



The Stolen Szechuan Sauce Forensic Case Study

Daniel (Zhiyi) Deng

Table of Contents

- Executive Summary
- Forensic Methodology
- Investigation Result:
 - What's the Operating System of the Server?
 - What's the Operating System of the Desktop?
 - What was the local time of the Server?
 - Was there a breach?
 - What was the initial entry vector (how did they get in)?
 - Was malware used? If so, what was it?
 - What process was malicious?
 - Identify the IP Address that delivered the payload.
 - What IP Address is the malware calling to?
 - Where is this malware on disk?
 - When did it first appear?
 - Did someone move it?
 - What were the capabilities of this malware?
 - Is this malware easily obtained?
 - Was this malware installed with persistence on any machine?
 - When?

- Where?
 - What malicious IP Addresses were involved?
 - Were any IP Addresses from known adversary infrastructure?
 - Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?
 - Did the attacker access any other systems?
 - How?
 - When?
 - Did the attacker steal or access any data?
 - When?
 - What was the network layout of the victim network?
- Additional investigation
- Advanced and Bonus Questions
- Summary
- Reference

Executive Summary:

Asian Fusion Wok, a growing restaurant business, experienced a cyberattack in September 2020 and engaged our services as a Managed Security Service Provider (MSSP) to investigate. With the assistance of AFW's executive team, we successfully carried out the forensic process, reconstructed the entire attack process.

The purpose of this forensic investigation was to determine the attack vector, evaluate the extent of the breach, and confirm whether any sensitive data was compromised within AFW's IT environment. This report details the connection between the attack and our investigative findings and provides recommendations for enhancing security measures to prevent similar incidents in the future.

Key Findings

- **Unauthorized Access Detected:**

Analysis of security logs and network traffic confirmed that both the server and desktop systems were compromised following a series of unsuccessful login attempts from a suspicious IP address.

- **Malware Infiltration:**

A malicious program was discovered on the system, granting the attacker long-term access to the network and facilitating the transfer of data to an external server.

- **Data Exfiltration Confirmed:**

Encrypted network traffic revealed data was being sent to a known Command and Control (C2) server, indicating that sensitive information, including the Szechuan sauce recipe, was accessed and extracted.

Our investigation determined that the attacker gained access to and exfiltrated sensitive files, including the **Szechuan sauce recipe**. The breach occurred via a brute-force attack on the Remote Desktop Protocol (RDP), allowing unauthorized entry into the system.

To mitigate the risk of similar incidents in the future, we recommend

- **Secure RDP Access:** Use a VPN with MFA for RDP, and regularly audit access permissions.
- **Network Isolation:** Isolate the DC in a separate network segment and prevent Internet exposure.
- **Disable External RDP:** Turn off RDP from the Internet; use secure methods like VPNs or jump servers for remote access.
- **Network Monitoring:** Continuously monitor network traffic and use IDS to detect and respond to suspicious activity.

Forensic Methodology

For the **Collection** phase, the original artifact (such as a disk image or memory dump) is provided by the certified entity, DFIR Madness, which owns the compromised system. This ensures that the evidence is handled and transferred properly, maintaining the integrity and chain of custody throughout the forensic investigation. Before conducting the analysis, we checked the hash to make sure the integrity of the artifact.

```

To get the EDI's you may need to use Firefox in a Private Window, hit the back button, select the file, and hit Download.
However, if you are worried about storage and bandwidth ditch the protected files and the pagefile for now.

DC01 Disk Image (E01)
DC01 Memory and PageFile
DC01 Autonus
DC01 Protected Files
Case001 PCAP
Desktop Disk Image (E01)
Desktop Memory and PageFile
Desktop Autonus
Desktop Protected Files
To verify file Integrity in Windows Powershell, from the Download Dir: Get-FileHash -Algorithm md5
To verify file Integrity in Linux, from the Download Dir: md5sum
MD5 4220466753C8A4DF49D2C4CEB92DB816 case001-pcap.zip
MD5 964B2D710687D10C77C94947D0A79E66 DC01-autonus.zip
MD5 E57FC434F833CE1A858DFACT87389DF DC01-E01.zip
MD5 A4A4E2CB4713804AASC287B064B2D7B1 DC01-memory.zip
MD5 964EA0F009708CC101DEA83AE4ED923 DC01-pagefile.zip
MD5 AD29830A583EEF49C8C1C59AFFD264F DC01-ProtectedFiles.zip
MD5 F13C5C509733147472ABC0B11B6EF1F07 DESKTOP-E01.zip
MD5 3697DCAFA5411365469A4EFA0C3D8A1C DESKTOP-SON1RPT-autonus.zip
MD5 CF31E2635C77811AA1B80A92A721E2 DESKTOP-SDN1RPT-memory.zip

```

Name	Date modified	Type
case001-pcap.zip	8/22/2024 1:18 PM	Compressed (z)
DC01-autonus.zip	8/22/2024 1:18 PM	Compressed (z)
DC01-E01.zip	8/22/2024 1:25 PM	Compressed (z)
DC01-memory.zip	8/22/2024 1:18 PM	Compressed (z)
DC01-pagefile.zip	8/22/2024 1:18 PM	Compressed (z)
DC01-ProtectedFiles.zip	8/22/2024 1:18 PM	Compressed (z)
DESKTOP-E01.zip	8/22/2024 1:25 PM	Compressed (z)
DESKTOP-SON1RPT-autonus.zip	8/22/2024 8:32 PM	Compressed (z)
DESKTOP-SON1RPT-memory.zip	3/20/2024 3:31 PM	Compressed (z)
DESKTOP-SDN1RPT-protected files.zip	8/22/2024 1:32 PM	Compressed (z)

```

Algorithm Hash
MD5 64AHE2CBH71300B4A5C287B066B2D7B91
PS C:\Users\leizy\OneDrive\桌面\CyberSecurity\Project assignment\Forensics> Get-FileHash -Algorithm MD5
Algorithm Hash
SHA256 285547282AF60448FE00CC7A62C3B467B6AA5A13BBAGA4F2600A9C5B58C854F
PS C:\Users\leizy\OneDrive\桌面\CyberSecurity\Project assignment\Forensics> Get-FileHash -Algorithm SHA256
Algorithm Hash
SHA256 B1D81979B290CF5C954C1965C5E783D259B88E3E88327D7F6D68B20E4C7CD5B9
PS C:\Users\leizy\OneDrive\桌面\CyberSecurity\Project assignment\Forensics>

```

The tools for carrying out the forensics:

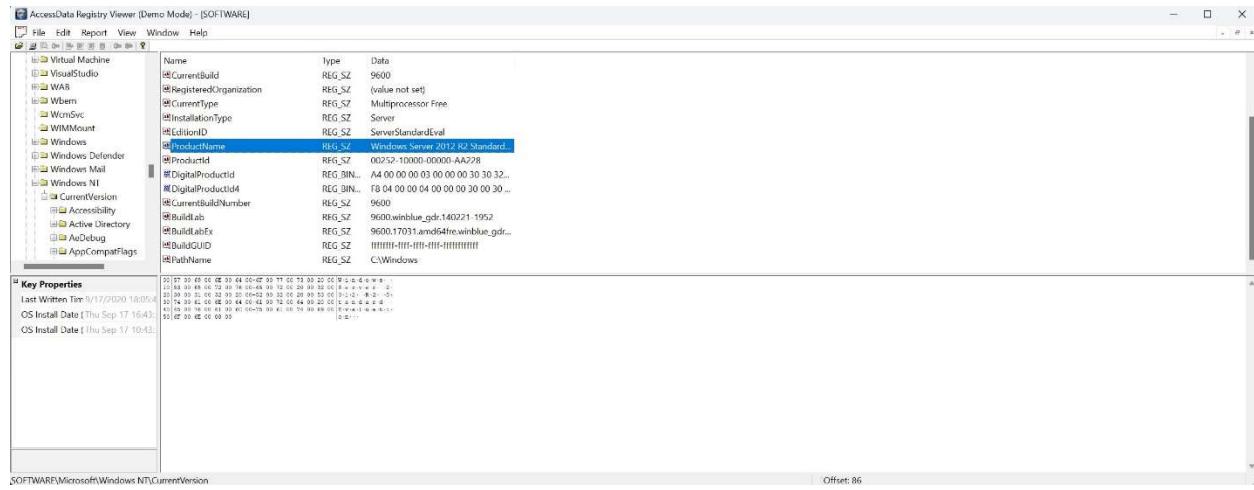
- PowerShell
- FTK imager
- Eric Zimmerman Registry Explorer (FTK registry viewer can be alternative)
- Wireshark
- Event Viewer (Event Log Explorer can be alternative)
- VirusTotal
- AlienVault

For the **Analysis** process, we mount forensic images using FTK imager to examine system images, establish dates, times, and operating systems, and document findings. Review system images for obvious malware and inspect user downloads for any intentional or accidental malware downloads. We used Wireshark to analyze the incident PCAP file and identify potential Indicators of Compromise (IOCs). OSINT tools such as VirusTotal and AlienVault were utilized to gather additional details. Registry Explorer was employed to delve into the evidence and confirm our suspicions. Finally, we drafted this report to document our detailed findings and provide recommendations.

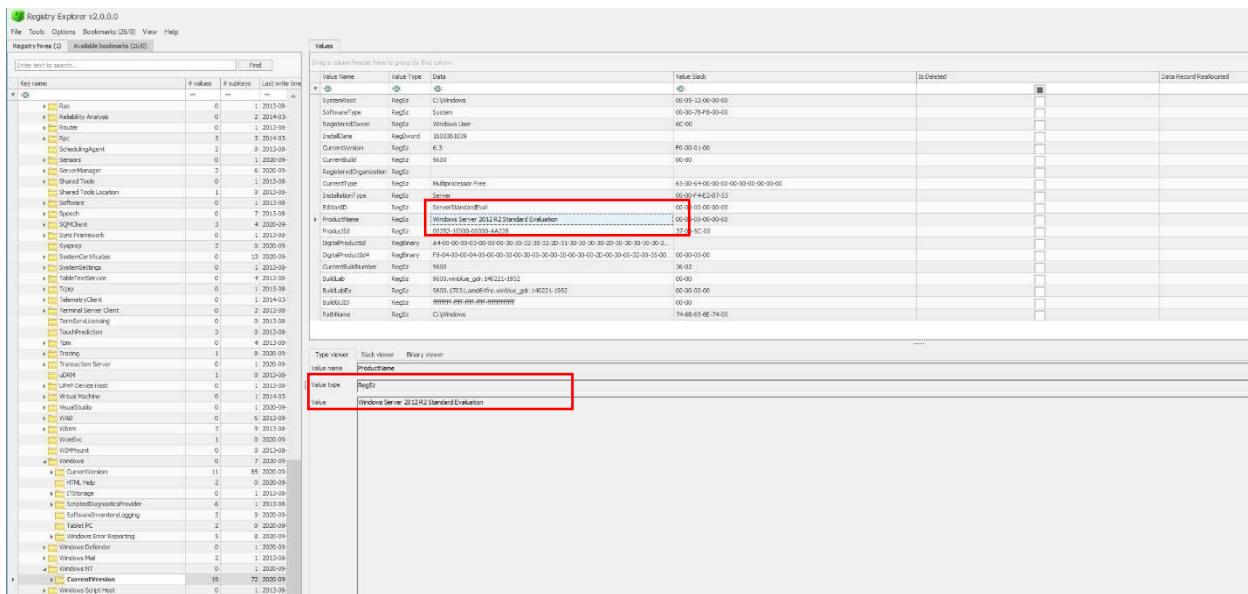
Investigation Result:

What's the Operating System of the Server? Windows Server 2012

We can obtain this information in different ways. One option is to read C:\Windows\System32\license.rtf from a disk image using an FTK imager. However, this path is outdated for modern Windows versions. While older versions like XP used this file for the EULA, newer versions (Windows 7, 8, 10, 11) have shifted to digital agreements and online activation services, so the file may no longer exist or be required.

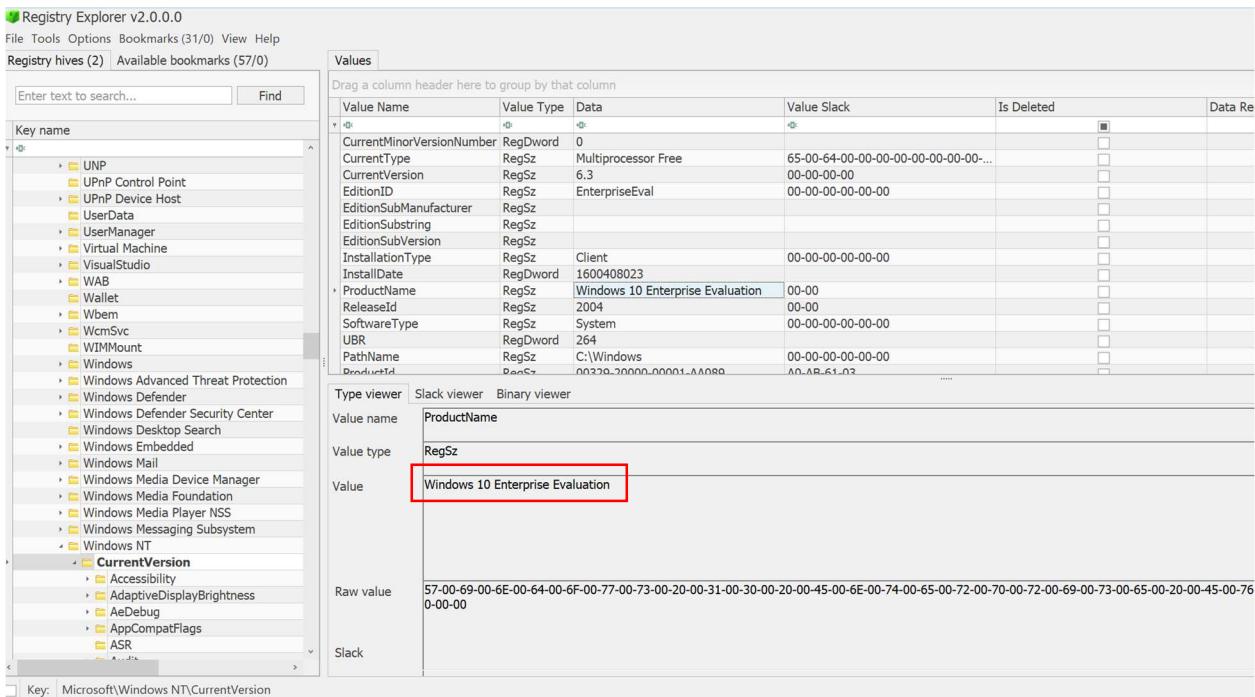


Another way to obtain this information is by mounting the disk image and navigating to C:\Windows\System32\config, where registry hive files like SOFTWARE are stored. These hives contain data such as the HKLM\Software\Microsoft\Windows NT\CurrentVersion key, which provides accurate system version and build details. You can export the registry hives for System, Software, and Security, then use Eric Zimmerman's Registry Viewer to open them.

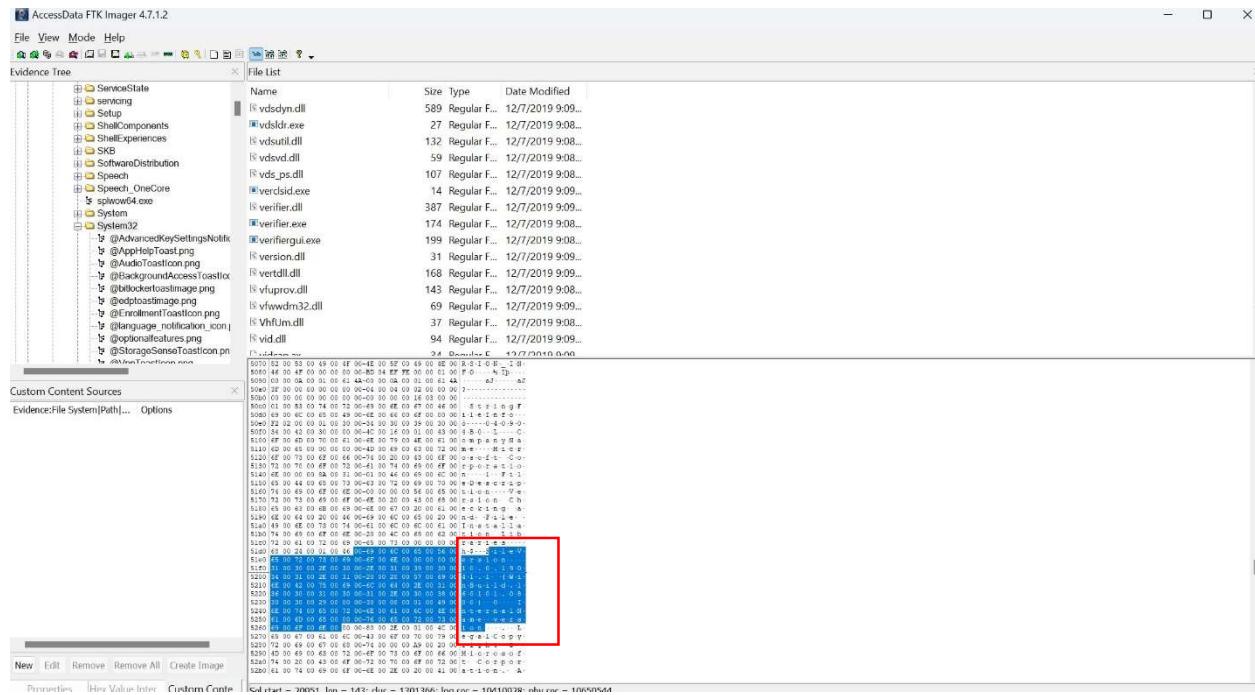


What's the Operating System of the Desktop? Windows 10

Using the same method mentioned above, we can obtain this information, first we use EZ Register Explorer to view the SOFTWARE registry file:



Or we can use FTK imager to read the version.dll file.



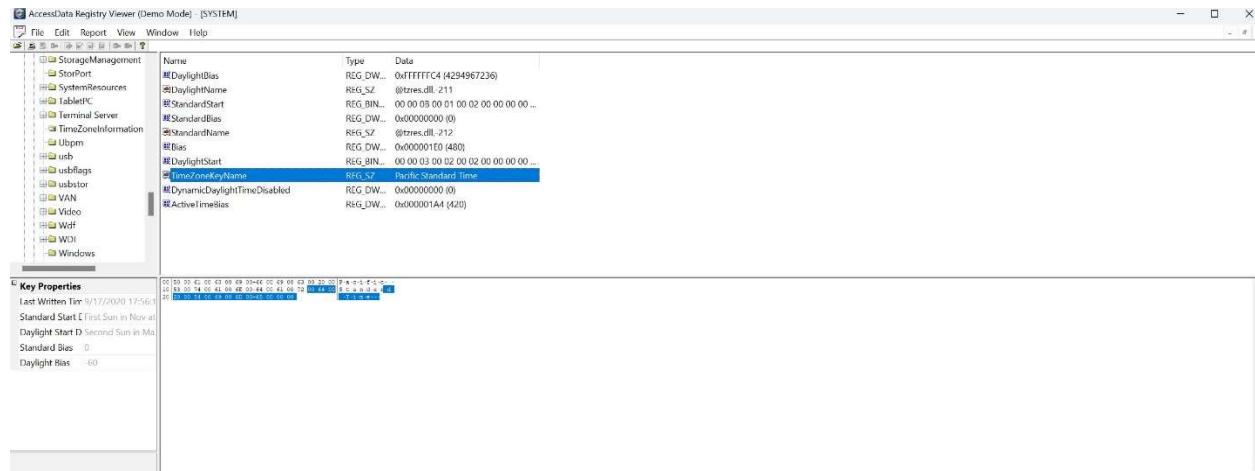
The version number **1.0.0.19041.1** in the version.dll file is indicative of the operating system version. This specific version number corresponds to: **Windows 10 Version 19041**, also known as **Windows 10 May 2020 Update (20H1)**.

What was the local time of the Server? PST

The local time of the server can be found in the **SYSTEM** registry hive. Specifically, it is located under the key:

`HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation`

We can obtain this information by exporting **SYSTEM** registry from FTK imager, then read it in FTK Registry Viewer.



Note: This incident took place in Colorado in September, which falls under UTC -6. However, the PST timestamps in the logs suggest they are using Pacific Time, which differs from the local time in Colorado. To ensure consistency and accurately analyze the incident's timing, it's important to choose a single time zone for all machines and align the timestamps accordingly.

Was there a breach? I will answer it later

What was the initial entry vector (how did they get in)? Brute Force

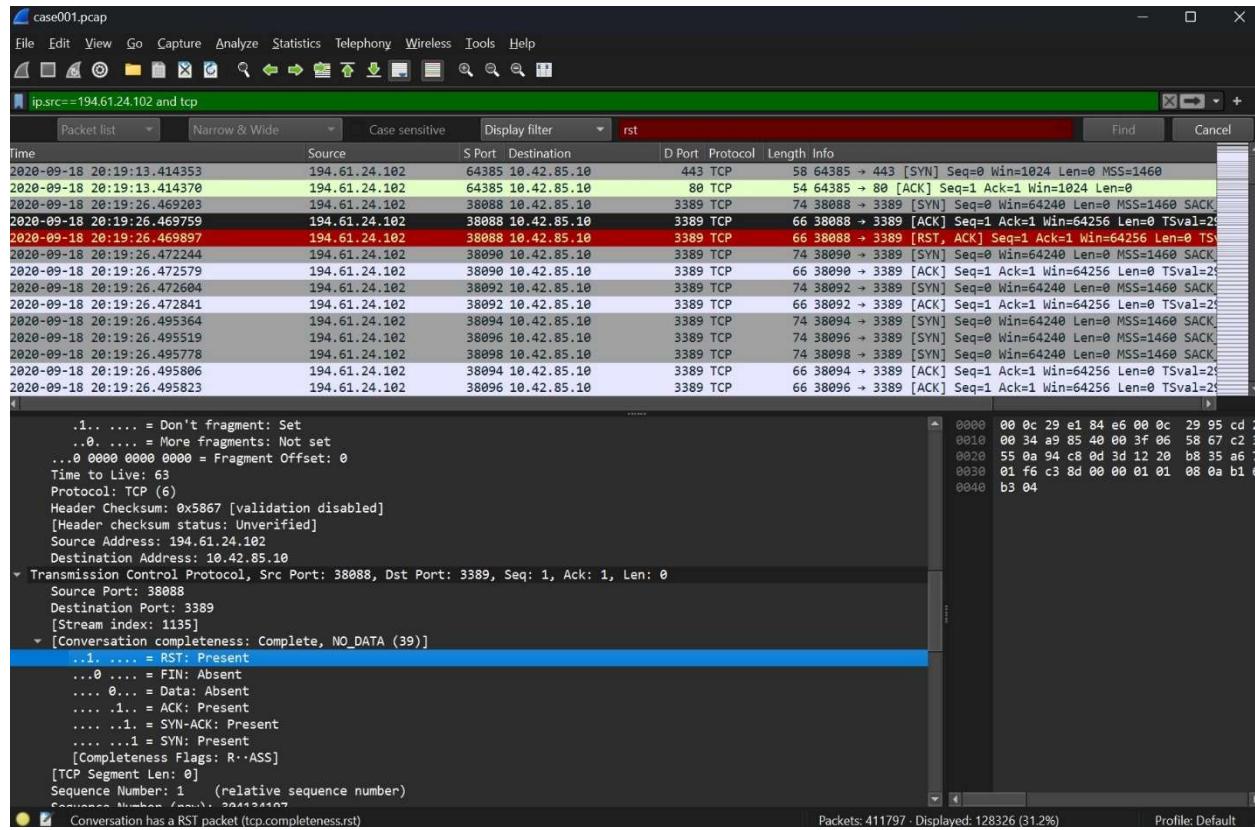
There are two ways to get the information, through PCAP file or Event logs. We will use both approaches. Export the **Security.evtx** log file from the following path:
C:\Windows\System32\winevt\Logs\Security.evtx. Once you open this file in **Windows Event Viewer**, you'll notice several event IDs in the 4625, indicating failed login attempts (Microsoft, 4625(F): An account failed to log on., n.d.). These failed attempts occurred in quick succession and originated from a Kali host on 9/18/2020 at 9:21, suggesting a possible brute-force attack on the Domain Controller.

The screenshot shows the Event Log Explorer interface with the Security.evtx log selected. The 'Network Information' section is highlighted with a red box, showing that the workstation name was 'kali'. This indicates a successful logon from the Kali Linux machine.

By following the timestamps and filtering event ID 4624, which indicates a successful logon, we confirmed that after the brute force attack, Kali successfully logged into our domain controller (Citadel-DC01) at 9:21:46 PST.

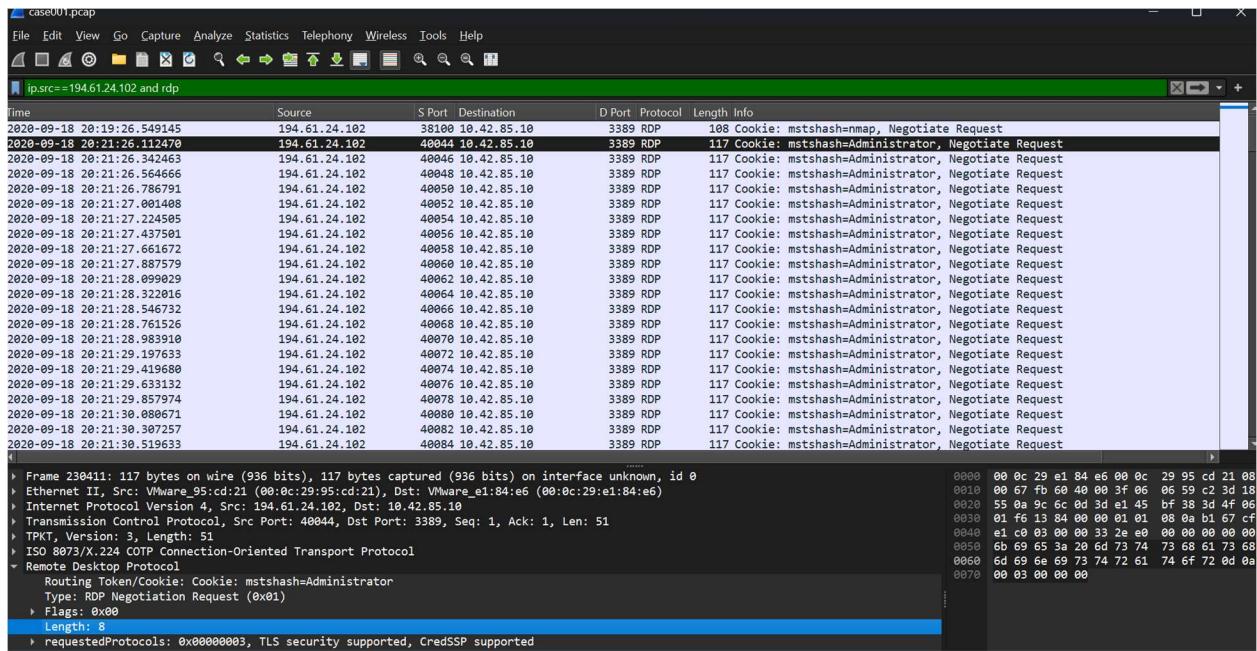
The screenshot shows the Event Log Explorer interface with the Security.evtx log selected. The 'Network Information' section is highlighted with a red box, showing that the workstation name was 'kali'. This indicates a successful logon from the Kali Linux machine.

Further investigation using Wireshark to analyze the accompanying PCAP file confirmed this suspicion. The reconnaissance from IP 194.61.24.102 (Kali) occurred on September 18, 2020, around 20:19 Mountain Time (19:19 PST). The initial ping, accompanied by an RST flag, indicated a terminated connection. Following this, a large number of pings were detected targeting the destination IP 10.42.85.10 (our DC) on port 3389 (RDP) within 1 second, suggesting a brute-force attack.



The brute force attack from a Kali machine targeting a Windows server via **port 3389** (RDP) seeks to exploit Remote Desktop Protocol, which is commonly used for Windows remote management and access, by repeatedly attempting to guess valid login credentials.

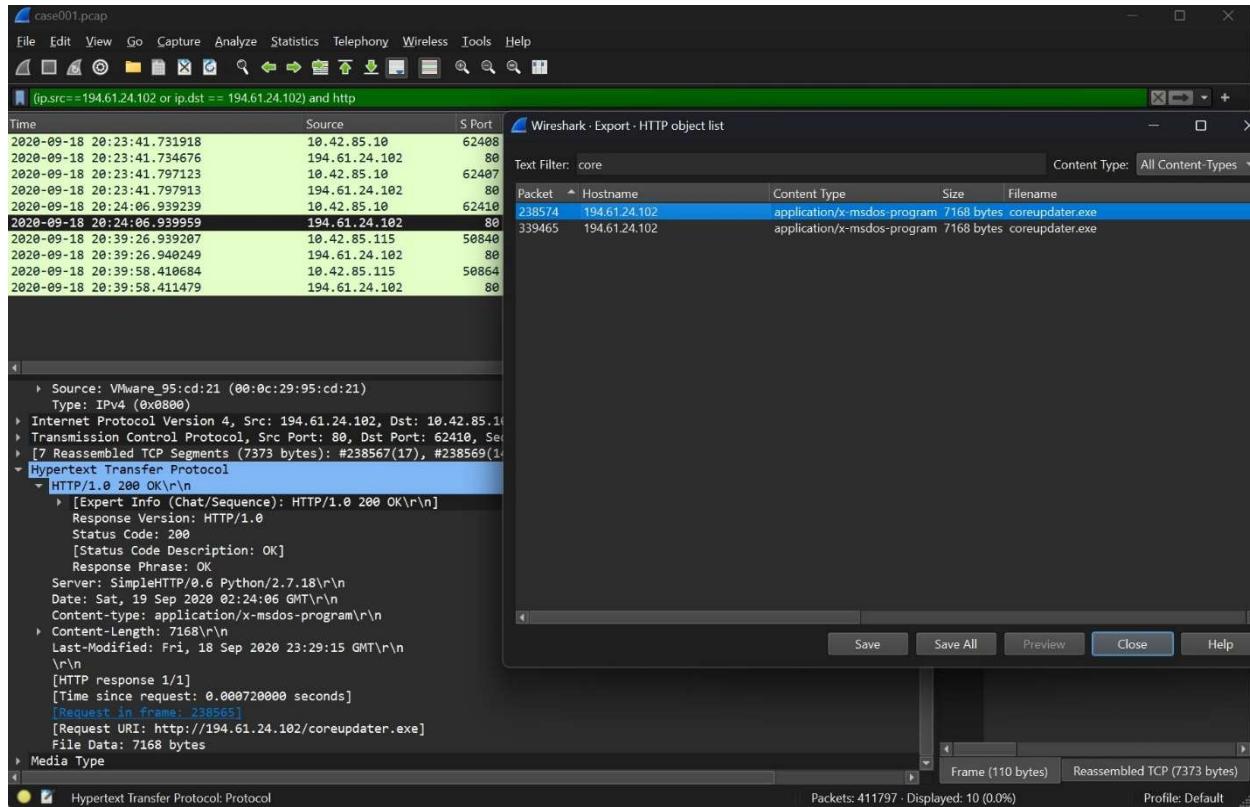
By further filtering out RDP traffic in Wireshark, the presence of **Cookie: mstshash=Administrator** indicates an attempt to connect to the target using the **Administrator** account. This suggests the client is specifically targeting our Domain Controller (DC) and trying to log in with elevated privileges. Given the suspicious nature of the activity, including the large number of pings and brute-force patterns, it's likely that the attacker is attempting to gain unauthorized access to the DC using the Administrator account.



Was malware used? If so, what was it? Yes, coreupdater.exe

While reviewing the PCAP file, I examined all traffic associated with the suspect IP to understand the activity beyond the initial access. I discovered several GET requests from the IP address 194.64.24.102 to a suspicious URI, "coreupdater.exe." Both the Domain Controller (IP 10.45.85.10) and the Workstation desktop (IP 10.45.85.115) sent GET requests to download this file.

To obtain the downloaded file, use Wireshark to extract it by navigating to File -> Export Objects -> HTTP and save. Be careful not to execute this file, just run the hash check.



Run PowerShell in the same folder where the malware is saved and run the command GET-FileHash .\coreupdate.exe to get the sha-256 hash. Check the hash on VirusTotal proves that this is indeed a malware.

Security vendor	Analysis result	Threat category	Family label
Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win64.RL_Shelma.R298109
Ali Baba	Trojan:Win64/Shelma.22b9092b	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/CryptXPACK.Gen7	BitDefender	Trojan.Metasploit.A
Bkav Pro	W64.AI DetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
Cyberason	Malicious.690ed7	Culance	Lunc.a

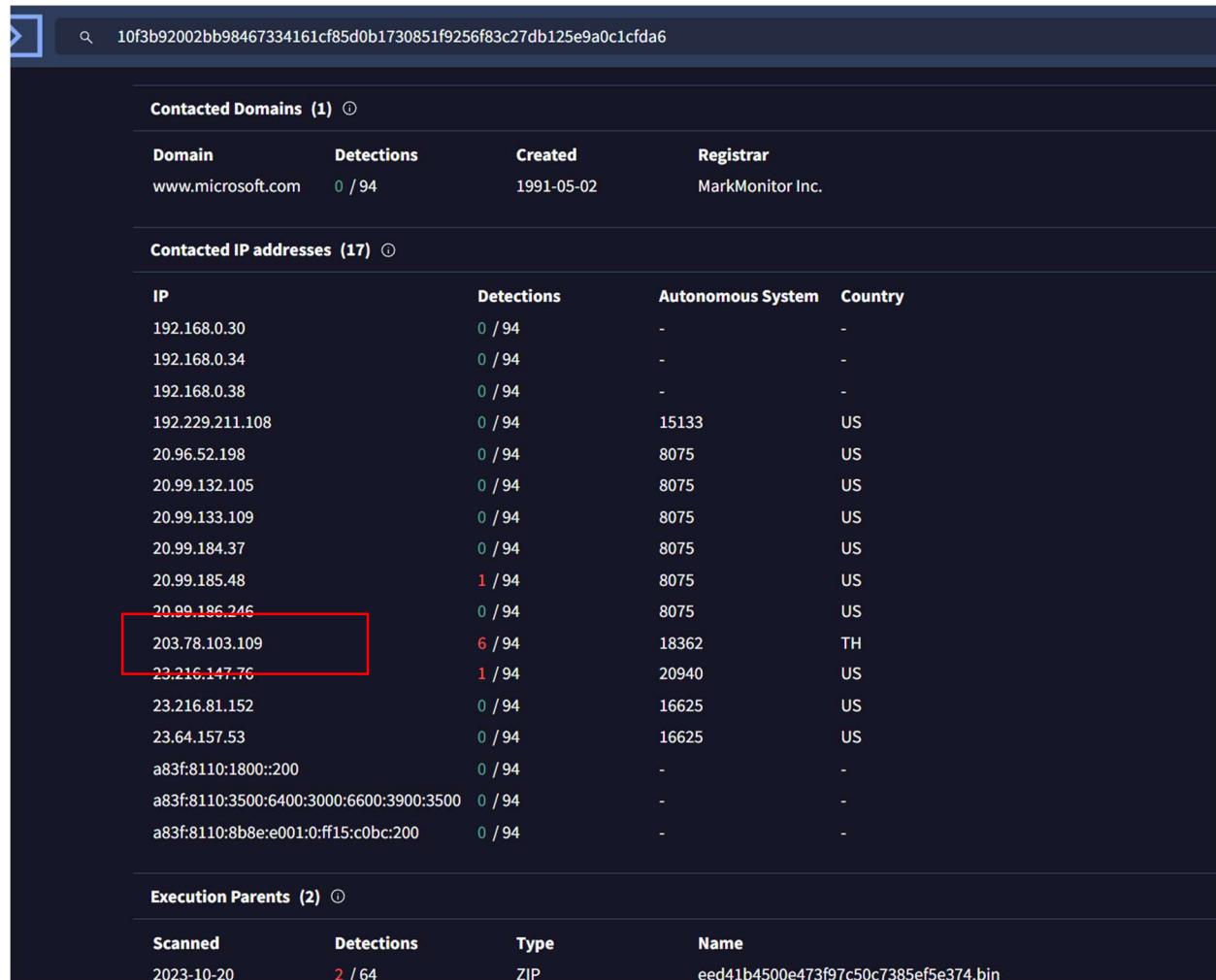
What process was malicious? **coreupdater.exe**

- Identify the IP Address that delivered the payload. **194.61.24.102**

From the PCAP analysis, we can easily obtain this information.

- What IP Address is the malware calling to? **203.78.103.109**

For this hash checked on VT, we can obtain IP addresses that are related to this malware in Contacted IP addresses.



The screenshot shows the VirusTotal analysis interface for the hash 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6. It displays three main sections: Contacted Domains, Contacted IP addresses, and Execution Parents.

Contacted Domains (1)			
Domain	Detections	Created	Registrar
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.

Contacted IP addresses (17)				
IP	Detections	Autonomous System	Country	
192.168.0.30	0 / 94	-	-	
192.168.0.34	0 / 94	-	-	
192.168.0.38	0 / 94	-	-	
192.229.211.108	0 / 94	15133	US	
20.96.52.198	0 / 94	8075	US	
20.99.132.105	0 / 94	8075	US	
20.99.133.109	0 / 94	8075	US	
20.99.184.37	0 / 94	8075	US	
20.99.185.48	1 / 94	8075	US	
20.99.186.246	0 / 94	8075	US	
203.78.103.109	6 / 94	18362	TH	
23.216.147.76	1 / 94	20940	US	
23.216.81.152	0 / 94	16625	US	
23.64.157.53	0 / 94	16625	US	
a83f:8110:1800::200	0 / 94	-	-	
a83f:8110:3500:6400:3000:6600:3900:3500	0 / 94	-	-	
a83f:8110:8b8e:e001:0:ff15:c0bc:200	0 / 94	-	-	

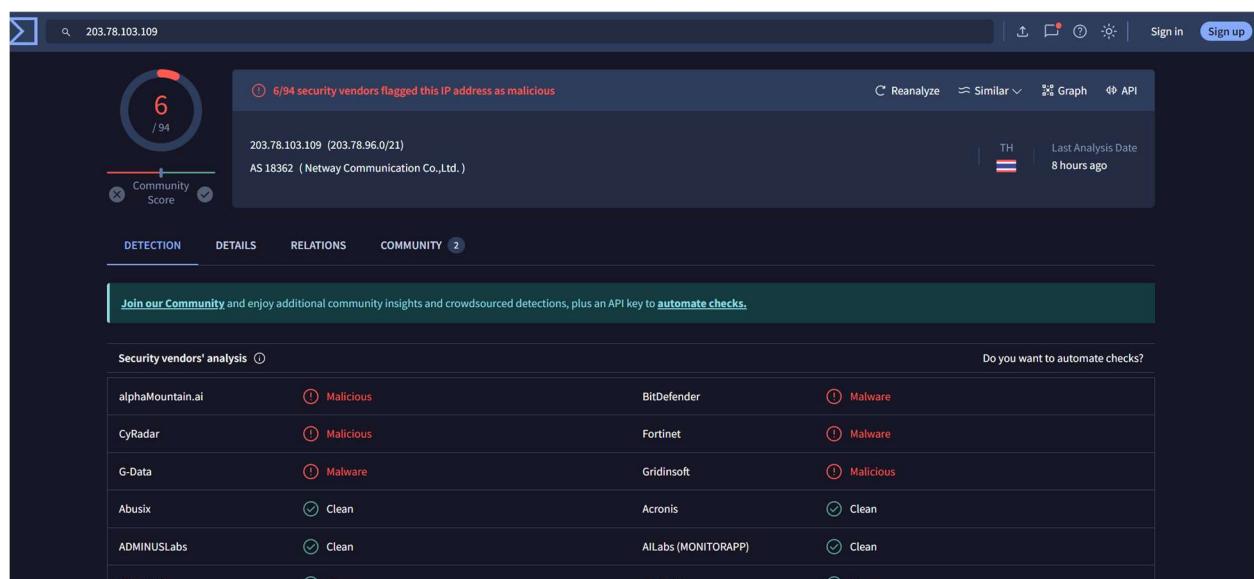
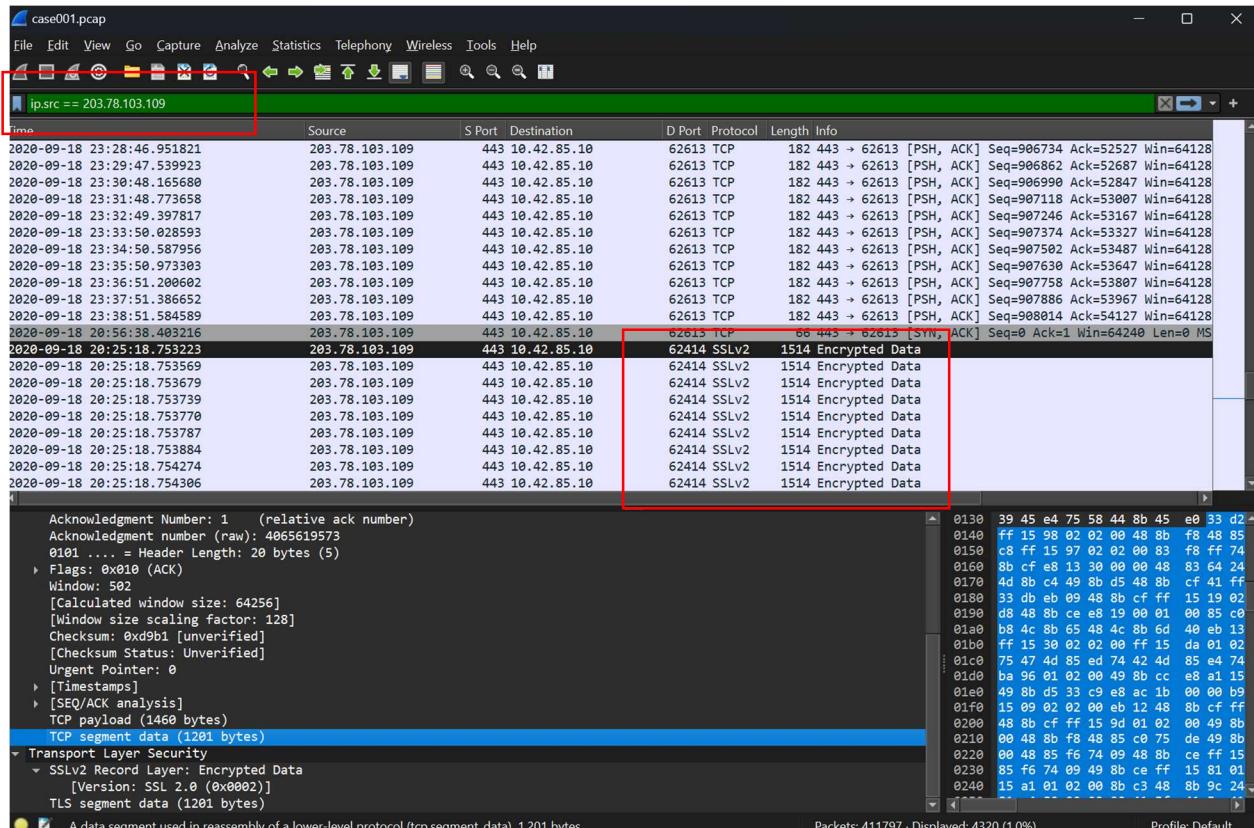
Execution Parents (2)			
Scanned	Detections	Type	Name
2023-10-20	2 / 64	ZIP	eed41b4500e473f97c50c7385ef5e374.bin

I analyzed the IP addresses in the provided PCAP and identified a match with VT: **203.78.103.109**. A further search on VT confirmed that this IP is listed in their database. Look into the traffic packet:

- **1514 bytes on wire:** This is the total size of the frame, including all headers and data.
- **1460 bytes of TCP payload:** This is the actual data transmitted at the application layer.

- 1201 bytes of TLS segment data:** This represents encrypted data within the Transport Layer Security (TLS) protocol, part of the total TCP payload.

So, the **total amount of data transmitted** in this frame is **1514 bytes**. The **TCP payload** itself (application data) is **1460 bytes**, with **1201 bytes** being specifically the TLS-encrypted portion. And as we can see from the picture below, there are multiple traffic captured from this IP to both DC and Workstation.



This is a typical download malware and post-download communication process: If the malware was indeed downloaded, the reason Wireshark captures other traffic related to IP **203.78.103.109** after the download could be that the malware is actively communicating with this IP address, which might be the attacker's command-and-control (C2) server (Novak, 2021).

This type of behavior is typical for malware:

- **Post-download communication:** After the malware is downloaded and executed, it often establishes a connection with a remote server (like **203.78.103.109**) to receive instructions, **exfiltrate data, or download additional payloads.**
- **Malware calling home:** The captured traffic may represent the malware "calling home" to the C2 server, sending or receiving data (in this case, encrypted via TLS).

Now I can answer this question: Was there a breach? **Yes.**

It is reasonable to conclude that the Szechuan sauce recipe has likely been exfiltrated, given the multiple instances of traffic captured between this IP and both the Domain Controller and Workstation. The use of the SSLv2 protocol suggests that the data was encrypted during transmission, likely as part of the exfiltration process.

- Where is this malware on disk? **Initially in C:\Users\Administrator\Downloads, Later was moved to C:\Windows\System32\coreupdate.exe**

In **FTK Imager**, you can find **WebCache** files, which are related to the browser's history and cached data including downloads (PCmag, n.d.), stored in the user's profile folder on Windows systems. These files are important for web activity. The path is **C:\Users<User>\AppData\Local\Microsoft\Windows\WebCache**.

Navigate to this path and parse the WebCacheV01 file. We can find that the coreupdater.exe was initially downloaded to the **C:\Users\Administrator\Downloads** folder which is the default folder for download.

For DC:

Screenshot of a forensic tool interface showing file system and memory analysis.

File System View:

- Root directory: \$UpCase
- Sub-directories: Documents and Settings, FileShare, PerfLogs, Program Files (x86), ProgramData, System Volume Information, Users, Administrator, AppData, Local, Application Data, ElevatedDiagnostics, EmieSiteList, EmieUserList, History, Microsoft, Credentials, Feeds, Feeds Cache, Internet Explorer, NetTraces, PlayReady, Terminal Server Client, Windows.
- Log files: V0100005.log, V0100006.log, V0100007.log, V0100008.log, V0100009.log, V01res00001.jrs, V01res00002.jrs, V01tmp.log, V01tmp.log.FileSlack, WebCacheV01.dat.
- File details for WebCacheV01.dat: 32,832 Regular F... 9/19/2020 4:37...

Hex Value Interpreter:

- Type: Si... Value
- Registers: signed int... 1-8, unsigned i... 1-8, FILETIME... 8, FILETIME... 8, DOS date 2, DOS time 2, time_t(UT...) 4, time_t(loc...) 4.
- Byte order: Little endian (selected).
- Properties: Sel start = 7537686, len = 90; dus = 875742; log sec = 7005938; phy sec = 7724786.

Search Dialog:

- Find What: Downloads\score
- Type: Text (selected), Binary (hex), ANSI, Upcode, Match Case, Regular Expression.
- Direction: Up (selected), Down, Wrap.
- Buttons: Find, Cancel.

For Desktop:

Screenshot of a forensic tool interface showing file system and memory analysis.

File System View:

- Root directory: Caches, CloudStore, Explorer, GameExplorer, History, IECompatCache, IECompatUaCache, INetCache, INetCookies, Notifications, Ringtones, RoamingTiles, Safety, SchCache, SettingSync, Shell, Temporary Internet Files, WebCache, WinX.
- Log files: V01tmp.log, V01tmp.log.FileSlack, WebCacheV01.dat, WebCacheV01.dat.FileSlack, WebCacheV01.jfm.
- File details for WebCacheV01.dat: 26,112 Regular F... 9/19/2020 3:52...

Hex Value Interpreter:

- Type: Si... Value
- Registers: signed int... 1-8, unsigned i... 1-8, FILETIME... 8, FILETIME... 8, DOS date 2, DOS time 2, time_t(UT...) 4, time_t(loc...) 4.
- Byte order: Little endian (selected).
- Properties: Sel start = 17826945, len = 111; dus = 399093; log sec = 3192746; phy sec = 3432362.

Has it been moved to another folder? We need to check the **Amcache registry**, it is a registry hive in Windows that stores information about executable files and their metadata,

including program installation details. It's useful for forensic investigations as it helps track which programs were executed, when they were executed, and other associated details (ForenSafe, 2022). Access this registry following this path:

C:\Windows\AppCompat\Programs\Amcache.hve, and parse it with EZ Registry Explorer, we can conclude that the file has been moved to C:\Windows\System32.

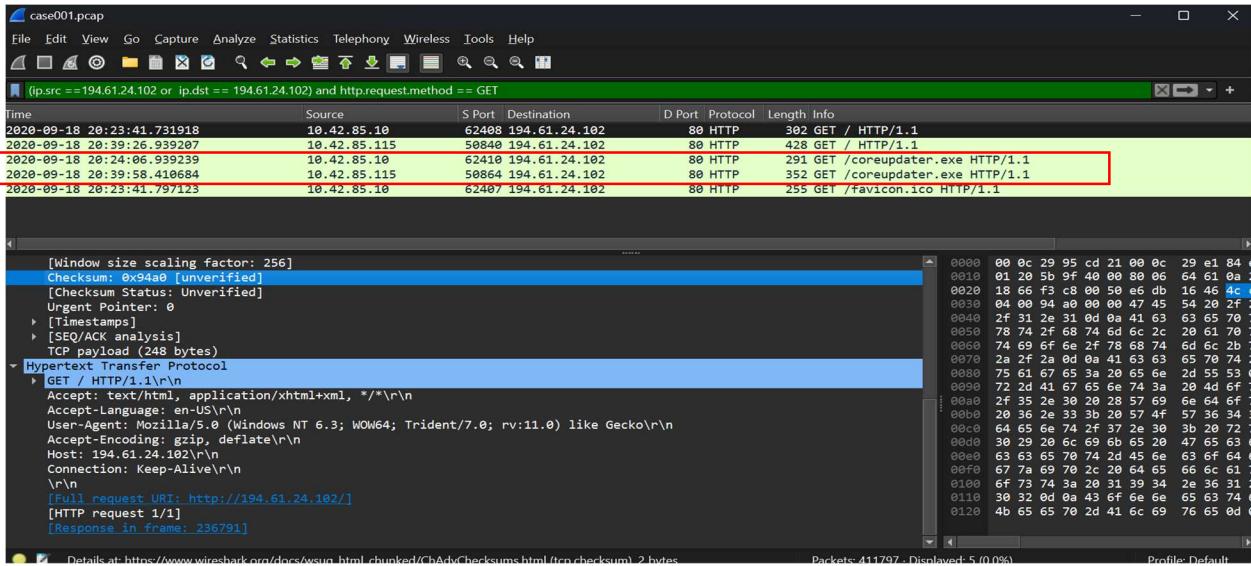
Value Name	Value Type	Data	Value Slack	Is Deleted
ProgramId	RegSz	0000485495bded616cd407985279849903e00000ff	00-00	
FileId	RegSz	0000fd153c66386ca3e9903d66a84d6fd129a3a5c	00-00	
LowerCaseLongPath	RegSz	c:\windows\system32\coreupdater.exe	00-00-00-00	
LongPathHash	RegSz	coreupdater.exe 4b283e5048abd88b		
Name	RegSz	coreupdater.exe	00-00-00-00	
Publisher	RegSz			
Version	RegSz			
BinaryVersion	RegSz			
BinaryType	RegSz	pe64_amd64	17-00-68-30-17-00	
ProductName	RegSz			
ProductVersion	RegSz			
LinkDate	RegSz	04/14/2010 22:06:53	00-00-00-00	
BinProductVersion	RegSz			
AppxPackageFullName	RegSz			
AppxPackageRelativeId	RegSz			
Size	RegQword	7168	C0-1F-17-00	
Language	RegQword	0		
IsPefile	RegQword	1		
IsOsComponent	RegQword	0		
Usn	RegQword	26277760	98-2E-17-00	

Type viewer	Slack viewer	Binary viewer
Value name	LowerCaseLongPath	
Value type	RegSz	
Value	c:\windows\system32\coreupdater.exe	

Fun fact: The malware was downloaded for both DC and Workstation, but only the workstation's registry file shows that the malware was moved to C:\Windows\System32 and executed.

- When did it first appear? September 18, 2020, at 20:24:06on DC

We have identified the malicious IP address and filtered out the GET requests. This packet suggests that a **GET request** was sent to **194.61.24.102** on port **80** (HTTP), which is typically used for downloading or retrieving data from a web server. The user agent making this request is posing as **Mozilla/5.0**, likely mimicking a legitimate browser. The first instance appears to target our Domain Controller (10.42.85.10) on September 18, 2020, at 20:24:06 Mountain Time.



- Did someone move it? Yes. From C:\Users\Administrator\Downloads\ to C:\Windows\System32\. I explained the process in the previous question: Where is this malware on disk?
- What were the capabilities of this malware?

From VT we can see this malware is related to the Metasploit framework. Further research shows that This tool offers a wide range of capabilities by providing the attacker with a command-and-control (C2) shell on the victim's machine. From this point, they can further explore the compromised device, pivot to other devices within the network, or execute additional payloads and commands.

The screenshot shows a forum post with the following details:

Voting details (1)

	TalionOwn	-1
1 year ago		

Comments (25)

joesecurity 6 months ago

Joe Sandbox Analysis:

Verdict: MAL
Score: 92/100
Threat Name: Metasploit

Malware Config: see the report for the full malware config

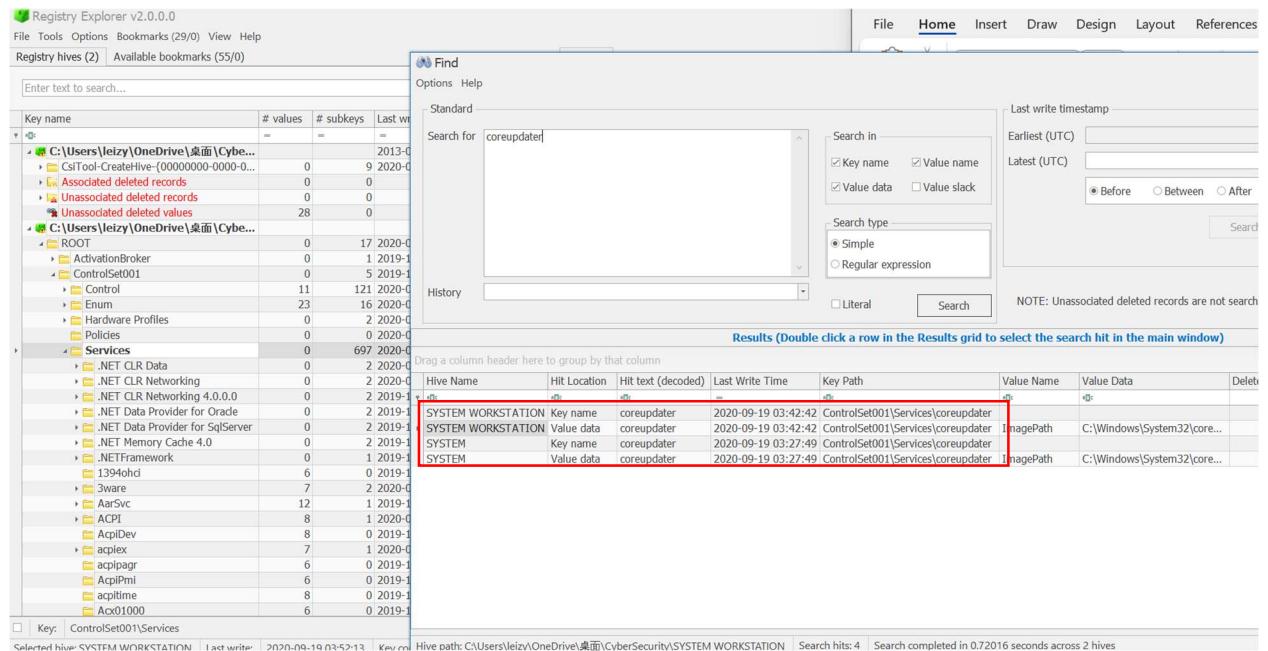
Hosts: 203.78.103.109

HTML Report: <https://www.joesandbox.com/analysis/1391302/0/html>
PDF Report: <https://www.joesandbox.com/analysis/1391302/0/pdf>
Executive Report: <https://www.joesandbox.com/analysis/1391302/0/executive>
Incident Report: <https://www.joesandbox.com/analysis/1391302/0/irxml>
IOCs: <https://www.joesandbox.com/analysis/1391302?dtype=analysisid>

[Show less](#)

- Is this malware easily obtained? **Yes. It comes with Metasploit Framework which is free to download and use (Metasploit, n.d.).**
- Was this malware installed with persistence on any machine? When and where?
**Yes, for both inside the Registry as service, DC: 2020-09-19 03:27:49 PST.
Workstation: 2020-09-19 03:42:42 PST**

For this I checked the **SYSTEM** registry using EZ Registry Explorer to see if there are any “coreupdater” services installed. We can also see a registry key was created “coreupdater” on both DC and Workstation. the presence of coreupdater under the **Services** registry key likely indicates that the **coreupdater** program is installed as a service and may be set to run persistently on the system.



- What malicious IP Addresses were involved? **194.61.24.102 and 203.78.103.109**
 - Were any IP Addresses from known adversary infrastructure? **Both belong to adversary infrastructure**

For IP address 194.61.24.102, VirusTotal shows a single appearance. In contrast, AlienVault lists 31 pulses for this IP, with tags indicating malicious activity and brute force attempts. For IP address 203.78.103.109, it has been flagged on multiple OSINT sites, including the 2nd picture shown below from VirusTotal (Sandbox, 2024).

LeveBlue/Labs Browse Scan Endpoints Create Pulse Submit Sample API Integration All ▾ Search O

IPV4
194.61.24.102

Add to Pulse +

Pulses	Passive DNS	URLs	Files
31	0	0	0

Analysis Overview

Location	Russian Federation	External Resources	Whois, VirusTotal
ASN	ASNone		
Related Pulses	OTX User-Created Pulses (31)		
Related Tags	9 Related Tags Nextray, cyber security, ioc, phishing, malicious, brute force, ssh, zmap, scan Less		

Analysis Related Pulses Comments (0)

User Created (31)

IOC Records Provided by @NextRayAI • IPv4 Indicator Inactive

CREATED 2 YEARS AGO | MODIFIED 1 MONTH AGO by NextRay-AI | Public | TLP: White

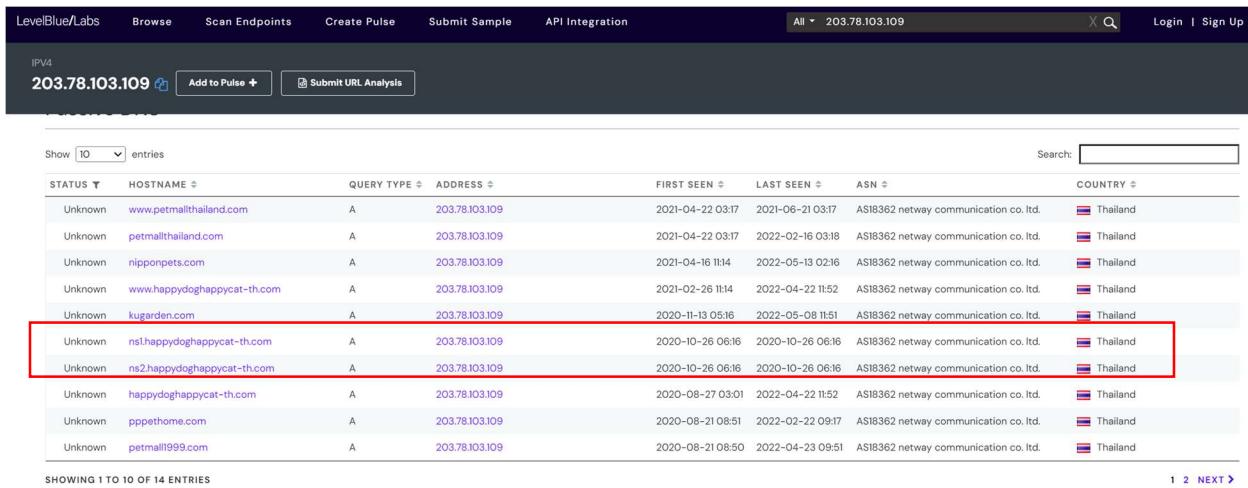
No. of IPs < 25%
25% < No. of IPs < 50%
50% < No. of IPs < 75%
75% < No. of IPs

Public IPs

IP	Domain	Country	Flag	ASN	ASN Name	Malicious
203.78.103.109	unknown	Thailand		18362	NETWAY-AS-APNetwayCommunicationCoLtdTH	true

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

According to AlienVault's data, on October 26, 2020, there were two additional attacks associated with the IP address 203.78.103.109, linked to the DNS hostname happydoghappycat-th.com.



STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN	COUNTRY
Unknown	www.petmallthailand.com	A	203.78.103.109	2021-04-22 03:17	2021-06-21 03:17	AS18362 netway communication co. ltd.	Thailand
Unknown	petmallthailand.com	A	203.78.103.109	2021-04-22 03:17	2022-02-16 03:18	AS18362 netway communication co. ltd.	Thailand
Unknown	nipponpets.com	A	203.78.103.109	2021-04-16 11:14	2022-05-13 02:16	AS18362 netway communication co. ltd.	Thailand
Unknown	www.happydoghappycat-th.com	A	203.78.103.109	2021-02-26 11:14	2022-04-22 11:52	AS18362 netway communication co. ltd.	Thailand
Unknown	kugarden.com	A	203.78.103.109	2020-11-13 05:16	2022-05-08 11:51	AS18362 netway communication co. ltd.	Thailand
Unknown	ns1happydoghappycat-th.com	A	203.78.103.109	2020-10-26 06:16	2020-10-26 06:16	AS18362 netway communication co. ltd.	Thailand
Unknown	ns2happydoghappycat-th.com	A	203.78.103.109	2020-10-26 06:16	2020-10-26 06:16	AS18362 netway communication co. ltd.	Thailand
Unknown	happydoghappycat-th.com	A	203.78.103.109	2020-08-27 03:01	2022-04-22 11:52	AS18362 netway communication co. ltd.	Thailand
Unknown	pppetthome.com	A	203.78.103.109	2020-08-21 08:51	2022-02-22 09:17	AS18362 netway communication co. ltd.	Thailand
Unknown	petmall999.com	A	203.78.103.109	2020-08-21 08:50	2022-04-23 09:51	AS18362 netway communication co. ltd.	Thailand

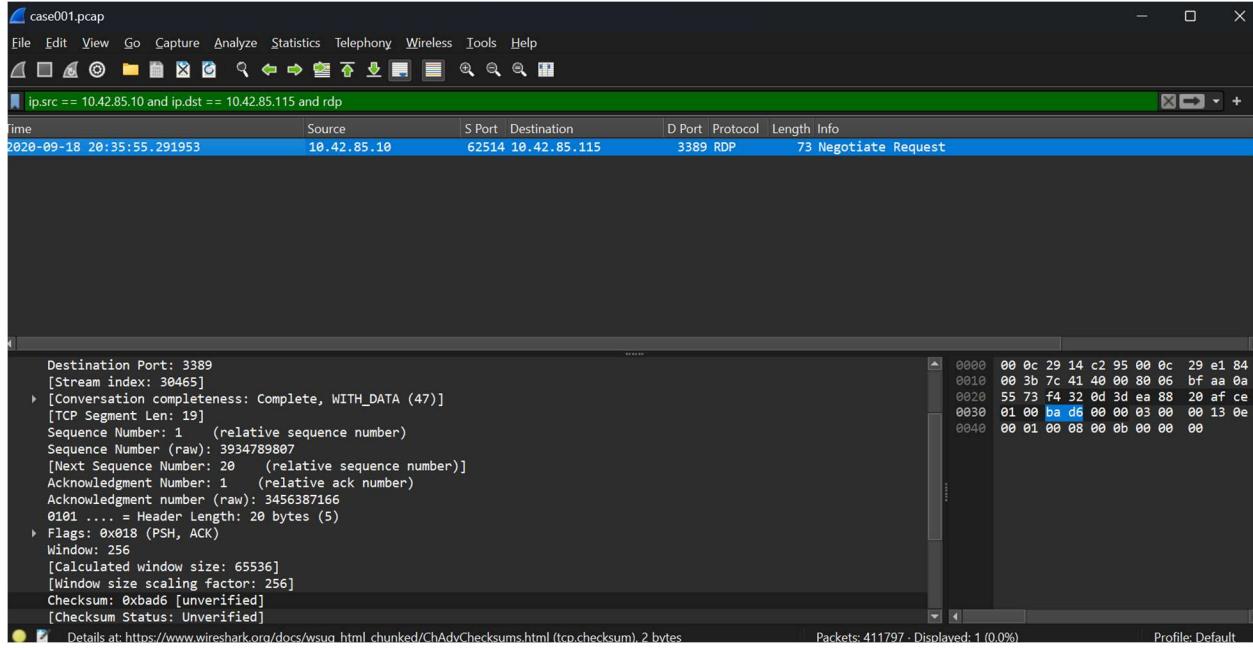
- Did the attacker access any other systems? **YES**

- How?

The attacker accessed the Workstation desktop machine, Desktop-SDN1RPT, via RDP. They used a brute-force attack to crack the Administrator account password on the Domain Controller (DC). After gaining access to the DC, they established a RDP session from the DC to the desktop machine, see picture below.

- When? **2020-9-18 at 20:35:55 Mountain Time**

The PCAP reveals that the RDP session from the Domain Controller to the workstation began on September 18, 2020, at 20:35:55 Mountain Time.



- Did the attacker steal or access any data? When?

Yes, at 3:35:06 AM PST from the DC. At 3:47:11 AM PST from Workstation. The following data has been accessed and stolen:

- Beth_Secret.txt
- NoJerry.txt
- Portal_gun.png
- PortalGunPlans.txt
- Szechuan Sauce.txt
- Plans.txt
- My Social Security Number.txt
- Thoughts.txt

Name	Type	Date Modified
\$I30	NTFS Ind...	9/19/2020 3:35...
Beth_Secret.txt	Regular F...	9/18/2020 11:3...
NoJerry.txt	Regular F...	9/18/2020 10:3...
PortalGunPlans.txt	Regular F...	9/18/2020 10:3...
Szechuan Sauce.txt	Regular F...	9/18/2020 10:3...

The entire secret folder on the DC was accessed at 3:35:06 AM PST. At this point, we can only confirm that the data was accessed. To determine if it was stolen, further investigation is required.

During data exfiltration, it's typical for a malicious actor to create a staging zip file to consolidate stolen data, enabling a quicker exfiltration process. After searching the **MFT files** (IDERA, n.d.) from the disk images of both the DC and the workstation, I found two files: *loot.zip* on the workstation and *secret.zip* on the DC. Given that the DC has a "secret" folder in its *FileShare* folder, I suspect that *secret.zip* contains all the exfiltrated data from DC, *loot.zip* contains all the exfiltrated data from the workstation.

Further investigation is needed on **WebCacheV01.dat** file (I mentioned this file earlier in this report) and **MFT file**, The Master File Table (MFT) is a crucial component of the NTFS (New Technology File System) used by Windows. It contains metadata about every file and directory on an NTFS volume, acting like an index or database that keeps track of important information about files (IDERA, n.d.).

Name	Size	Type	Date Modified
\$I30	4	NTFS Ind...	9/19/2020 3:44...
V01.chk	8	Regular F...	9/19/2020 3:52...
V01.log	512	Regular F...	9/19/2020 3:52...
V0100002.log	512	Regular F...	9/19/2020 3:39...
V0100003.log	512	Regular F...	9/19/2020 3:39...
V0100004.log	512	Regular F...	9/19/2020 3:39...
V0100005.log	512	Regular F...	9/19/2020 3:39...
V0100006.log	512	Regular F...	9/19/2020 3:39...
V01res00001.jrs	512	Regular F...	9/19/2020 3:44...
V01res00001.jrs.FileSlack	512	File Slack	
V01res00002.jrs	512	Regular F...	9/19/2020 3:36...
V01res00002.jrs.FileSlack	512	File Slack	
V01tmp.log	512	Regular F...	9/19/2020 3:52...
V01tmp.log.FileSlack	128	File Slack	
WebCacheV01.dat	26,112	Regular F...	9/19/2020 3:52...
WebCacheV01.dat.FileSlack	4,576	File Slack	
WebCacheV01.jfm	16	Regular F...	9/19/2020 3:52...

In the image above, we see the WebCacheV01 from the workstation's disk image, which not only reveals the presence of **loot.zip** but also pinpoints its location at **C:/Users/mortysmith/Documents**. This path requires further investigation, and unsurprisingly, I discovered additional files that were exfiltrated from Morty Smith's workstation to the DC. These documents are: **Portal_gun.png**, **My Social Security Number.txt**, **Plans.txt** and **Thought.txt**. Please refer to the image below. Upon further investigation, I found a file named **Thought.txt** on Morty's desktop folder. Although it was not located in the same folder as the other files, it was still listed in WebCacheV01.dat, indicating that this file was also accessed.

The screenshot shows a forensic interface with two main panes. The left pane, titled 'Evidence Tree', displays a hierarchical view of file system paths under 'mortysmith'. The right pane, titled 'File List', shows a table of files with columns for Name, Size, Type, and Date Modified. A red box highlights the following files:

Name	Type	Date Modified
My Music	Reparse	9/18/2020 10:4...
My Pictures	Reparse	9/18/2020 10:4...
My Videos	Reparse	9/18/2020 10:4...
\$I30	NTFS Ind...	9/19/2020 3:47...
desktop.ini	Regular F...	9/18/2020 10:4...
My Social Security Number...	Regular F...	9/18/2020 10:5...
Plans.txt	Regular F...	9/18/2020 10:5...
Portal_gun.png	Regular F...	9/18/2020 11:0...

The MFT file on the DC reveals the existence of secret.zip. The attacker successfully compressed the data from both the DC (secret.zip) and the workstation (loot.zip), then exfiltrated both files.

The screenshot shows a forensic interface with two main panes. The left pane, titled 'Evidence Tree', displays a hierarchical view of file system paths under '[root]'. The right pane, titled 'File List', shows a table of files with columns for Name, Type, and Date Modified. A red box highlights the following files:

Name	Type	Date Modified
ProgramData	Directory	9/17/2020 6:05...
System Volume Information	Directory	9/17/2020 5:51...
Users	Directory	9/17/2020 4:46...
Windows	Directory	9/17/2020 5:55...
\$AttrDef	Regular F...	9/17/2020 4:47...
\$BadClus	Regular F...	9/17/2020 4:47...
\$Bitmap	Regular F...	9/17/2020 4:47...
\$Boot	Regular F...	9/17/2020 4:47...
\$I30	NTFS Ind...	9/18/2020 4:48...
\$LogFile	Regular F...	9/17/2020 4:47...
\$MFT	Regular F...	9/17/2020 4:47...
1,788,888	Regular F...	9/17/2020 4:47...
87,296	Regular F...	9/17/2020 4:47...

The following images are extracted from the WebCacheV01.dat file on both the DC and workstation. They show the appearance of the accessed and exfiltrated files.

Date Modified	9/19/2020 3:52:13 AM	010ddaa0 00 69 00 6C 00 65 00 3A-00 2F 00 2F 00 2F 00 43 i-l-e-:-/-/-C
Encrypted	False	010db0 00 3A 00 2F 00 55 00 73-00 65 00 72 00 73 00 2F ::-U-s-e-r-s-/
Compressed	False	010dc0 00 6D 00 6F 00 72 00 74-00 79 00 73 00 6D 00 69 m-o-r-t-y-s-m-i
Actual File	True	010dd0 00 74 00 68 00 2F 00 44-00 EF 00 63 00 75 00 6D t-h-/-D-o-c-u-m
Start Sector	0 770 504	010dd0e0 00 65 00 6E 00 74 00 73-00 2F 00 50 00 6F 00 72 e-n-t-s-/-P-o-r
		010dd0f0 00 74 00 61 00 6C 00 5F-00 67 00 75 00 6E 00 2E t-a-l_g-u-n-
		010de00 00 70 00 6E 00 67 00 00-00 01 79 00 00 75 00 p-n-o-----y-u-
		010de10 00 00 31 53 50 53 A1 14-02 00 00 00 00 C0 00 1 -S-E-S;-----A-
		010de20 00 00 00 00 46 11 00-00 00 17 00 00 00 00 13 -----F-----

Date Modified	9/19/2020 3:52:13 AM
Encrypted	False
Compressed	False
Actual File	True
Start Sector	2 270 504

Hex Value Interpreter Custom Content Sources

Encrypted	False
Compressed	False
Actual File	True
Start Sector	2 270 504

Properties Hex Value Interpreter Custom Content Sources

Encrypted	False
Compressed	False
Actual File	True
Start Sector	2 270 504

- What was the network layout of the victim network? Two machines in the subnet 10.42.85.0/24. Windows Server DC 10.42.85.10 and workstation 10.42.85.115

To find network configuration details such as IP addresses and DNS servers from a disk image, you can examine the Windows registry key located at (Microsoft, n.d.):
HKLM\SYSTEM32\CurrentControlSet01\Services\Tcpip\Parameters

We use EZ Registry Explorer, follow the path inside interfaces we know our DC is 10.42.85.10 inside Subnet with a Mask 255.255.255.0, we can conclude that the Subnet is 10.42.85.0/24

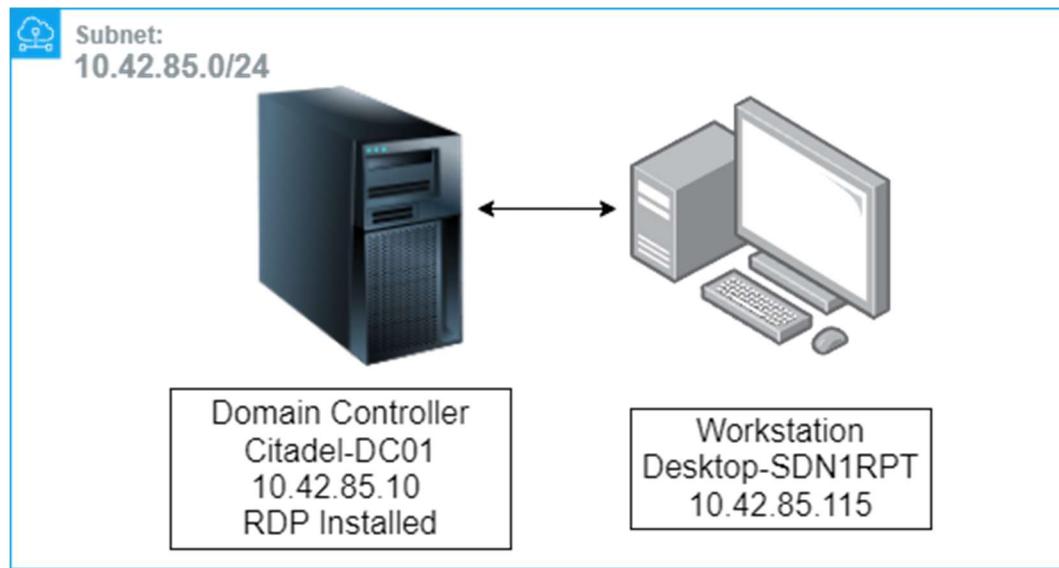
IP Address	Subnet Mask	DHCP Subnet Mask	DHCP Server	DHCP Name Server	DHCP IP Address	DHCP Default Gateway	Enabled DHCP
10.42.85.10	255.255.255.0	255.255.255.255					<input checked="" type="checkbox"/>

We used the same approach to check our desktop's SYSTEM registry, which revealed the IP address 10.42.85.115 with the same subnet mask. This confirms that within this subnet, there are two hosts: one is our DC, and the other is the workstation desktop.

The screenshot shows the Registry Explorer interface with the title "Registry Explorer v2.0.0.0". The menu bar includes File, Tools, Options, Bookmarks (29/0), View, and Help. The main window displays the "NetworkSettings" tab for a registry key named "10.42.85.115". The table has columns for IP Address, Subnet Mask, DHCP Subnet Mask, DHCP Server, DHCP Name Server, DHCP IP Address, and DHCP Default Gateway. The data row shows: IP Address: 10.42.85.115, Subnet Mask: 255.255.255.0, DHCP Subnet Mask: 255.255.255.255, DHCP Server: 255.255.255.255, and all other fields are empty. The left pane shows a tree view of registry keys under "Key name".

This network design is problematic. Placing the DC on the same subnet as workstations compromises security, as it allows potential attackers who gain access to a workstation to move laterally and target other system within the subnet.

Topology:



In one of my blog posts, I outlined the best practices for network and system administration, including the importance of a well-structured network layout:

<https://github.com/DanielDzy/Windows-Server-Active-Directory-management>

Additional investigation

- What architectural changes should be made immediately?

Given that initial access was gained through an RDP brute force attack on the DC:

- Secure RDP Access: Place RDP behind a carefully configured VPN.
- Network Isolation: Ensure the DC is accessible only within an isolated network segment and not exposed to the public Internet.
- Disable External RDP: Turn off RDP access from the Internet to prevent unauthorized external connections.

- Did the attacker steal the Szechuan sauce? If so, what time?

Yes, at 3:35:06 AM PST from the DC, the secret folder was accessed, Szechuan sauce Recipe and other documents were stolen.

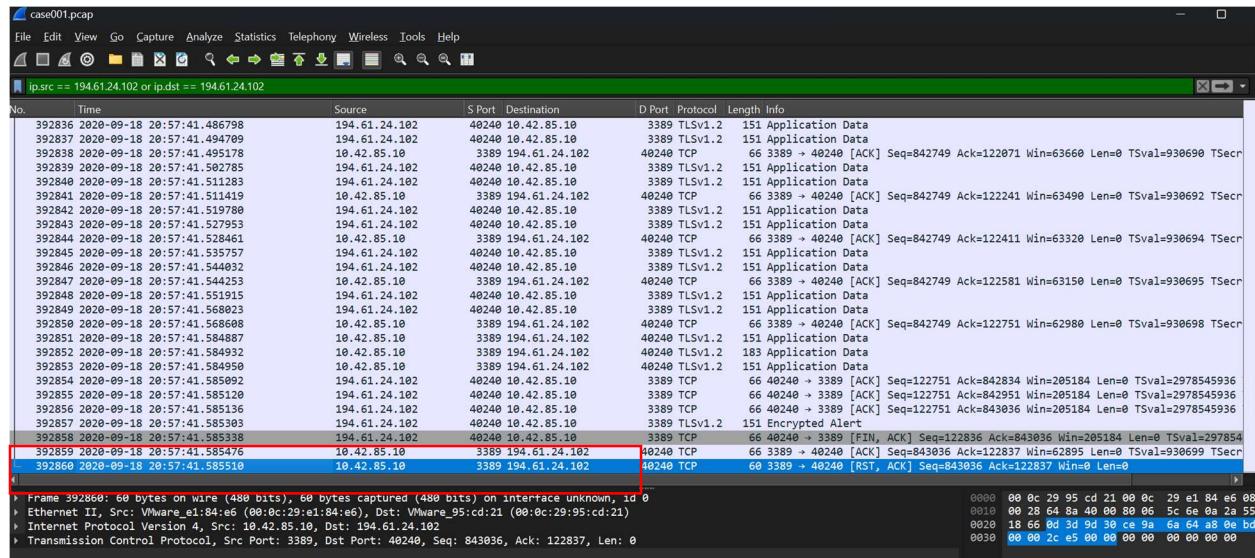
- Did the attacker steal or access any other sensitive files? If so, what times?

Yes, as I explained previously: at 3:35:06 AM PST from the DC. At 3:47:11 AM PST from Workstation. The following data has been accessed and stolen:

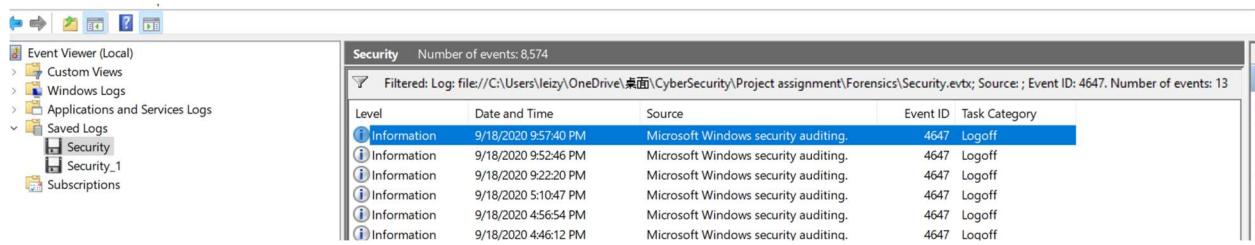
- Beth_Secret.txt
- NoJerry.txt
- Portal_gun.png (Morty Workstation)
- PortalGunPlans.txt
- Plans.txt (Morty Workstation)
- My Social Security Number.txt (Morty Workstation)
- Thoughts.txt (Morty Workstation)

- Finally, when was the last known contact with the adversary?

The PCAP file indicates that the last known connection with the malicious IP was established on 9/18/2020 at 20:57:41 Mountain Time. This is further confirmed by the exported Windows Security event log from the Domain Controller, showing the last successful logoff under Event ID 4647 (Microsoft, 4647(S): User initiated logoff., 2021).



No.	Time	Source	S Port	Destination	D Port	Protocol	Length Info
392836	2020-09-18 20:57:41.486798	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392837	2020-09-18 20:57:41.494709	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392838	2020-09-18 20:57:41.495718	10.42.85.10	3389	194.61.24.102	40249	TCP	66 3389 → 40249 [ACK] Seq=842749 Ack=122071 Win=63660 Len=0 TSval=930690 TSecr
392839	2020-09-18 20:57:41.502785	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392840	2020-09-18 20:57:41.511383	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392841	2020-09-18 20:57:41.511419	10.42.85.10	3389	194.61.24.102	40249	TCP	66 3389 → 40249 [ACK] Seq=842749 Ack=122241 Win=63490 Len=0 TSval=930692 TSecr
392842	2020-09-18 20:57:41.519780	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392843	2020-09-18 20:57:41.527953	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392844	2020-09-18 20:57:41.528461	10.42.85.10	3389	194.61.24.102	40249	TCP	66 3389 → 40249 [ACK] Seq=842749 Ack=122411 Win=63320 Len=0 TSval=930694 TSecr
392845	2020-09-18 20:57:41.535757	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392846	2020-09-18 20:57:41.544032	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392847	2020-09-18 20:57:41.544253	10.42.85.10	3389	194.61.24.102	40248	TCP	66 3389 → 40249 [ACK] Seq=842749 Ack=122581 Win=63150 Len=0 TSval=930695 TSecr
392848	2020-09-18 20:57:41.551915	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392849	2020-09-18 20:57:41.568023	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Application Data
392850	2020-09-18 20:57:41.568608	10.42.85.10	3389	194.61.24.102	40248	TCP	66 3389 → 40249 [ACK] Seq=842749 Ack=122751 Win=62980 Len=0 TSval=930698 TSecr
392851	2020-09-18 20:57:41.584887	10.42.85.10	3389	194.61.24.102	40248	TLSv1.2	151 Application Data
392852	2020-09-18 20:57:41.584932	10.42.85.10	3389	194.61.24.102	40248	TLSv1.2	183 Application Data
392853	2020-09-18 20:57:41.584950	10.42.85.10	3389	194.61.24.102	40248	TLSv1.2	151 Application Data
392854	2020-09-18 20:57:41.585092	194.61.24.102	40248	10.42.85.10	3389	TCP	66 40248 → 3389 [ACK] Seq=122751 Ack=842834 Win=205184 Len=0 TSval=2978545936
392855	2020-09-18 20:57:41.585120	194.61.24.102	40248	10.42.85.10	3389	TCP	66 40248 → 3389 [ACK] Seq=122751 Ack=842951 Win=205184 Len=0 TSval=2978545936
392856	2020-09-18 20:57:41.585136	194.61.24.102	40248	10.42.85.10	3389	TCP	66 40248 → 3389 [ACK] Seq=122751 Ack=843036 Win=205184 Len=0 TSval=2978545936
392857	2020-09-18 20:57:41.585303	194.61.24.102	40248	10.42.85.10	3389	TLSv1.2	151 Encrypted Alert
392858	2020-09-18 20:57:41.585338	194.61.24.102	40248	10.42.85.10	3389	TCP	66 40248 → 3389 [FIN, ACK] Seq=122836 Ack=843036 Win=205184 Len=0 TSval=2978545936
392859	2020-09-18 20:57:41.585476	10.42.85.10	3389	194.61.24.102	40248	TCP	66 3389 → 40248 [ACK] Seq=843036 Ack=122837 Win=62895 Len=0 TSval=930699 TSecr
392860	2020-09-18 20:57:41.585510	10.42.85.10	3389	194.61.24.102	40248	TCP	66 3389 → 40248 [RST, ACK] Seq=843036 Ack=122837 Win=0 Len=0



Security Number of events: 8574							
Filtered: Log: file:///C:/Users/leizy/OneDrive/桌面/CyberSecurity/Project assignment/Forensics/Security.evtx; Source: ; Event ID: 4647. Number of events: 13							
Level	Date and Time	Source	Event ID	Task Category			
Information	9/18/2020 9:57:40 PM	Microsoft Windows security auditing.	4647	Logoff			
Information	9/18/2020 9:57:46 PM	Microsoft Windows security auditing.	4647	Logoff			
Information	9/18/2020 9:22:20 PM	Microsoft Windows security auditing.	4647	Logoff			
Information	9/18/2020 9:10:47 PM	Microsoft Windows security auditing.	4647	Logoff			
Information	9/18/2020 4:56:54 PM	Microsoft Windows security auditing.	4647	Logoff			
Information	9/18/2020 4:46:12 PM	Microsoft Windows security auditing.	4647	Logoff			

Advanced and Bonus Questions:

- What CIS Top 20 or SANS Top 20 Controls would have directly prevented this breach?
 - **CIS Control 8: Malware Defenses** (Tenable, CIS Control 8, n.d.)
 - **CIS Control 9: Limitation and Control of Network Ports, Protocols, and Services** (Tenable, CIS Control 9, n.d.)
- What major architecture improvement could be made that would have prevented this breach?
 - **Implement VPN Access**: Ensure all remote access, including RDP to the Domain Controller, is securely routed through a VPN to prevent unauthorized external access.
 - **Deploy IPS**: Install an Intrusion Prevention System (IPS) to monitor and block suspicious activities, such as brute force attacks, on the network.
 - **Enforce Network Segmentation**: Segregate critical systems like Domain Controllers into isolated subnets to limit exposure and reduce the risk of lateral movement in case of a breach.

- Can you recover the original file about Beth's Secrets?

- What was the original name? **Secret_Beth.txt**
- Original Contents? **Earth Beth is the real Beth.**

Based on the image below, we can confirm that in the recycle bin of the DC disk image, the original file, **Secret_Beth.txt**, was modified. The initial content stated: "*Earth Beth is the real Beth.*" After the incident, the file was removed and a new file named **Beth_secret.txt** was created, and the content was altered to: "*Space Beth is the real Beth.*"

Name	Type	Date Modified
\$IU2L112.txt	Regular File	9/19/2020 3:34...
\$RU2L112.txt	Regular File	9/18/2020 10:4...
desktop.ini	Regular File	9/17/2020 4:46...

Name
\$IU2L112.txt
\$RU2L112.txt
desktop.ini

Name	Type	Date Modified
\$RU2L112.txt	Regular File	9/18/2020 10:40:00 PM

Properties

Name	Beth_Secret.txt
File Class	Regular File
File Size	27
Physical Size	32
Date Accessed	9/18/2020 11:33:54 PM
Date Created	9/18/2020 11:33:54 PM
Date Modified	9/18/2020 11:35:35 PM
Encrypted	False

Space Beth is the real Beth

- What file was time stomped? **Secret_beth.txt**

We can see from the image above, original file was removed to recycle bin, the modified the file was created at 11:33:54 PST.

Summary:

Our digital forensics investigation into the Stolen Szechuan Sauce revealed valuable details about the attack methods and the consequences for the Asian Fusion Wok's IT infrastructure and sensitive files. The investigation confirmed that the attacker successfully breached the network via a brute force attack targeting the Remote Desktop Protocol (RDP) service. This unauthorized access enabled the attacker to move laterally to the desktop machine after compromising the server.

We recommend the following enhancements to strengthen AFW's IT infrastructure, mitigate future threats, and support ongoing business growth.

- **Secure RDP Access:** Ensure RDP connections are routed through a well-configured VPN and enforce multi-factor authentication (MFA) for added security. Regularly review and update VPN settings and user permissions to safeguard access. Disable RDP access from the public Internet entirely
- **Network Isolation:** Place the Domain Controller (DC) in a dedicated, isolated network segment, accessible only to essential internal systems. Use firewalls and access control lists (ACLs) to manage traffic and prevent public Internet exposure.
- **Network Monitoring:** Implement comprehensive network monitoring solutions to detect and analyze unusual activity. Utilize Intrusion Prevention Systems (IPS) and network traffic analysis tools to promptly identify and address potential threats.

References:

ForenSafe. (2022). Retrieved from AmCache: <https://forensafe.com/blogs/AmCache.html>

IDERA. (n.d.). Retrieved from Master File Table: <https://www.idera.com/glossary/master-file-table/>

Metasploit. (n.d.). Retrieved from The world's most used penetration testing framework: <https://www.metasploit.com/>

Microsoft. (n.d.). Retrieved from 4625(F): An account failed to log on.: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4625>

Microsoft. (n.d.). Retrieved from TCP/IP and NBT configuration parameters for Windows XP: <https://learn.microsoft.com/en-us/troubleshoot/windows-client/networking/tcpip-and-nbt-configuration-parameters>

Microsoft. (2021). Retrieved from 4647(S): User initiated logoff.: <https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4647>

Novak, L. G. (2021). Retrieved from Network Forensic Investigation: Identifying Malware in Network Traffic: <https://lynnsseygrahamnovak.medium.com/network-forensic-investigation-identifying-malware-in-network-traffic-9a6bc32116dc>

PCmag. (n.d.). Retrieved from Web cache:

C:\Users\<User>\AppData\Local\Microsoft\Windows\WebCache

Sandbox, J. (2024). Retrieved from Joe Sandbox:

<https://www.joesandbox.com/analysis/1391302/0/pdf>

Tenable. (n.d.). Retrieved from CIS Control 9: <https://docs.tenable.com/security-center/CIS-CAS/Content/Controls/Foundational/Control-9/Control-9.htm>

Tenable. (n.d.). Retrieved from CIS Control 8: <https://docs.tenable.com/security-center/CIS-CAS/Content/Controls/Foundational/Control-8/Control-8.htm>