

The Stolen Szechuan Sauce



Table of Contents

EXECUTIVE SUMMARY	1
CASE OVERVIEW	1
TOOLS USED	1
QUESTIONS	1-17
REFERENCES.....	18

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 career 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.

The screenshot shows the FTK Imager interface with the file list on the left and the content of the selected file, license.rtf, displayed in the main pane. The file list includes various system files and folders, such as en-US, es-ES, et-EE, fi-FI, fr-FR, gpfixup.exe, gpmmc.msc, gpme.dll, gpme.msc, gpmmgt.dll, GPOAdmin.dll, GPOAdminCommon.dll, GPOAdminCustom.dll, gppref.dll, gprefbr.dll, gprefcn.dll, gpregistrybrowser.dll, GPRSoP.dll, gptedit.msc, GroupPolicy, GroupPolicyUsers, he-IL, hr-HR, hu-HU, ias, icsxml, ime, inetsrv, InputMethod, lpmi, ismip.dll, ismserv.exe, it-IT, ja-JP, kdcplw.dll, kdcsvc.dll, KdsSvc.dll, ko-KR, ldifde.dll, ldifde.exe, ldp.exe, Licenses, neutral, Eval, and ServerStands. The file list also shows the size, type, and date modified for each file.

The content of the license.rtf file is displayed in the main pane, showing the Microsoft Windows Server 2012 R2 Standard Evaluation license terms. The text is formatted with bold headings and bullet points, and includes the following information:

- Product name: MICROSOFT WINDOWS SERVER 2012 R2 STANDARD
- License type: EVALUATION
- License terms: The software is licensed "as-is" and does not include any warranty or support services.
- Limitation on remedies and damages: The user may not recover from Microsoft and its suppliers for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tortious or contractual claims.

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

AccessData Registry Viewer (Demo Mode) - [SOFTWARE]

File Edit Report View Window Help

Transaction Server
uDRM
UPnP Device Host
Virtual Machine
VisualStudio
WAB
Wbem
WcmSvc
WIMMount
Windows
Windows Defender
Windows Mail
Windows NT
CurrentVersion
Windows Script Host
Windows Search
WindowsRuntime
Wisp
WSDAPI
ODBC
Policies
RegisteredApplications
VMware, Inc.

Name	Type	Data
SystemRoot	REG_SZ	C:\Windows
SoftwareType	REG_SZ	System
RegisteredO...	REG_SZ	Windows User
InstallDate	REG_DWORD	0x5F63924F (1600361039)
CurrentVersi...	REG_SZ	6.3
CurrentBuild	REG_SZ	9600
RegisteredO...	REG_SZ	(value not set)
CurrentType	REG_SZ	Multiprocessor Free
InstallationT...	REG_SZ	Server
EditionID	REG_SZ	ServerStandardEval
ProductName	REG_SZ	Windows Server 2012 R2 Standard Evaluation
ProductId	REG_SZ	00252-10000-00000-AA228
DigitalProdu...	REG_BINARY	A4 00 00 00 03 00 00 00 30 30 32 35 32 2D 31 30 30 30 ...
DigitalProdu...	REG_BINARY	F8 04 00 00 04 00 00 00 30 00 30 00 30 00 30 00 2...
CurrentBuild...	REG_SZ	9600
BuildLab	REG_SZ	9600.winblue_gdr.140221-1952
BuildLabEx	REG_SZ	9600.17031.amd64fre.winblue_gdr.140221-1952
BuildGUID	REG_SZ	ffffffff-ffff-ffff-ffff-ffffffffffff
PathName	REG_SZ	C:\Windows

Key Properties

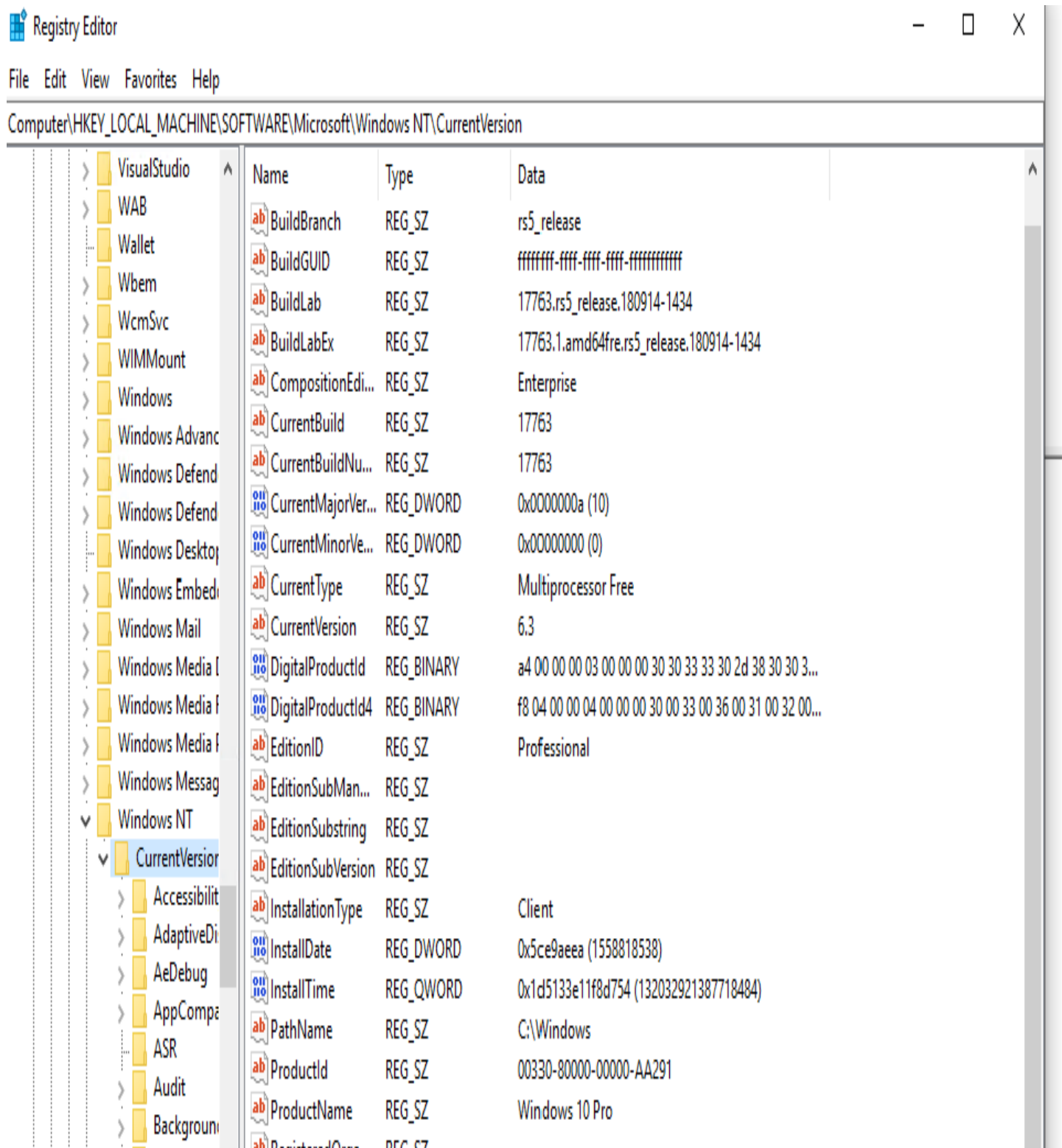
Last Written Time	9/17/2020 18:05:43 UTC
OS Install Date (UTC)	Thu Sep 17 16:43:59 202
OS Install Date (Local)	Thu Sep 17 16:43:59 202

SOFTWARE\Microsoft\Windows NT\CurrentVersion Offset: 0

00 43 00 3A 00 5C 00 57 00-69 00 6E 00 64 00 6F 00 C:\Windows
10 77 00 73 00 00 00 W.S...

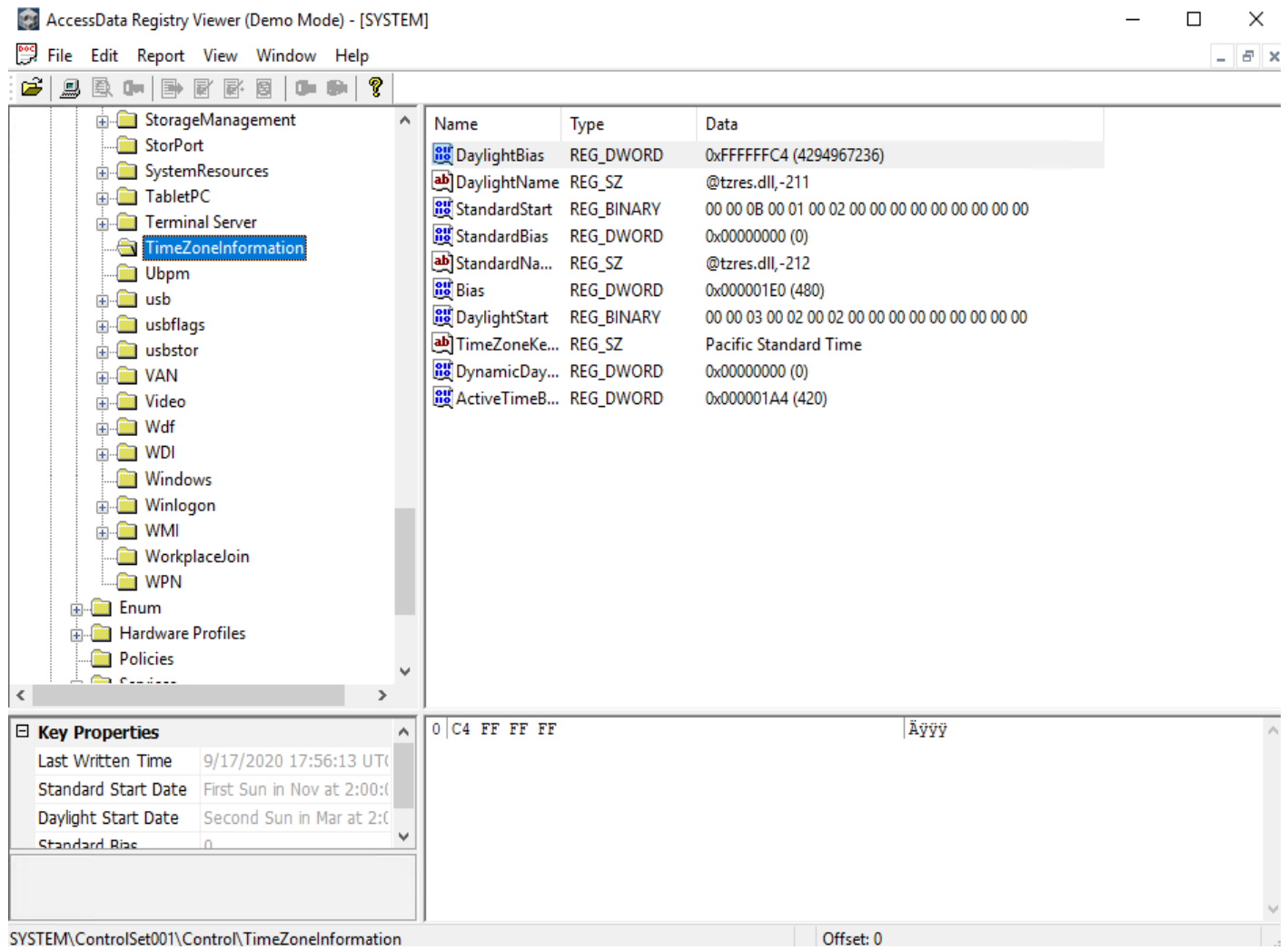
Question 2: What's the Operating System of the Desktop?

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)



AccessData Registry Viewer (Demo Mode) - [SYSTEM]

File Edit Report View Window Help

StorageManagement
 StorPort
 SystemResources
 TabletPC
 Terminal Server
TimeZoneInformation
 Ubpm
 usb
 usbflags
 usbstor
 VAN
 Video
 Wdf
 WDI
 Windows
 Winlogon
 WMI
 WorkplaceJoin
 WPN
 Enum
 Hardware Profiles
 Policies
 Services

Name	Type	Data
DaylightBias	REG_DWORD	0xFFFFFFFF (4294967236)
DaylightName	REG_SZ	@tzres.dll,-211
StandardStart	REG_BINARY	00 00 0B 00 01 00 02 00 00 00 00 00 00 00 00
StandardBias	REG_DWORD	0x00000000 (0)
StandardName	REG_SZ	@tzres.dll,-212
Bias	REG_DWORD	0x000001E0 (480)
DaylightStart	REG_BINARY	00 00 03 00 02 00 02 00 00 00 00 00 00 00 00
TimeZoneKeyName	REG_SZ	Pacific Standard Time
DynamicDaylightTime	REG_DWORD	0x00000000 (0)
ActiveTimeBias	REG_DWORD	0x000001A4 (420)

Key Properties

Last Written Time	9/17/2020 17:56:13 UTC
Standard Start Date	First Sun in Nov at 2:00:00
Daylight Start Date	Second Sun in Mar at 2:00:00
Standard Bias	0

SYSTEM\ControlSet001\Control\TimeZoneInformation Offset: 0

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.

The screenshot displays the Wireshark network protocol analyzer interface. The top status bar shows the capture is running on interface 'eth0' with a packet rate of 38.103.158.66. The filter bar at the top contains the filter `ip.addr == 194.61.24.102 and tcp`. The packet list pane shows a series of TCP packets, with packet 84320 selected. The packet details pane for packet 84320 shows the following structure:

- Ethernet II, Src: VMware_95:cd:21 (00:0c:29:95:cd:21), Dst: VMware_e1:84:e6 (00:0c:29:e1:84:e6)
 - Destination: VMware_e1:84:e6 (00:0c:29:e1:84:e6)
 - Source: VMware_95:cd:21 (00:0c:29:95:cd:21)
 - Type: IPv4 (0x0800)
- Internet Protocol Version 4, Src: 194.61.24.102, Dst: 10.42.85.10
 - 0100 = Version: 4
 - 0101 = Header Length: 20 bytes (5)
 - > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
 - Total Length: 44
 - Identification: 0x1432 (5170)
 - > 0000 = Flags: 0x0
 - ...0 0000 0000 0000 = Fragment Offset: 0
 - Time to Live: 42
 - Protocol: TCP (6)
 - Header Checksum: 0x42c3 [validation disabled]
 - [Header checksum status: Unverified]
 - Source Address: 194.61.24.102
 - Destination Address: 10.42.85.10
- Transmission Control Protocol, Src Port: 64385, Dst Port: 443, Seq: 0, Len: 0
 - Source Port: 64385
 - Destination Port: 443
 - [Stream index: 1133]

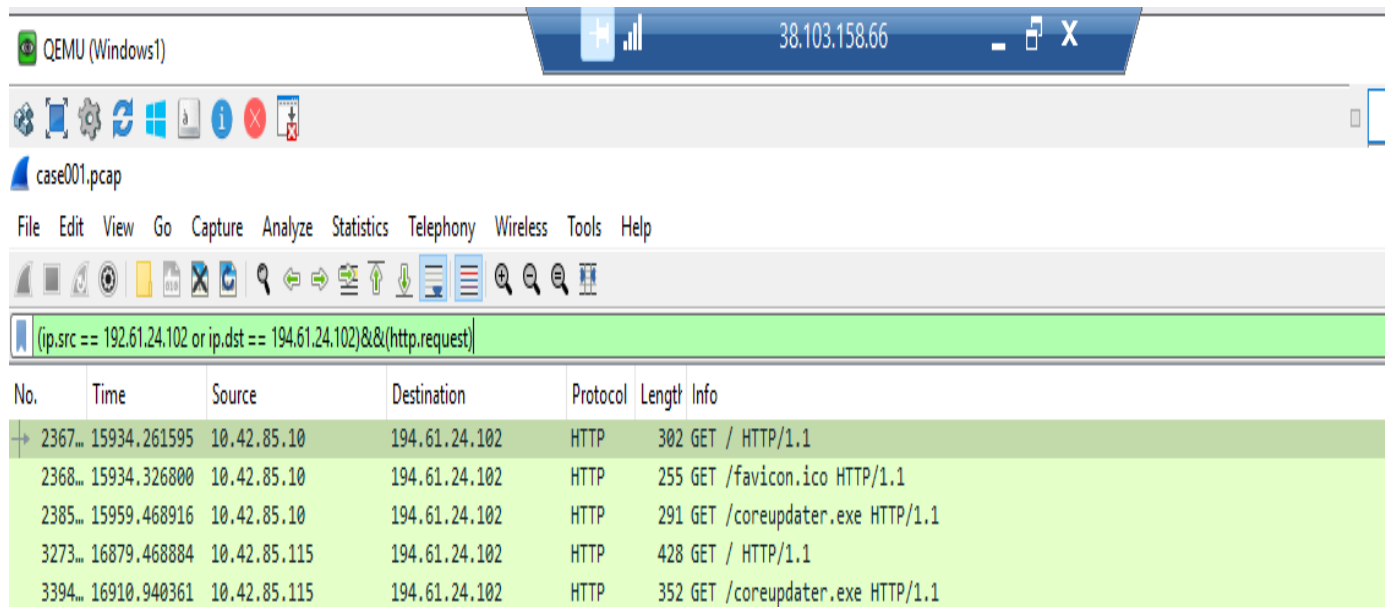
The packet bytes pane on the right shows the raw data of the selected packet, starting with the Ethernet II header.

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

```
Microsoft Windows [Version 10.0.17763.107]
(c) 2018 Microsoft Corporation. All rights reserved.

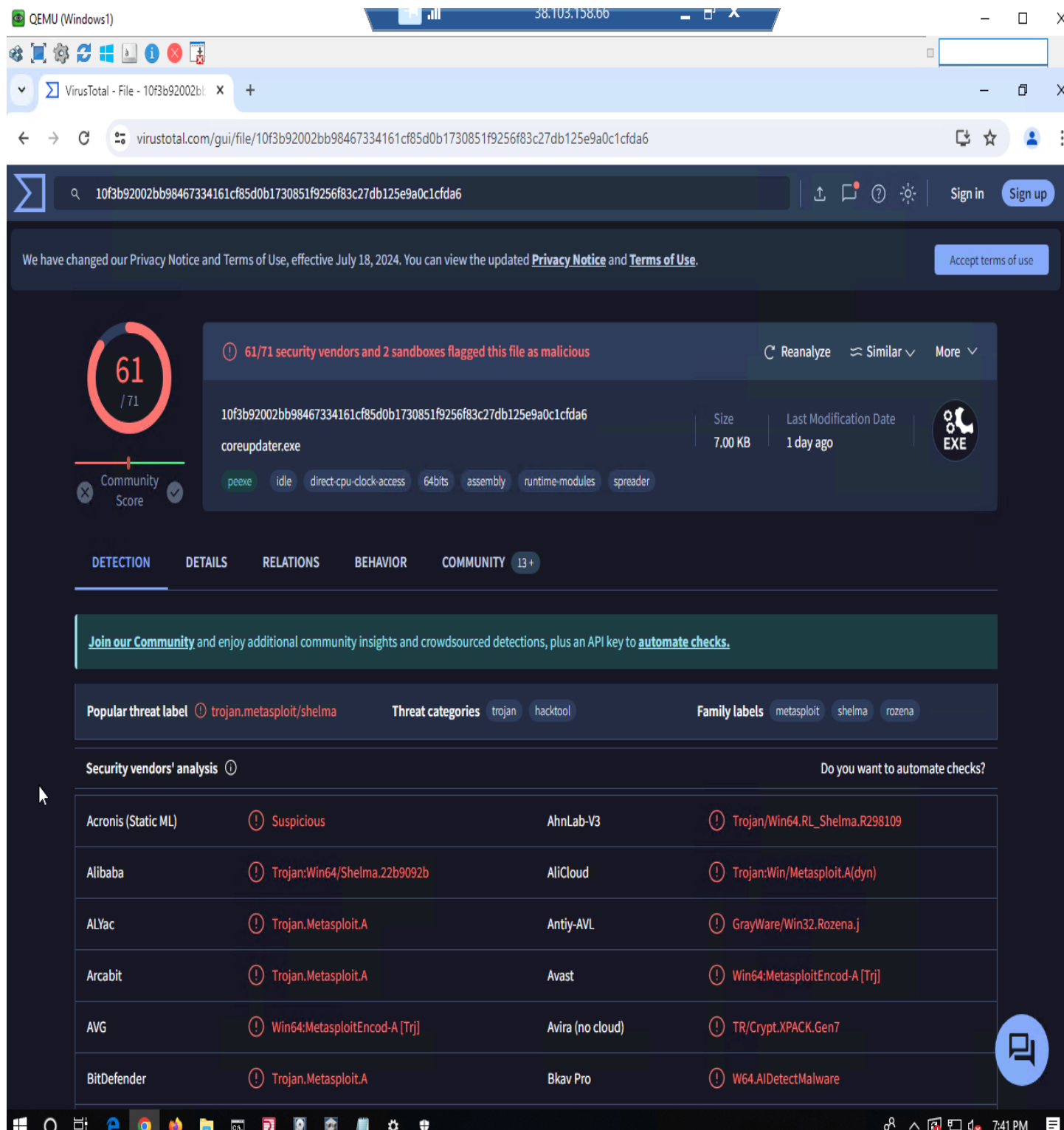
C:\Users\user>cd Desktop

C:\Users\user\Desktop>certutil -hashfile coreupdater.exe SHA256
SHA256 hash of coreupdater.exe:
0f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6
certUtil: -hashfile command completed successfully.

C:\Users\user\Desktop>
```

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 a Windows 10 desktop with a QEMU window and a web browser displaying the VirusTotal analysis page for the file **coreupdater.exe**. The browser address bar shows the URL: `virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6`.

VirusTotal Analysis Summary:

- Score:** 61 / 71 (Community Score)
- Status:** 61/71 security vendors and 2 sandboxes flagged this file as malicious
- File Name:** coreupdater.exe
- Size:** 7.00 KB
- Last Modification Date:** 1 day ago
- File Type:** EXE
- Tags:** peexe, idle, direct-cpu-clock-access, 64bits, assembly, runtime-modules, spreader

Threat Information:

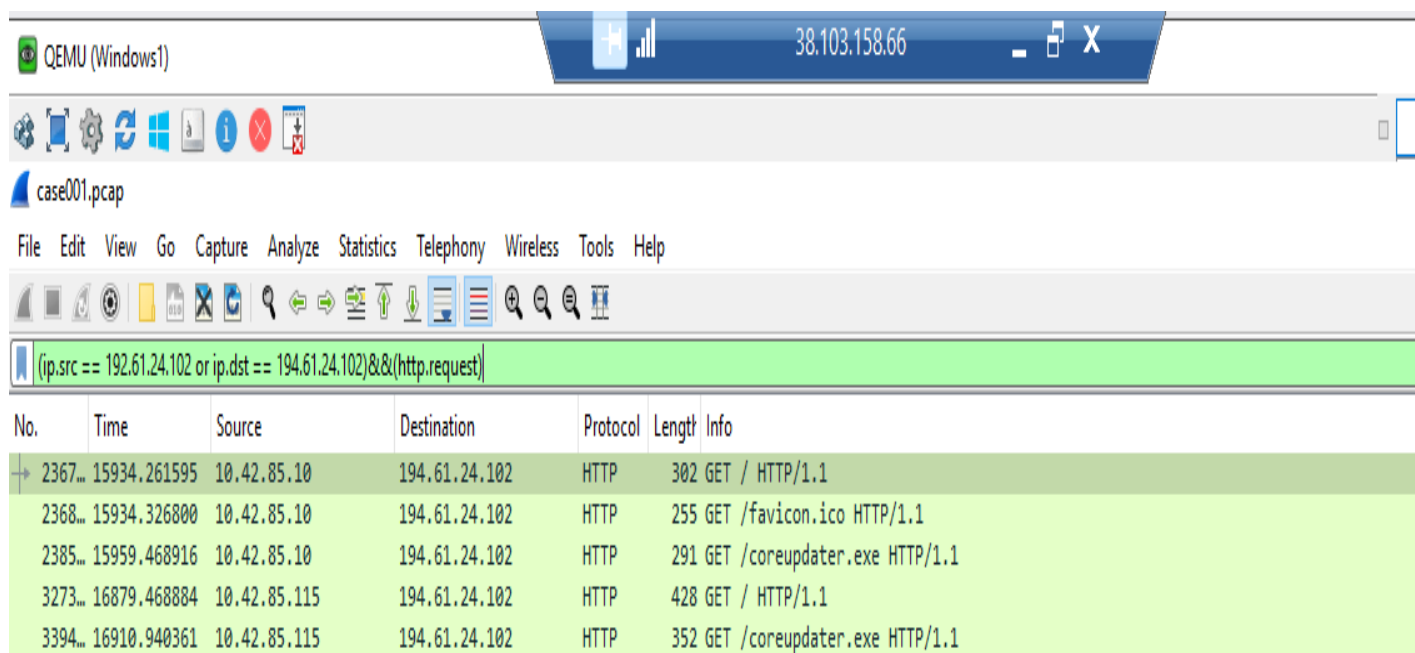
- Popular threat label:** trojan.metasploit/shelma
- Threat categories:** trojan, hacktool
- Family labels:** metasploit, shelma, rozena

Security vendors' analysis:

Vendor	Detection	Vendor	Detection
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.

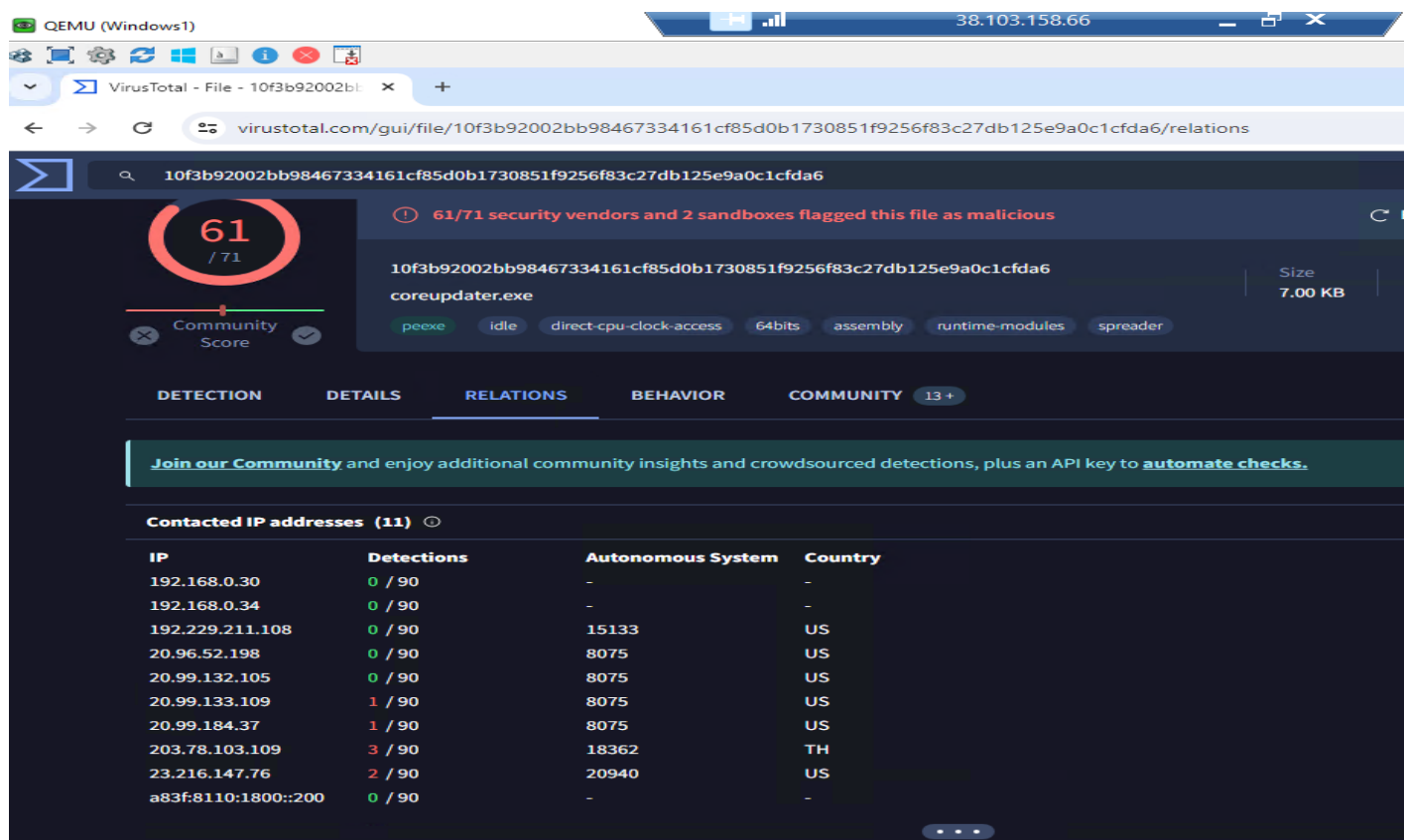


The screenshot shows a Wireshark packet capture window titled "case001.pcap". The filter bar contains the expression `(ip.src == 192.61.24.102 or ip.dst == 194.61.24.102)&&(http.request)`. The packet list shows five HTTP GET requests to 194.61.24.102. The first packet (No. 2367) is a GET request for `/`. The second packet (No. 2368) is a GET request for `/favicon.ico`. The third packet (No. 2385) is a GET request for `/coreupdater.exe`. The fourth packet (No. 3273) is a GET request for `/`. The fifth packet (No. 3394) is a GET request for `/coreupdater.exe`.

No.	Time	Source	Destination	Protocol	Length	Info
2367...	15934.261595	10.42.85.10	194.61.24.102	HTTP	302	GET / HTTP/1.1
2368...	15934.326800	10.42.85.10	194.61.24.102	HTTP	255	GET /favicon.ico HTTP/1.1
2385...	15959.468916	10.42.85.10	194.61.24.102	HTTP	291	GET /coreupdater.exe HTTP/1.1
3273...	16879.468884	10.42.85.115	194.61.24.102	HTTP	428	GET / HTTP/1.1
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.



The screenshot shows the VirusTotal interface for the file `10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6`. The file is identified as `coreupdater.exe` (Size: 7.00 KB). The Relations tab is selected, showing a list of contacted IP addresses (11 total). The list includes the IP address 203.78.103.109, which is highlighted in red.

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
a83f:8110:1800::200	0 / 90	-	-

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

QEMU (Windows1) 38.103.158.66

case001.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

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

QEMU (Windows1) 38.103.158.66

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

Name	Size	Type	Date Modified
connectedsearch-paths.searchconnector...	1	Regular File	6/18/2013 2:59:26 PM
connectedsearch-protocol.searchconnec...	1	Regular File	6/18/2013 2:59:26 PM
connectedsearch-results.searchconnec...	11	Regular File	3/21/2014 6:49:19 PM
connectedsearch-suggestions.searchcon...	8	Regular File	3/21/2014 6:49:19 PM
connectedsearch-zeroinput.searchconne...	7	Regular File	3/21/2014 6:49:19 PM
consent.exe	112	Regular File	8/22/2013 12:44:43 PM
console.dll	79	Regular File	8/22/2013 11:17:25 AM
control.exe	113	Regular File	8/22/2013 11:03:56 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
cryptbase.dll	30	Regular File	8/22/2013 1:25:35 PM

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 11:03:56 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.

QEMU (Windows1)



38.103.158.66



Wireshark · Follow TCP Stream (tcp.stream eq 30468) · case001.pcap

```

....j..0.....
..0.0..... ..0.....0.....@.....0.....0..
Administrator...
C137.LOCAL..0.....0...krbtgt.
C137.LOCAL....20370913024805Z....20370913024805Z....
$.0.....y.....0.0.....DESKTOP-SDN1RPT ....~..0.....20200919033624Z.....L....
C137.LOCAL..0.....0...krbtgt.
C137.LOCAL.9.7050..... 0.0.....0 .....0 .....0 .....

```

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

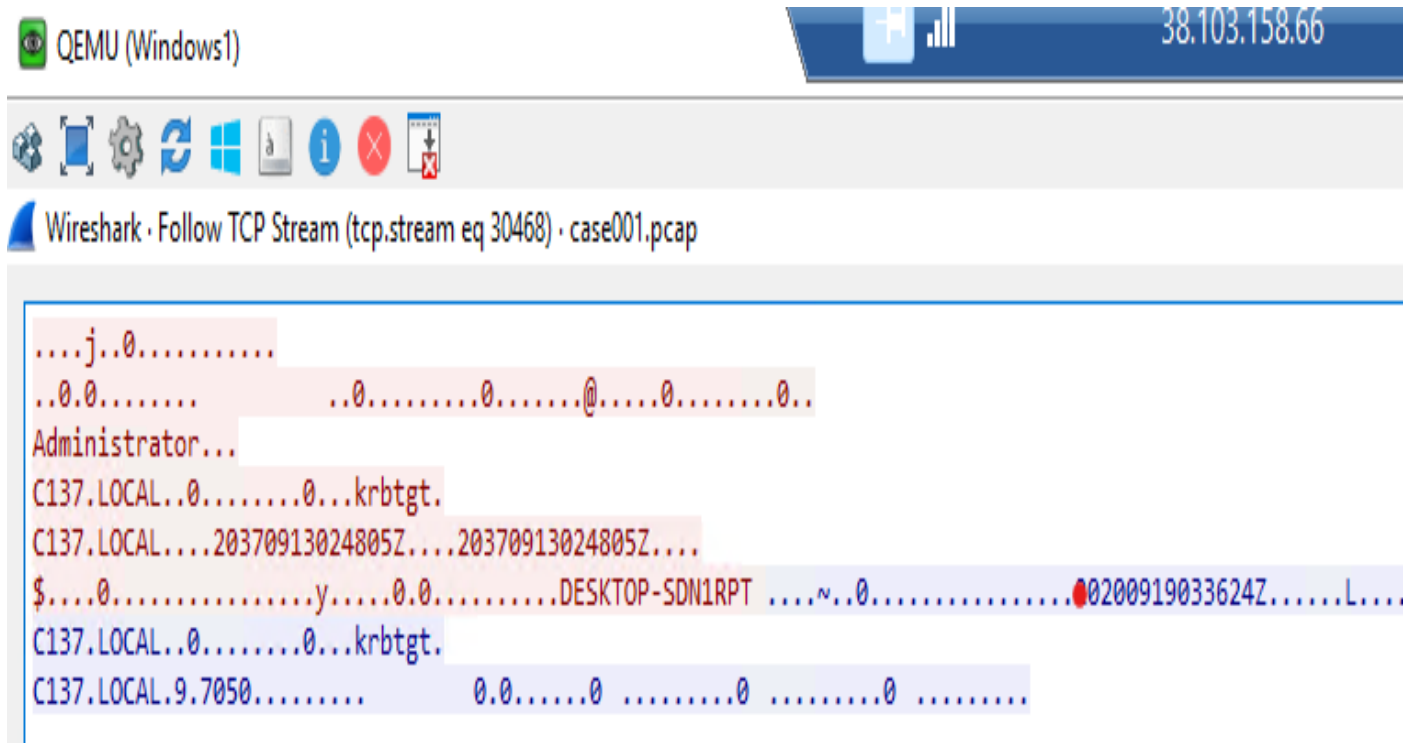
Answer: The following were the capabilities of this malware:

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.

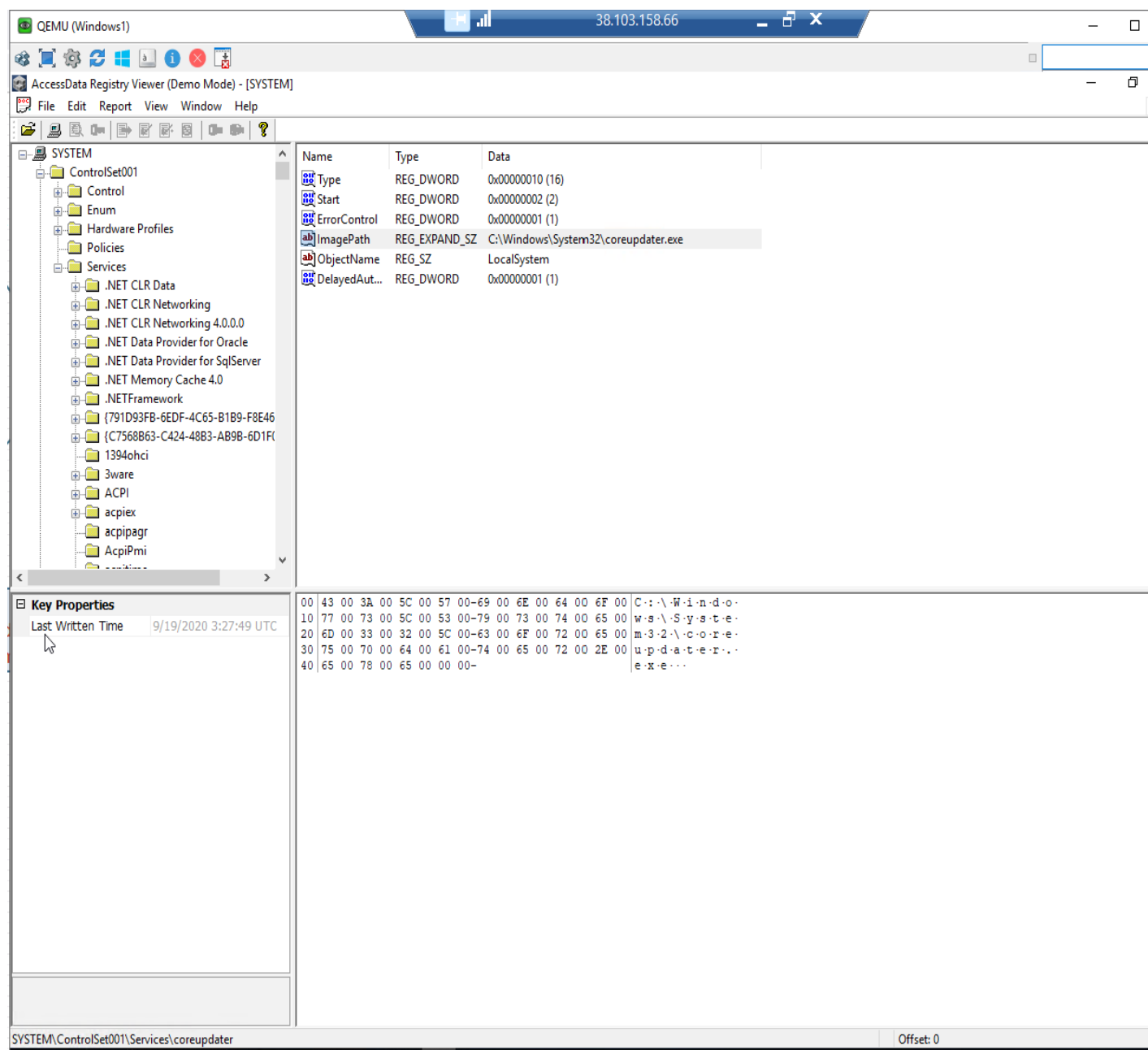


Also, Metasploit is a red teaming tool which is open source, so safe to say accessible.

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.

The screenshot displays a QEMU (Windows1) window with a Wireshark packet capture. The top bar shows the IP address 38.103.158.66. The Wireshark interface shows a packet capture of a TCP stream (eq 30468) from case001.pcap. The packet list on the left shows several packets from 2660 to 266027. The packet details pane on the right shows the raw data of the selected packet (266027), which is a TCP reset (RST) from 10.42.0.1 to 10.42.0.1. The raw data includes the text 'Administrator...' and 'C137.LOCAL...krbtgt...'.

No.	Time	Source
2660...	16697.431833	10.42
2660...	16697.431839	10.42
2660...	16697.431987	10.42
2660...	16697.431988	10.42
2660...	16697.442143	10.42
2660...	16697.442247	10.42
2660...	16697.442414	10.42
2660...	16697.442482	10.42

Frame 266027: 60 bytes on
 Ethernet II, Src: VMware_e
 Internet Protocol Version
 Transmission Control Proto

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.

QEMU (Windows1) 38.103.158.00

case001.pcap

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Apply a display filter ... <Ctrl-/>

No.	Time	Source	Destination	Protocol	Length	Info
266798	2020/263 02:36:25.638015	20.189.118.208	10.42.85.115	TCP	54	80 → 50693 [ACK] Seq=4197 Ack=4494 Win=64240 Len=0
266797	2020/263 02:36:25.638002	10.42.85.115	10.42.85.10	LDAP	404	searchRequest(37) "<ROOT>" baseObject
266796	2020/263 02:36:25.637870	10.42.85.115	10.42.85.10	TCP	60	50706 → 389 [ACK] Seq=1 Ack=1 Win=262656 Len=0
266795	2020/263 02:36:25.637849	10.42.85.115	20.189.118.208	HTTP/X...	1474	POST /metadata.svc HTTP/1.1
266794	2020/263 02:36:25.637848	10.42.85.10	10.42.85.115	TCP	66	389 → 50706 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM
266793	2020/263 02:36:25.637803	10.42.85.115	20.189.118.208	TCP	393	50693 → 80 [PSH, ACK] Seq=4155 Ack=4197 Win=64240 Len=339 [TCP segment of a reass...

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.

QEMU (Windows1) 38.103.158.66

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- 20200918_0347_CDrive.E01
 - Partition 1 [350MB]
 - Partition 2 [11168MB]
 - NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - \$UpCase
 - Documents and Settings
 - FileShare
 - Secret
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - System Volume Information
 - Users
 - Windows
 - [unallocated space]

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	9/19/2020 3:35:06 AM
Beth_Secret.txt	1	Regular File	9/18/2020 11:35:35 PM
NoJerry.txt	1	Regular File	9/18/2020 10:30:24 PM
PortalGunPlans.txt	1	Regular File	9/18/2020 10:35:35 PM
Szechuan Sauce.txt	1	Regular File	9/18/2020 10:38:56 PM

20200918_0417_DESKTOP-SDN1RPT.E01

```

1/4 cup low sodium soy sauce
2 tablespoons maple syrup or brown sugar
1 tablespoon cornstarch (optional*)
1 tablespoon chili garlic sauce
1 tablespoon rice vinegar
1/2 tspoon Chinese 5 spice
1/2 tspoon crushed red pepper flakes
1/2 tspoon garlic powder
1/2 tspoon ground ginger

1. Whisk all ingredients together in a bowl until combined.
Taste and adjust seasonings as needed.
2. Use immediately, or refrigerate in a sealed container up to 4 days.

From gimmesomeoven.com
  
```

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.

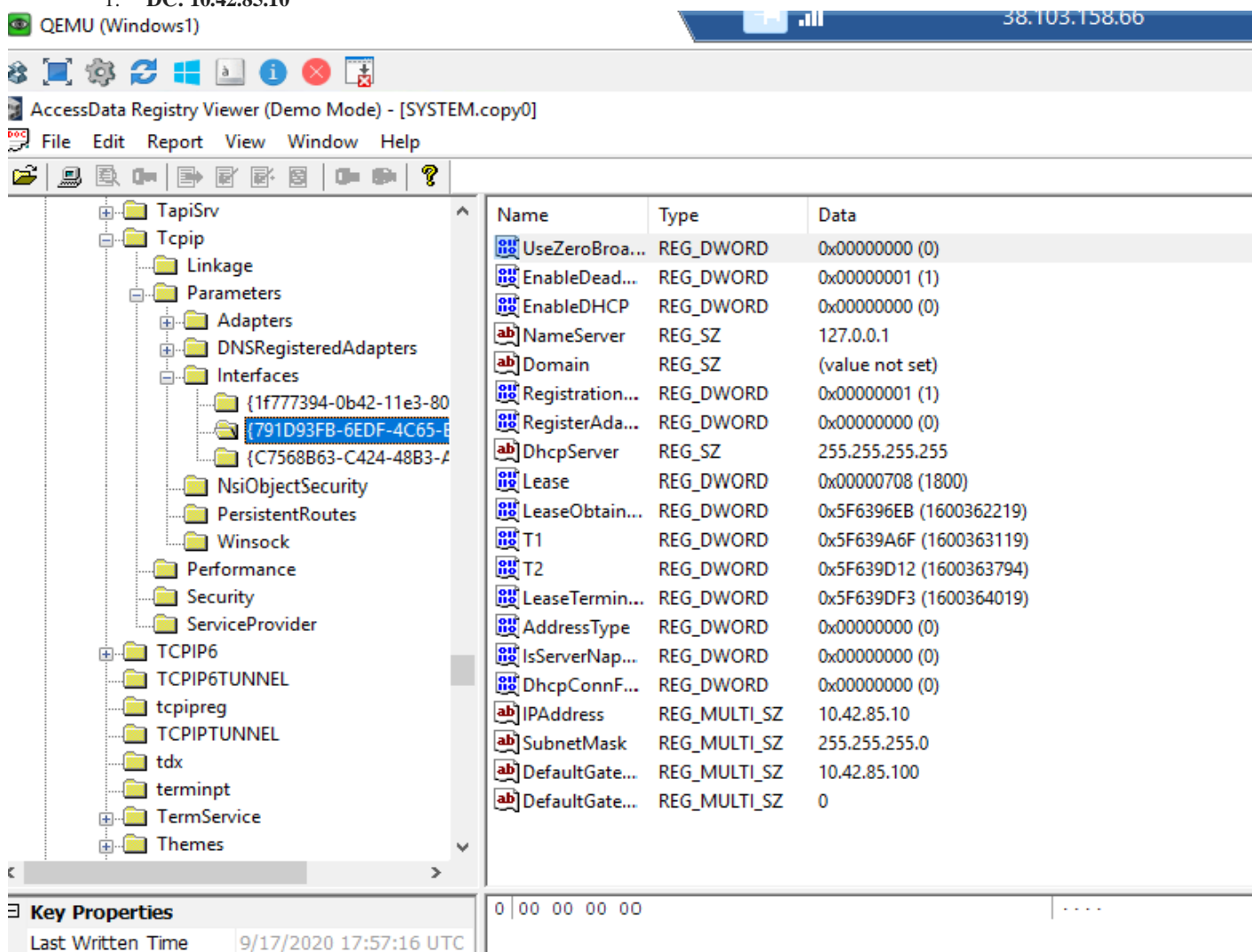
- Navigate to the following path: System > ControlSet001 > Services > Tcpip > Parameters > Interfaces. In this context, it's observed that two hosts share an identical subnet, specifically 10.42.85.0/24.

- 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



Name	Type	Data
UseZeroBroa...	REG_DWORD	0x00000000 (0)
EnableDead...	REG_DWORD	0x00000001 (1)
EnableDHCP	REG_DWORD	0x00000000 (0)
NameServer	REG_SZ	127.0.0.1
Domain	REG_SZ	(value not set)
Registration...	REG_DWORD	0x00000001 (1)
RegisterAda...	REG_DWORD	0x00000000 (0)
DhcpServer	REG_SZ	255.255.255.255
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtain...	REG_DWORD	0x5F6396EB (1600362219)
T1	REG_DWORD	0x5F639A6F (1600363119)
T2	REG_DWORD	0x5F639D12 (1600363794)
LeaseTermin...	REG_DWORD	0x5F639DF3 (1600364019)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNap...	REG_DWORD	0x00000000 (0)
DhcpConnF...	REG_DWORD	0x00000000 (0)
IPAddress	REG_MULTI_SZ	10.42.85.10
SubnetMask	REG_MULTI_SZ	255.255.255.0
DefaultGate...	REG_MULTI_SZ	10.42.85.100
DefaultGate...	REG_MULTI_SZ	0

Key Properties

Last Written Time: 9/17/2020 17:57:16 UTC

2. Desktop: 10.42.85.115

QEMU (Windows1) 38.103.158.66

AccessData Registry Viewer (Demo Mode) - [SYSTEM]

File Edit Report View Window Help

Name	Type	Data
EnableDHCP	REG_DWORD	0x00000000 (0)
Domain	REG_SZ	(value not set)
NameServer	REG_SZ	10.42.85.10
DhcpServer	REG_SZ	255.255.255.255
Lease	REG_DWORD	0x00000708 (1800)
LeaseObtain...	REG_DWORD	0x5F6449BF (1600407999)
T1	REG_DWORD	0x5F644D43 (1600408899)
T2	REG_DWORD	0x5F644FE6 (1600409574)
LeaseTermin...	REG_DWORD	0x5F6450C7 (1600409799)
AddressType	REG_DWORD	0x00000000 (0)
IsServerNap...	REG_DWORD	0x00000000 (0)
DhcpConnF...	REG_DWORD	0x00000000 (0)
Registration...	REG_DWORD	0x00000001 (1)
RegisterAda...	REG_DWORD	0x00000000 (0)
IPAddress	REG_MULTI_SZ	10.42.85.115
SubnetMask	REG_MULTI_SZ	255.255.255.0
DefaultGate...	REG_MULTI_SZ	10.42.85.100
DefaultGate...	REG_MULTI_SZ	0

Key Properties

Last Written Time 9/18/2020 21:40:22 UTC

0 00 00 00 00

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

QEMU (Windows1) 38.103.158.66

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- 20200918_0347_CDrive.E01
 - Partition 1 [350MB]
 - Partition 2 [11168MB]
 - NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - \$UpCase
 - Documents and Settings
 - FileShare
 - Secret
 - PerfLogs
 - Program Files
 - Program Files (x86)
 - ProgramData
 - System Volume Information
 - Users
 - Windows
 - [unallocated space]

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	9/19/2020 3:35:06 AM
Beth_Secret.txt	1	Regular File	9/18/2020 11:35:35 PM
NoJerry.txt	1	Regular File	9/18/2020 10:30:24 PM
PortalGunPlans.txt	1	Regular File	9/18/2020 10:35:35 PM
Szechuan Sauce.txt	1	Regular File	9/18/2020 10:38:56 PM

1/4 cup low sodium soy sauce
 2 tablespoons maple syrup or brown sugar
 1 tablespoon cornstarch (optional*)
 1 tablespoon chili garlic sauce
 1 tablespoon rice vinegar
 1/2 teaspoon Chinese 5 spice
 1/2 teaspoon crushed red pepper flakes
 1/2 teaspoon garlic powder
 1/2 teaspoon ground ginger

1. Whisk all ingredients together in a bowl until combined.
 Taste and adjust seasonings as needed.
 2. Use immediately, or refrigerate in a sealed container up to 4 days.

From gimmesomeoven.com

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.

QEMU (Windows1) 38.103.158.66

AccessData FTK Imager 4.7.1.2

File View Mode Help

Evidence Tree

- 20200918_0347_CDrive.E01
 - Partition 1 [350MB]
 - Partition 2 [11168MB]
 - NONAME [NTFS]
 - [orphan]
 - [root]
 - \$BadClus
 - \$Extend
 - \$Recycle.Bin
 - \$Secure
 - \$InCase

File List

Name	Size	Type	Date Modified
\$I30	4	NTFS Index All...	9/19/2020 3:35:06 AM
Beth_Secret.txt	1	Regular File	9/18/2020 11:35:35 PM
NoJerry.txt	1	Regular File	9/18/2020 10:30:24 PM
PortalGunPlans.txt	1	Regular File	9/18/2020 10:35:35 PM
Szechuan Sauce.txt	1	Regular File	9/18/2020 10:38:56 PM

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
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>