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

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.

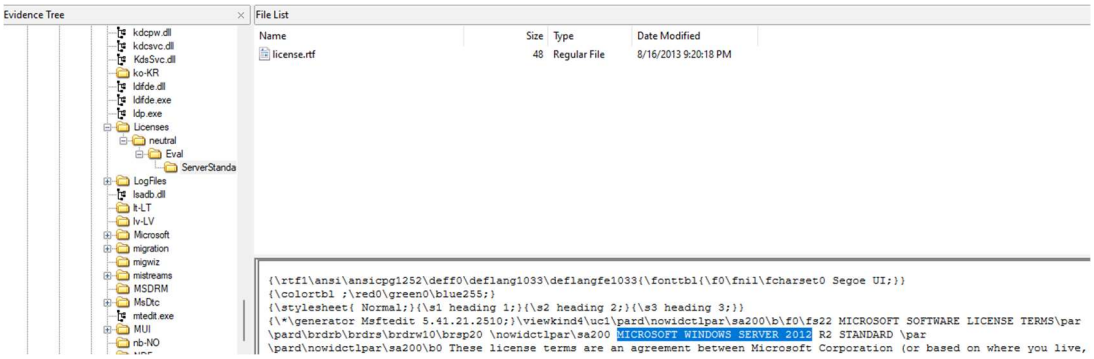
3. Analysis and Findings

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**: Bellow is the screenshot of the DC01-E01 Disc image opened using FTK Imager.

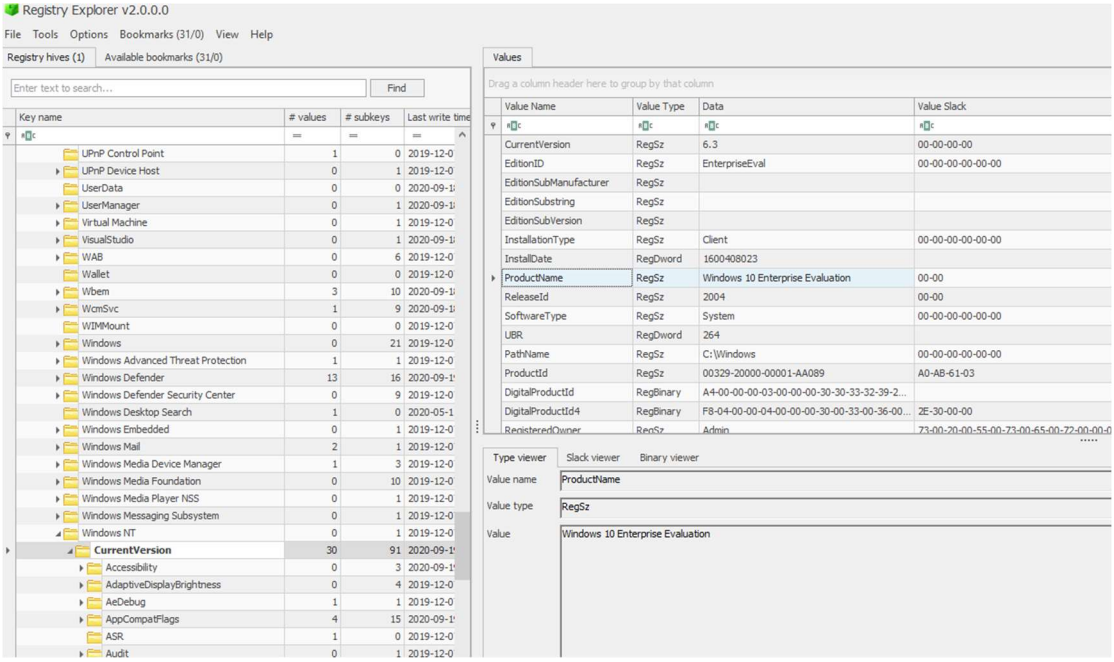


3.2. Operating System of the Desktop

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:** Bellow is the screenshot of the DC01 Protected Files using Registry Explorer.

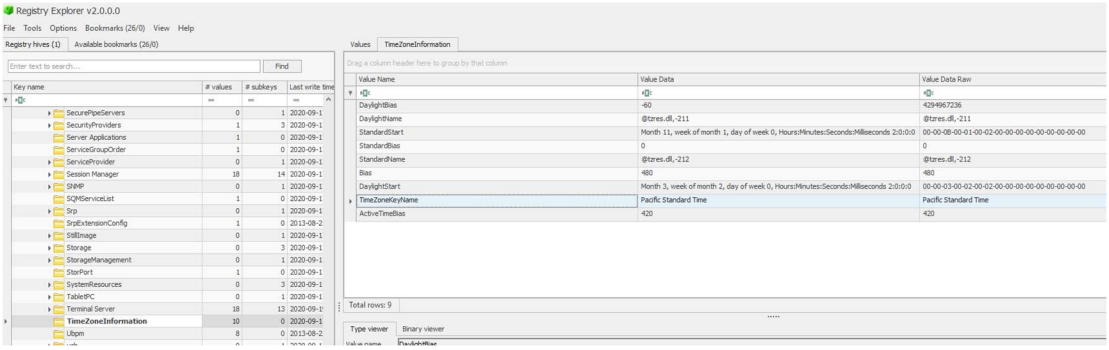


3.3. Local Time of the Server

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**: Bellow 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

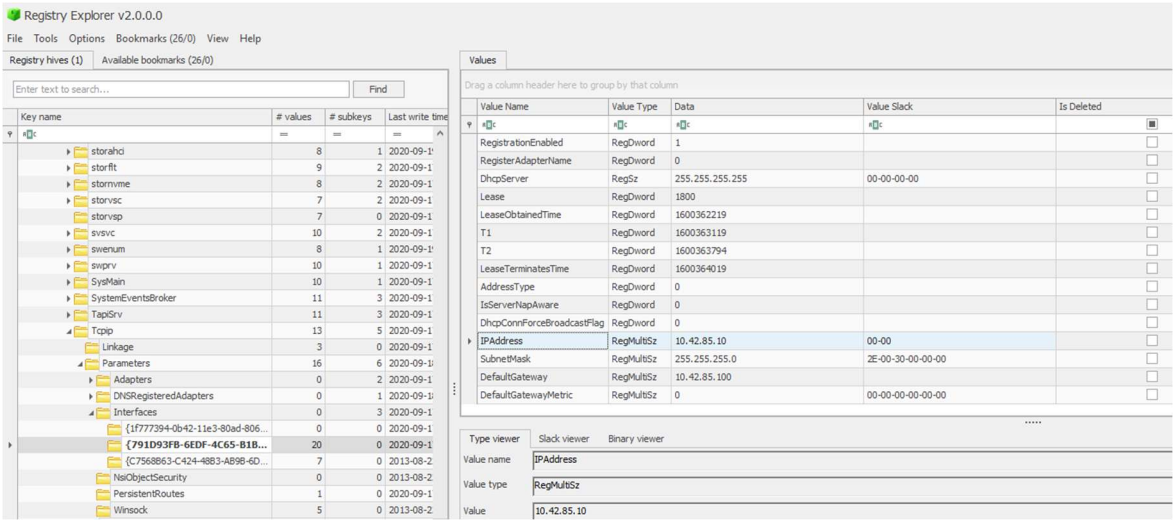
- **Answer:** Yes, unauthorized access was detected.
- **Evidence & Process:**
  - Analysed PCAP file using Wireshark and found brute-force attempts.
  - Detected tampered files and irregular network activity on the disc memory.

3.5. Initial Entry Vector

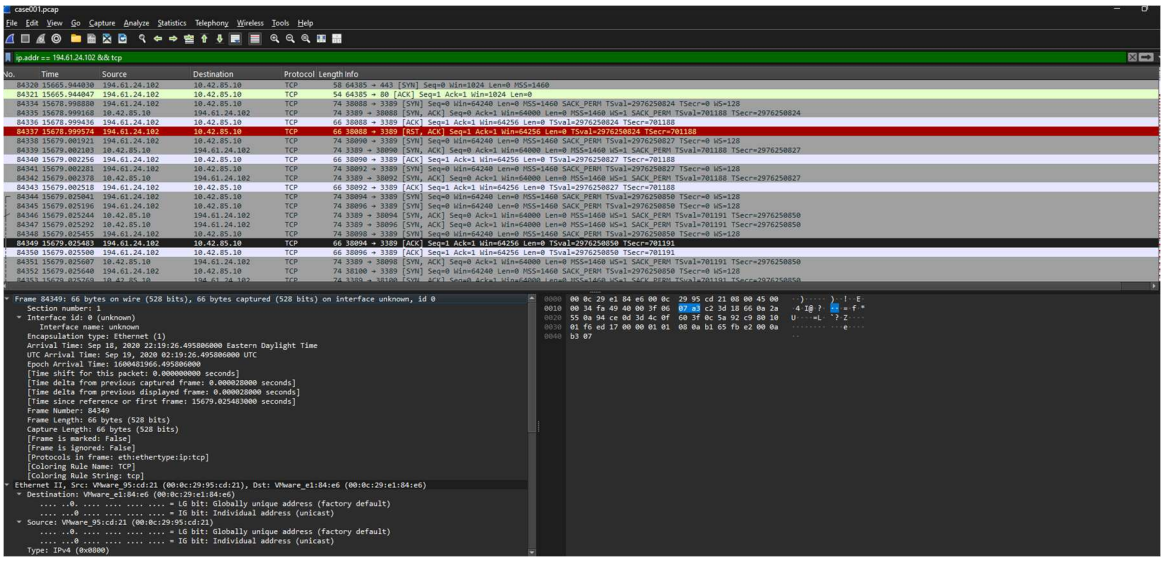
Answer: Brute-force attack via TCP/IP communication

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.



- 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.

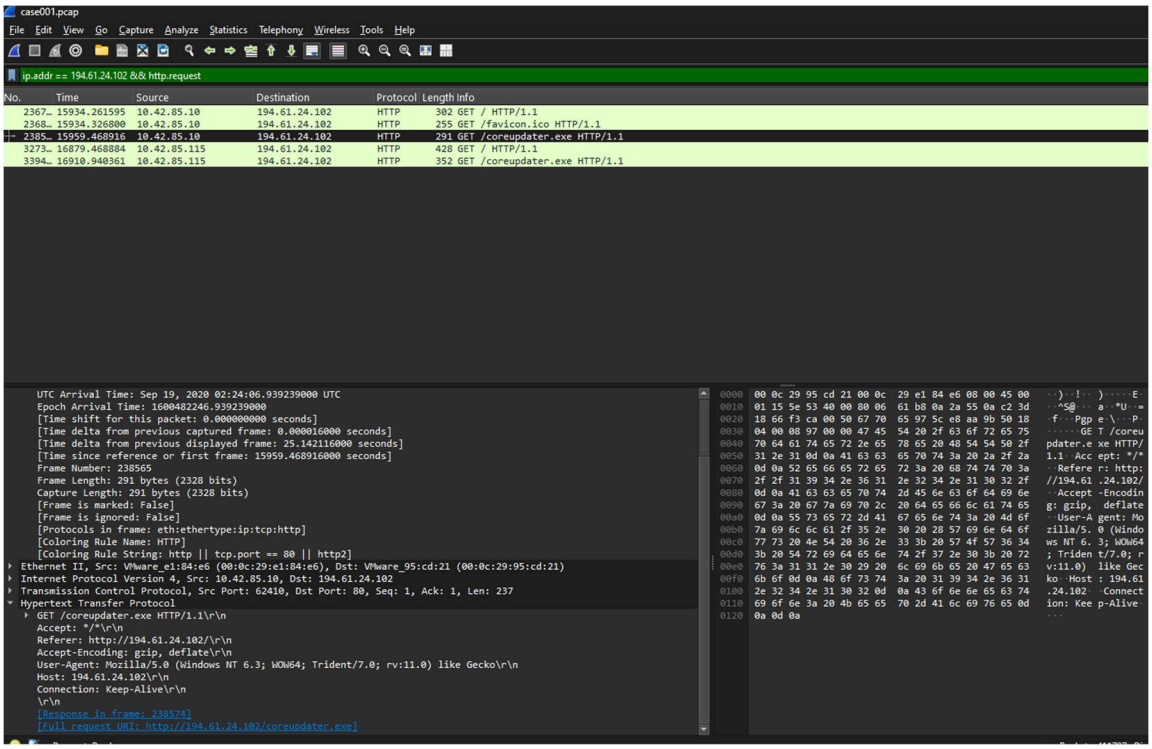


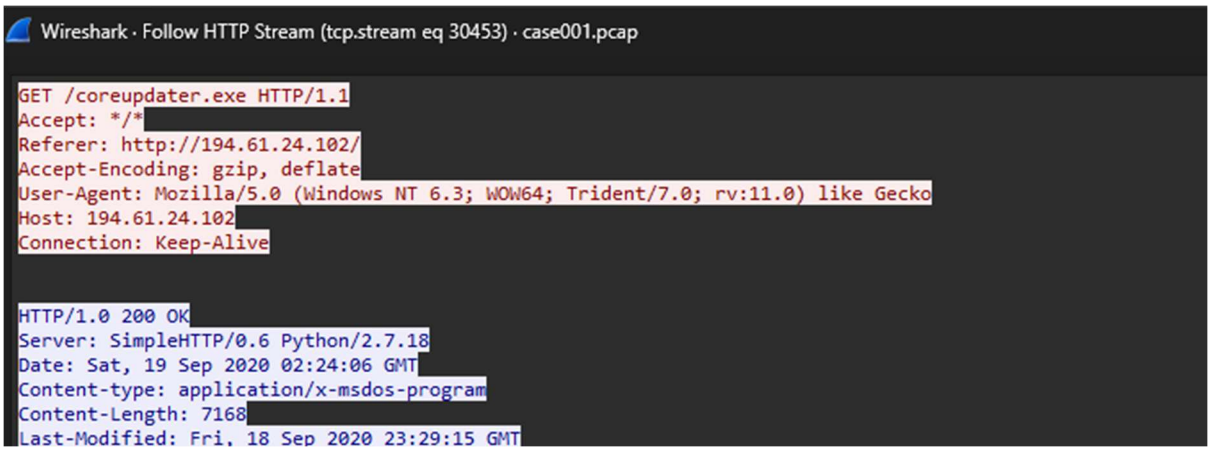
3.6. Malware Analysis

3.6.1. Malware Identification

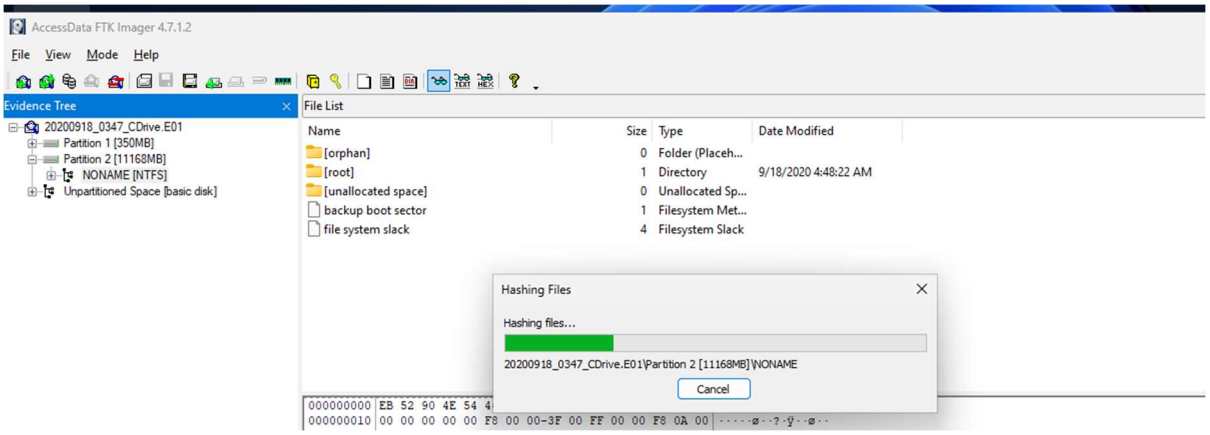
Answer: CoreUpdater.exe (Malware confirmed as Meterpreter/Metasploit)
Evidence & Process:

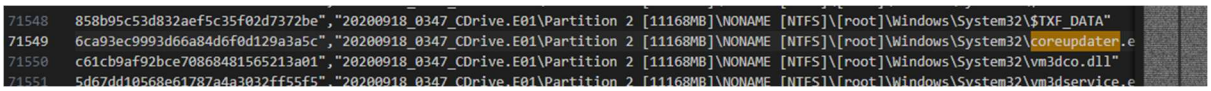
- The suspicious file **coreupdater.exe** was delivered via an **HTTP GET request** from the IP address **194.61.24.102**, identified in the PCAP file using Wireshark with the filter ip.addr == 194.61.24.102 && (http.request).



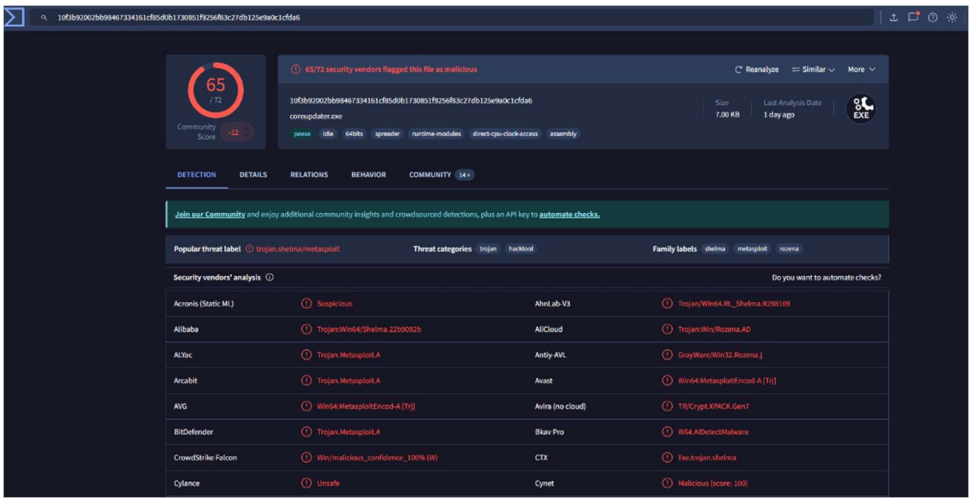


- The malware's hash was extracted using **FTK Imager** by computing the hash of all the files on the DC01 disc image and checking the hash of the file from the extracted hash list. Bellow are the screenshots of the process.





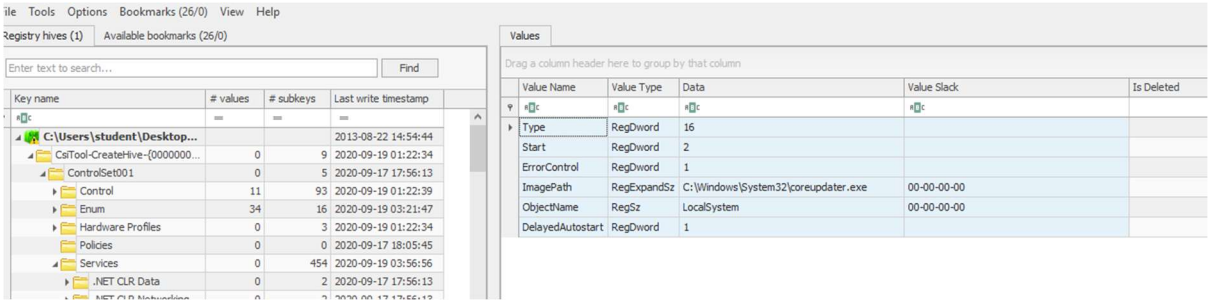
- The hash value in the above screenshot was checked against **VirusTotal**, which confirmed the file as a known malware payload, specifically linked to **Meterpreter/Metasploit**.



3.6.2. Malicious Process

Answer: coreupdater.exe
Evidence & Process:

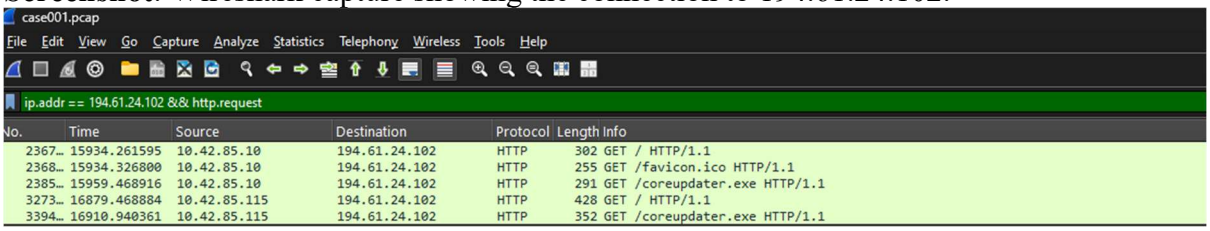
- **coreupdater.exe** was identified as the malicious process.
- The process was confirmed by inspecting the file path on the server, where it was located in **C:\Windows\System32\coreupdater.exe**, after being moved from the Administrator's **Downloads** folder. The screenshot of the Registry Explorer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



3.6.3. IP Address Delivering the Payload

Answer: 194.61.24.102
Evidence & Process:

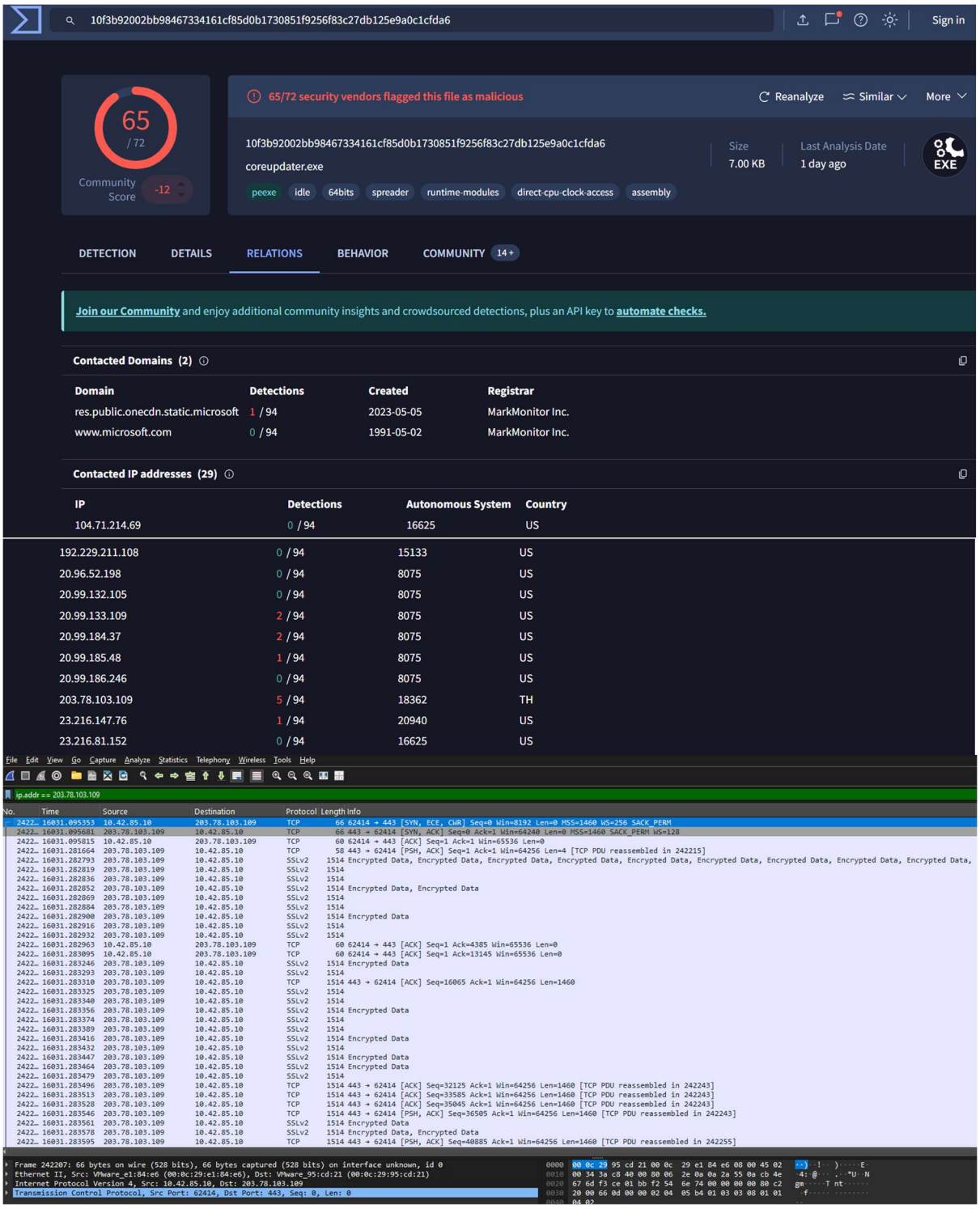
- The **IP address 194.61.24.102** was found to be the source of the HTTP request delivering **coreupdater.exe** to the server. This was identified using a display filter in **Wireshark** for ip.addr == 194.61.24.102 && (http.request).
- **Screenshot**: Wireshark capture showing the connection to 194.61.24.102.



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.

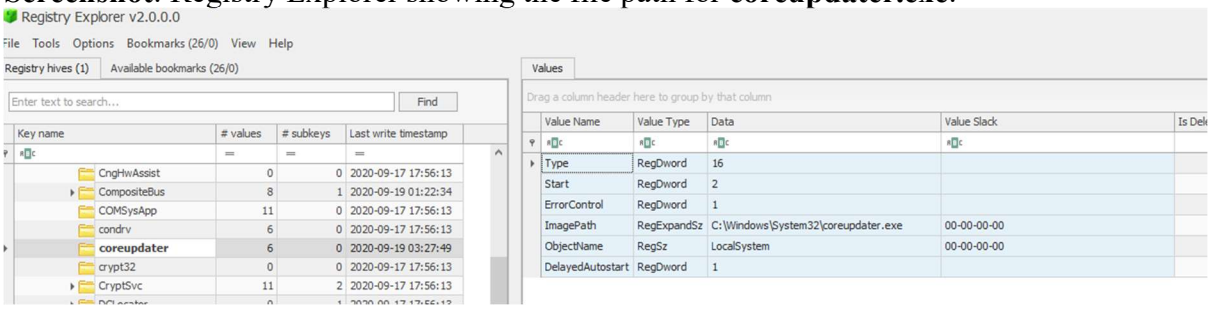


3.6.5. Malware Location on Disk

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.

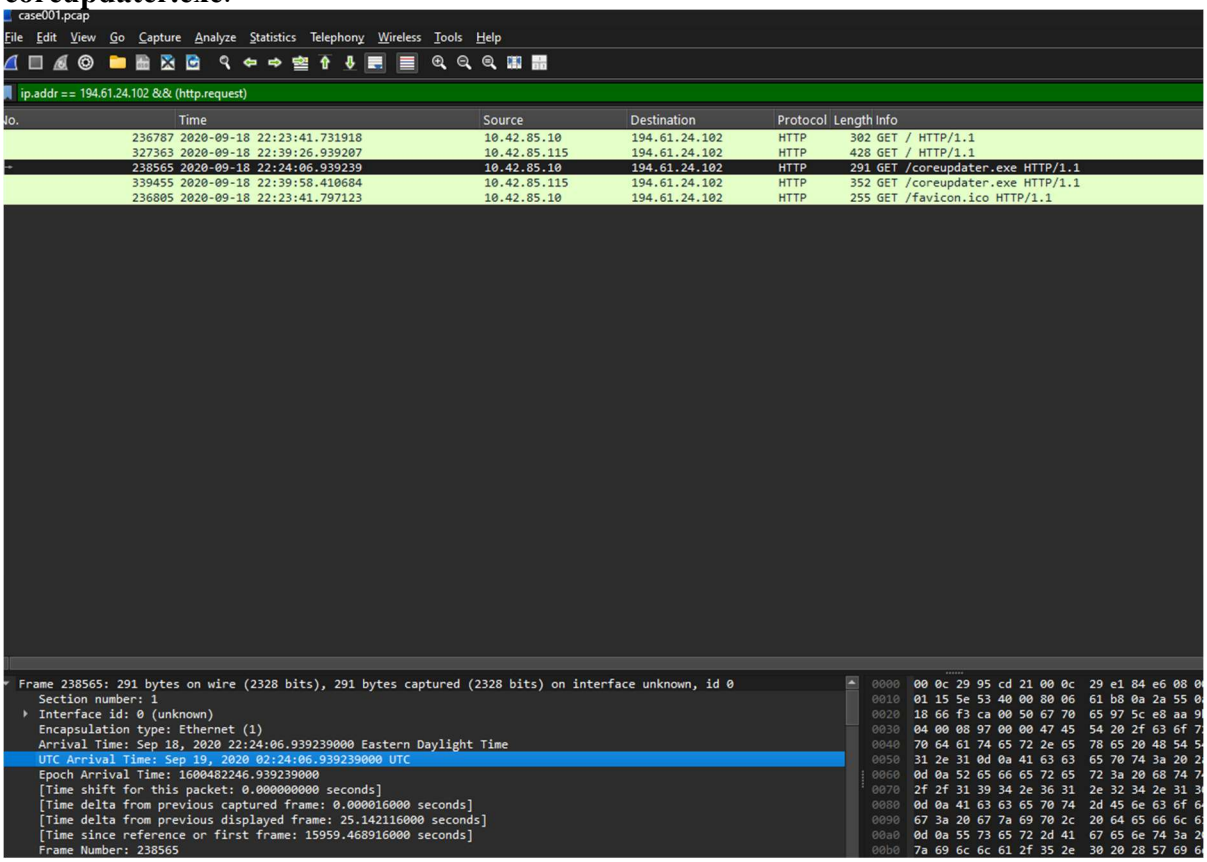
- **Screenshot**: Registry Explorer showing the file path for **coreupdater.exe**.



3.6.6. First Appearance of Malware

Answer: 2024-11-10 at 02:24:07 UTC
Evidence & Process:

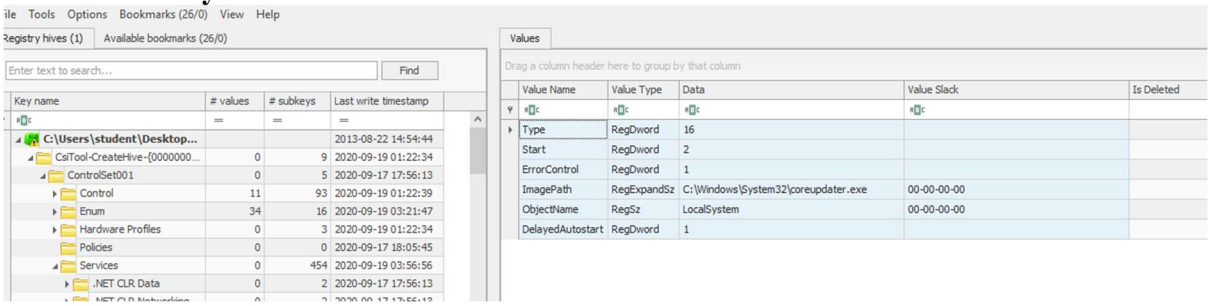
- The first appearance of **coreupdater.exe** was detected in the **Wireshark** capture, filtered with ip.addr == 194.61.24.102 && (http.request). The timestamp for the first HTTP GET request was **2024-11-10 at 02:24:07 UTC**.
- **Screenshot**: Wireshark packet capture showing the first appearance of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



3.6.7. Evidence of Movement

Answer: Moved from Downloads to C:\Windows\System32
Evidence & Process:

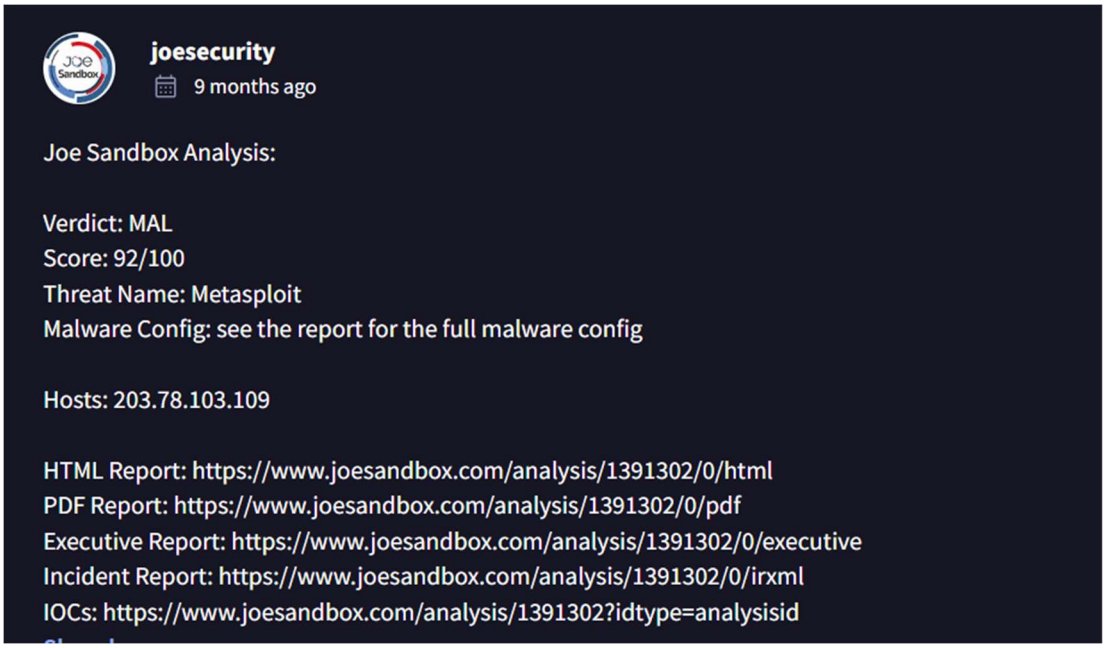
- The file **coreupdater.exe** was initially found in the **Downloads** folder of the Administrator account and later moved to **C:\Windows\System32**, indicating an attempt to hide and ensure persistence.
- **Screenshot**: File path analysis and logs showing movement from **Downloads** to **C:\Windows\System32**.



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 th **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).



3.6.9. Accessibility of the Malware

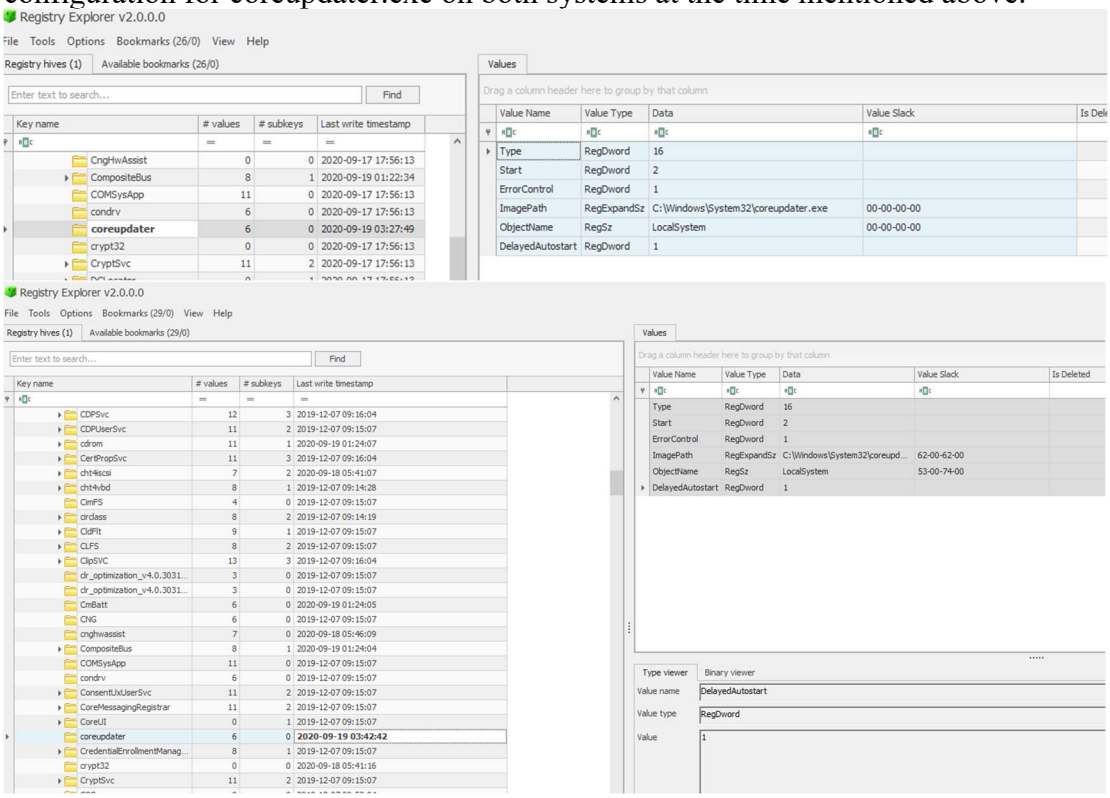
The malware, identified as a payload delivered via Metasploit, is highly accessible. Metasploit is an open-source red teaming tool, widely available for both legitimate and malicious purposes. Online research and VirusTotal analysis confirm its prevalence and ease of use for attackers.

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.



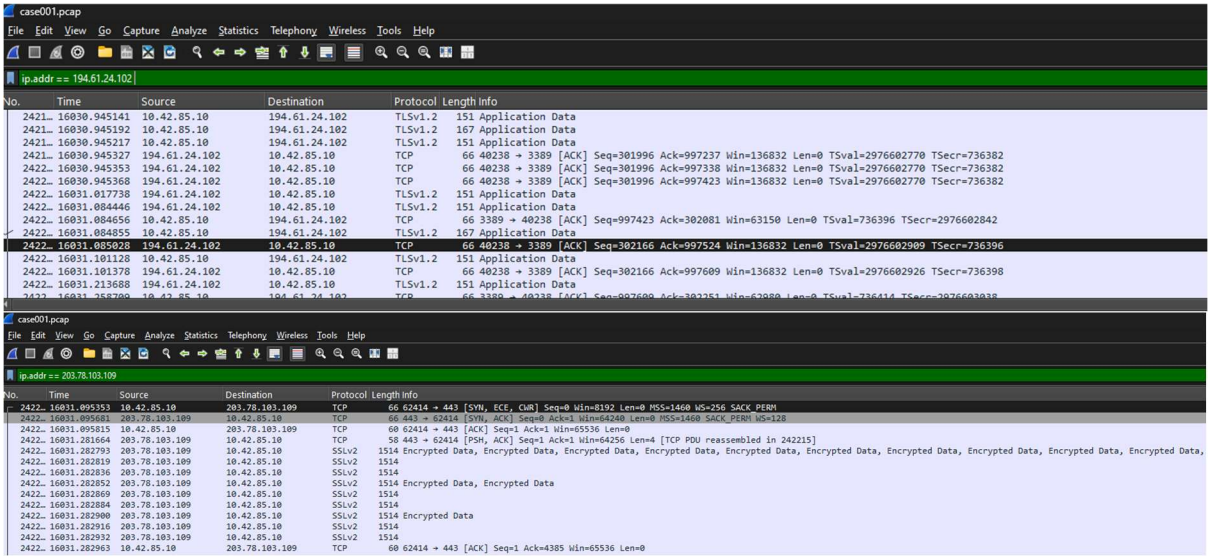
3.7. Malicious IP Address Analysis

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.



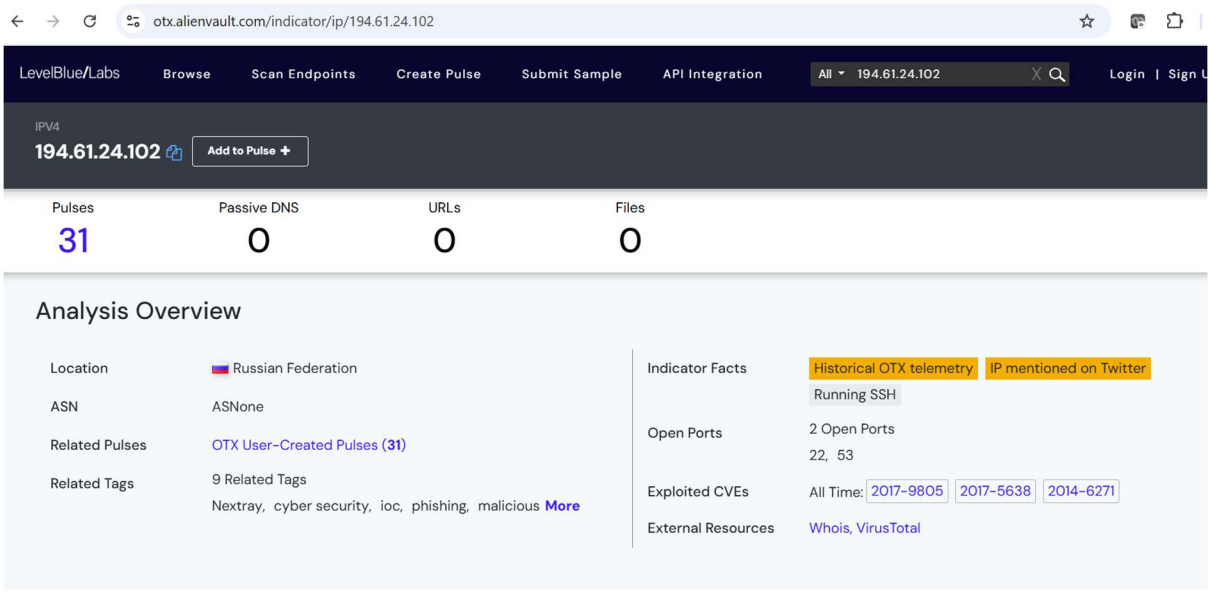
3.7.2. Connection to Adversary Infrastructure

Answer: Confirmed involvement in known adversary infrastructure.

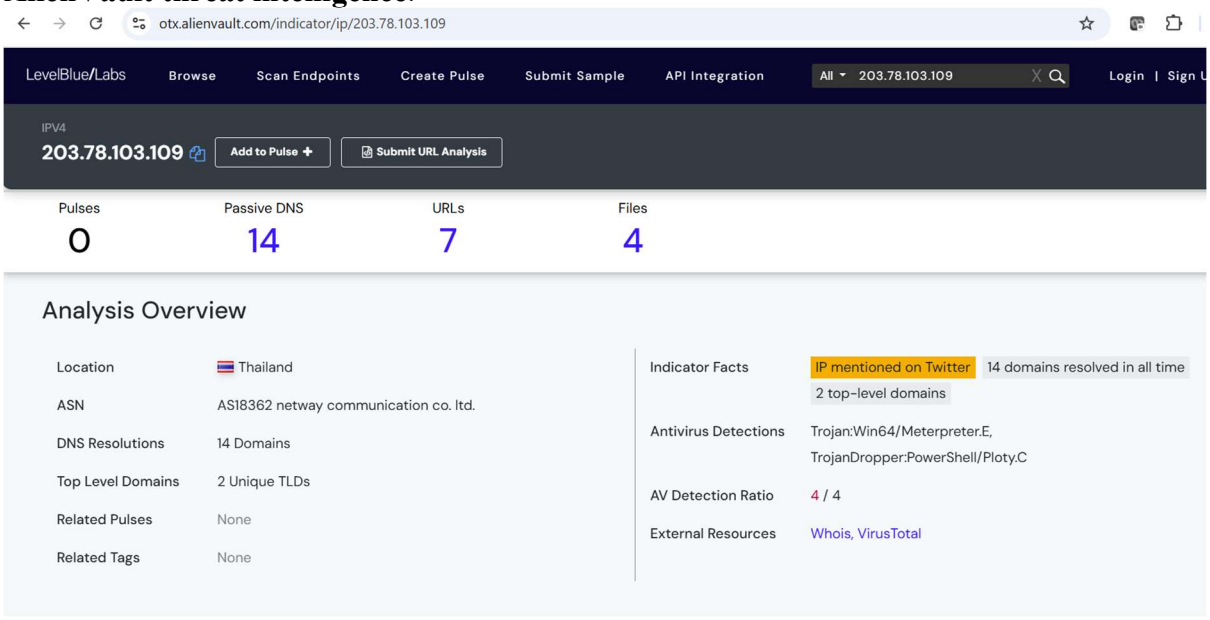
Evidence & Process:

- **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.



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

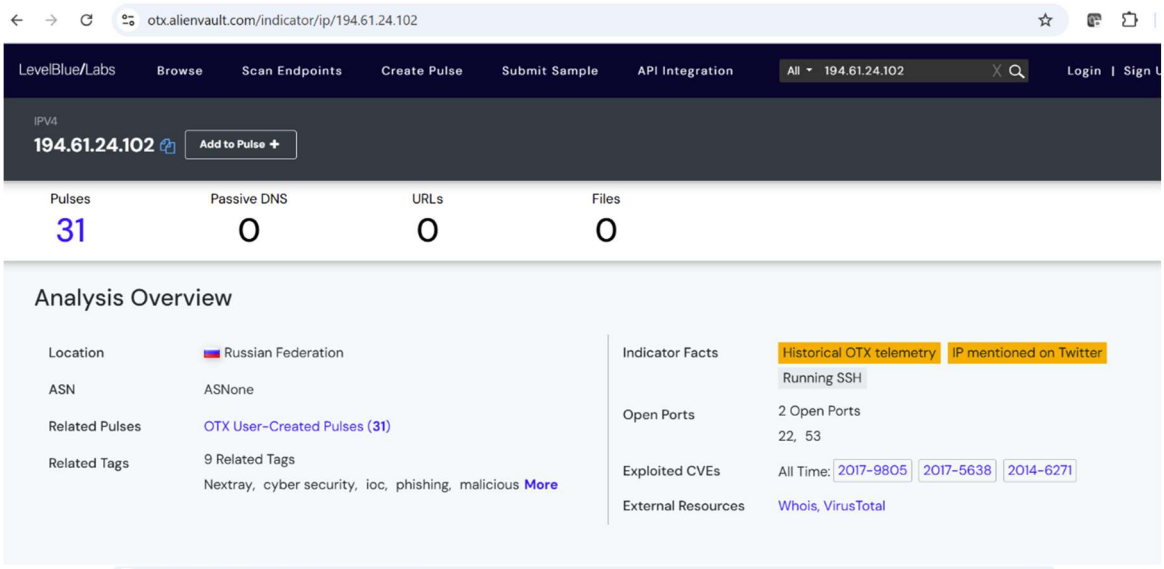


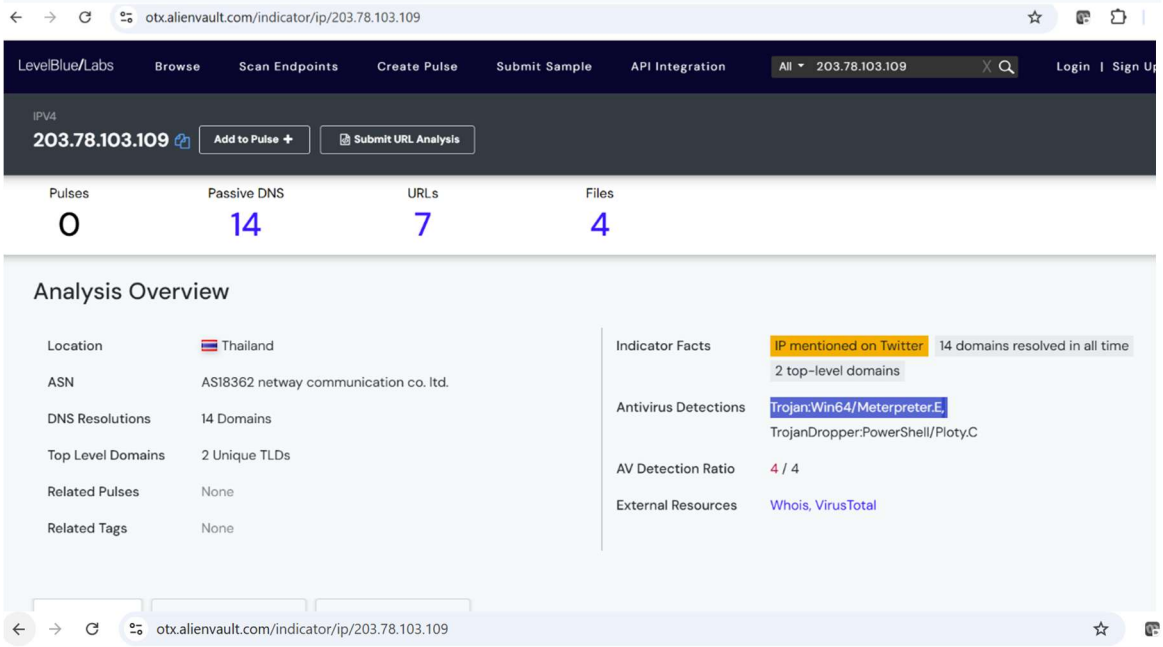
3.7.3. Involvement in Other Attacks

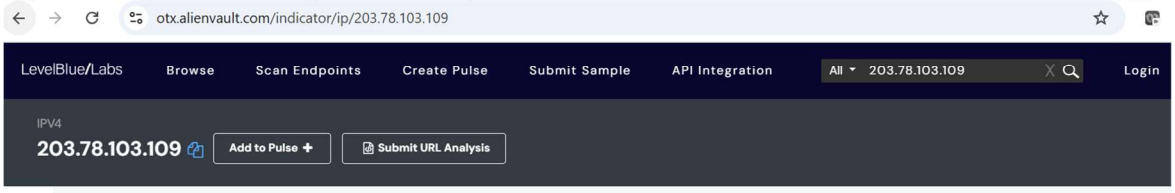
Answer: Yes, both IPs were involved in other attacks during the time of this incident.

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.







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

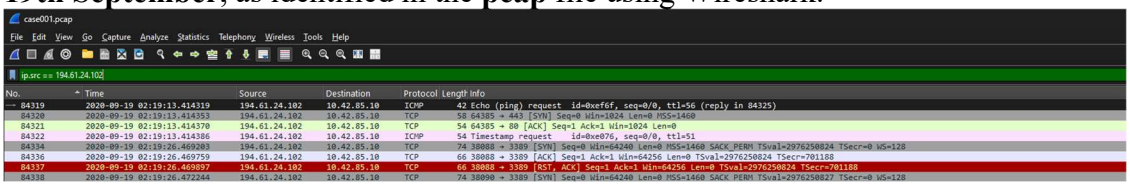
3.8. Data Access and Exfiltration

3.8.1. Did the Attacker Access Any Other Systems?

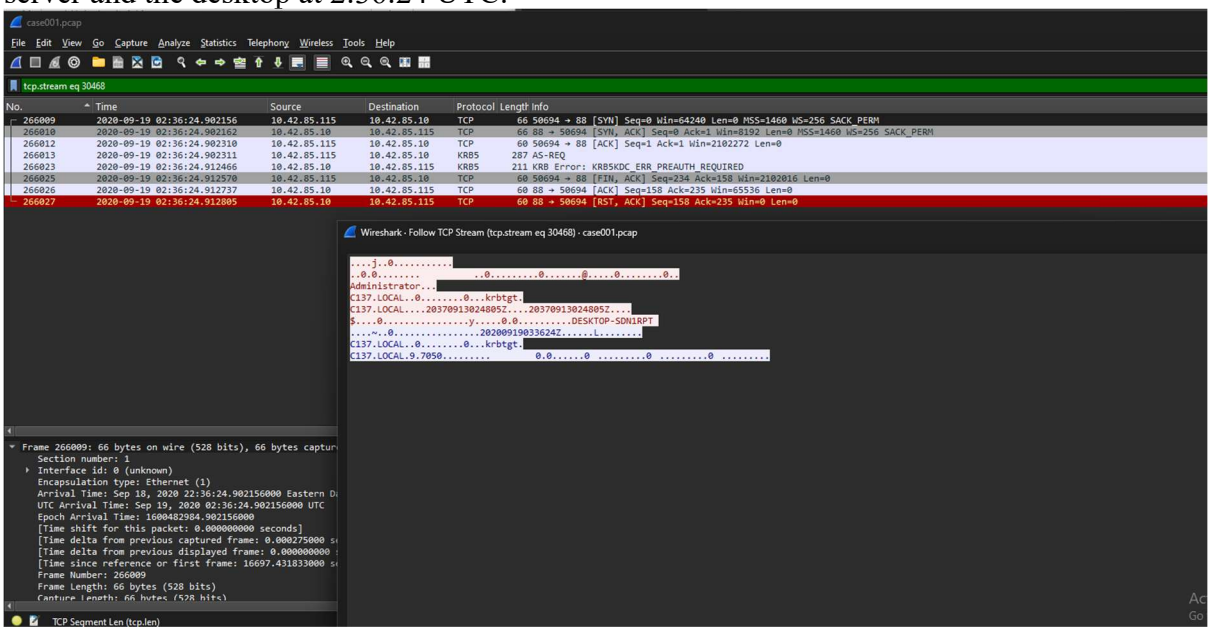
Answer: Yes, the attacker accessed the desktop system **C137\DESKTOP-SDN1RPT$** from the Domain Controller (DC).

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)**. Bellow 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.

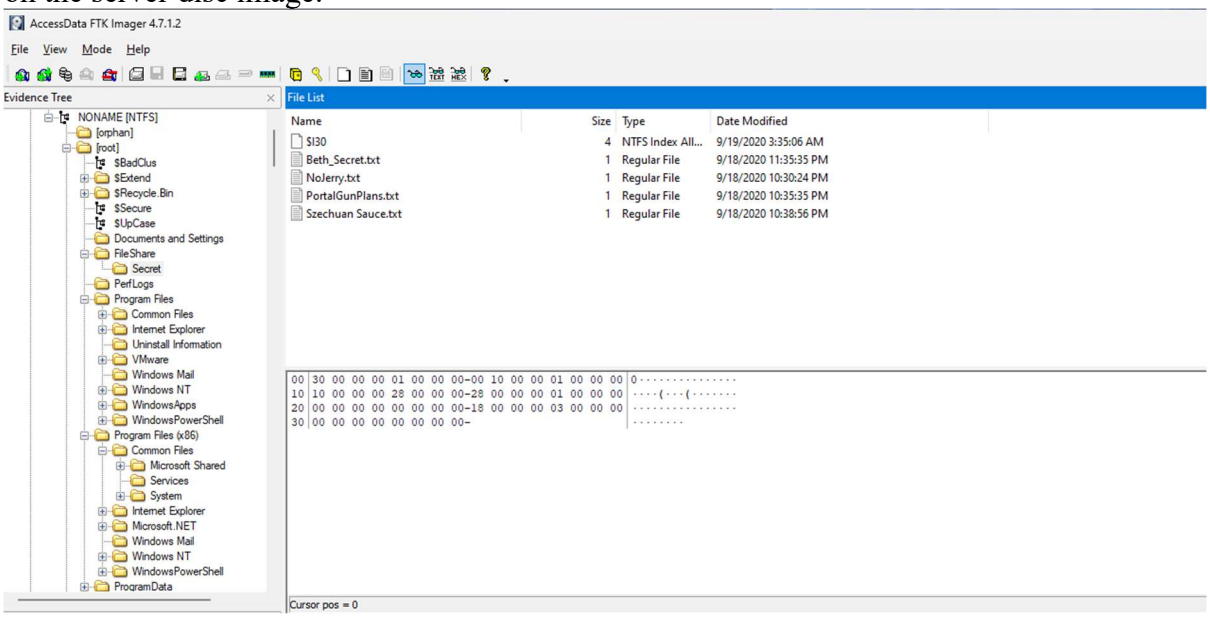
3.8.2. Did the Attacker Steal or Access Any Data?

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

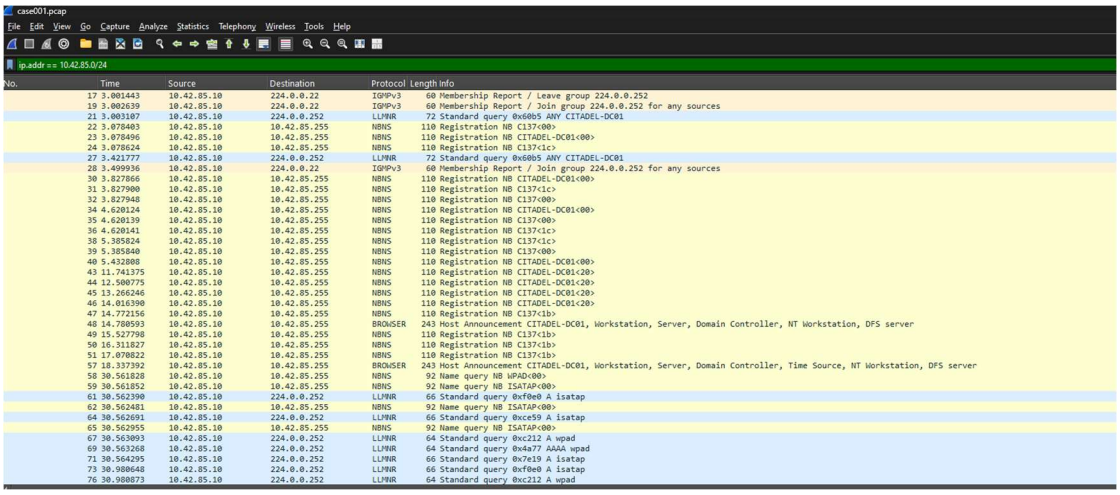
Answer: The victim's network consisted of a Domain Controller (DC) and an endpoint device:

- **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.



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/