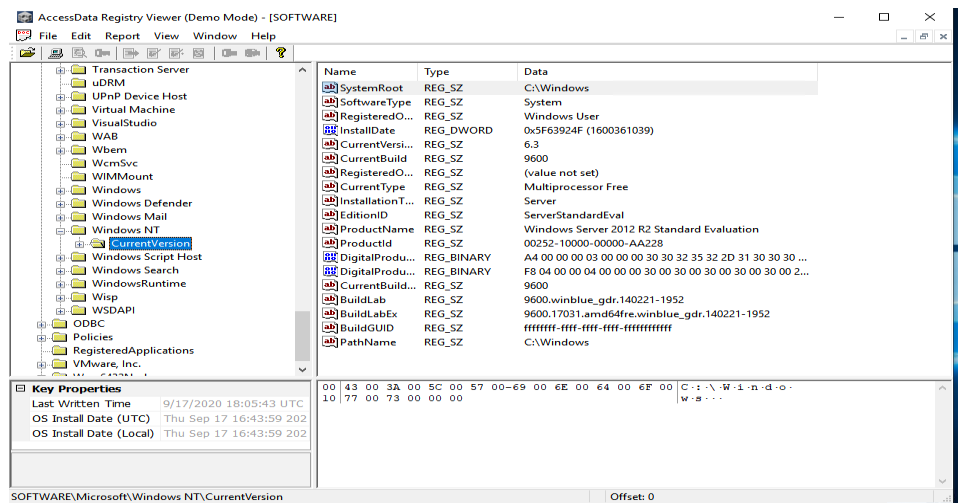
**Question 1:** What’s the Operating System of the Server?

**Answer:** Using the FTK Imager tool for the DC01-EC01 data folder we got the Operating System of the server as Windows Server 2012 R2 Standard Evaluation. To find this we can check in a few places like, using the file path C:\Windows\System32\license.



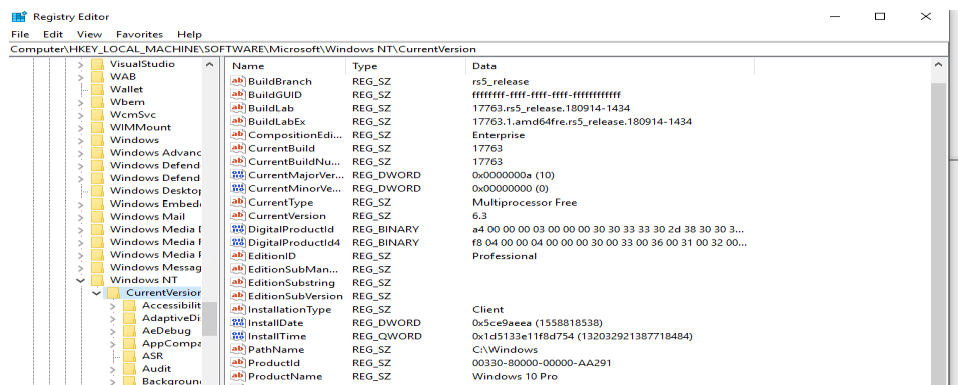
Another way to identify the operating system is through the Access data registry viewer **HKLM\Software\Microsoft\Windows NT\CurrentVersion**

## Forensic Report and Documentation



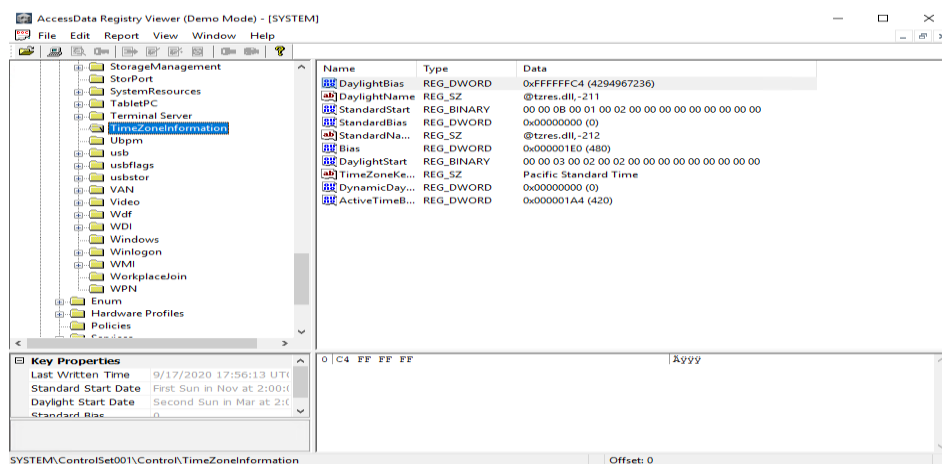
**Question 2:** What's the Operating System of the Desktop?

**Answer:** Following this same idea as above I was able to identify the OS of the Desktop.



**Question 3:** What was the local time of the Server?

**Answer:** Pacific Standard Time (PST)

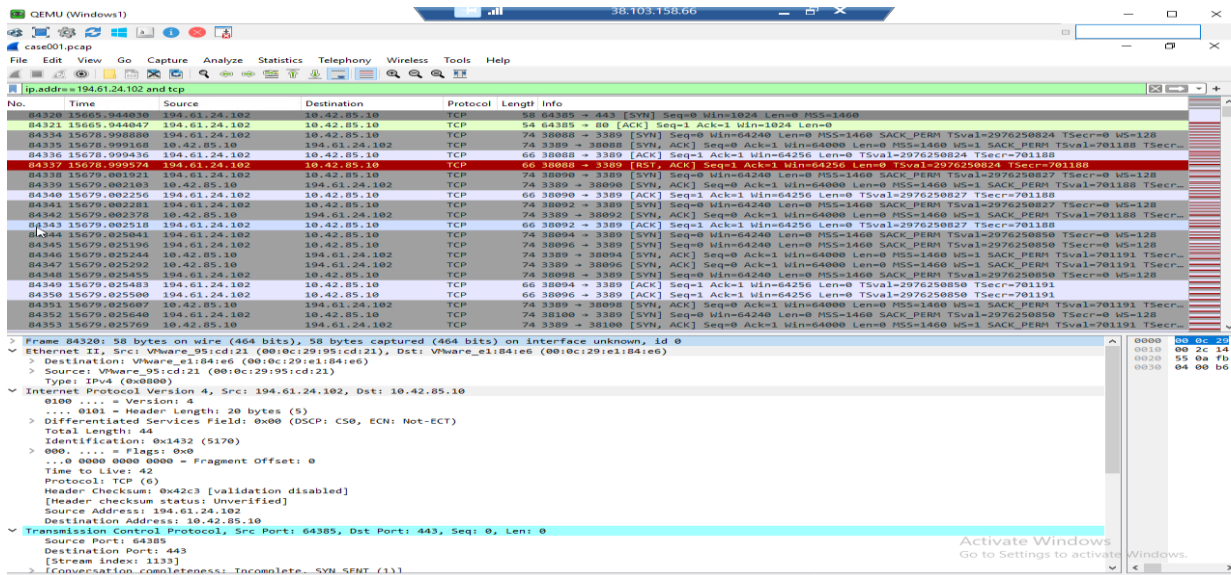


**Question 4:** Was there a breach?

**Answer:** Yes, we know from the case summary that the recipe was stolen.

**Question 5:** What was the initial entry vector (how did they get in)?

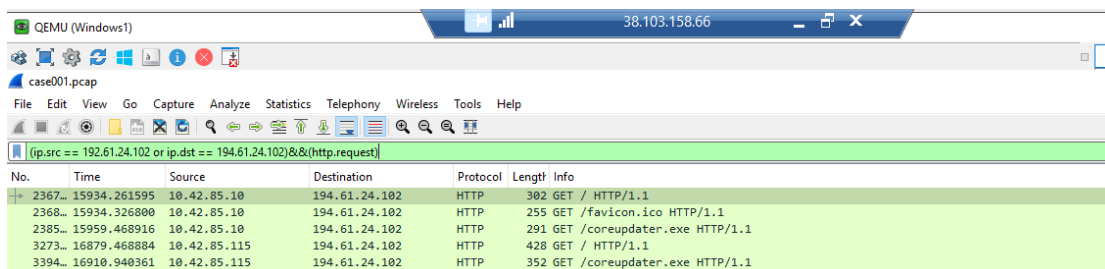
**Answer:** RDP Brute Force was employed initially due to the numerous SYN requests directed at the same destination port I found this using this filter ip.addr == 194.61.24.102 and tcp in the case001.pcap.



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

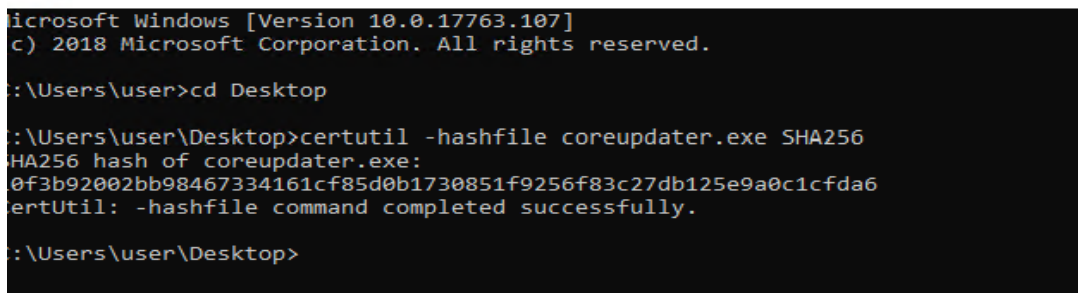
**6.a.** What process was malicious?

**Answer:** coreupdater.exe, we can explore the potential malware utilized by referring to IP address 194.61.24.102. To conduct this investigation, apply the subsequent filter within the case001.pcap file:  
(ip.src == 194.61.24.102 or ip.dst == 194.61.24.102) && (http.request)



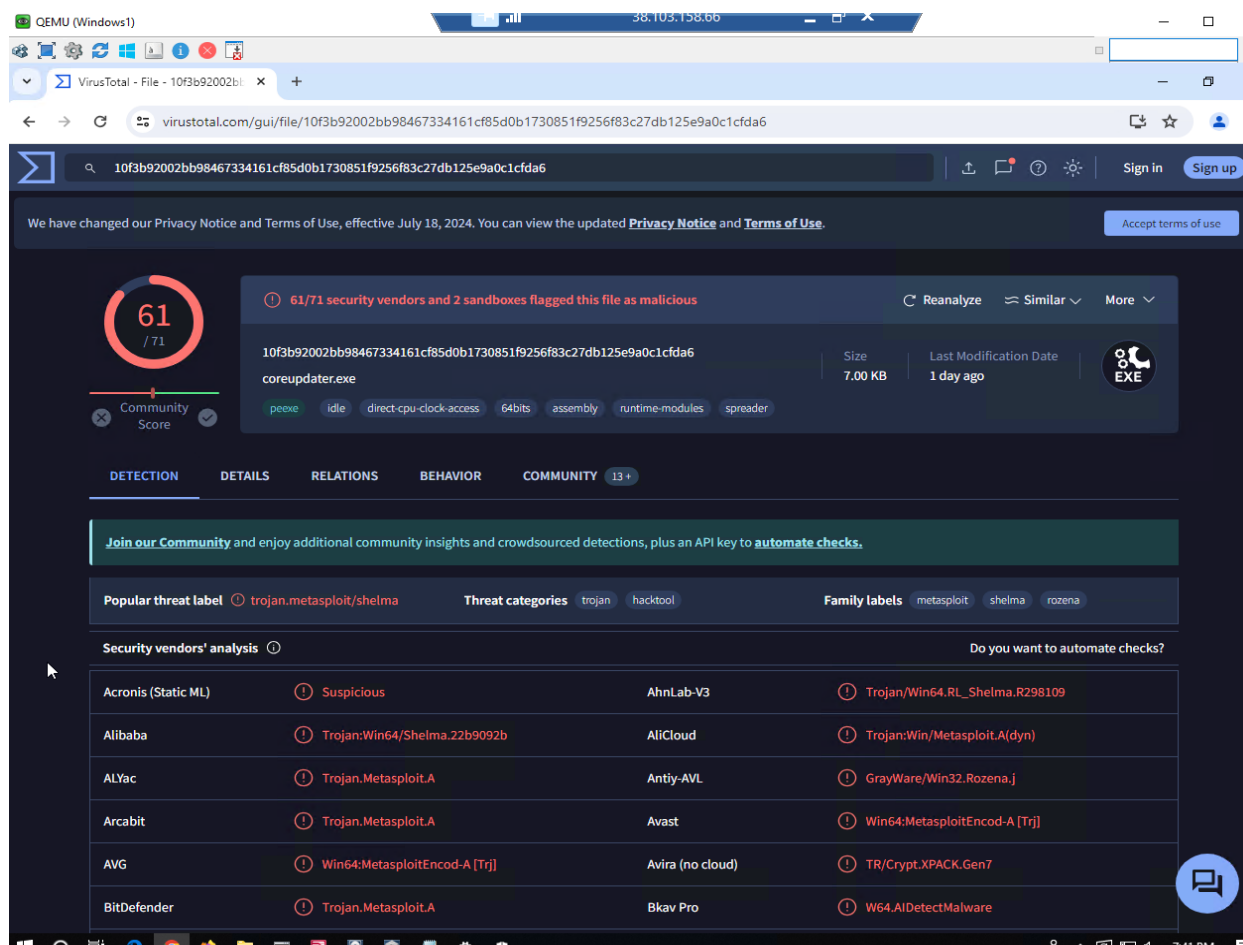
To determine whether “coreapdater.exe” is truly a malicious process or not, we will export the .exe file and examine its hash value for verification in command prompt.

**Command Prompt**



## Forensic Report and Documentation

Now we got the hash value of the **coreupdater.exe**. Subsequently, we entered this hash into VirusTotal, revealing that the hash associated with coreupdater.exe was indeed identified as malicious.

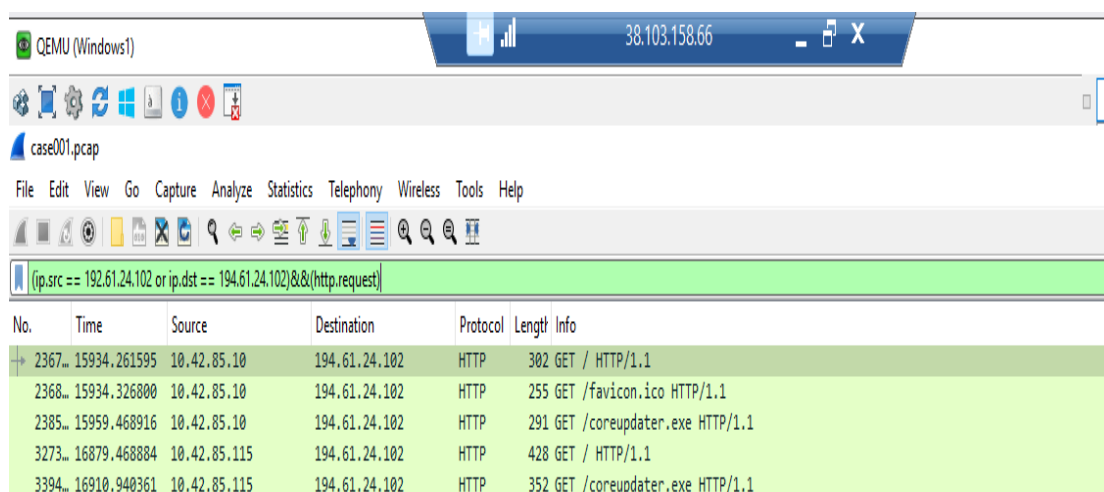


The screenshot shows the VirusTotal web interface for the file **coreupdater.exe** with hash **10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfa6**. The file is flagged as malicious by 61/71 security vendors. The interface includes tabs for Detection, Details, Relations, Behavior, and Community. The Detection tab is active, showing a list of security vendors and their analysis results.

Security vendors' analysis	Do you want to automate checks?
Acronis (Static ML) Suspicious	AhnLab-V3 Trojan/Win64.RL_Shelma.R298109
Alibaba Trojan:Win64/Shelma.22b9092b	AliCloud Trojan:Win/Metasploit.A(dyn)
ALYac Trojan.Metasploit.A	Antiy-AVL GrayWare/Win32.Rozena.j
Arcabit Trojan.Metasploit.A	Avast Win64:MetasploitEncod-A [Trj]
AVG Win64:MetasploitEncod-A [Trj]	Avira (no cloud) TR/Crypt.XPACK.Gen7
BitDefender Trojan.Metasploit.A	Bkav Pro W64.AIDetectMalware

### 6.b. Identify the IP Address that delivered the payload?

**Answer:** Above we got the coreupdater.exe with the hostname's IP 194.61.24.102 which is the potential one to deliver the payload.



The screenshot shows the Wireshark interface for the file **case001.pcap**. The packet list pane shows several HTTP GET requests to the IP address 194.61.24.102. The packet details pane shows the selected packet (No. 3394) with the following information:

No.	Time	Source	Destination	Protocol	Length	Info
3394	16910.940361	10.42.85.115	194.61.24.102	HTTP	352	GET /coreupdater.exe HTTP/1.1

### 6.c. What IP Address is the malware calling to?

**Answer:** 203.78.103.109 is the IP Address that the malware is calling. I verified this by looking into the VirusTotal > Relations Tab and noticed that there were 11 IP addresses associated with it.

**10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfd6a6**

61/71 security vendors and 2 sandboxes flagged this file as malicious

coreupdater.exe

Size: 7.00 KB | Last Modification Date: 1 day ago

**CONTACTED IP ADDRESSES (11)**

IP	Detections	Autonomous System	Country
192.168.0.30	0 / 90	-	-
192.168.0.34	0 / 90	-	-
192.229.211.108	0 / 90	15133	US
20.96.52.198	0 / 90	8075	US
20.99.132.105	0 / 90	8075	US
20.99.133.109	1 / 90	8075	US
20.99.184.37	1 / 90	8075	US
203.78.103.109	3 / 90	18362	TH
23.216.147.76	2 / 90	20940	US
a83f8110:1800::200	0 / 90	-	-

**Execution Parents (2)**

Scanned	Detections	Type	Name
2023-10-20	2 / 64	ZIP	eed41b4500e473f97c50c7385ef5e374.bin
2021-12-16	0 / 63	710	coreupdater.exe

Then I investigated case001.pcap file and observed that the most called IP Address was 203.78.103.109.

**ip.addr == 203.78.103.109**

No.	Time	Source	Destination	Protocol	Length	Info
2422...	16031.095353	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
2422...	16031.095681	203.78.103.109	10.42.85.10	TCP	66	443 → 62414 [SYN, ACK] Seq=0 Ack=1 Win=64240 Len=0 MSS=1460 SACK_PERM WS=128
2422...	16031.095815	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=1 Ack=1 Win=65536 Len=0
2422...	16031.281664	203.78.103.109	10.42.85.10	TCP	58	443 → 62414 [PSH, ACK] Seq=1 Ack=1 Win=64256 Len=4 [TCP segment of a reassembled PDU]
2422...	16031.282793	203.78.103.109	10.42.85.10	SSLV2	1514	Encrypted Data, Encrypted Data, Encrypted Data, Encrypted Data, Encrypted Data, Encrypted Data...
2422...	16031.282819	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.282836	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.282852	203.78.103.109	10.42.85.10	SSLV2	1514	Encrypted Data, Encrypted Data
2422...	16031.282869	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.282884	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.282900	203.78.103.109	10.42.85.10	SSLV2	1514	Encrypted Data
2422...	16031.282916	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.282932	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.282963	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=1 Ack=4385 Win=65536 Len=0
2422...	16031.283095	10.42.85.10	203.78.103.109	TCP	60	62414 → 443 [ACK] Seq=1 Ack=13145 Win=65536 Len=0
2422...	16031.283246	203.78.103.109	10.42.85.10	SSLV2	1514	Encrypted Data
2422...	16031.283293	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.283310	203.78.103.109	10.42.85.10	TCP	1514	443 → 62414 [ACK] Seq=16065 Ack=1 Win=64256 Len=1460
2422...	16031.283325	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.283340	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]
2422...	16031.283356	203.78.103.109	10.42.85.10	SSLV2	1514	Encrypted Data
2422...	16031.283374	203.78.103.109	10.42.85.10	TCP	1514	[TCP segment of a reassembled PDU]

Frame 242207: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) on interface unknown, id 0

Ethernet II, Src: VMware\_e1:84:e6 (00:0c:29:e1:84:e6), Dst: VMware\_95:cd:21 (00:0c:29:95:cd:21)

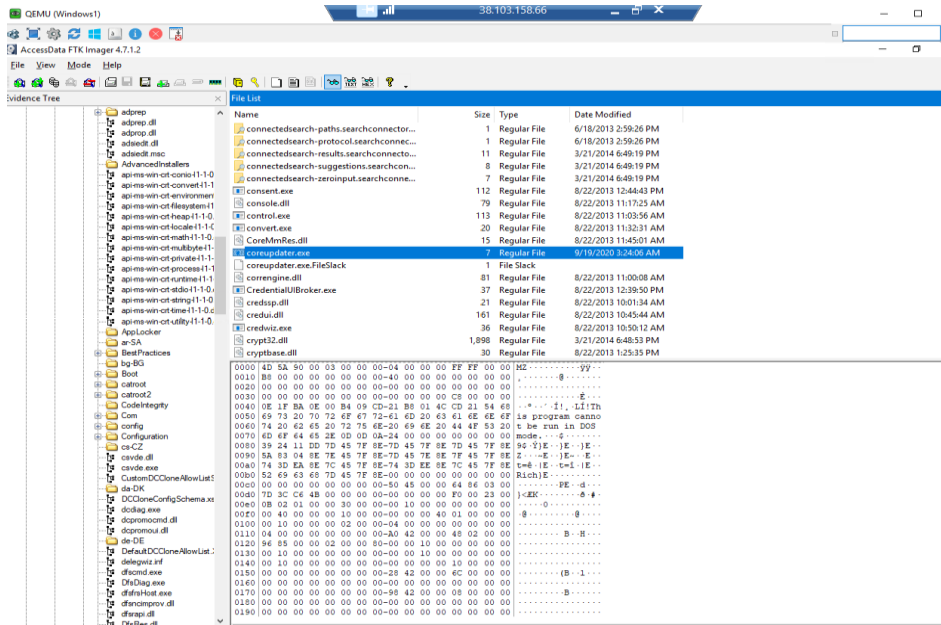
Internet Protocol Version 4, Src: 10.42.85.10, Dst: 203.78.103.109

Transmission Control Protocol, Src Port: 62414, Dst Port: 443, Seq: 0, Len: 0



## 6.d. Where is this malware on disk?

**Answer:** Using the FTK Imager, we got the malware on this path Windows\System32\coreupdater.exe



## 6.e. When did it first appear?

**Answer:** It first appeared on 2020-09-19 03:24:06 AM

control.exe	113	Regular File	8/22/2013 11:03:36 AM
convert.exe	20	Regular File	8/22/2013 11:32:31 AM
CoreMmRes.dll	15	Regular File	8/22/2013 11:45:01 AM
coreupdater.exe	7	Regular File	9/19/2020 3:24:06 AM
coreupdater.exe.FileSlack	1	File Slack	
corengine.dll	81	Regular File	8/22/2013 11:00:08 AM
CredentialUIBroker.exe	37	Regular File	8/22/2013 12:39:50 PM
credssp.dll	21	Regular File	8/22/2013 10:01:34 AM
credui.dll	161	Regular File	8/22/2013 10:45:44 AM
credwiz.exe	36	Regular File	8/22/2013 10:50:12 AM
crypt32.dll	1,898	Regular File	3/21/2014 6:48:53 PM

## 6.f. Did someone move it?

**Answer:** It was moved from the Administrators Downloads folder to the C drive of the DC and desktop systems.



### 6.g. What were the capabilities of this malware?

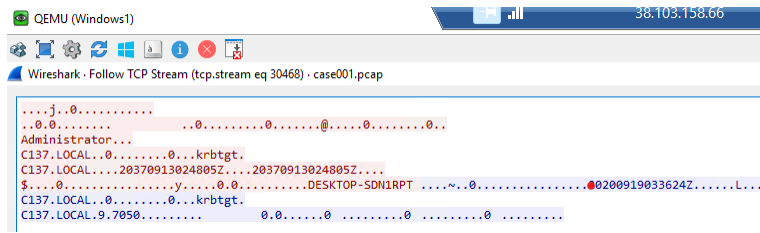
**Answer:** The following were the capabilities of this malware:

Exfiltration of data is the theft of private data, including passwords or proprietary information.

- Remote control: Giving the attacker access through a backdoor so they can take control of the compromised machine from a distance.
- File encryption and ransom demand are two related concepts that are frequently used in ransomware.
- Spreading to external contacts or other systems inside the network is known as propagation.
- Destruction: In some cases, attackers can intentionally break or completely erase the computer systems, causing a lot of harm.

### 6.h. Is this malware easily obtained?

**Answer:** The harmful program was found to have moved from the Administrator's Downloads area. This kind of action suggests that the program is trying to hide within important system files, possibly to stay there for a long time and gain more control.

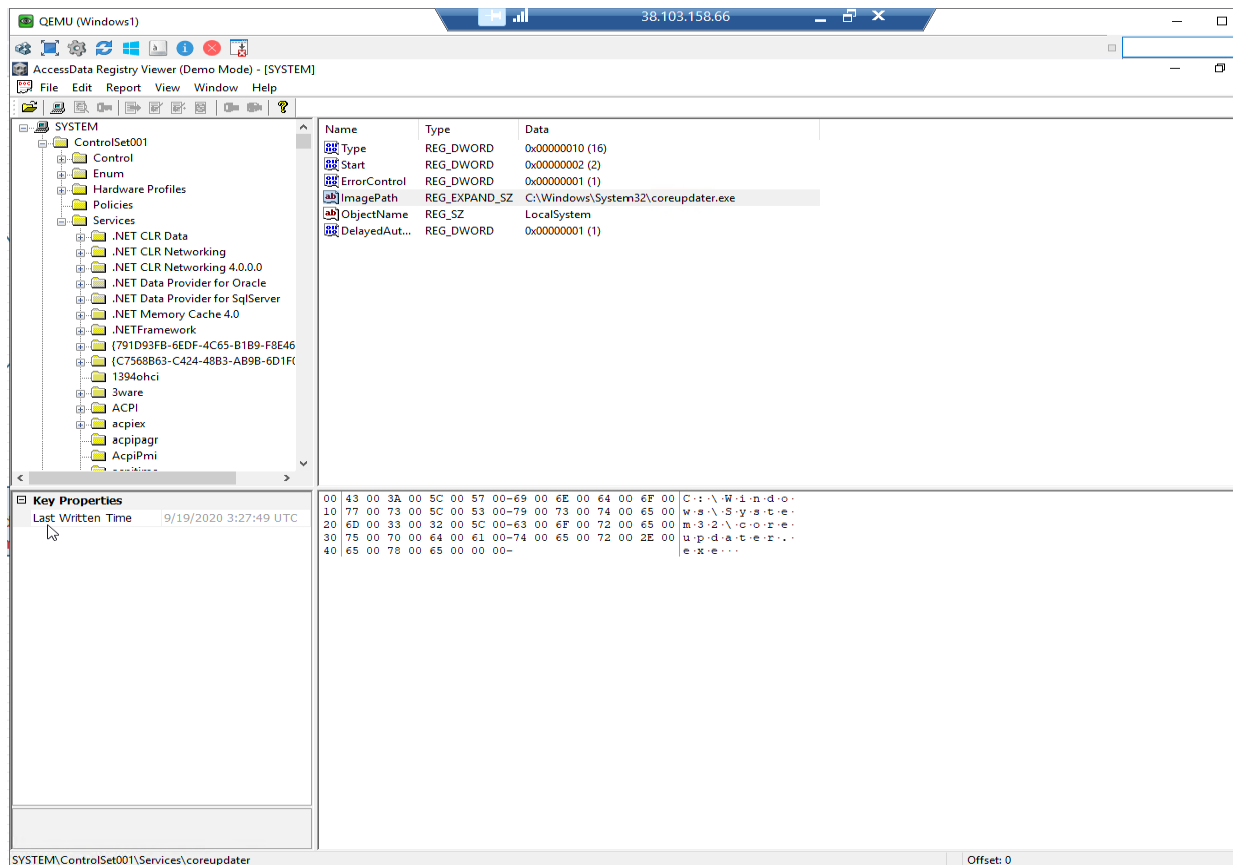


Also, Metasploit is a red teaming tool which is open source, so safe to say accessible.

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

Where?

**Answer:** Using AccessData Registry Viewer, I found the malware in C:\system\windows\System32\Conytrolset001\services\coreupdater.exe.





**Question 7:** What malicious IP Addresses were involved?**7.a.** Were any IP Addresses from known adversary infrastructure?

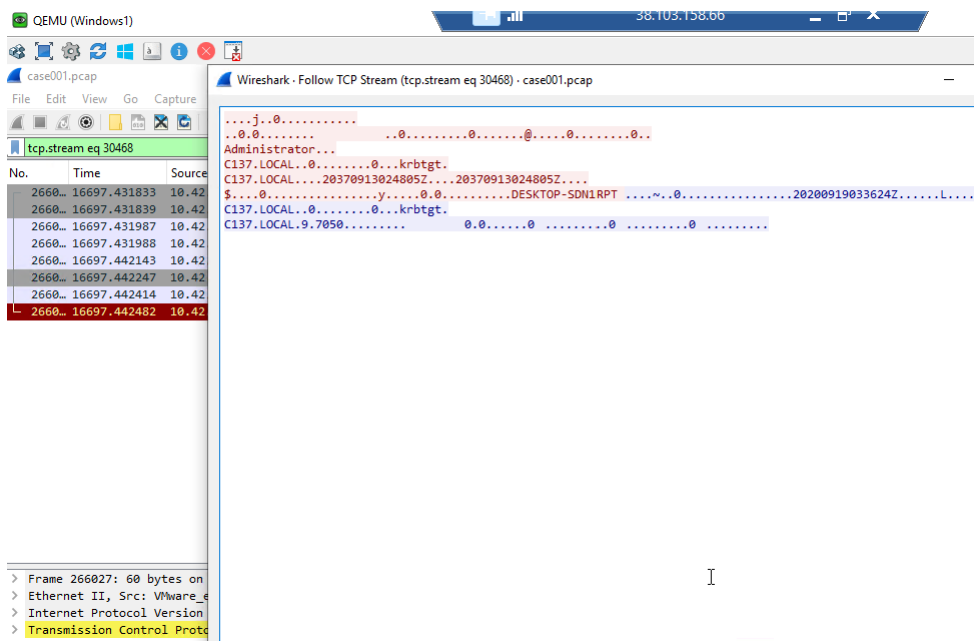
**Answer:** The IP address 194.61.24.102 has been traced in the past for its use in RDP Brute Force attacks, hence it has been confirmed that it is a part of known adversary infrastructure. The IP address 203.78.103.109 was briefly connected to a suspicious website, but it was later verified that this connection had no connection.

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

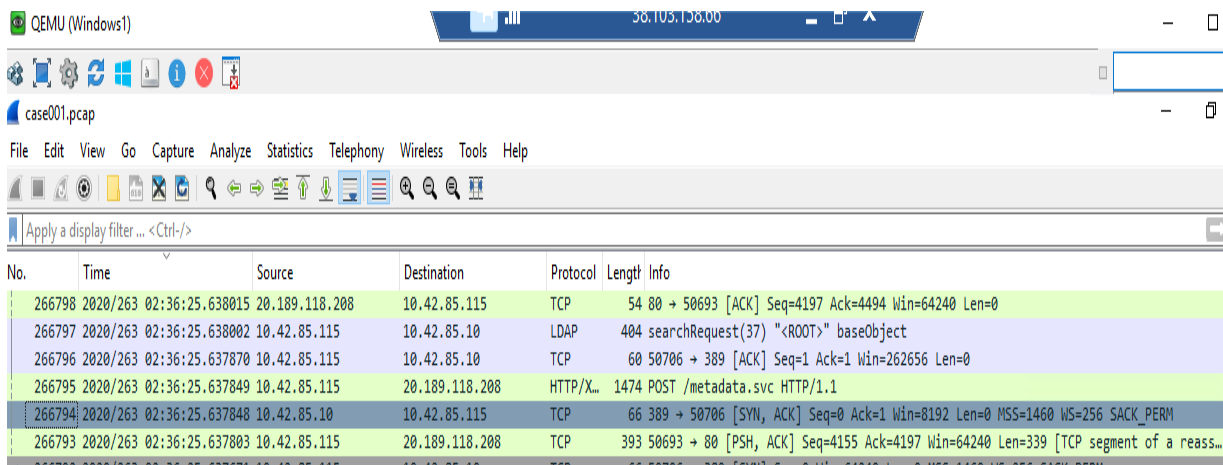
**Answer:** Yes, the information suggests that at that moment, these components of unfriendly computer systems were engaged in other harmful activities and attacks. The ongoing monitoring and connections to previously recognized hostile actions underscore the constantly changing nature of the risky situation.

**Question 8:** Did the attacker access any other systems?How and When?

**Answer:** The attack managed to enter C137\DESKTOP-SDN1RPT\$ by utilizing Remote Desktop Protocol (RDP) from the Domain Controller (DC) while using the Administrator account. This took place around 2:36 on the 19th, and we detected this activity within the pcap file.

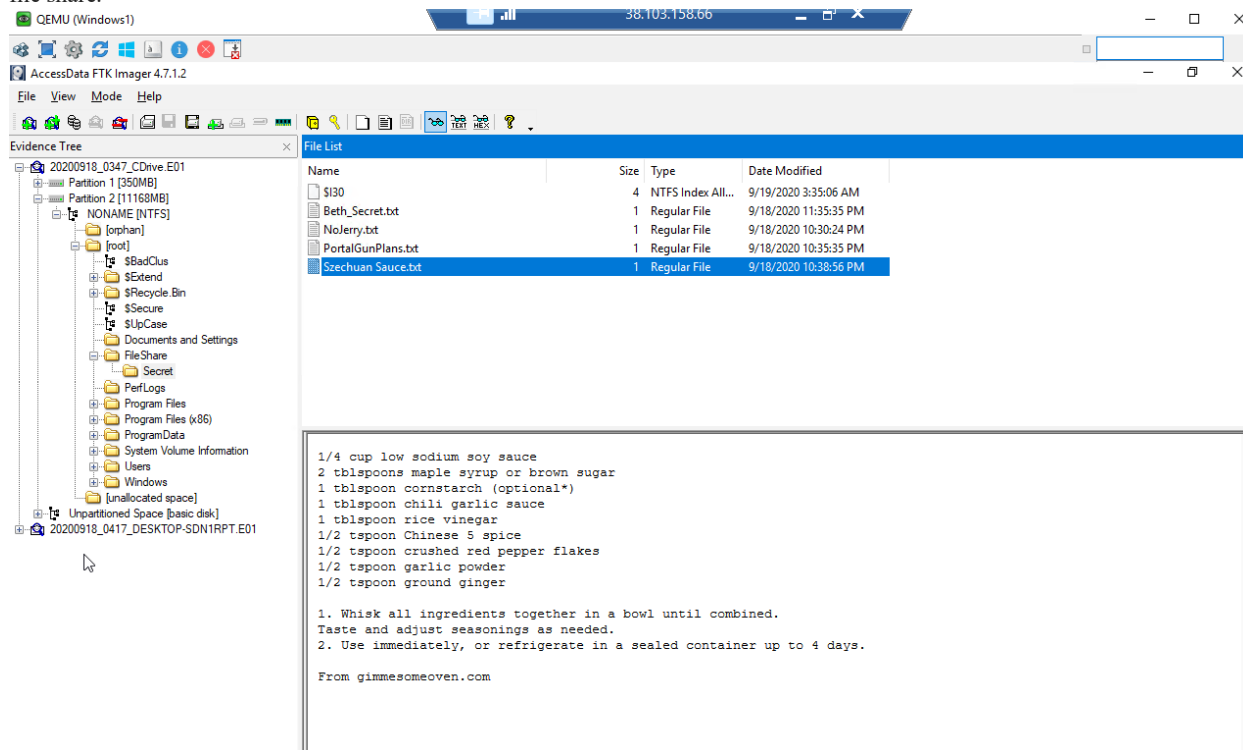


Also, when reviewing the pcap file in Wireshark, we can search for RDP connections from the DC to the desktop after the initial access. By doing this we can see a connection from the DC to desktop at 2:36:25.



## 8.c. Did the attacker steal or access any data?

**Answer:** Through FTK Imager, it's evident that the Administrator has recently interacted with all the files located within the "Secret" folder within the file share.



## Question 9: What was the network layout of the victim network?

**Answer:** To determine the network configuration of the targeted system, we can examine the process in registry viewer.

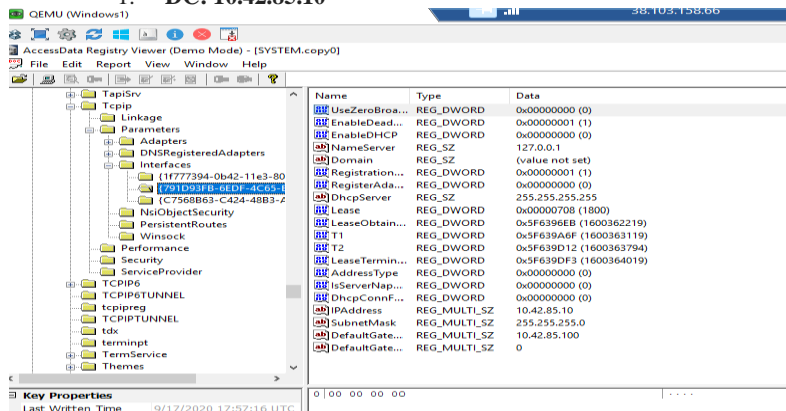
- Navigate to the following path: System > ControlSet001 > Services > Tcpip > Parameters > Interfaces. In this context, it's observed that two hosts share an identical subnet, specifically 10.42.85.0/24.

- The two devices on this subnet include a Domain Controller with an IP address of 10.42.85.10, and a desktop computer with an IP address of 10.42.85.115.

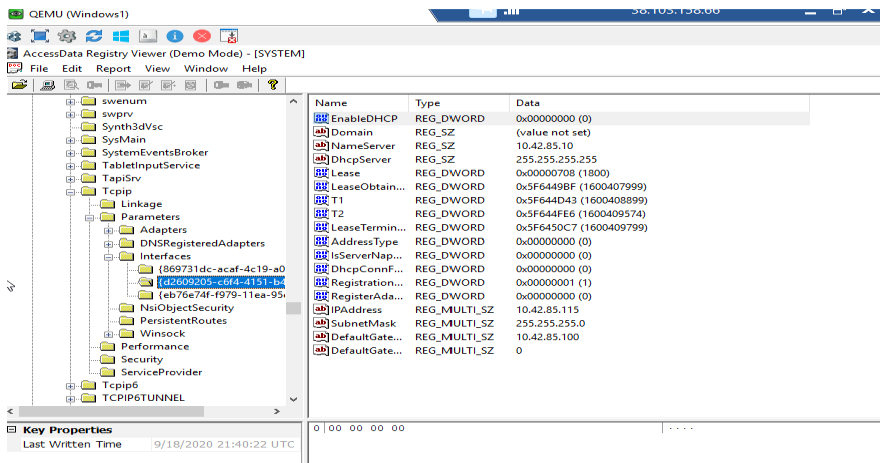
- To look for victim network layout let's investigate registry viewer path System>ControlSet001>Services>Tcpip>Parameters>Interfaces

Two hosts are in the same subnet 10.42.85.0/24.

### 1. DC: 10.42.85.10



## 2. Desktop: 10.42.85.115

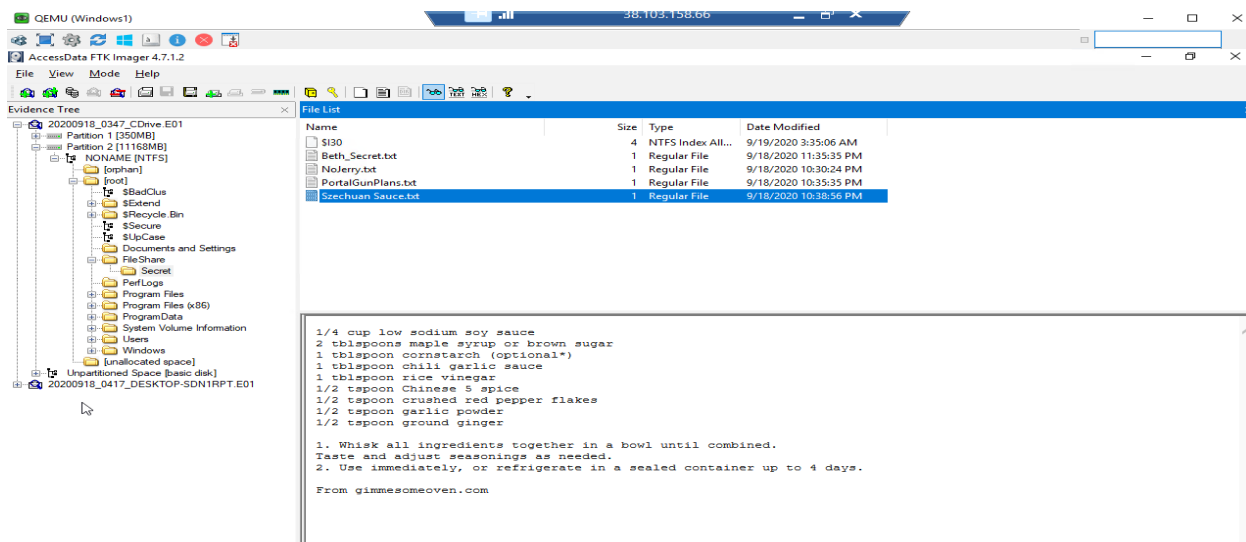


**Question 10:** What architecture changes should be made immediately?

**Answer:** The ability to RDP to the DC should be immediately removed for external connections given that the first access was achieved through an RDP brute force assault against the DC. Only users connected to the same local network should have access to the DC through RDP.

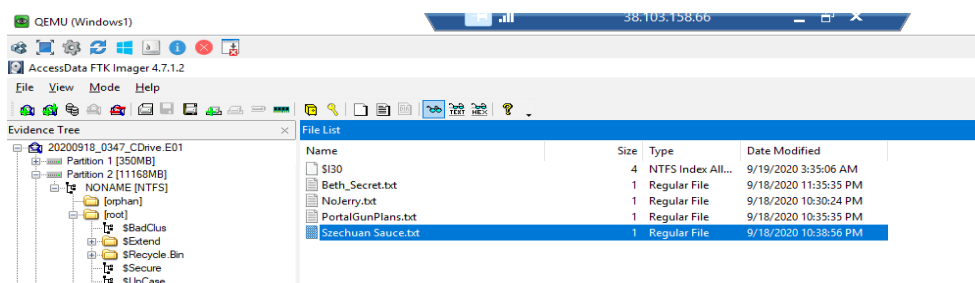
**Question 11:** Did the attacker steal the Szechuan sauce? If so, what time?

**Answer:** Certainly, the attacker indeed took the Szechuan sauce. This event occurred on September 18, 2020, at 10:38:56 PM



**Question 12:** Did the attacker steal or access any other sensitive files? If so, what times?

**Answer:** Yes, these were the files that the attacker tried to access and edit.



**References:**

The case of the Stolen Szechuan Sauce - <https://dfirmadness.com/the-stolen-szechuan-sauce/>  
OpenAI. (n.d.). ChatGPT . Retrieved from- <https://openai.com/chatgpt>  
DFIR madness - <https://dfirmadness.com/answers-to-szechuan-case-001/>  
Wireshark Version 4.2.2(v4.2.2-0-g404592842786), developed by Gerald Combs and contributors. <https://www.wireshark.org/>  
AccessData Registry Viewer 1.7.4.2 - <https://accessdata-registry-viewer.software.informer.com/download/>  
FTK Imager - <https://accessdata-ftk-imager.software.informer.com/download/>  
AccessData FTK Imager 4.7.1.2 - <https://accessdata-ftk-imager.software.informer.com/download/>  
Windows 10 Registry editor, Microsoft windows version 1809, 2018 Microsoft Corporation - <https://support.microsoft.com/en-us/windows/how-to-open-registry-editor-in-windows-10-deab38e6-91d6-e0aa-4b7c-8878d9e07b11>  
How to open Registry editor in windows 10 - <https://support.microsoft.com/en-us/windows/how-to-open-registry-editor-in-windows-10-deab38e6-91d6-e0aa-4b7c-8878d9e07b11>  
Stolen Szechuan Sauce Case study - [https://www.linkedin.com/search/results/all/?keywords=stolen%20szechuan%20sauce%20case%20study&origin=GLOBAL\\_SEARCH\\_HEADER&id=w.n](https://www.linkedin.com/search/results/all/?keywords=stolen%20szechuan%20sauce%20case%20study&origin=GLOBAL_SEARCH_HEADER&id=w.n)  
Case of Stolen Szechuan Sauce - <https://medium.com/@tanvilalwani5/case-of-the-stolen-szechuan-sauce-bd440e5c2a6d>  
Case Write Up : The Stolen Szechuan Sauce - <https://walshcat.medium.com/case-write-up-the-stolen-szechuan-sauce-2409344264c3>