Digital Forensics Report & Documentation:
The Stolen Szechuan Sauce
By DFIR Madness

Prepared on April 28, 2025 by:

Ifeanyi Christian Edeh
Cybersecurity Specialist

https://www.linkedin.com/in/ifeanyiedeh

Toolbox:

MITRE ATT&CK, FTKImager, Autopsy, Wireshark, Volatility Workbench, Eric Zimmerman's Registry Explorer, OTX AlienVault LevelBlue, VMWare, Virus Total, NIST SP 800-53, NIST CSF

Table of Contents

Forensics Report & Documentation:
The Stolen Szechuan Sauce
By DFIR Madness

Executive Summary

Intro to Case - The Stolen Szechuan Sauce

The digital forensics investigation explores a security breach using advanced analytical techniques. Through detailed examination of network traffic and system artifacts, we identified key insights into the incident, including the timeline, points of entry, and nature of the malicious activities involved.

Key findings include:

- the breach's initial entry via RDP brute force,
- the presence of malware ("coreupdater.exe"), and
- the compromise of sensitive information.

This investigation highlights the importance of digital forensics in unraveling complex security incidents and strengthening cyber defenses. It also provides recommendations for architectural improvements and preventive measures to bolster security.

This report is the result of a collaborative effort by RM and Bernadette Chan. Richard focused on analyzing desktop artifacts, while I concentrated on server files. We both independently reviewed the PCAP file.

Key Cybersecurity Tools Used

- FTKImager
- Autopsy 4.21.0
- Wireshark
- Volatility Workbench V3.0 Build 1008
- EvtxeCmd V1.5.0.0
- Timeline Explorer V2.0.0.1
- Microsoft Windows Powershell V1.20.1178

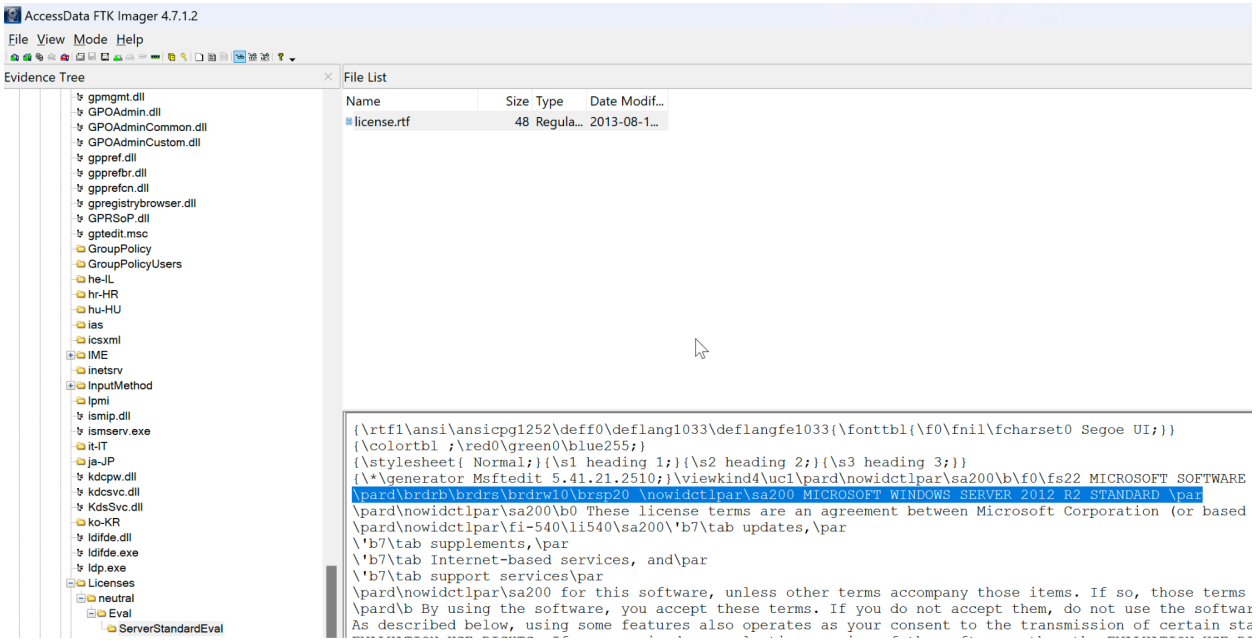
Artifacts

- DC01 Disk Image (E01)
- DC01 Memory file
- Case 001 PCAP
- Desktop Disk Image (E01)
- Desktop Memory file

Solving the Case

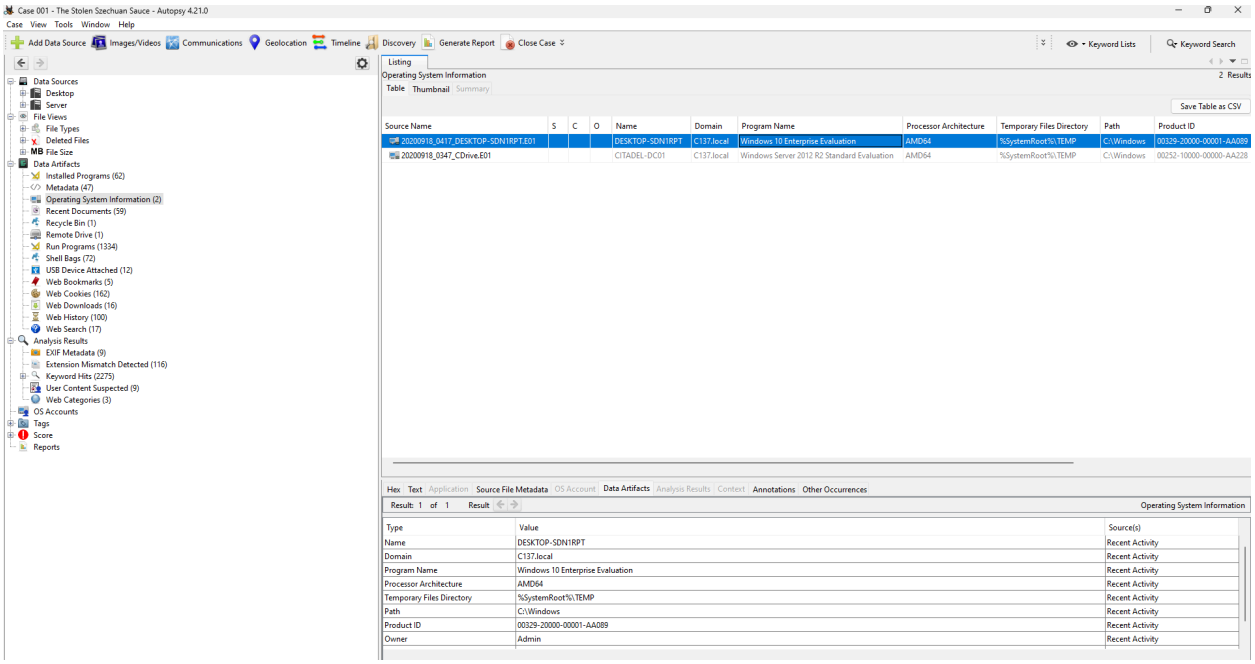
1. What's the Operating System of the Server?

Using FTKImager to view the server's disk image, we found the operating system of the server to be **Windows 2012 R2 standard.**



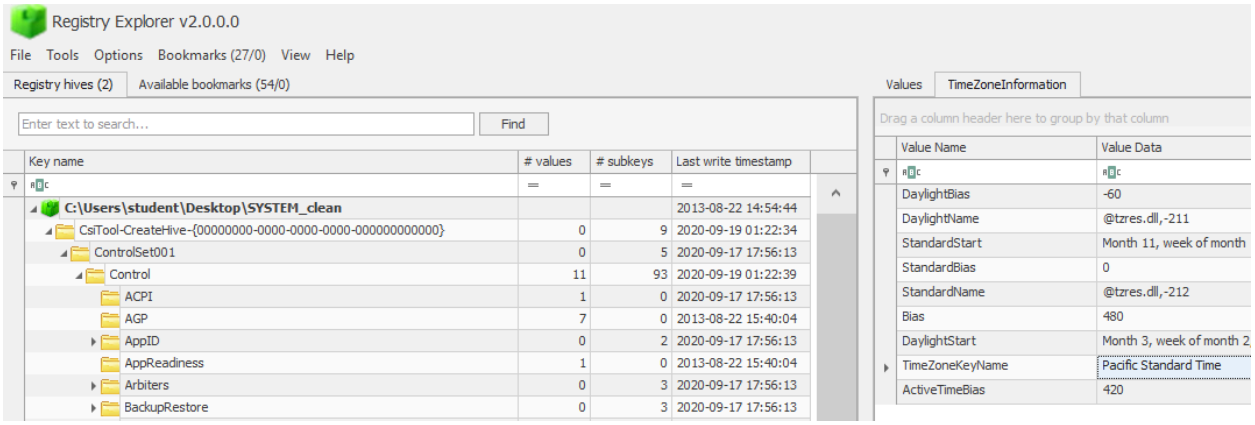
2. What's the Operating System of the Desktop?

Using Autopsy 4.21.0 to view the desktop disk image, the operating system present on the host machine DESKTOP-SDN1RPT was **Microsoft Windows 10** Enterprise Evaluation.



3. What was the local time of the Server?

Extracting the System32 > Config > System log files from FTKImager and importing into Eric Zimmerman's Registry Explorer, we found the local time of the server to be **Pacific Standard Time.**



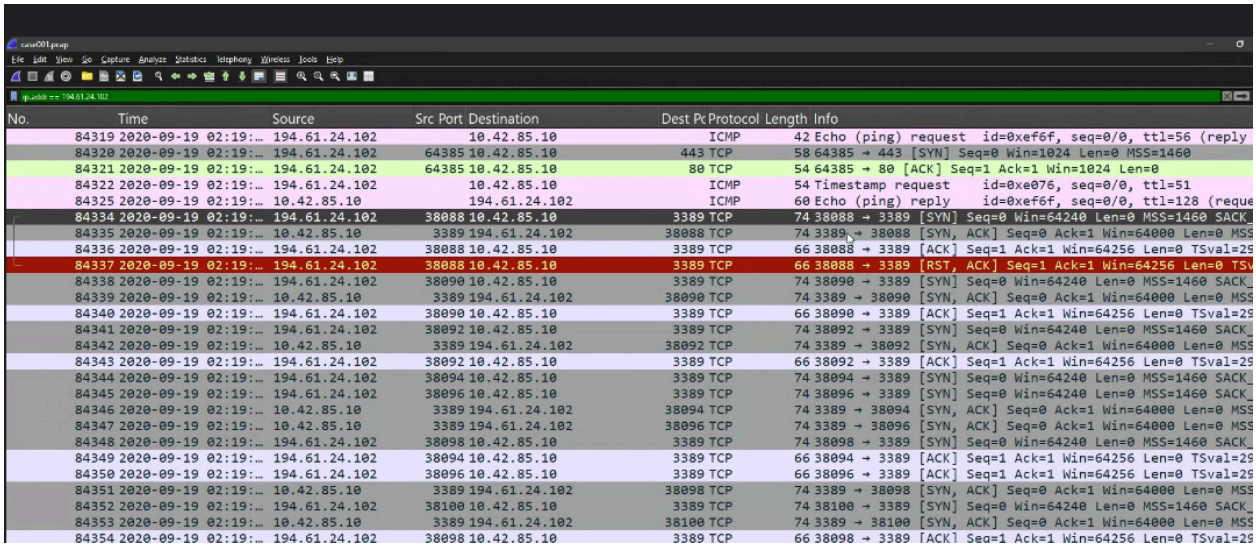
4. Was there a breach?

Yes.

5. What was the initial entry vector?

According to the analysis of the PCAP file on Wireshark, a suspicious IP address 194.61.24.102 sent a Ping Request to our machine (10.42.85.10) with no response. It tried to start a 3-way handshake with port 443 (https), no response. It tried again to start a 3-way handshake with port 80 (http), and our server sent a Ping Reply. From then on, we see many back-and-forth pings to port 3389 (RDP = remote desktop protocol).

This is an indication of a **RDP bruteforce attack** - someone is trying to guess the password so that they can log on and control our machine remotely.



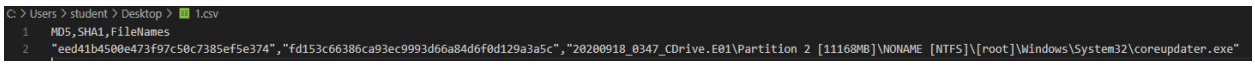
6. Was malware used? If so, what was it? If there was malware answer the following:

What process was malicious?

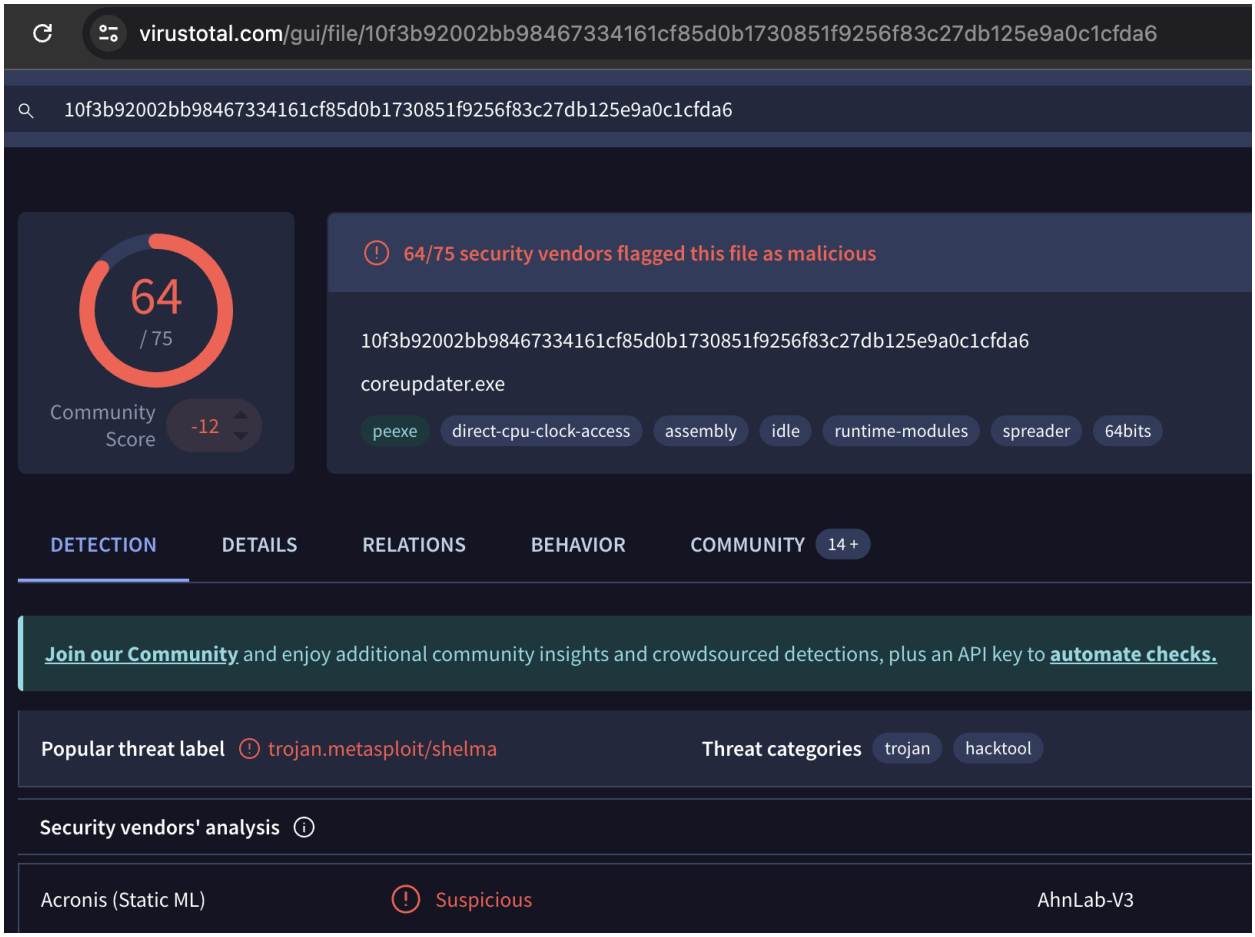
Yes, malware was used.

We were able to verify that the file '**coreupdater.exe**' was the initial malicious process. Searching for the hash of this file in Autopsy (hash value: Fd153c66386ca93ec9993d66a84d6f0d129a3a5c), we put it in VirusTotal and received a

Community Source of 64/75, confirming that coreupdater.exe is indeed a malicious file. Virustotal. (n.d.).

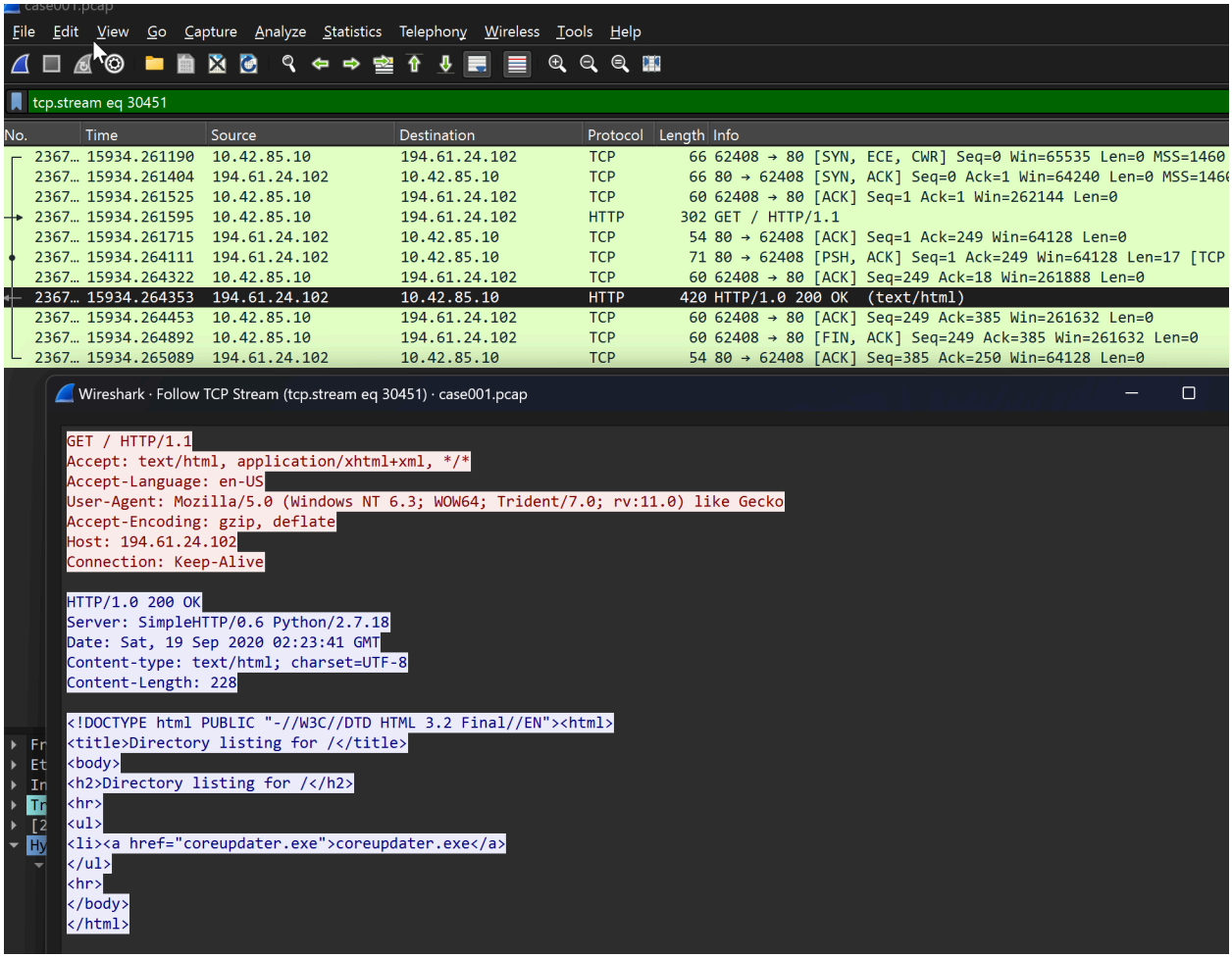


hash value



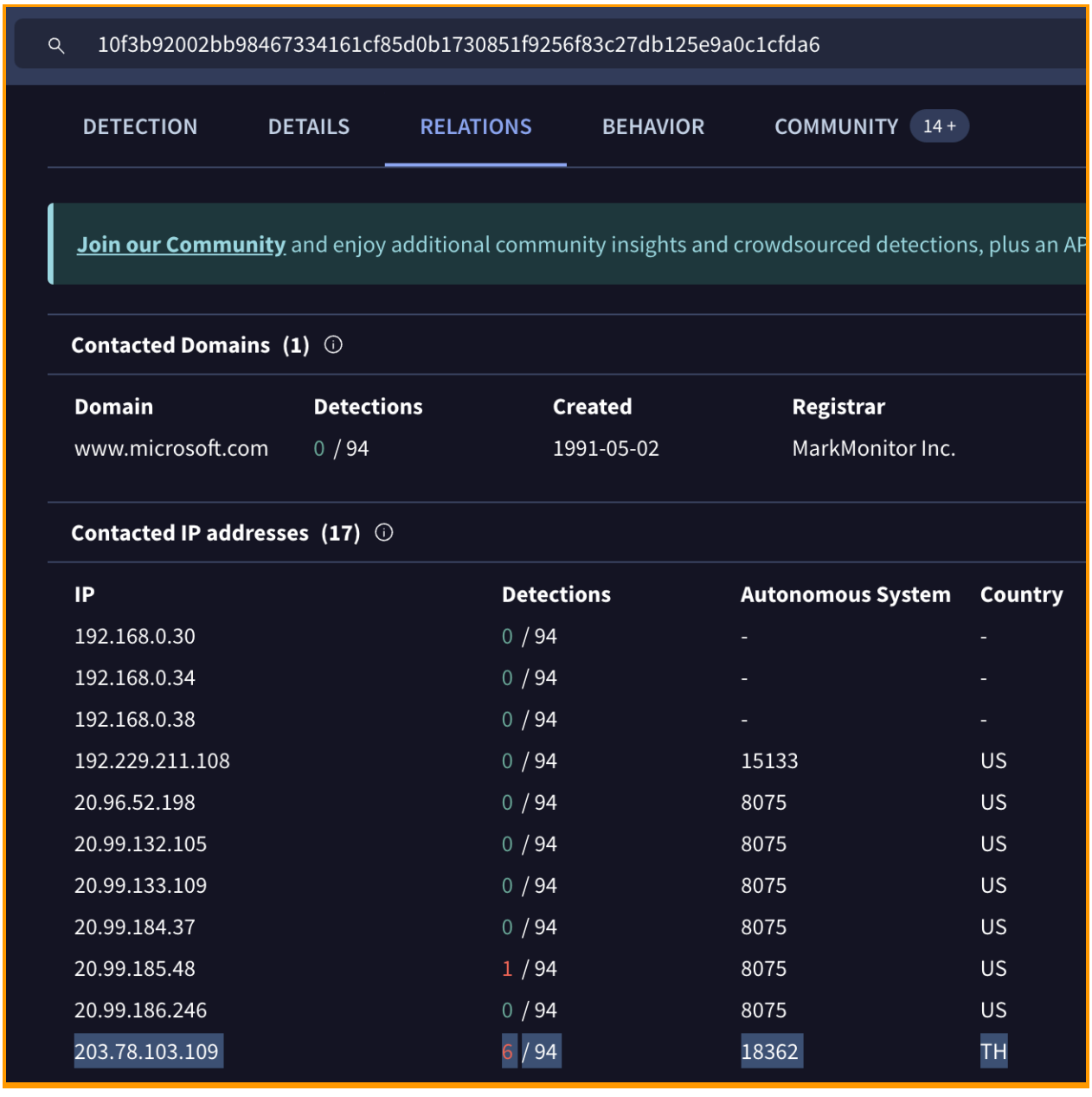
Identify the IP Address that delivered the payload.

While analyzing PCAP file on Wireshark, we see that the source IP address is **194.61.24.102** that navigated to the website on http (port 80) to download the coreupdater.exe file.



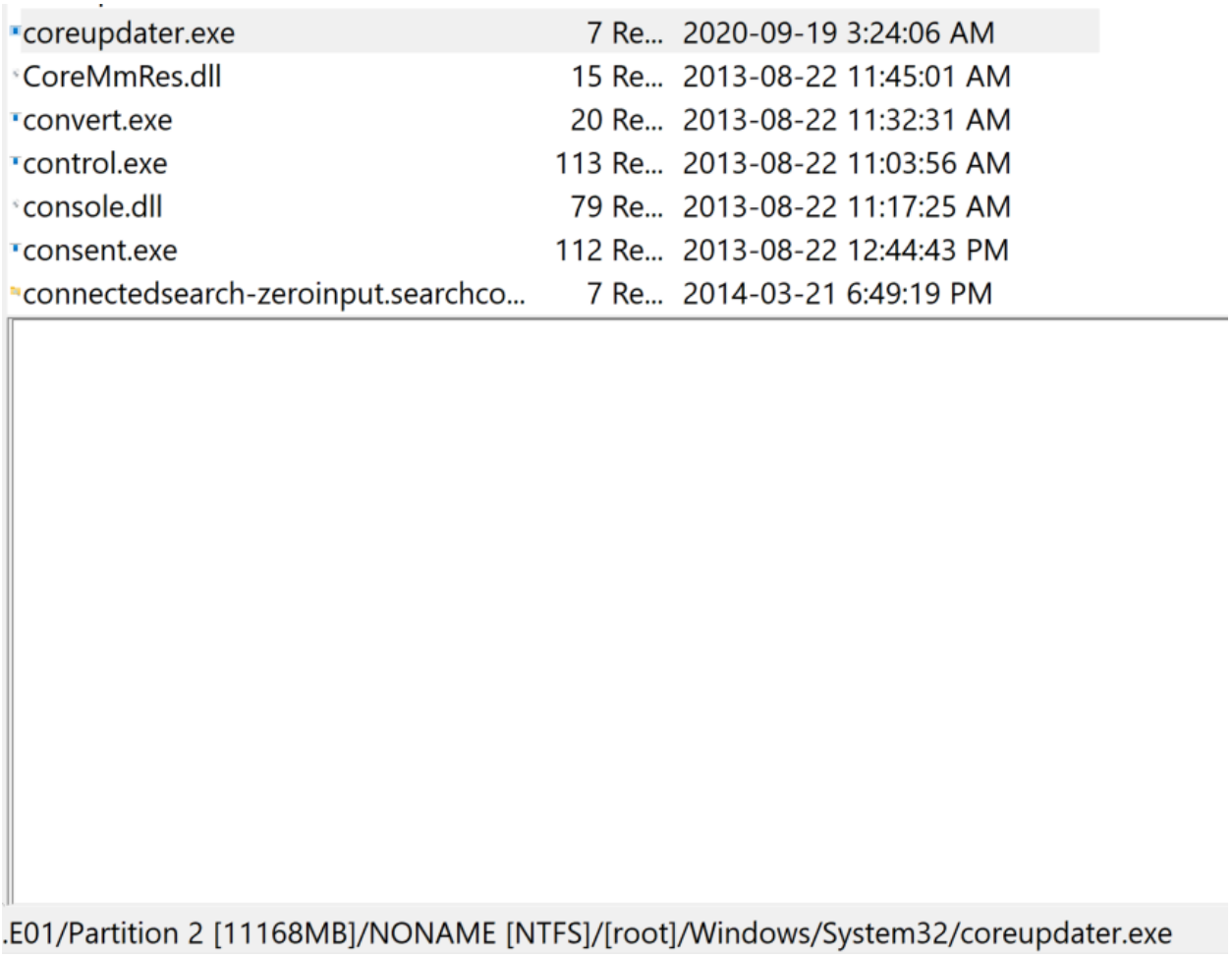
What IP Address is the malware calling to?

After searching the hash on virus total, we were able to find that the malware was calling to another suspicious IP address: **203.78.103.109** from Thailand. And we were also able to verify that this IP address was involved in breach as we analyzed the PCAP file on Wireshark.



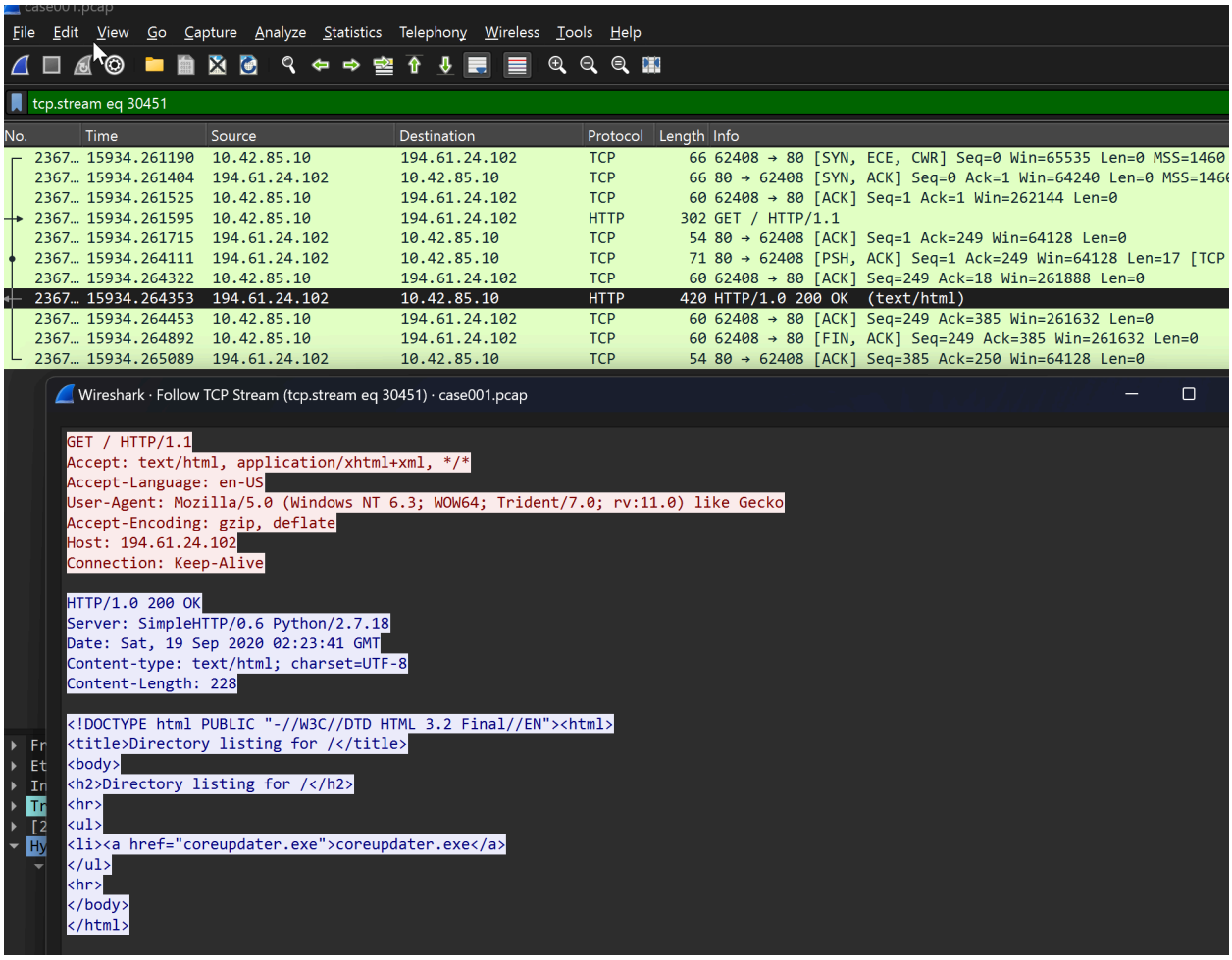
Where is this malware on disk?

While analyzing the Server's disk image using FTKImager, we found that the malware was downloaded to **C:\\Windows\System32**



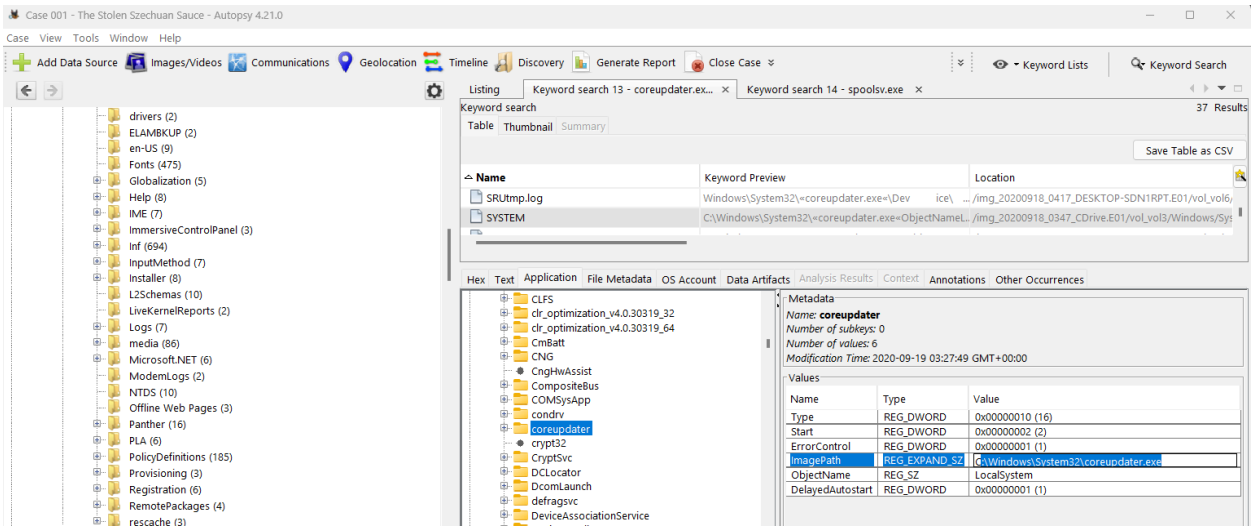
When did it first appear?

According to the PCAP file analyzed on Wireshark, the timestamp of the GET Request was **September 19, 2020 at 02:23:41 GMT.**



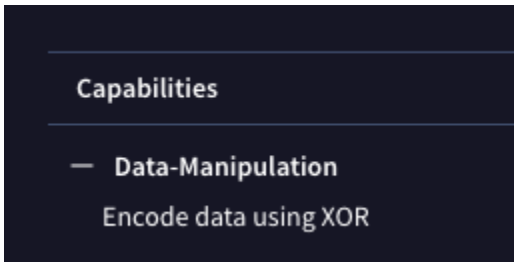
Did someone move it?

Using Autopsy 4.21.0 and viewing the SYSTEM log file, we found the file was moved into **C:\Windows\System32\config\system** in the registry.



What were the capabilities of this malware?

According to VirusTotal, this malware has data manipulation capabilities, specifically with encoding data using XOR (E**x**clusive **OR**). XOR is a common technique used by malware to obfuscate its code and evade detection. (PCMAG, n.d.)



Is this malware easily obtained?

Yes, this malware is easy to obtain as it's part of the free, open-source Metasploit Framework, which, unfortunately, is a widely used open-source penetration testing tool. This means it can be used by both ethical security professionals and malicious actors. While its primary purpose is to help organizations identify and address vulnerabilities, it can also be exploited by attackers to compromise systems. (Metasploit, n.d.)

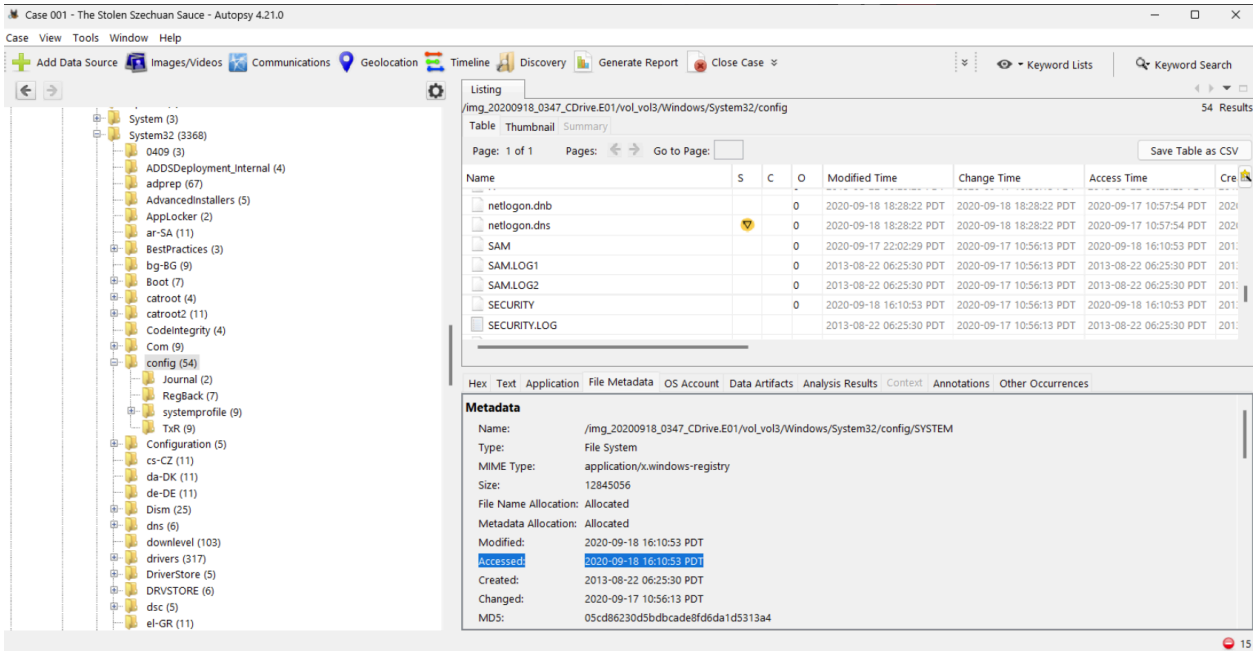
Was this malware installed with persistence on any machine?

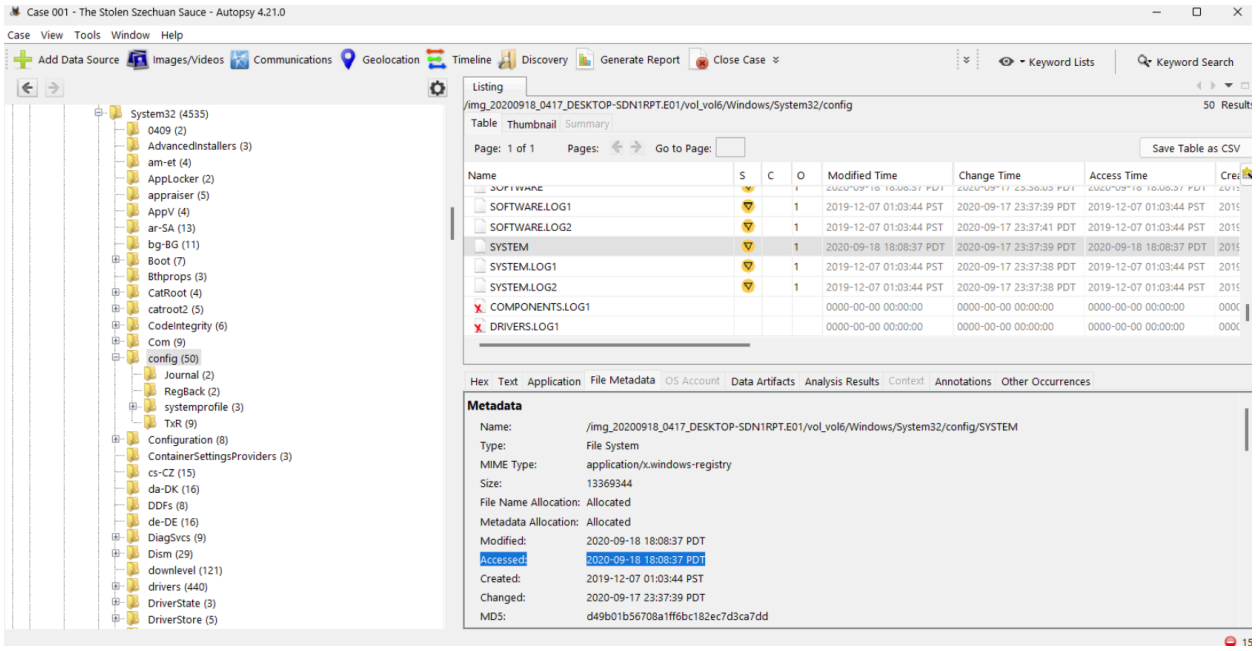
According to MITRE ATT&CK, “Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.” (MITRE ATT&CK, n.d.)

Based on this definition, yes, this malware was persistent. Coreupdater.exe was installed in the registry and as a service on the Server CITADEL-DC01 and the Desktop DESKTOP-SDN1RPT.

When?

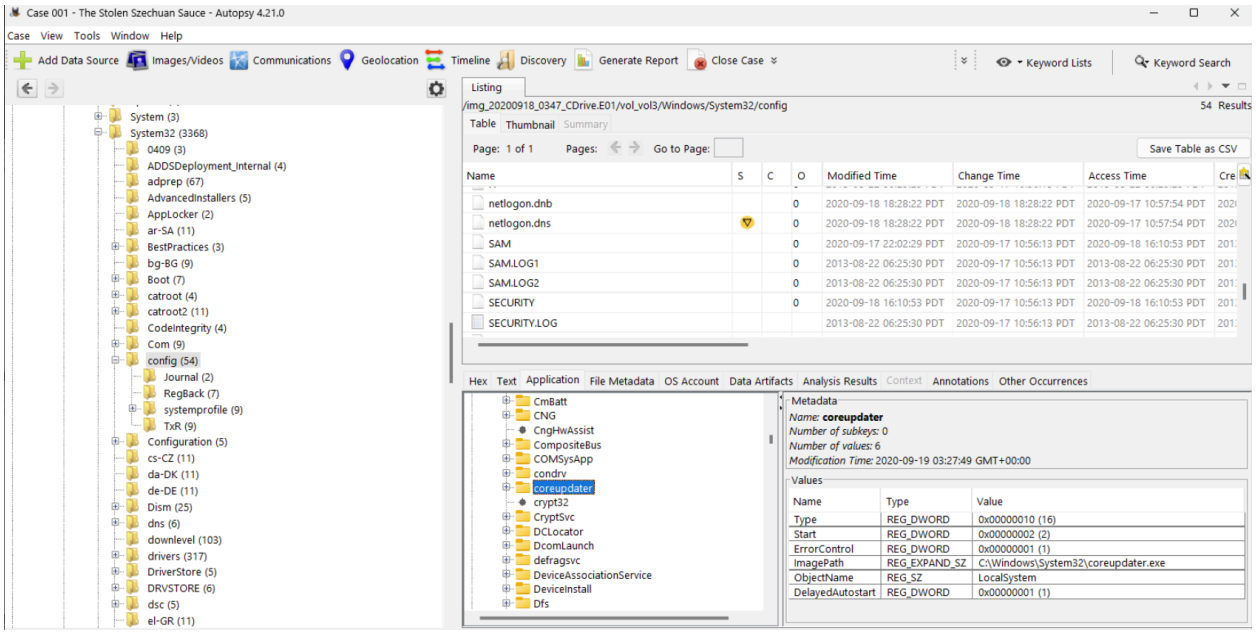
Using Autopsy 4.21.0, we found “coreupdater.exe” installed on September 18th 2020 at 16:10:53 PDT on the Server and on September 18th 2020 18:08:37 PDT on the Desktop.

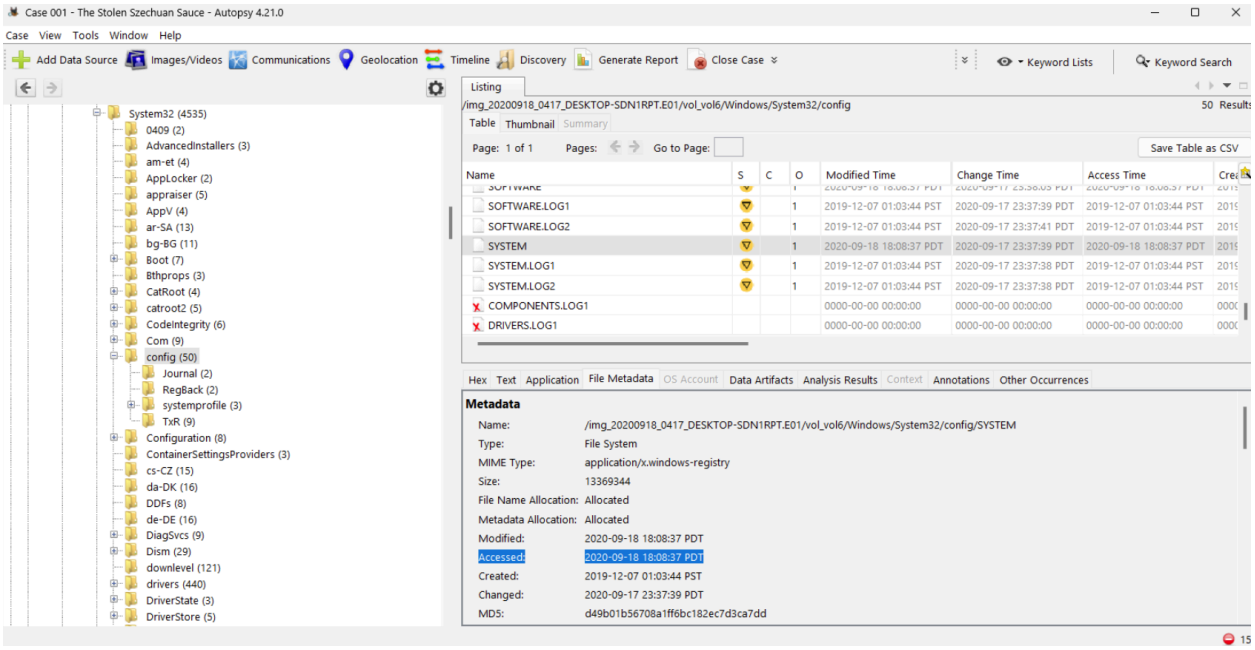




Where?

Using Autopsy 4.21.0, we found “coreupdater.exe” in the registry in C:/windows/System32 under ControlSet001 > Services > coreupdater on the Server and the Desktop.

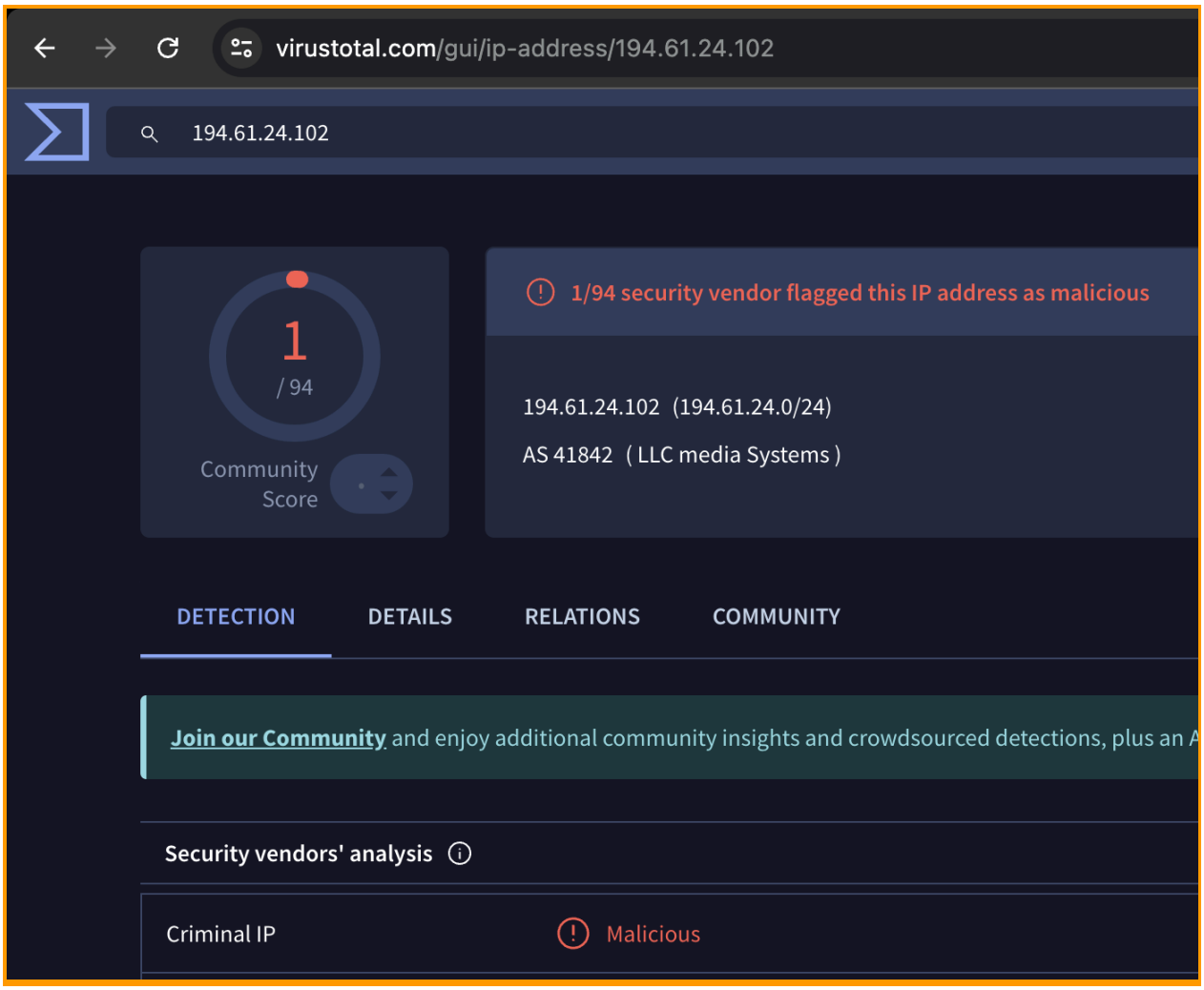


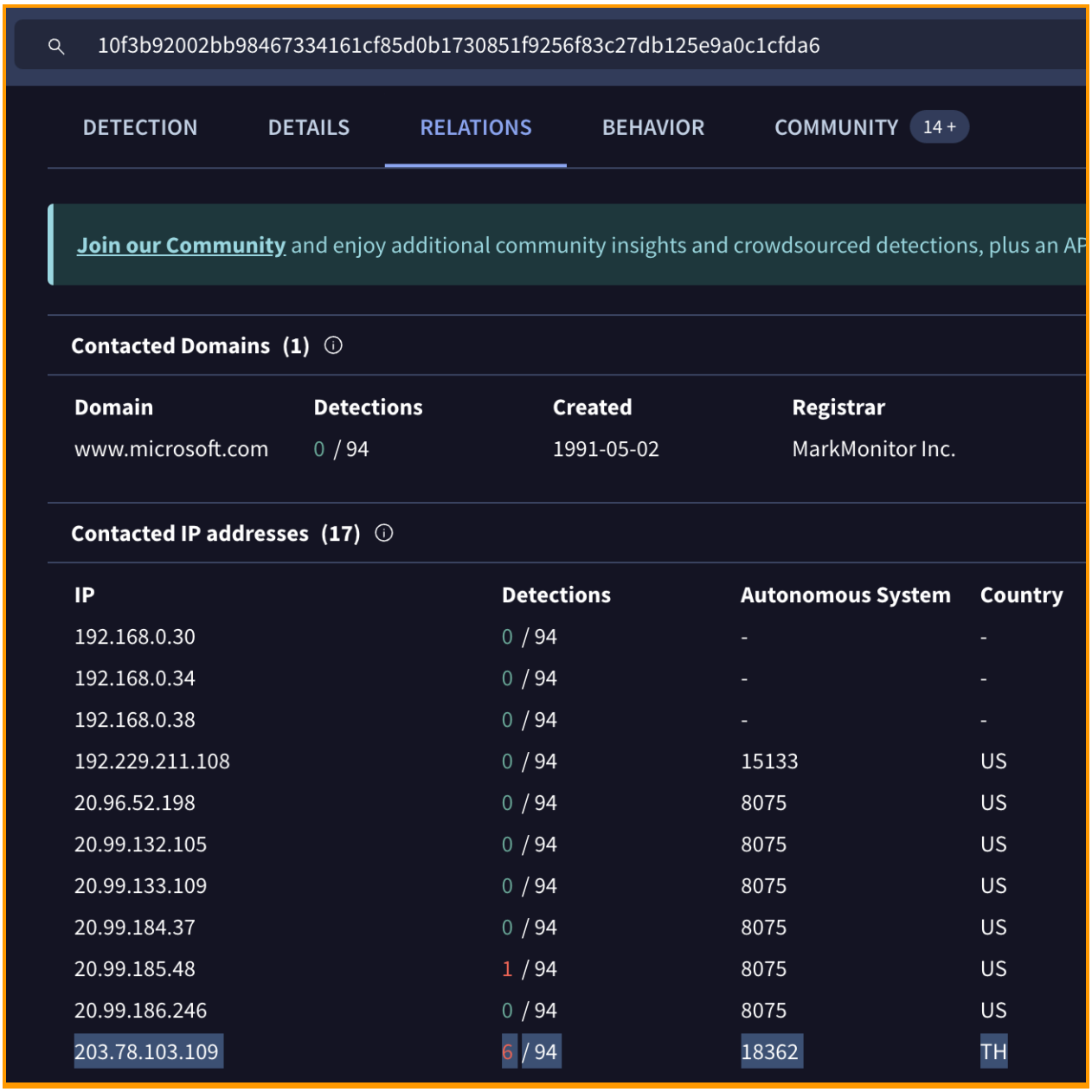


7. What malicious IP Addresses were involved?

After inputting the suspicious IP address **194.61.24.102** into VirusTotal.com, it resulted in 1/94 security vendor flagging it as malicious from Criminal IP. This IP initiated the attack on CITADEL-DC01.

While searching the hash on VirusTotal, we were able to find another suspicious IP address: **203.78.103.109.** This one is from Thailand and has a community score of 6/94. Wireshark shows that this IP contacted our server after the RDP bruteforce was successful. Then 194.61.24.102 accessed DESKTOP-SDN1RPT.


virustotal.com/gui/ip-address/194.61.24.102
194.61.24.102
1
/ 94
Community Score
1/94 security vendor flagged this IP address as malicious
194.61.24.102 (194.61.24.0/24)
AS 41842 (LLC media Systems)
DETECTION
DETAILS
RELATIONS
COMMUNITY
Join our Community and enjoy additional community insights and crowdsourced detections, plus an A
Security vendors' analysis
Criminal IP
Malicious



10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 14 +

Join our Community and enjoy additional community insights and crowdsourced detections, plus an AP

Contacted Domains (1)

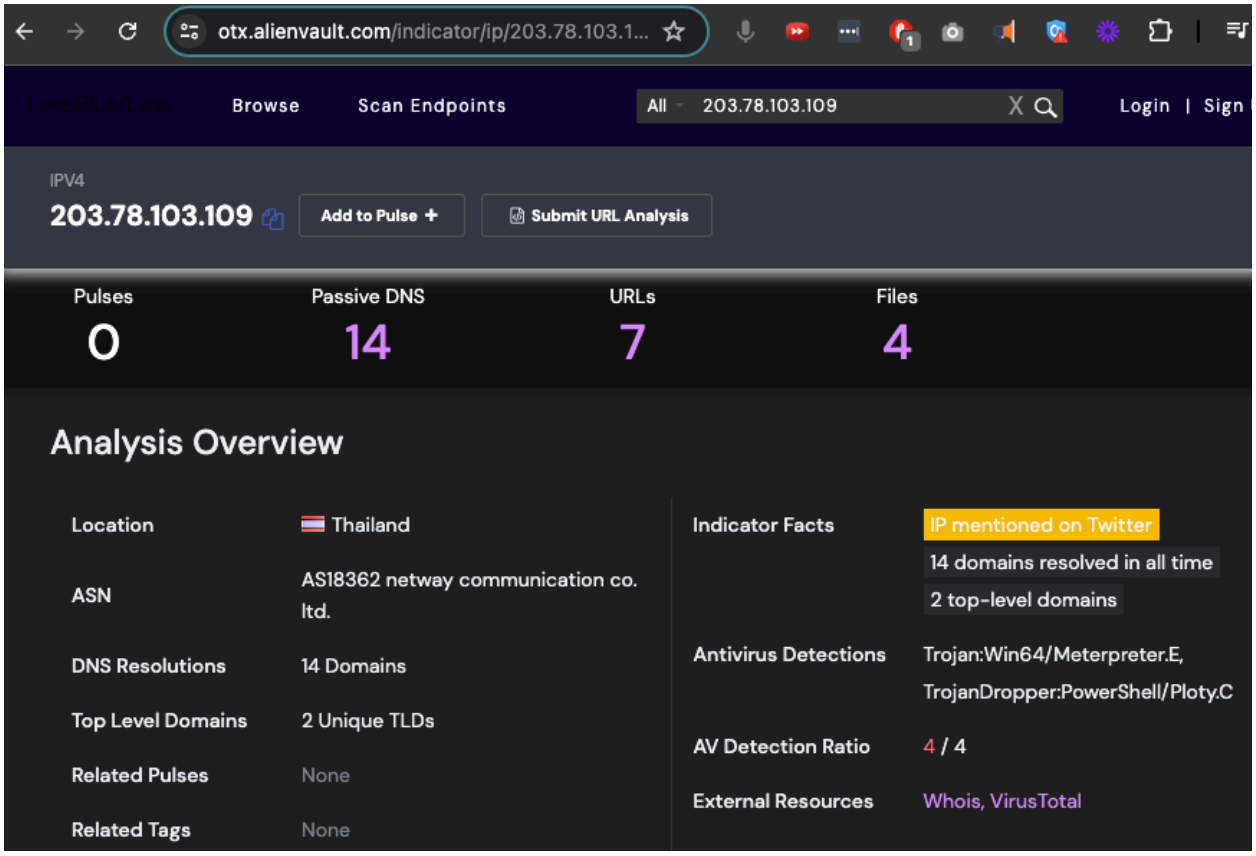
Domain	Detections	Created	Registrar
www.microsoft.com	0 / 94	1991-05-02	MarkMonitor Inc.

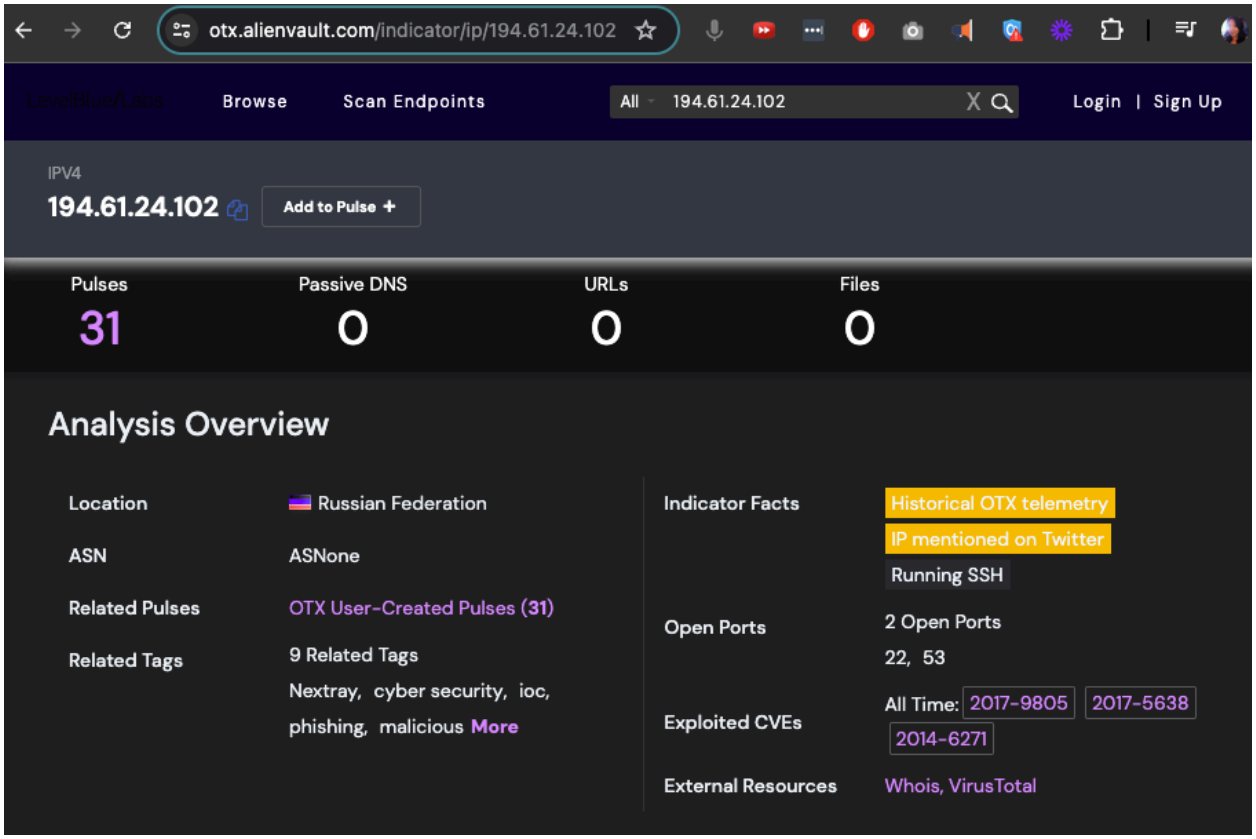
Contacted IP addresses (17)

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

Were any IP Addresses from known adversary infrastructure?

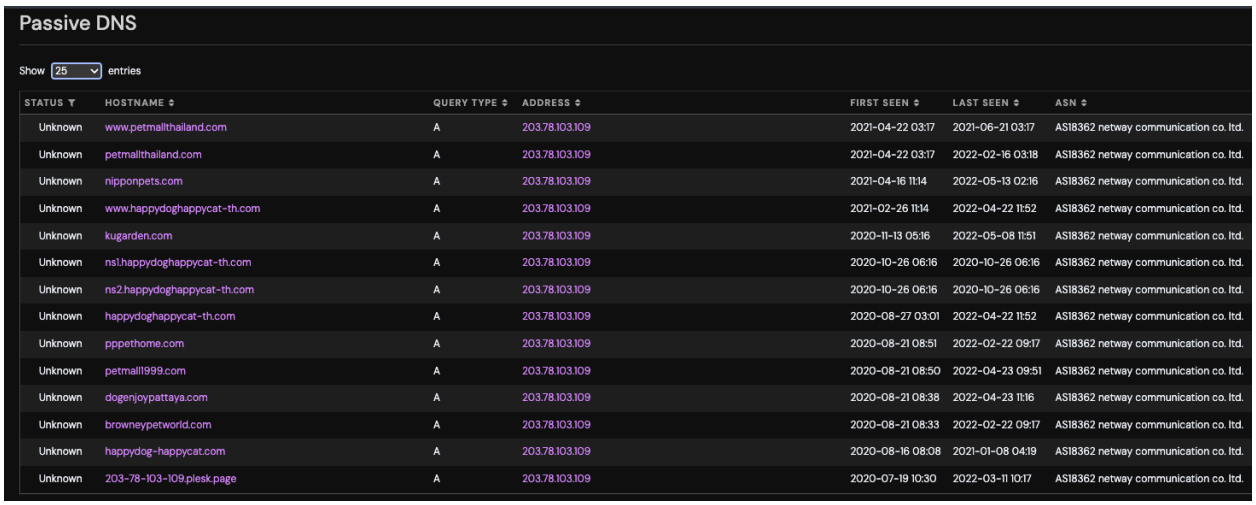
Yes, according to Level Blue/Labs, both IP addresses: 203.78.103.109 (Thailand) & 194.61.24.102 (Russia) are associated with various CVEs. (LevelBlue Open Threat Exchange, n.d.)





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

Yes, according to Level Blue/Labs, 203.78.103.109 was involved in other attacks around the same time under hostname related to pets like: www.petmallthailand.com, www.happydoghappycat-th.com, or pppethome.com



STATUS	HOSTNAME	QUERY TYPE	ADDRESS	FIRST SEEN	LAST SEEN	ASN
Unknown	www.petmallthailand.com	A	203.78.103.109	2021-04-22 03:17	2021-06-21 03:17	AS18362 netway communication co. ltd.
Unknown	petmallthailand.com	A	203.78.103.109	2021-04-22 03:17	2022-02-16 03:18	AS18362 netway communication co. ltd.
Unknown	nipponpets.com	A	203.78.103.109	2021-04-16 11:14	2022-05-13 02:16	AS18362 netway communication co. ltd.
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.
Unknown	kugarden.com	A	203.78.103.109	2020-11-13 05:16	2022-05-08 11:51	AS18362 netway communication co. ltd.
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.
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.
Unknown	happydoghappycat-th.com	A	203.78.103.109	2020-08-27 03:01	2022-04-22 11:52	AS18362 netway communication co. ltd.
Unknown	pppethome.com	A	203.78.103.109	2020-08-21 08:51	2022-02-22 09:17	AS18362 netway communication co. ltd.
Unknown	petmall1999.com	A	203.78.103.109	2020-08-21 08:50	2022-04-23 09:51	AS18362 netway communication co. ltd.
Unknown	dogenjoypattaya.com	A	203.78.103.109	2020-08-21 08:38	2022-04-23 11:16	AS18362 netway communication co. ltd.
Unknown	browneypetworld.com	A	203.78.103.109	2020-08-21 08:33	2022-02-22 09:17	AS18362 netway communication co. ltd.
Unknown	happydog-happycat.com	A	203.78.103.109	2020-08-16 08:08	2021-01-08 04:19	AS18362 netway communication co. ltd.
Unknown	203-78-103-109.plesk.page	A	203.78.103.109	2020-07-19 10:30	2022-03-11 10:17	AS18362 netway communication co. ltd.

8. Did the attacker access any other systems?

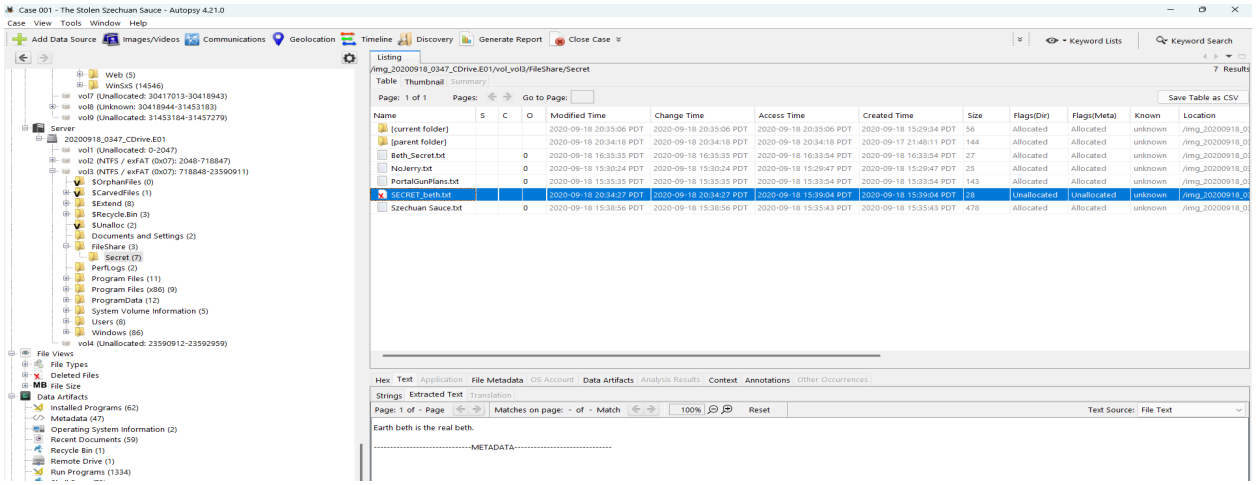
Yes, the attacker accessed the desktop (named DESKTOP-SDN1RPT at IP address 10.42.85.115) and the Server (named CITADEL-DC01 at IP address 10.42.85.10.

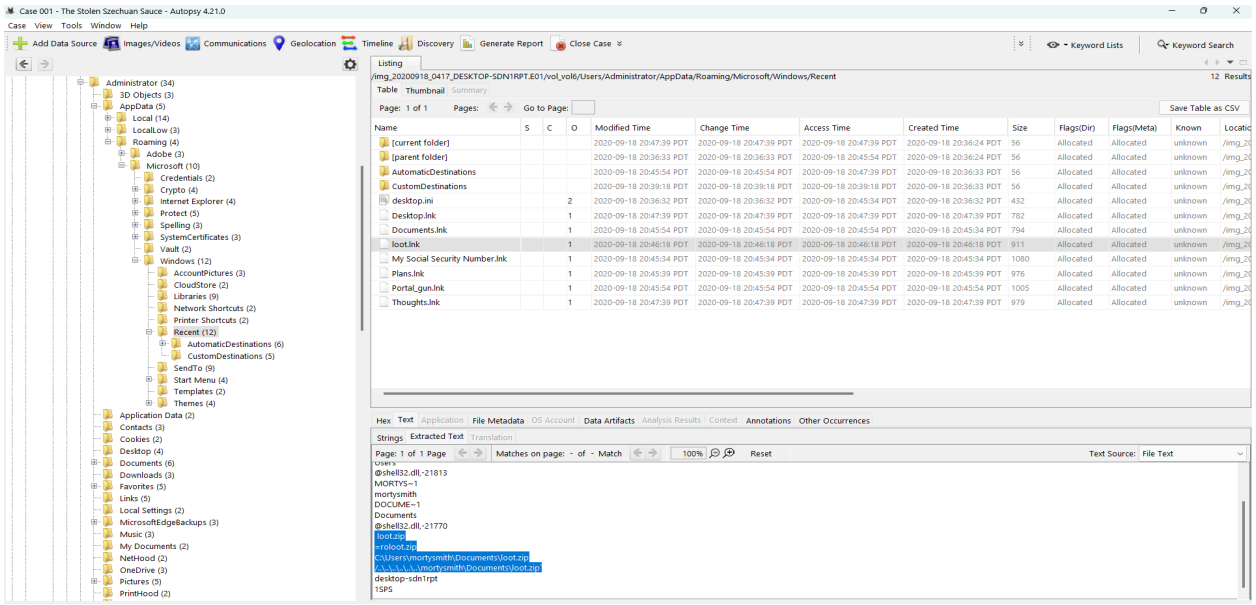
How? When?

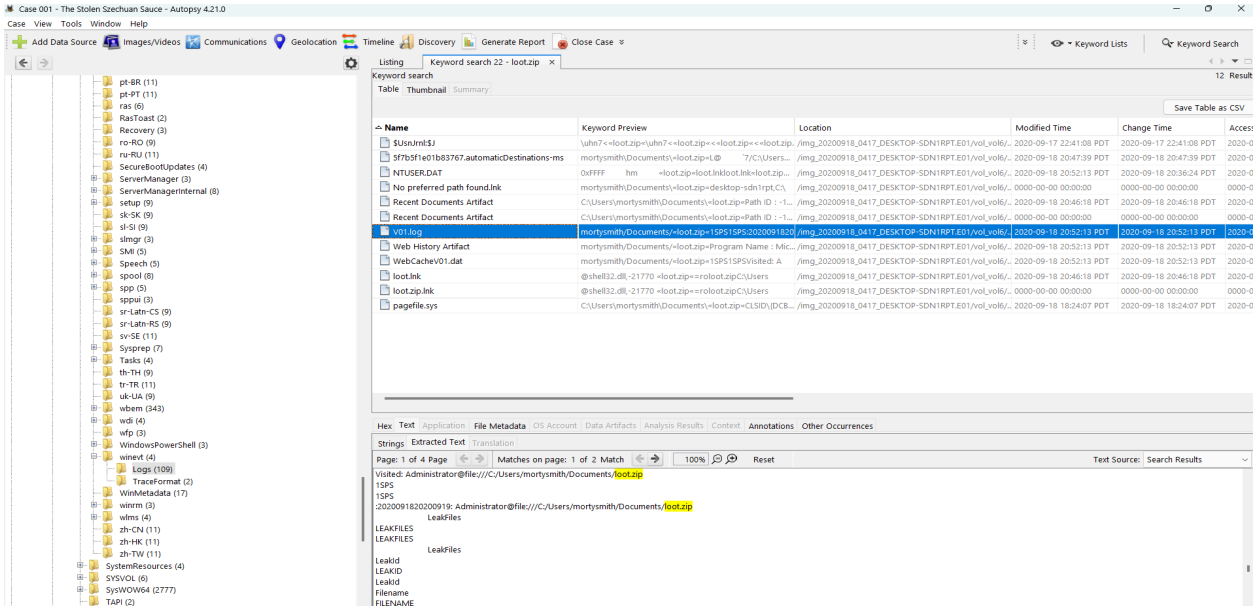
The attacker performed a RDP bruteforce attack on the Server. Once successful, they moved to the Desktop. This happened on **September 18 2020 between 15:38:56 PDT and 20:34:18 PDT,** as evident by a few files being accessed as seen on Autopsy.

Did the attacker steal or access any data? When?

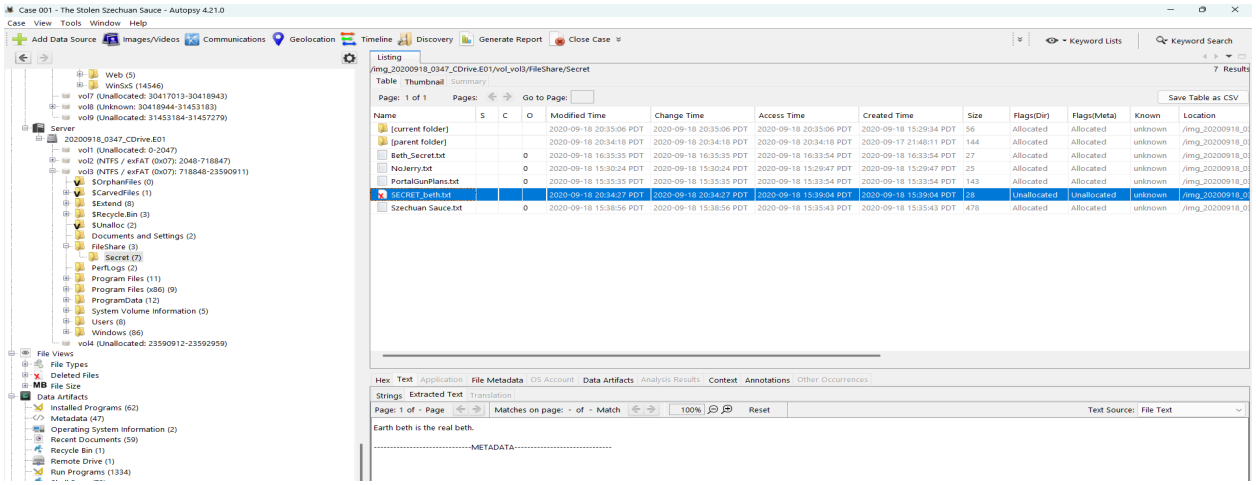
Yes, the attacker accessed and stole data on both server and desktop. Two files were created and exfiltrated called “**Loot.zip” and “Secret.zip.”**





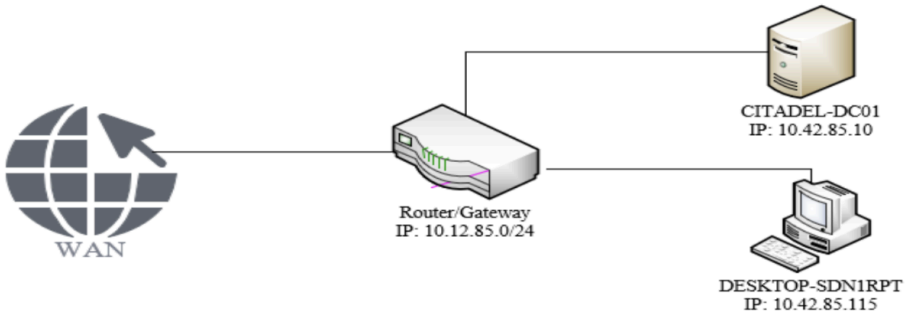


The attacker stole data from the **Server CITADEL-DC01 on September 18 2020 at 15:38:56 PDT** from the “Secret” folder in “FileShare” by archiving the “Secret” folder to Secret.zip. We believe the Secret Szechuan Sauce recipe was inside the file.



9. What was the network layout of the victim network?

Gateway: C137 (10.42.85.0/24)
Desktop: DESKTOP-SDN1RPT (10.42.85.115)
Server: CITADEL-DC01 (10.42.85.10)



10. What architecture changes should be made immediately?

Given the attacker's successful RDP brute force access to CITADEL-DC01, it's imperative to bolster RDP security. Here are specific recommendations as per NIST Cybersecurity Framework (NIST, 2020)

- **Patch Management:** Ensure operating systems and applications are updated with the latest security patches to address known vulnerabilities.
- **Multi-Factor Authentication (MFA):** Implement MFA as a mandatory requirement for all RDP connections, adding an extra layer of protection beyond passwords.
- **Privileged Access Management (PAM):** Enforce strict controls on privileged access, granting only necessary permissions to authorized users.
- **Password Hygiene:** Mandate strong, unique passwords for RDP accounts and enforce regular password changes.
- **Stored Password Elimination:** Avoid storing passwords locally. Consider using password vaults or single sign-on (SSO) solutions.
- **RDP Connection History:** Regularly clean RDP connection history to minimize the risk of unauthorized access.
- **Network Level Authentication (NLA):** Require NLA for all RDP sessions to verify user credentials before allowing a connection.
- **Firewall Restrictions:** Configure firewalls to strictly allow only authorized IP addresses to connect to RDP.
- **RDP Gateways:** Deploy RDP gateways to centralize and manage RDP connections, providing additional security measures.
- **Port Number Change:** Modify the default RDP port to make it less discoverable by attackers.

By implementing these security measures, you can significantly reduce the risk of future RDP-based attacks and protect your systems from unauthorized access.

References

Definition of XOR. PCMAG. (n.d.). https://www.pcmag.com/encyclopedia/term/xor

Force, J. T. (2020, December 10). *Security and Privacy Controls for Information Systems and organizations*. CSRC. https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final

James. (2021, January 15). *Answers to the case of the stolen szechuan sauce (CASE001)*. DFIR Madness. https://dfirmadness.com/answers-to-szechuan-case-001/

LevelBlue - Open Threat Exchange. LevelBlue Open Threat Exchange. (n.d.). https://otx.alienvault.com/indicator/ip/203.78.103.109

Pearson, A. (2021, May 10). *Volatility 3 CheatSheet*. onfvp. https://blog.onfvp.com/post/volatility-cheatsheet/

Penetration testing software, PEN testing security. Metasploit. (n.d.). https://www.metasploit.com/

Persistence. Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®. (n.d.). https://attack.mitre.org/tactics/TA0003/

Shah, P. (2022, December 27). *How to change the time zone settings on windows*. MUO. https://www.makeuseof.com/windows-change-time-zone/#:~:text=In%20the%20Registry%20Editor%20window,to%20use%20and%20click%20OK

Virustotal. (n.d.). https://www.virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6/behavior