

Forensic Investigation Report

Case 001 – The Stolen Szechuan Sauce

Name: Sumit Giri

Organization: Lighthouse Labs

Date: 23-11-2024

Table of Contents

1. Executive Summary	3
2. Methodology	3
3. Analysis and Findings	4
○ 3.1. Operating System of the Server	4
○ 3.2. Operating System of the Desktop	4
○ 3.3. Local Time of the Server	5
○ 3.4. Evidence of Breach	6
○ 3.5. Initial Entry Vector	6
○ 3.6. Malware Analysis	7
▪ 3.6.1. Malware Identification	7
▪ 3.6.2. Malicious Processes	9
▪ 3.6.3. IP Address Delivering the Payload	9
▪ 3.6.4. Malware Callback IP	9
▪ 3.6.5. Malware Location on Disk	10
▪ 3.6.6. First Appearance of Malware	11
▪ 3.6.7. Evidence of Movement	11
▪ 3.6.8. Malware Capabilities	12
▪ 3.6.9. Accessibility of the malware	13
▪ 3.6.10. Persistence Evidence	13
○ 3.7. Malicious IP Address Analysis	14
▪ 3.7.1. Malicious IP Addresses Involved	14
▪ 3.7.2. Connection to Adversary Infrastructure	14
▪ 3.7.3. Involvement in Other Attacks	15
○ 3.8. Data Access and Exfiltration	17
▪ 3.8.1. Did the Attacker Access Any Other Systems?	17
▪ 3.8.2. Did the Attacker Steal or Access Any Data?	17
▪ 3.8.3. When Was Data Accessed?	18
○ 3.9. Network Layout of the Victim Network	18
4. Optional Questions	19
○ 4.1. What Architecture Changes Should Be Made Immediately? ..	19
○ 4.2. Did the Attacker Steal the Szechuan Sauce?	19
○ 4.3. Did the Attacker Steal or Access Any Other Sensitive Files? ..	19
5. Recommendations	19
6. References	21

1. Executive Summary

This report presents the findings of an investigation into a cybersecurity breach described in **Case 001 – The Stolen Szechuan Sauce**. The breach involved the exploitation of the organization's network infrastructure, culminating in unauthorized access to sensitive data and malicious activity. Key findings include:

- **Initial Access Vector:** Exploitation of RDP vulnerabilities via IP address 194.61.24.102, a known adversary infrastructure.
- **Malware Used:** A malicious file, coreupdater.exe, delivered through HTTP, executed from C:\Windows\System32, and used for remote access and data exfiltration.
- **Network Impact:** Lateral movement was observed between the domain controller (CITADEL-DC01) and an endpoint device (DESKTOP-SDN1RPT).
- **Data Exfiltration:** Sensitive files from the "Secret" folder on the file share were accessed and exfiltrated.
- **Adversary Persistence:** The attacker installed persistence mechanisms via registry keys and services, ensuring control over compromised systems.

The investigation employed industry-standard digital forensic methodologies and tools, providing a comprehensive analysis of the breach. This report outlines the findings, associated evidence, and recommendations for strengthening the organization's cybersecurity posture to mitigate future threats.

2. Methodology

The investigation adhered to established digital forensic best practices, ensuring the integrity and reliability of findings. The steps included:

1. **Artifact Analysis:** Examined disk images, memory dumps, and registry files for malicious artifacts.
2. **Network Analysis:** Analyzed packet capture (PCAP) files to identify suspicious communication and malicious IP addresses.
3. **Timeline Correlation:** Created a detailed timeline of events to trace the attack progression and exfiltration activities.
4. **Malware Analysis:** Identified and analyzed malicious files to determine capabilities and adversary intent.
5. **Documentation:** Compiled findings with supporting evidence, including screenshots and detailed justifications.

Tools Used:

- **FTK Imager:** Disk imaging and file hash analysis. (AccessData, n.d.)
- **Wireshark:** Network traffic and packet analysis to trace malicious activity. (Wireshark User's Guide, n.d.)
- **Registry Explorer:** Analysis of registry hives for persistence mechanisms. (Eric Zimmerman Tools, n.d.)
- **VirusTotal:** Verification and classification of malware. (VirusTotal, n.d.)

- **Threat Intelligence Databases:** Cross-referenced malicious IP addresses and adversary activity. (AlienVault, n.d.)

This structured approach ensured a thorough investigation of the breach and provided actionable insights into its causes and impact.

3. Analysis and Findings

3.1. Operating System of the Server

Answer: Windows Server 2012 R2 Standard

Evidence & Process:

Using FTK Imager, the following steps were taken to identify the operating system of the server:

- Navigated to **DC01-E01 > Partition 2 > root > Windows > System32 > Licenses**.
- The license information retrieved from this path confirmed the operating system version as **Windows Server 2012 R2 Standard**.
- **Screenshot:** Below is the screenshot of the DC01-E01 Disc image opened using FTK Imager.



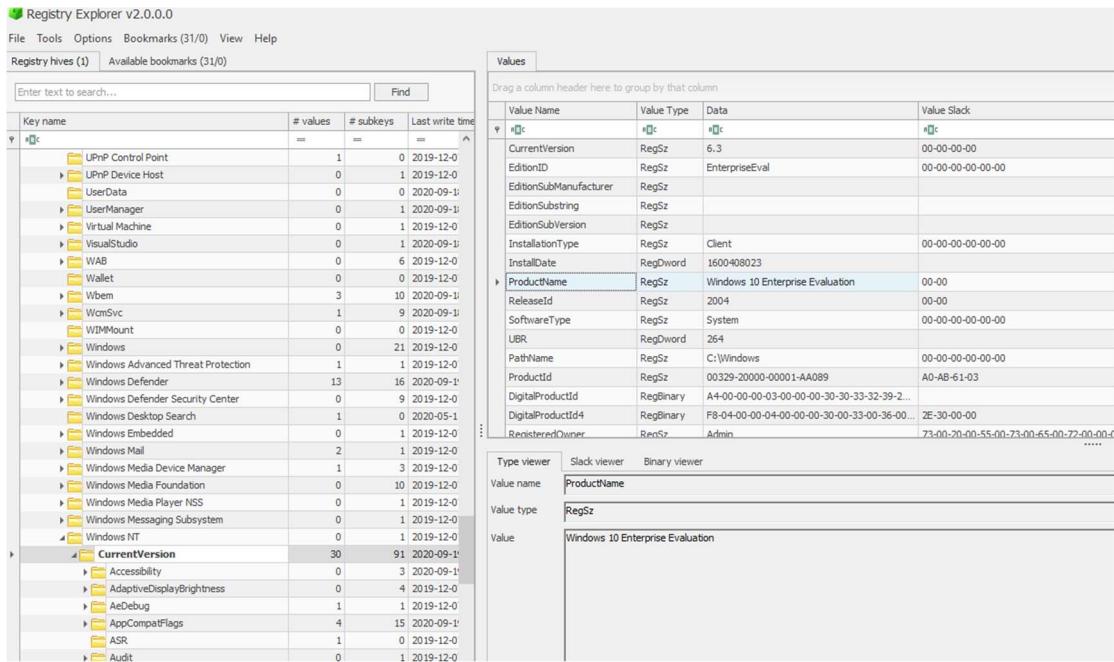
3.2. Operating System of the Desktop

Answer: Windows 10 Enterprise

Evidence & Process:

Using Registry Explorer, the following steps were taken to identify the operating system of the desktop:

- Navigated to **ROOT > Microsoft > Windows NT > CurrentVersion** in the registry.
- The registry details retrieved from this path confirmed the operating system version as **Windows 10 Enterprise**.
- **Screenshot:** Below is the screenshot of the DC01 Protected Files using Registry Explorer.



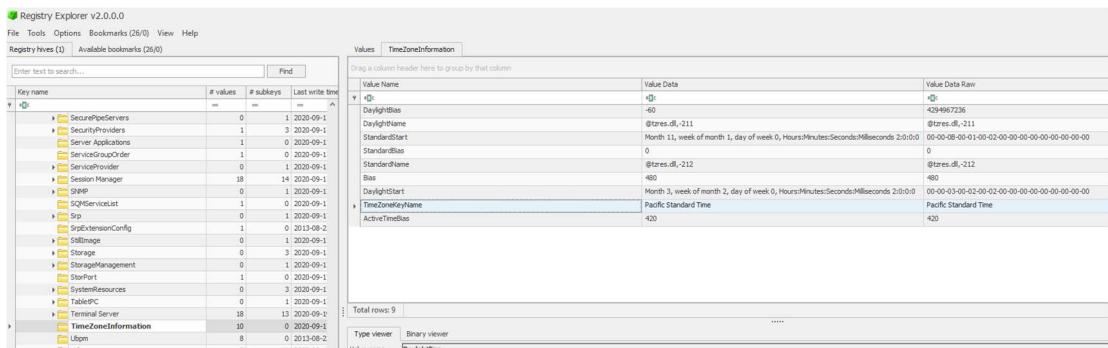
3.3. Local Time of the Server

Answer: Pacific Standard Time (UTC–08:00)

Evidence & Process:

To determine the local time zone of the server, the following steps were taken:

- Accessed the registry using **Registry Explorer** again.
- Navigated to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\TimeZoneInformation**.
- Found the **TimeZoneInformation** registry key, which confirmed the server's time zone setting as **Pacific Standard Time (UTC–08:00)**.
- Screenshot:** Below is the screenshot of the DC01 Protected Files using Registry Explorer.



Although the server is based in Colorado, which typically follows Mountain Standard Time (UTC–06:00), the time zone setting appears to be configured incorrectly, likely indicating a misconfiguration of the system's time zone on the server.

3.4. Evidence of Breach

- **Answer:** Yes, unauthorized access was detected.
- **Evidence & Process:**
 - Analysed PCAP file using Wireshark and found brute-force attempts.
 - Detected tampered files and irregular network activity on the disc memory.

3.5. Initial Entry Vector

Answer: Brute-force attack via TCP/IP communication

Evidence & Process:

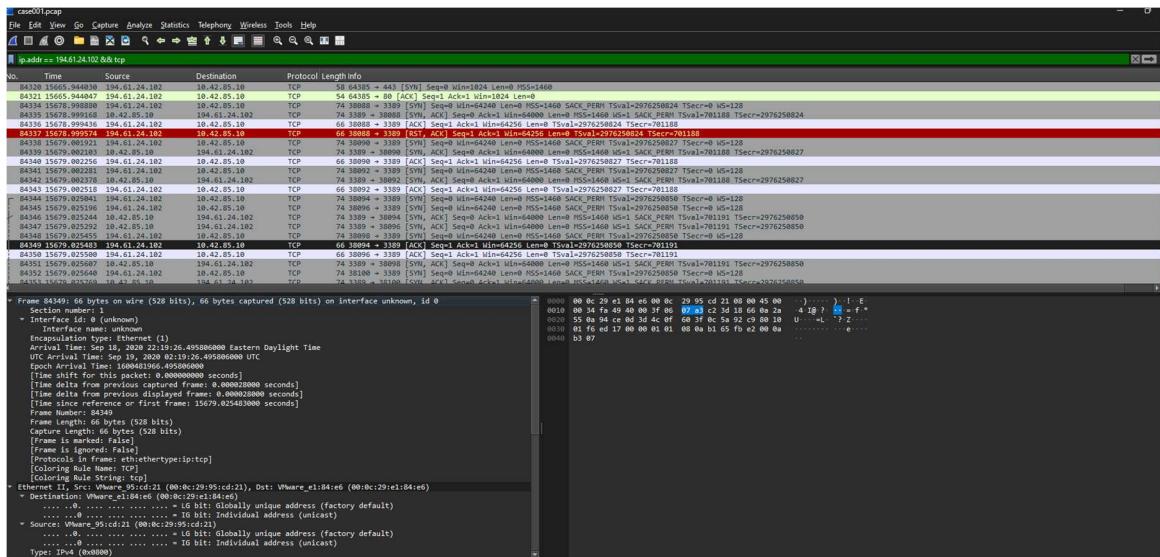
To identify the initial entry vector, the following steps were performed:

- Accessed the **SYSTEM registry hive** in the **ControlSet001\Services\Tcpip\Parameters\Interfaces** path to retrieve the server's IP address, which was **10.42.85.10**. Screenshot is provided bellow.

Value Name	Value Type	Data	Value Slack	Is Deleted
RegistrationEnabled	RegDword	1		
RegisterAdapterName	RegDword	0		
DhcpServer	RegDword	255.255.255.255	00-00-00-00	
Lease	RegDword	1800		
LeaseObtainedTime	RegDword	1600362219		
T1	RegDword	1600363119		
T2	RegDword	1600363794		
LeaseTerminatesTime	RegDword	1600364019		
AddressType	RegDword	0		
IsServerNapAware	RegDword	0		
DhcpConnForceBroadcastFlag	RegDword	0		
IpAddress	RegMultiSz	10.42.85.10	00-00	
SubnetMask	RegMultiSz	255.255.255.0	2E-00-30-00-00-00	
DefaultGateway	RegMultiSz	10.42.85.100		
DefaultGatewayMetric	RegMultiSz	0	00-00-00-00-00-00	

Type viewer Slack viewer Binary viewer
 Value name: **IpAddress**
 Value type: **RegMultiSz**
 Value: **10.42.85.10**

- Used **Wireshark** to filter traffic for the IP address **10.42.85.10** within the **case001.pcap** file.
- Noticed suspicious communication between the server and an external IP address, **194.61.24.102**.
- Applied a filter for **ip.addr == 194.61.24.102** and **tcp** to observe traffic patterns. The analysis revealed signs of a brute-force attack, with multiple SYN requests to the same port, indicating a possible attempt to exploit the system via a brute-force method.
- **Screenshot:** The screenshot of the Wireshark capture of the network traffic between the server and the potential malicious IP address **194.61.24.102** is provided bellow.

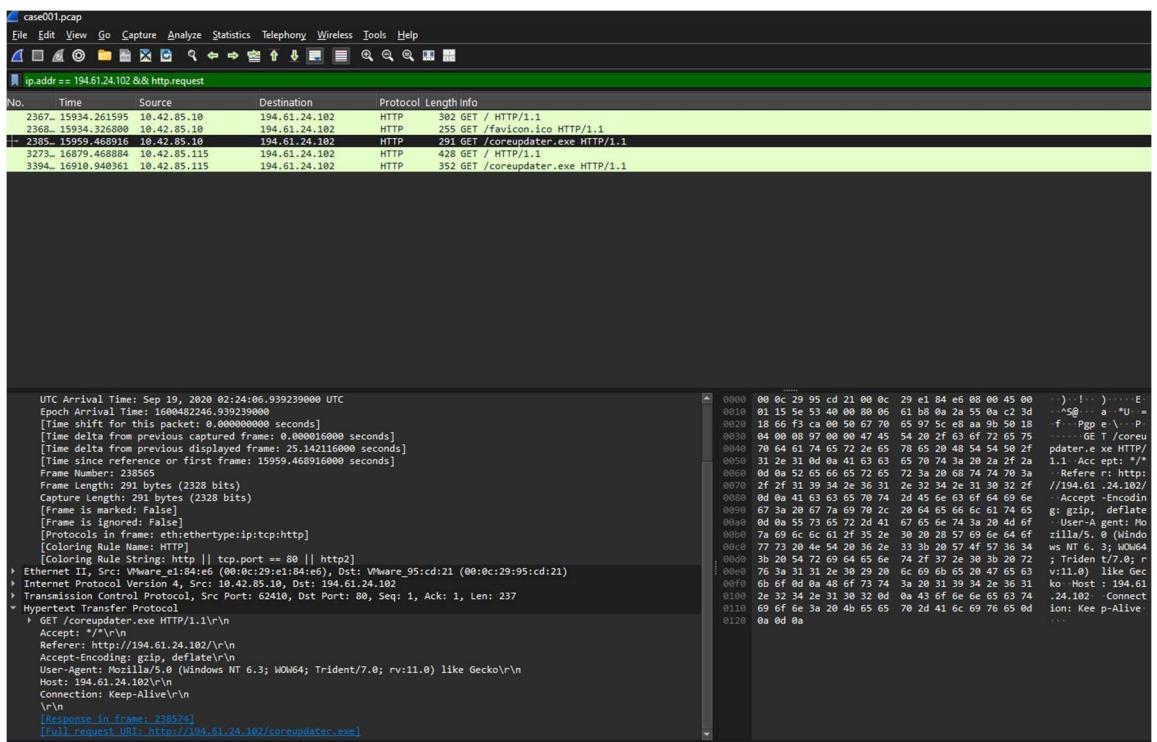


3.6. Malware Analysis

3.6.1. Malware Identification

Answer: CoreUpdater.exe (Malware confirmed as Meterpreter/Metasploit)
Evidence & Process:

- The suspicious file **coreupdater.exe** was delivered via an **HTTP GET request** from the IP address **194.61.24.102**, identified in the PCAP file using Wireshark with the filter `ip.addr == 194.61.24.102 && (http.request)`.



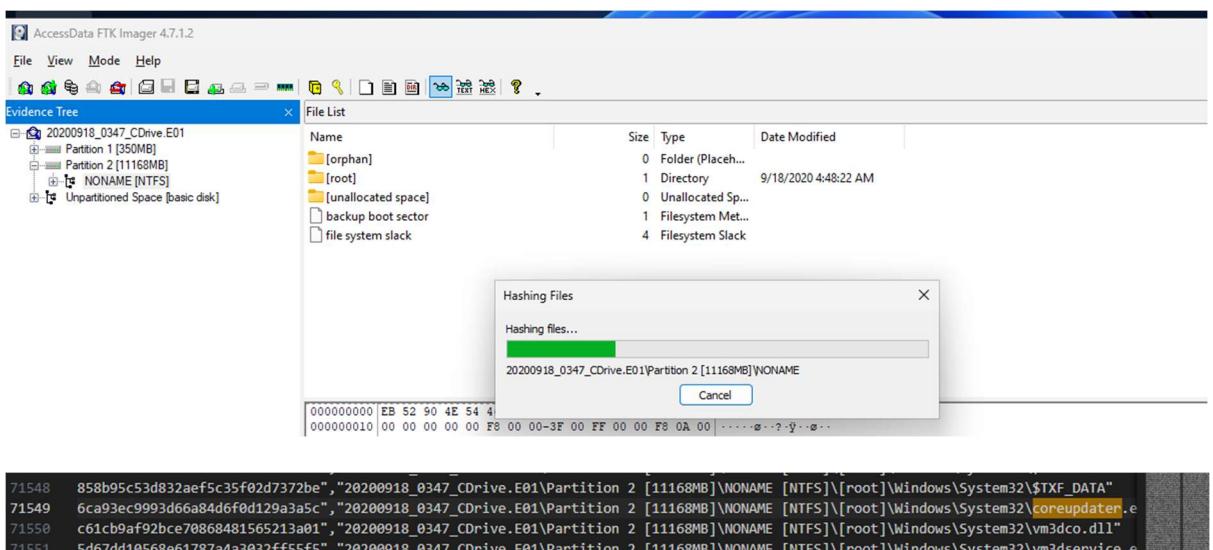
```

GET /coreupdater.exe HTTP/1.1
Accept: */*
Referer: http://194.61.24.102/
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko
Host: 194.61.24.102
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.18
Date: Sat, 19 Sep 2020 02:24:06 GMT
Content-type: application/x-msdos-program
Content-Length: 7168
Last-Modified: Fri, 18 Sep 2020 23:29:15 GMT

```

- The malware's hash was extracted using **FTK Imager** by computing the hash of all the files on the DC01 disc image and checking the hash of the file from the extracted hash list. Below are the screenshots of the process.



- The hash value in the above screenshot was checked against **VirusTotal**, which confirmed the file as a known malware payload, specifically linked to **Meterpreter/Metasploit**.

Community Score: 65 / 72

65/72 security vendors flagged this file as malicious

File: 10fb9002bb9846f7334161cf85d0b173081ff25ef8c27db125ea0c1cf5a6 coreupdater.exe

File Type: EXE

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

Threat categories: Benign, Malware, Exploit, Worm, Trojan, Backdoor, Rootkit, Adware, PUA, Ransomware, Spyware, Downloader, Botnet, Info stealer,勒索病毒, 恶意软件, 后门, 蠕虫, 木马, 勒索软件, 间谍软件, 下载器, 机器人, 信息窃取者, 勒索病毒, 恶意软件, 后门, 蠕虫, 木马, 勒索软件, 间谍软件, 下载器, 机器人, 信息窃取者

Popular threat label: Trojan.Shelma/metasploit

Threat categories: Benign, Malware, Exploit, Worm, Trojan, Backdoor, Rootkit, Adware, PUA, Ransomware, Spyware, Downloader, Botnet, Info stealer, 勒索病毒, 恶意软件, 后门, 蠕虫, 木马, 勒索软件, 间谍软件, 下载器, 机器人, 信息窃取者

Family labels: shelma, metasploit, rozema

Security vendors' analysis:

Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win32_Shelma.R/Gen!tr
Alibaba	Trojan/Win32/Shelma.2208092b	AICloud	Trojan.Win/Rozema.AD
AVG	Trojan.Metasploit.A	Anti-AVL	GrayWorm.Win32.Rozema.J
Arabit	Trojan.Metasploit.A	Avast	Win32-Metasploit!Encod.A [Tr]
AVG	Win32-Metasploit!Encod.A [Tr]	Avira (no cloud)	TB/CryptXPACK.Gen!7
BitDefender	Trojan.Metasploit.A	Bkav Pro	W32/ADetectedMalware
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	CTX	Fax.Trojan.Shelma
Cylance	Unsafe	Cynet	Malicious (Score: 100)

3.6.2. Malicious Process

Answer: coreupdater.exe

Evidence & Process:

- **coreupdater.exe** was identified as the malicious process.
- The process was confirmed by inspecting the file path on the server, where it was located in **C:\Windows\System32\coreupdater.exe**, after being moved from the Administrator's **Downloads** folder. The screenshot of the Registry Explorer capture of existence of the process on the DC01 Protected files.

Value Name	Value Type	Data	Value Slack	Is Deleted
Type	RegDword	16		
Start	RegDword	2		
ErrorControl	RegDword	1		
ImagePath	RegExpandSz	C:\Windows\System32\coreupdater.exe	00-00-00-00	
ObjectName	RegSz	LocalSystem	00-00-00-00	
DelayedAutoStart	RegDword	1		

3.6.3. IP Address Delivering the Payload

Answer: 194.61.24.102

Evidence & Process:

- The **IP address 194.61.24.102** was found to be the source of the HTTP request delivering **coreupdater.exe** to the server. This was identified using a display filter in **Wireshark** for ip.addr == 194.61.24.102 && (http.request).
- **Screenshot:** Wireshark capture showing the connection to 194.61.24.102.

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

3.6.4. Malware Callback IP

Answer: 203.78.103.109

Evidence & Process:

- Using **VirusTotal** and the **relations tab** for the IP addresses associated with **coreupdater.exe**, it was identified that the malware frequently contacted the IP **203.78.103.109**.
- **Screenshot:** VirusTotal relationship analysis and network traffic logs showing communication with 203.78.103.109. We also provide the screenshot of the evidence of the interaction between the above IP address and the Server on the PCAP file.

The screenshot shows the VirusShare analysis interface for a file identified by hash 10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6. The file is a coreupdater.exe file, which is a PE executable (PE32+). The analysis results show a high community score of 65/72, with 12 detections. The file was last analyzed 1 day ago. The interface includes tabs for DETECTION, DETAILS, RELATIONS, BEHAVIOR, and COMMUNITY (14+ members). A sidebar encourages joining the community. Below the main analysis area, there are sections for Contacted Domains (2) and Contacted IP addresses (29), each with tables showing domain/IP, detections, creation date, and registrar information. At the bottom, there is a network traffic analysis section titled 'ip.addr == 203.78.103.109' with a table of captured packets and a detailed packet dump.

3.6.5. Malware Location on Disk

Answer: C:\Windows\System32\coreupdater.exe
Evidence & Process:

- coreupdater.exe was located in C:\Windows\System32, as confirmed by Registry Explorer during the analysis of the DC01 Protected files of the server.

- Screenshot:** Registry Explorer showing the file path for **coreupdater.exe**.

The screenshot shows the Windows Registry Explorer interface. The left pane displays a tree view of registry keys under 'Registry hives (1)'. One key is expanded, showing subkeys like CngHwAssist, CompositeBus, COMSysApp, condrv, coreupdater, crypt32, and CryptSvc. The right pane is titled 'Values' and lists specific registry entries for the coreupdater key. The table has columns for Value Name, Value Type, Data, Value Slack, and Is Del.

Value Name	Value Type	Data	Value Slack	Is Del
Type	RegDword	16		
Start	RegDword	2		
ErrorControl	RegDword	1		
ImagePath	RegExpandSz	C:\Windows\System32\coreupdater.exe	00-00-00-00	
ObjectName	RegSz	LocalSystem	00-00-00-00	
DelayedAutoStart	RegDword	1		

3.6.6. First Appearance of Malware

Answer: 2024-11-10 at 02:24:07 UTC

Evidence & Process:

- The first appearance of **coreupdater.exe** was detected in the **Wireshark** capture, filtered with ip.addr == 194.61.24.102 && (http.request). The timestamp for the first HTTP GET request was **2024-11-10 at 02:24:07 UTC**.
- Screenshot:** Wireshark packet capture showing the first appearance of **coreupdater.exe**.

The screenshot shows a Wireshark capture window with the filter set to 'ip.addr == 194.61.24.102 && (http.request)'. The packet list pane shows several HTTP requests from 194.61.24.102 to 194.61.24.102. The details pane shows the first packet, which is a GET request for '/coreupdater.exe' with a timestamp of Sep 18, 2020 22:24:06.939239000 Eastern Daylight Time. The bytes pane shows the raw hex and ASCII data of the packet.

```

Frame 238565: 291 bytes on wire (2328 bits), 291 bytes captured (2328 bits) on interface unknown, id 0
  Section number: 1
  Interface id: 0 (unknown)
  Encapsulation type: Ethernet (1)
  Arrival Time: Sep 18, 2020 22:24:06.939239000 Eastern Daylight Time
  UTC Arrival Time: Sep 18, 2020 02:24:06.939239000 UTC
  Epoch Arrival Time: 1600482246.939239000
  [Time shift for this packet: 0.000000000 seconds]
  [Time delta from previous captured frame: 0.000016000 seconds]
  [Time delta from previous displayed frame: 25.142116000 seconds]
  [Time since reference or first frame: 15959.468916000 seconds]
  Frame Number: 238565

```

```

0000  00 0c 29 95 cd 21 00 0c 29 e1 84 e6 08 0
0010  01 15 5e 53 40 00 80 06 61 b8 0a 2a 55 0
0020  18 66 f3 ca 00 50 67 70 65 97 5c e8 aa 9
0030  04 00 08 97 00 00 47 45 54 28 2f 63 6f 7
0040  70 64 61 74 65 72 2e 65 78 65 20 48 54 5
0050  31 2e 31 0d 0a 41 63 63 65 70 74 3a 20 2
0060  0d 0a 52 65 66 65 72 65 72 3a 20 68 74 7
0070  2f 2f 31 39 34 2e 36 31 2e 32 34 2e 31 3
0080  0d 0a 41 63 63 65 70 74 2d 45 66 63 6f 6
0090  67 3a 20 67 7a 69 70 2c 20 64 65 66 6c 6
00a0  0d 0a 55 73 65 72 2d 41 67 65 66 74 3a 2
00b0  7a 69 6c 66 61 2f 35 2e 30 28 28 57 69 6

```

3.6.7. Evidence of Movement

Answer: Moved from Downloads to C:\Windows\System32

Evidence & Process:

- The file **coreupdater.exe** was initially found in the **Downloads** folder of the Administrator account and later moved to **C:\Windows\System32**, indicating an attempt to hide and ensure persistence.
- Screenshot:** File path analysis and logs showing movement from **Downloads** to **C:\Windows\System32**.

Value Name	Value Type	Data	Value Slack	Is Deleted
Type	RegDword	16		
Start	RegDword	2		
ErrorControl	RegDword	1		
ImagePath	RegExpandSz	C:\Windows\System32\coreupdater.exe	00-00-00-00	
ObjectName	RegSz	LocalSystem	00-00-00-00	
DelayedAutostart	RegDword	1		

3.6.8. Malware Capabilities

Answer: Data exfiltration, remote control, lateral movement, propagation, and destruction
Evidence & Process:

- The malware **coreupdater.exe** is linked to **Meterpreter/Metasploit**, a tool known for providing remote access to attackers.
- Based on the Windows analysis report of the **coreupdater.exe** (Joe Sandbox Cloud, n.d.), the malware's capabilities include:
 - Exfiltration of sensitive data**, including credentials and proprietary information.
 - Remote control**, allowing attackers to control the compromised system.
 - Lateral movement**, enabling attackers to pivot to other devices on the network.
 - Propagation**, spreading to other systems within the network.
 - Destruction**, in cases where attackers may corrupt or delete system files.
- Screenshot:** VirusTotal report summarizing capabilities of **coreupdater.exe** (Meterpreter/Metasploit).

joesecurity
9 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?idtype=analysisid>

3.6.9. Accessibility of the Malware

The malware, identified as a payload delivered via Metasploit, is highly accessible. Metasploit is an open-source red teaming tool, widely available for both legitimate and malicious purposes. Online research and VirusTotal analysis confirm its prevalence and ease of use for attackers.

3.6.10. Persistence Evidence

Answer: Yes, the malware was installed with persistence on both the server and the desktop by creating a registry entry and registering as a service.

Evidence & Process:

- The malware established persistence by creating a registry entry under HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services to ensure it runs at startup.
- Using Registry Explorer, we located the registry entries for both the server and the desktop, confirming the malware's persistence configuration under ControlSet001\Services.
- **When:**
 - Server: 2020-09-19 3:27:49 UTC
 - Desktop: 2020-09-19 3:42:42 UTC
- **Where:**
 - Persistence was established in the Windows Registry and configured to run as a service.
- **Screenshot:** Both DC01 and Desktop Registry entries showing the persistence configuration for coreupdater.exe on both systems at the time mentioned above.

Value Name	Value Type	Data	Value Slack	Is Deleted
Type	RegDword	16		
Start	RegDword	2		
ErrorControl	RegDword	1		
ImagePath	RegExpandSz	C:\Windows\System32\coreupdater.exe	00-00-00-00	
ObjectName	RegSz	LocalSystem	00-00-00-00	
DelayedAutoStart	RegDword	1		

Value Name	Value Type	Data	Value Slack	Is Deleted
Type	RegDword	16		
Start	RegDword	2		
ErrorControl	RegDword	1		
ImagePath	RegExpandSz	C:\Windows\System32\coreupd...	62-00-62-00	
ObjectName	RegSz	LocalSystem	53-00-74-00	
DelayedAutoStart	RegDword	1		

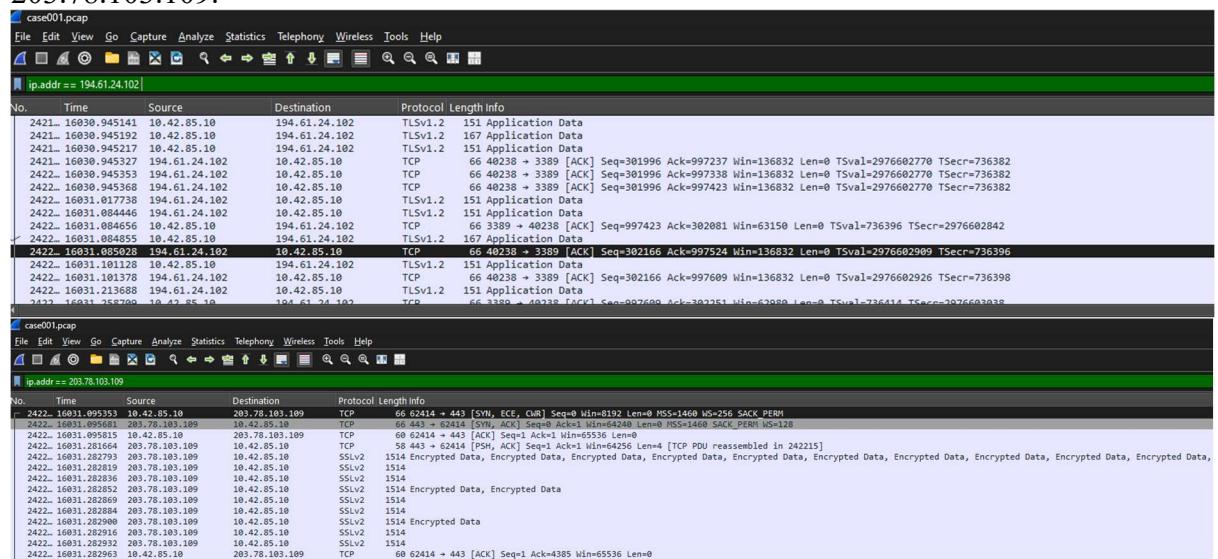
3.7. Malicious IP Address Analysis

3.7.1. Malicious IP Addresses Involved

Answer: 194.61.24.102 and 203.78.103.109

Evidence & Process:

- **IP Address 194.61.24.102** was identified as delivering the malicious payload **coreupdater.exe** via an HTTP GET request.
- This IP has a history of involvement in **RDP brute force attacks** and is associated with the exploitation of vulnerabilities **CVE-2017-9805**, **CVE-2017-5638**, and **CVE-2014-6271** (NIST, n.d.).
- **IP Address 203.78.103.109** was flagged in **AlienVault** as linked to **Meterpreter**, indicating its use as a command-and-control (C2) server.
- **Screenshot:** Wireshark traffic showing communication with 194.61.24.102 and 203.78.103.109.



3.7.2. Connection to Adversary Infrastructure

Answer: Confirmed involvement in known adversary infrastructure.

Evidence & Process:

- **194.61.24.102** is associated with known adversary infrastructure due to its frequent use in RDP brute force attacks and exploitation of historical vulnerabilities. Here is

the screenshot from AlienVault.

The screenshot shows the AlienVault OTX interface for the IP address 194.61.24.102. The top navigation bar includes LevelBlue/Labs, Browse, Scan Endpoints, Create Pulse, Submit Sample, API Integration, and a search bar set to 194.61.24.102. Below the navigation is a summary section with counts for Pulses (31), Passive DNS (0), URLs (0), and Files (0). The main content area is titled 'Analysis Overview' and contains two tables of data. The left table includes columns for Location (Russian Federation), ASN (ASNone), Related Pulses (OTX User-Created Pulses (31)), and Related Tags (9 Related Tags: Nextray, cyber security, ioc, phishing, malicious). The right table includes columns for Indicator Facts (Historical OTX telemetry, IP mentioned on Twitter, Running SSH), Open Ports (2 Open Ports: 22, 53), Exploited CVEs (All Time: 2017-9805, 2017-5638, 2014-6271), and External Resources (Whois, VirusTotal).

- 203.78.103.109 is flagged as an active C2 server for **Meterpreter**, corroborated by **AlienVault threat intelligence**.

The screenshot shows the AlienVault OTX interface for the IP address 203.78.103.109. The top navigation bar includes LevelBlue/Labs, Browse, Scan Endpoints, Create Pulse, Submit Sample, API Integration, and a search bar set to 203.78.103.109. Below the navigation is a summary section with counts for Pulses (0), Passive DNS (14), URLs (7), and Files (4). The main content area is titled 'Analysis Overview' and contains two tables of data. The left table includes columns for Location (Thailand), ASN (AS18362 netway communication co. ltd.), DNS Resolutions (14 Domains), Top Level Domains (2 Unique TLDs), Related Pulses (None), and Related Tags (None). The right table includes columns for Indicator Facts (IP mentioned on Twitter, 14 domains resolved in all time, 2 top-level domains), Antivirus Detections (Trojan:Win64/Meterpreter.E, TrojanDropper:PowerShell/Ploty.C), AV Detection Ratio (4 / 4), and External Resources (Whois, VirusTotal).

3.7.3. Involvement in Other Attacks

Answer: Yes, both IPs were involved in other attacks during the time of this incident.

Evidence & Process:

- Threat intelligence data indicates both 194.61.24.102 and 203.78.103.109 were part of other malicious activities and cyberattacks around the time of this incident.
- **Screenshot:** Here are the screenshots of search results associated to these two IPs from AlienVault(AlienVault, n.d.) that shows both the IP address were flagged as malicious during the time of the attack.

otx.alienvault.com/indicator/ip/194.61.24.102

LevelBlue/Labs Browse Scan Endpoints Create Pulse Submit Sample API Integration All ▾ 194.61.24.102 X Search Login | Sign Up

IPv4
194.61.24.102 Add to Pulse +

Pulses	Passive DNS	URLs	Files
31	0	0	0

Analysis Overview

Location	Russian Federation	Indicator Facts	Historical OTX telemetry, IP mentioned on Twitter, Running SSH
ASN	ASNone	Open Ports	2 Open Ports 22, 53
Related Pulses	OTX User-Created Pulses (31)	Exploited CVEs	All Time: 2017-9805, 2017-5638, 2014-6271
Related Tags	9 Related Tags Nextray, cyber security, ioc, phishing, malicious More	External Resources	Whois , VirusTotal

otx.alienvault.com/indicator/ip/203.78.103.109

LevelBlue/Labs Browse Scan Endpoints Create Pulse Submit Sample API Integration All ▾ 203.78.103.109 X Search Login | Sign Up

IPv4
203.78.103.109 Add to Pulse + Submit URL Analysis

Pulses	Passive DNS	URLs	Files
0	14	7	4

Analysis Overview

Location	Thailand	Indicator Facts	IP mentioned on Twitter, 14 domains resolved in all time, 2 top-level domains
ASN	AS18362 netway communication co. ltd.	Antivirus Detections	Trojan:Win64/Meterpreter.E, TrojanDropper:PowerShell/Ploty.C
DNS Resolutions	14 Domains	AV Detection Ratio	4 / 4
Top Level Domains	2 Unique TLDs	External Resources	Whois , VirusTotal
Related Pulses	None		
Related Tags	None		

otx.alienvault.com/indicator/ip/203.78.103.109

LevelBlue/Labs Browse Scan Endpoints Create Pulse Submit Sample API Integration All ▾ 203.78.103.109 X Search Login

IPv4
203.78.103.109 Add to Pulse + Submit URL Analysis

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	ns1.happydoghappycat-th.com	A	203.78.103.109	2020-10-26 06:16	2020-10-26 06:16	AS18362 netway communication co. ltd.	Thailand
Unknown	ns2.happydoghappycat-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	pppethome.com	A	203.78.103.109	2020-08-21 08:51	2022-02-22 09:17	AS18362 netway communication co. ltd.	Thailand
Unknown	petmall1999.com	A	203.78.103.109	2020-08-21 08:50	2022-04-23 09:51	AS18362 netway communication co. ltd.	Thailand

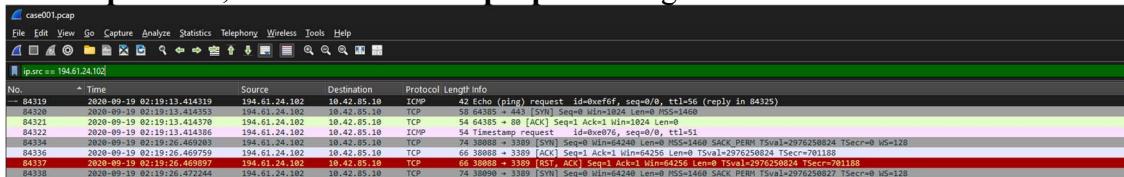
3.8. Data Access and Exfiltration

3.8.1. Did the Attacker Access Any Other Systems?

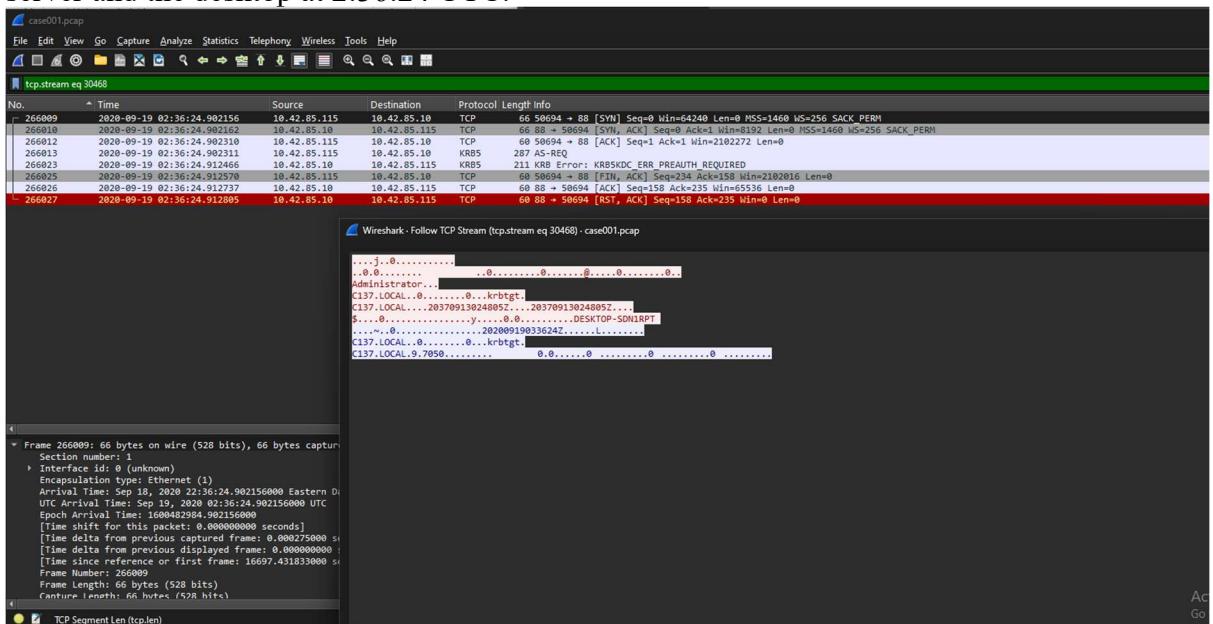
Answer: Yes, the attacker accessed the desktop system **C137\DESKTOP-SDN1RPT\$** from the Domain Controller (DC).

Evidence & Process:

- The first contact with the malicious IP **194.61.24.102** occurred at **2:19:13 UTC on 19th September**, as identified in the **pcap** file using Wireshark.



- Shortly afterward, the Domain Controller established communication with **10.42.85.115**, the desktop system, via **Remote Desktop Protocol (RDP)**. Below screenshot of Wireshark session showing RDP communication between the domain server and the desktop at 2:36:24 UTC.



- The attacker utilized the **Administrator account** to gain RDP access to the desktop soon after the server was compromised.

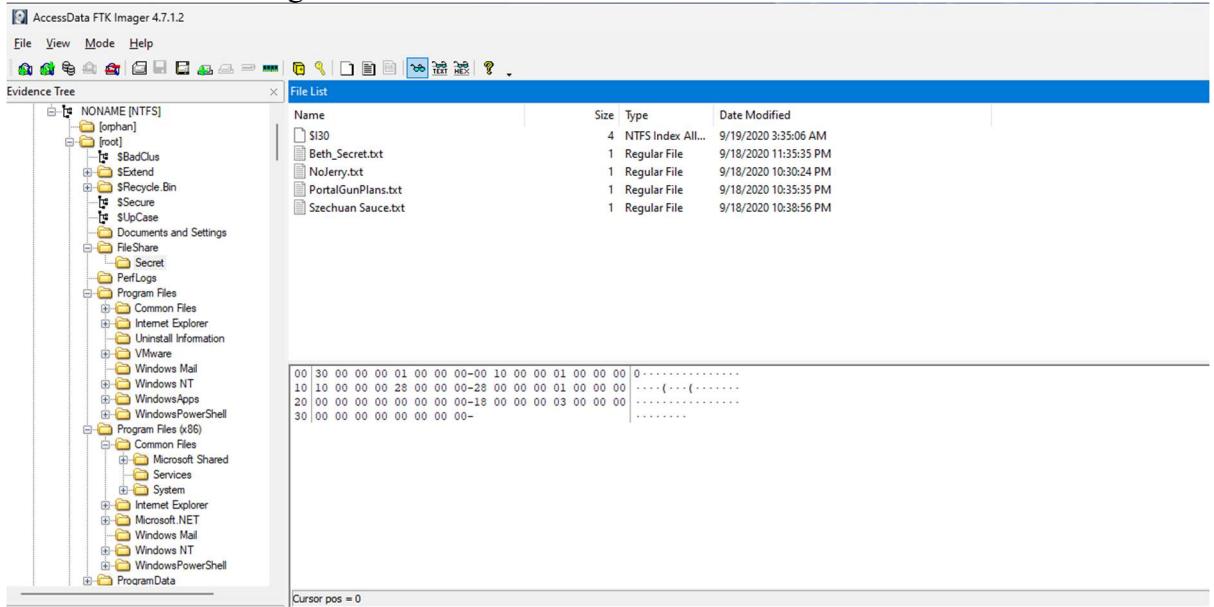
3.8.2. Did the Attacker Steal or Access Any Data?

Answer: Yes, the attacker accessed and interacted with sensitive data in the "Secret" folder.

Evidence & Process:

- Using **FTK Imager**, it was confirmed that the Administrator account recently interacted with all the files located in the "**Secret**" folder within the file share.

- This activity occurred around **2:30 AM UTC** on **19th September**, indicating access to sensitive data before the exfiltration attempt.
- **Screenshot:** FTK Imager metadata showing recent file access in the "Secret" folder on the server disc image.



3.8.3. When Was Data Accessed?

Answer: Sensitive data was accessed at approximately **2:30 AM UTC** on **19th September**, shortly after the attacker gained RDP access to the desktop system.

This timeline shows that the attacker successfully accessed the system, interacted with sensitive files, and likely prepared them for exfiltration.

3.9. Network Layout of the Victim Network

Answer: The victim's network consisted of a Domain Controller (DC) and an endpoint device:

- **Domain:** C137 (IP range: 10.42.85.0/24)
- **Endpoint Device:** DESKTOP-SDN1RPT (IP: 10.42.85.10)
- **Domain Controller:** CITADEL-DC01 (IP: 10.42.85.115)

Evidence & Process:

- The network layout was derived by analyzing the IP address ranges and hostnames from the **pcap file** using **Wireshark**.
- Key devices in the network were identified through traffic analysis and cross-referencing hostnames and IP addresses.

- Screenshot:** Annotated Wireshark capture showing network activity and identified devices.

No.	Time	Source	Destination	Protocol	Length	Info
17	3.001453	10.42.85.10	224.0.0.22	IGMPv3	60	Membership Report / Leave group 224.0.0.252
19	3.002639	10.42.85.10	224.0.0.22	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
21	3.0083107	10.42.85.10	224.0.0.252	LLNLR	72	Standard query 0x8085 ANY CITADEL-DC01
22	3.078483	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
23	3.078496	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
24	3.078504	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
27	3.421777	10.42.85.10	224.0.0.252	LLNLR	72	Standard query 0x8085 ANY CITADEL-DC01
28	3.499936	10.42.85.10	224.0.0.252	IGMPv3	60	Membership Report / Join group 224.0.0.252 for any sources
30	3.827865	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
31	3.827890	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
32	3.827948	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
34	4.620124	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
35	4.620129	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
36	4.620141	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
38	5.385824	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
39	5.385845	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
40	5.385848	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
43	11.741375	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<2>
44	12.5080775	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<2>
45	13.266246	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<2>
46	14.201999	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<2>
47	14.772156	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<2>
48	14.780593	10.42.85.10	10.42.85.255	BROWSER	243	Host Announcement CITADEL-DC01, Workstation, Server, Domain Controller, NT Workstation, DFS server
49	15.227798	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
50	15.227807	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
51	17.070822	10.42.85.10	10.42.85.255	NBNS	110	Registration NB CITADEL-DC01<0>
57	18.337392	10.42.85.10	10.42.85.255	BROWSER	243	Host Announcement CITADEL-DC01, Workstation, Server, Domain Controller, Time Source, NT Workstation, DFS server
58	30.561628	10.42.85.10	10.42.85.255	NBNS	92	Name query NB UPnD<0>
59	30.561632	10.42.85.10	10.42.85.255	NBNS	92	Name query NB UPnD<0>
61	30.562390	10.42.85.10	224.0.0.252	LLNLR	66	Standard query 0x8085 A isatap
62	30.562481	10.42.85.10	10.42.85.255	NBNS	92	Name query NB ISATAP<0>
64	30.562519	10.42.85.10	10.42.85.255	LLNLR	66	Standard query 0x8085 A isatap
65	30.562555	10.42.85.10	10.42.85.255	NBNS	92	Name query NB ISATAP<0>
67	30.563093	10.42.85.10	224.0.0.252	LLNLR	64	Standard query 0xc212 AAAA wpad
69	30.563268	10.42.85.10	224.0.0.252	LLNLR	64	Standard query 0x4797 AAAA wpad
71	30.564295	10.42.85.10	224.0.0.252	LLNLR	66	Standard query 0x7e10 A isatap
73	30.568048	10.42.85.10	224.0.0.252	LLNLR	66	Standard query 0x8085 A isatap
76	30.998973	10.42.85.10	224.0.0.252	LLNLR	64	Standard query 0x210 A wpad

This layout highlights the minimal structure of the network, with a single DC and one desktop endpoint device, emphasizing the attack's impact on a compact infrastructure.

4. Optional Questions

4.1. What architectural changes should be made immediately?

- Answer:** RDP access should be moved behind a VPN, and direct RDP access to the Domain Controller from the internet should be disabled immediately.

4.2. Did the attacker steal the Szechuan Sauce?

- Answer:** Yes, the Szechuan Sauce was stolen at approximately 02:30 UTC on 19 September 2020. We get these details by looking into the file-sharing folder in the server disc image via FTK Imager.

4.3. Did the attacker steal or access any other sensitive files?

- Answer:** Beth's secrets were accessed and manipulated around 03:35 UTC on 19 September 2020. This is also noticed in the server disc image.

5. Recommendations

1. Patch RDP Vulnerabilities and Disable Direct RDP Access to Critical Systems

- Ensure all systems are updated with the latest security patches (Microsoft, 2019) to mitigate vulnerabilities such as BlueKeep (NIST, n.d. | CVE-2019-0708).
- Disable RDP entirely for systems that do not require remote access. For critical systems where RDP is necessary, implement stringent access controls.

2. Lock Down RDP Port (3389) Access

- Configure secure tunneling solutions, such as Cloudflare Tunnel, to block unauthorized requests to port 3389 (Cloudflare, n.d.).

- Implement strict firewall rules to allow RDP traffic only from allowlisted IP ranges or through authenticated secure tunnels.
- 3. Strengthen Authentication for RDP Connections**
- Require the use of strong, unique passwords for all RDP sessions (Cloudflare, n.d.).
 - Implement single sign-on (SSO) solutions that enforce robust password policies and multi-factor authentication (MFA) for RDP access.
- 4. Move RDP Access Behind a Secure VPN or Zero Trust Architecture**
- Use a secure VPN for remote access to internal systems. Alternatively, adopt a Zero Trust model that authenticates users and devices before granting access to RDP.
- 5. Implement Network Segmentation to Isolate Sensitive Systems**
- Segment networks to restrict RDP access only to specific systems required for operational purposes. Sensitive systems should remain isolated and accessible only through secure channels.
- 6. Deploy Advanced Endpoint Detection and Response (EDR) Solutions**
- Utilize advanced EDR tools to monitor for malicious activity on endpoints, focusing on detecting unauthorized RDP use or brute force attempts.
- 7. Provide Training and Awareness on RDP Security Best Practices**
- Educate employees on the risks associated with RDP, emphasizing secure credential practices and the importance of reporting unusual activity.

These recommendations address both the immediate threats posed by RDP vulnerabilities and the underlying structural weaknesses in access management and network configuration.

6. References

1. AccessData. (n.d.). Forensic Toolkit user guide. Retrieved from https://www.exterro.com/uploads/documents/FTK_7.4.2_UG.pdf
2. AlienVault. (n.d.). Domain: ip-lookup.net. LevelBlue Open Threat Exchange. Retrieved from <https://otx.alienvault.com/indicator/domain/ip-lookup.net>
3. Cloudflare. (n.d.). What are the security risks of RDP? Retrieved from <https://www.cloudflare.com/learning/access-management/rdp-security-risks/>
4. Eric Zimmerman Tools. (n.d.). Registry Explorer. Retrieved from <https://ericzimmerman.github.io/#!index.md>
5. Joe Sandbox Cloud. (n.d.). Windows analysis report: coreupdater.exe. Retrieved from <https://www.joesandbox.com/analysis/1391302/0/html>
6. Microsoft. (2019, May 14). Customer guidance for CVE-2019-0708: Remote desktop services remote code execution vulnerability. Retrieved from <https://support.microsoft.com/en-us/topic/customer-guidance-for-cve-2019-0708-remote-desktop-services-remote-code-execution-vulnerability-may-14-2019-0624e35b-5f5d-6da7-632c-27066a79262e>
7. National Institute of Standards and Technology (NIST). (n.d.). National vulnerability database. Retrieved from <https://nvd.nist.gov/vuln>
8. VirusTotal. (n.d.). VirusTotal. Retrieved from <https://www.virustotal.com/gui/home/search>
9. Wireshark Foundation. (n.d.). Wireshark user's guide. Retrieved from https://www.wireshark.org/docs/wsug_html/