

The Stolen Szechuan Sauce



Sabah Dürkiye and Raquel Bueno

October 23, 2023

Lighthouse Labs

Executive Summary

In the realm of increasingly complex cyber threats, our project investigates a simulated cyber incident called "The Stolen Szechuan Sauce," crafted by DFIR Madness to emulate real-world scenarios. Utilizing forensic tools such as Autopsy, FTK Imager, Volatility, and Wireshark, our team—comprising Sabah and Raquel—developed into disk images, packet captures, and memory dumps from two implicated systems: a Microsoft Windows Server 2012 and a Windows 10 desktop. Our investigation confirmed a security breach executed through RDP brute-force attacks, identifying the use of a Metasploit Trojan named Coreupdater.exe. We also pinpointed malicious IP addresses 194.61.24.102 and 203.78.103.109 as being involved in the attack. Intriguingly, files in a "Secret" folder were found to be accessed and modified, indicating data compromise. Both systems were part of the same network block 10.42.85.0/24. Conclusively, our findings offer a detailed forensic account, highlighting areas of vulnerability while recommending immediate containment and long-term security enhancements. The insights gained from this investigation not only resolve the questions posed by this particular case but also serve as educational material for future cybersecurity efforts.

Introduction

The landscape of cybersecurity is rife with complexities, requiring experts to not only thwart cyber threats but also to dig deep into the digital remnants left behind during security incidents. One such intricate case that necessitates thorough investigation is the case of "The Stolen Szechuan Sauce." Crafted as a hands-on exercise by DFIR Madness, this project offers a simulated environment that aims to imitate real-world cybersecurity issues. This report serves as a comprehensive account of our digital forensic investigation, delving into the various questions surrounding the cyber event in question.

The scenario involves two distinct computational systems: a server and a desktop each implicated in the cyber event under investigation. We have acquired multiple types of evidence files, ranging from disk images (E01) to packet capture files (PCAP) and memory dumps, to develop a holistic understanding of the incident. By leveraging a range of forensic tools and methodologies, this investigation endeavors to uncover the facts related to the cyber incident, from confirming a breach to identifying malware and tracing the adversary's steps.

Our investigation is framed by a series of questions aimed at driving the inquiry to achieve its intended goals. Each question will be addressed methodically, leveraging appropriate forensic tools and techniques. This report not only documents our findings but also substantiates them with necessary screenshots, logs, and other relevant artifacts.

Due to the extensive nature of the evidence files, this project has been undertaken collaboratively. Both team members have contributed actively to the investigative process, as detailed within the report.

Overview of Forensic Tools

First of all, to understand the analysis done, it is important to know a few key concepts.

According to Forensics College, “Autopsy, it is a digital forensics platform and graphical interface that forensic investigators use to understand what happened on a phone or computer.. Select modules in Autopsy can do timeline analysis, hash filtering, and keyword search. In addition, they can extract web artifacts, recover deleted files from unallocated space, and find indicators of compromise. All of this can be done relatively rapidly”.

According to the same source about FTK Imager, it is possible to learn that it is a “tool that analyzes images of a drive and preserves the original integrity of the evidence without affecting its original state”.

Another very important forensic tool according to Forensics College, “the Volatility Foundation focuses on volatile memory (RAM) forensics. This allows the preservation of evidence in memory that would otherwise be lost during a system shutdown”.

Wireshark is the world’s most-used network protocol analysis tool, that according to the same source “implemented by governments, private corporations, and academic institutions worldwide. Wireshark lets a user see what is happening on a network at the microscopic level. By capturing network traffic, users can then scan for malicious activity”.

Considerations

The project was written and analyzed by both students, Sabah and Raquel, together via google doc and zoom meetings, respectively.

Raquel was responsible to download the six first files while Sabah downloaded the Desktop files, as shown below:

DC01 Disk Image (E01)

DC01 Memory and PageFile

DC01 Autoruns

DC01 Protected Files

Case001 PCAP

Desktop Disk Image (E01)

Desktop Memory and PageFile

Desktop Autoruns

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 422046B753CF8A4DF49D2C4CE892DB16 case001-pcap.zip

MD5 964F2D710687D170C77C94947DA29E66 DC01-autorunsc.zip

MD5 E57FC636E833C5F1AB58DFACE873BBDE DC01-E01.zip

MD5 64A4E2CB47138084A5C2878066B2D7B1 DC01-memory.zip

MD5 964EEAF0009D08CC101DE4A83A4E5D23 DC01-pagefile.zip

MD5 AD29830A583EFE49C8C1C35FAFFD264F DC01-ProtectedFiles.zip

MD5 71C5C3509331F472ABCDF81EB6EFF07 DESKTOP-E01.zip

MD5 3627DCAFA54E1365489A4EC0CC3D6A1C DESKTOP-SDN1RPT-autrunsc.zip

MD5 CF31E2635C77811AAA1BB04A92A721E2 DESKTOP-SDN1RPT-memory.zip

MD5 45C096F2688A0B5DE0346FB72391B245 Desktop-SDN1RPT-pagefile.zip

MD5 3E1A358D50003A9351AC2160AE6F0495 DESKTOP-SDN1RPT-Protected Files.zip

Question

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

The Operating System is Microsoft Windows Server 2012.

Using Autopsy, we were able to identify the OS in the file tree.

The screenshot shows the Autopsy Forensic Browser interface. On the left is a file tree view of a QEMU (Windows1) image. The tree includes various language and regional settings like hr-HR, hu-HU, and ko-KR, along with system folders such as InputMethod, LogFiles, and Microsoft. A 'Licenses' folder is expanded, showing 'neutral' and 'Eval' sub-folders, with 'ServerStar' being the file selected. The main pane displays a table titled 'Table' with three results. The columns are Name, S, C, O, Modified Time, Change Time, Access Time, and Created Time. The table shows three entries: '[current folder]', '[parent folder]', and 'license.rtf'. The 'license.rtf' entry has a modified time of 2014-03-21 14:27:38 EDT, a change time of 2020-09-17 12:50:47 EDT, and an access time of 2014-03-21 14:27:38 EDT. The created time is 2013-08-22 11:23:45. Below the table are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The 'Text' tab is active, showing the content of the 'license.rtf' file. The text is the Microsoft Software License Terms for Windows Server 2012 R2 Standard, which states that the terms apply to the software named above and any Microsoft updates, supplements, Internet-based services, and support services. It also mentions that other terms apply if specific items are included. The 'Activate Windows' watermark is visible across the text area.

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
[current folder]				2014-03-21 14:27:38 EDT	2020-09-17 12:50:47 EDT	2014-03-21 14:27:38 EDT	2014-03-21 14:27:38 EDT
[parent folder]				2014-03-21 14:27:38 EDT	2020-09-17 12:50:47 EDT	2014-03-21 14:27:38 EDT	2013-08-22 11:23:45
license.rtf	1			2013-08-16 17:20:18 EDT	2020-09-17 12:48:51 EDT	2013-08-22 08:12:39 EDT	2013-08-22 08:12:39 EDT

And also using Volatility, we were to prove that the server is Windows 2012, as shown in the image below.

```

38.103.158.146:11236
C:\ Command Prompt - volatility -f C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem psxview
PsActiveProcessHead : 0xffffffff800cbab40a0 (40 processes)
PsLoadedModuleList : 0xffffffff800cbace2d0 (154 modules)
KernelBase : 0xffffffff800cb804000 (Matches MZ: True)
Major (OptionalHeader) : 6
Minor (OptionalHeader) : 3
KPCR : 0xffffffff800cbaeaa000 (CPU 0)
KPCR : 0xfffffd00019fd55000 (CPU 1)

Interrupted

C:\Users\user1\Desktop\VolLab2>volatility -f C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win8SP0x64, Win81U1x64, Win2012R2x64, Win2012x64, Win8SP1x64_18340, Win8SP1x64 (Instantiated with Win8SP1x64)
          AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
          AS Layer2 : FileAddressSpace (C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem)
            PAE type : No PAE
            DTB : 0x1a7000L
            KDBG : 0xf800cba9ba20L
  Number of Processors : 2
Image Type (Service Pack) : 0
          KPCR for CPU 0 : 0xffffffff800cbaea000L
          KPCR for CPU 1 : 0xfffffd00019fd55000L
        KUSER_SHARED_DATA : 0xffffffff78000000000L
  Image date and time : 2020-09-19 04:39:59 UTC+0000
Image local date and time : 2020-09-18 21:39:59 -0700

C:\Users\user1\Desktop\VolLab2>
C:\Users\user1\Desktop\VolLab2>volatility -f C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
-----
```

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

The operating system of the desktop is Windows 10, and the way this was found using Autopsy.

Source Name	S	C	O	Name	Domain	Program Name
20200918_0417_DESKTOP-SDN1RPT.E01				DESKTOP-SDN1RPT	C137.local	Windows 10 Enterprise Evaluation

Type	Value	Source(s)
Name	DESKTOP-SDN1RPT	Recent Activity
Domain	C137.local	Recent Activity
Processor	AMD64	Recent Activity
Temporary F	%SystemRoot%\TEMP	Recent Activity
Path	C:\Windows	Recent Activity
Product ID	00329-20000-00001-AA089	Recent Activity
Owner	Admin	Recent Activity
Source File P	/img_20200918_0417_DESKTOP-SDN1RPT.E01	
Artifact ID	-9223372036854775616	

3. What was the local time of the Server?

According to dfirmadness.com, there is a note that says: "Incident occurred at an organization located in Colorado in September. So, this places the incident at UTC-6".

Note: This incident occurred at an organization located in Colorado in September. So, this places the incident at UTC -6. Keep this in mind when looking at the output of various tools.

So, it is safe to say that it is talking about Mountain Standard Time (MST).

```
38.103.158.146:11236
C:\ Command Prompt - volatility -f C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem psxview
PsActiveProcessHead : 0xfffffff800cbab40a0 (40 processes)
PsLoadedModuleList : 0xfffffff800cbace2d0 (154 modules)
KernelBase : 0xfffffff800cb804000 (Matches MZ: True)
Major (OptionalHeader) : 6
Minor (OptionalHeader) : 3
KPCR : 0xfffffff800cbaea000 (CPU 0)
KPCR : 0xffffffd0019fd50000 (CPU 1)

Interrupted

C:\Users\user1\Desktop\Vollab2>volatility -f C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem imageinfo
Volatility Foundation Volatility Framework 2.6
INFO : volatility.debug : Determining profile based on KDBG search...
Suggested Profile(s) : Win8SP0x64, Win81UIx64, Win2012R2x64_18340, Win2012R2x64, Win2012x64, Win8SP1x64_18340, Win8SP1x64 (Instantiated with Win8SP1x64)
AS Layer1 : WindowsAMD64PagedMemory (Kernel AS)
AS Layer2 : FileAddressSpace (C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem)
PAE type : No PAE
DTB : 0x1a7000L
KDBG : 0xf800cba9ba20L
Number of Processors : 2
Image Type (Service Pack) : 0
KPCR for CPU 0 : 0xfffffff800cbaea000L
KPCR for CPU 1 : 0xffffffd0019fd50000L
KUSER_SHARED_DATA : 0xfffffff780000000000L
Image date and time : 2020-09-19 04:39:59 UTC+0000
Image local date and time : 2020-09-18 21:39:59 -0700

C:\Users\user1\Desktop\Vollab2>
C:\Users\user1\Desktop\Vollab2>
C:\Users\user1\Desktop\Vollab2>volatility -f C:\Users\user1\Desktop\VolatilityWorkbench\citadeldc01.mem psxview
Volatility Foundation Volatility Framework 2.6
Offset(P) Name PID pslist psscan thrdproc pspcid csrss session deskthrd ExitTime
-----
```

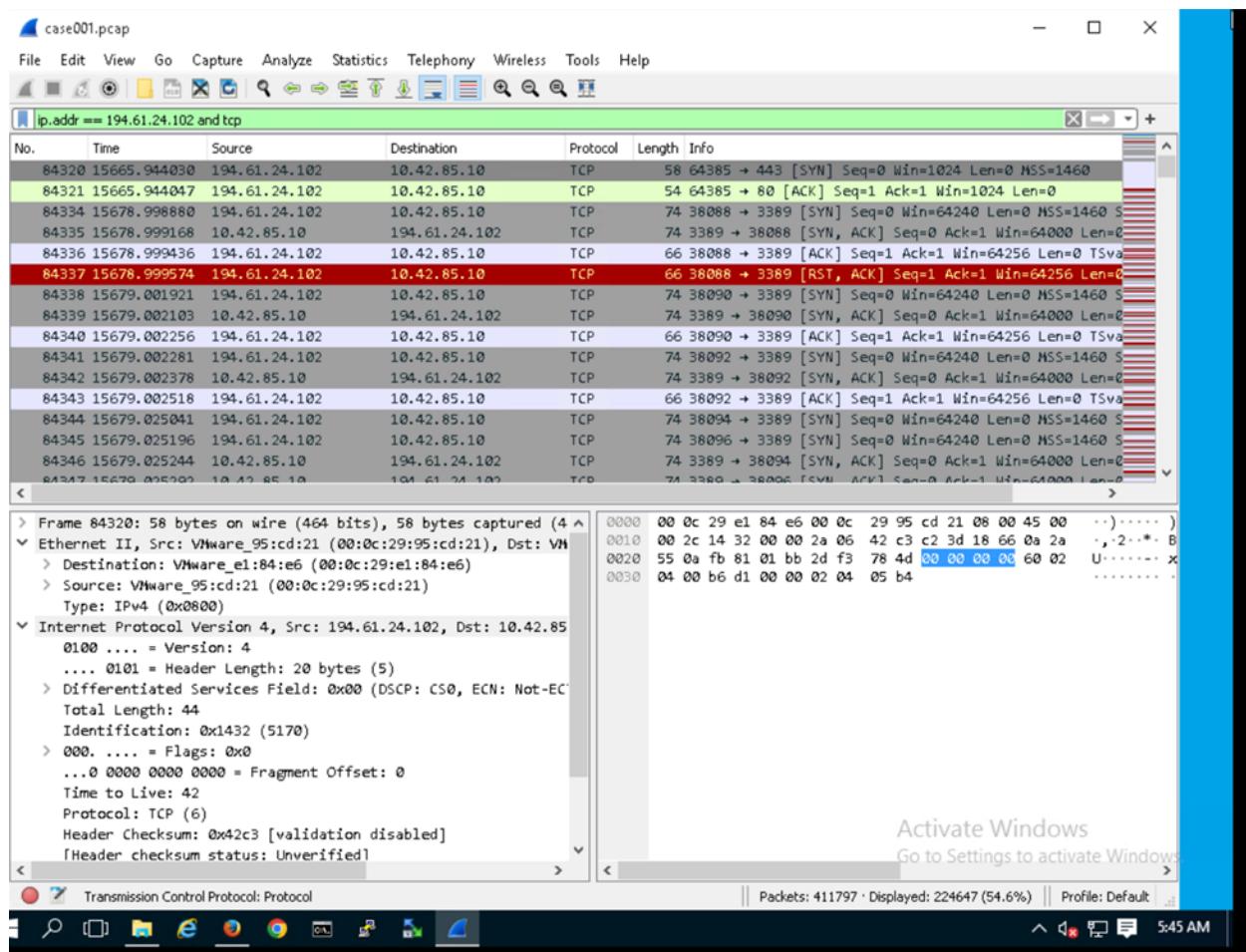
However, when we used Volatility to read the memory, we found that the image local time was 21:39:49 (UTC -0700).

4. Was there a breach?

Yes, it will be provided more information throughout this project.

5. What was the initial entry vector (how did they get in)?

The initial attack vector was identified as RDP brute force, as evidenced by multiple SYN requests targeting the same destination port. This observation was made using the filter ip.addr==194.61.24.102 and tcp in the analysis of the case001.PCAP file.



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

Malware was indeed employed in the form of a metasploit Trojan. To verify the malicious nature of the Coreupdater.exe process, it can be analyzed using threat detection platforms like VirusTotal.

59 / 71

① 59 security vendors and 1 sandbox flagged this file as malicious

10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

coreupdater.exe

Size 7.00 KB | Last Analysis Date 2 months ago | EXE

peexe assembly runtime-modules idle spreader direct-cpu-clock-access 64bits

Community Score

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 13 +

Join the VT Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

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

Security vendors' analysis

Vendor	Status	Analysis	Action
Acronis (Static ML)	Suspicious	AhnLab-V3	① Trojan:Win64.RL_Shelma.R298109
Alibaba	① Trojan:Win64/Shelma.27173393	ALYac	① Trojan.Metasploit Go to Settings to activate Windows
Anti~AVL	① GrayWare/Win32.Rozena.j	Arcabit	① Trojan.Metasploit.A

Do you want to automate checks?

eed41b4500e473197c50c7385ef5e379

1d153c66386ca93ec993d66a84d6fd129a35c

10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

07303615165b2z12

88763e60ed0afdf8a0a1647782b597542d9667d2b9a35fb2623967e302fa28e

b4c6ff030479aa3b12625be67bf4914

1b4d46e6987f41400b39f78a8cc6ce739

24:eFGStrJ9u0/6ZAGnZd0@QAVs2Pb85n8acX3bTJBm2uJ65OxCLYk9fpmBis0e0BQx2Pbqn8LHCJ65+CR9sB

T1A3EB947379C96FC0EE577501E6F69831841522BF7875905411090CC232C5AB8F85

Win32 EXE executable windows win32 pe peexe

PEx32+ executable (GUI) x86-64, for MS Windows

Win16 NE executable (generic) (38.3%) Windows Icons Library (generic) (15.6%) OS/2 Executable (generic) (15.4%) Generic

WinxDOS Executable (15.2%) DDS Executable Generic (15.2%)

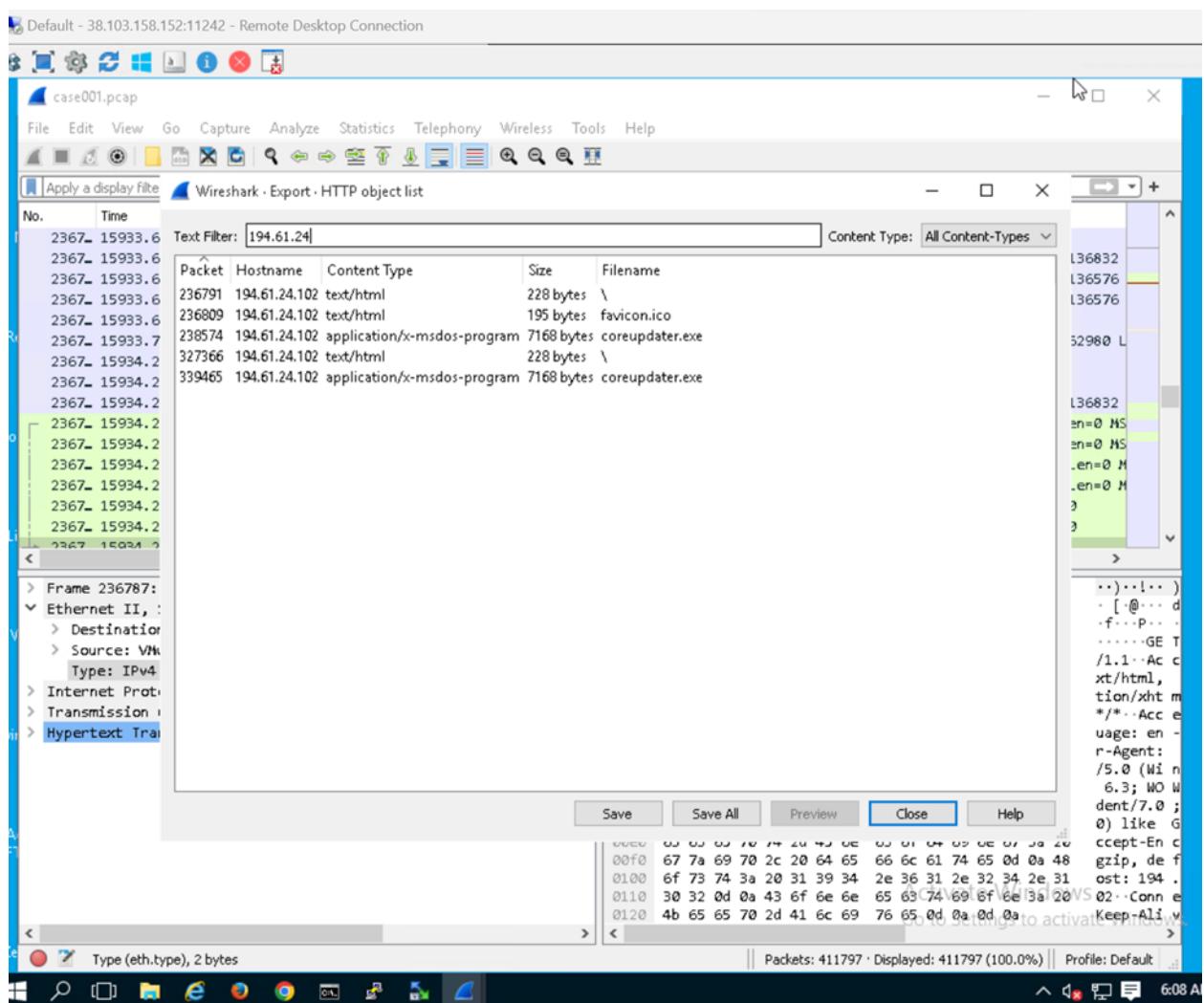
PEx64 Compiler: Microsoft Visual C/C++ (2008 SP1) Compiler: MASM (9.00.30729) Linker: Microsoft Linker (9.00.30729)

7.00 KB (7168 bytes)

Activate Windows Go to Settings to activate Windows

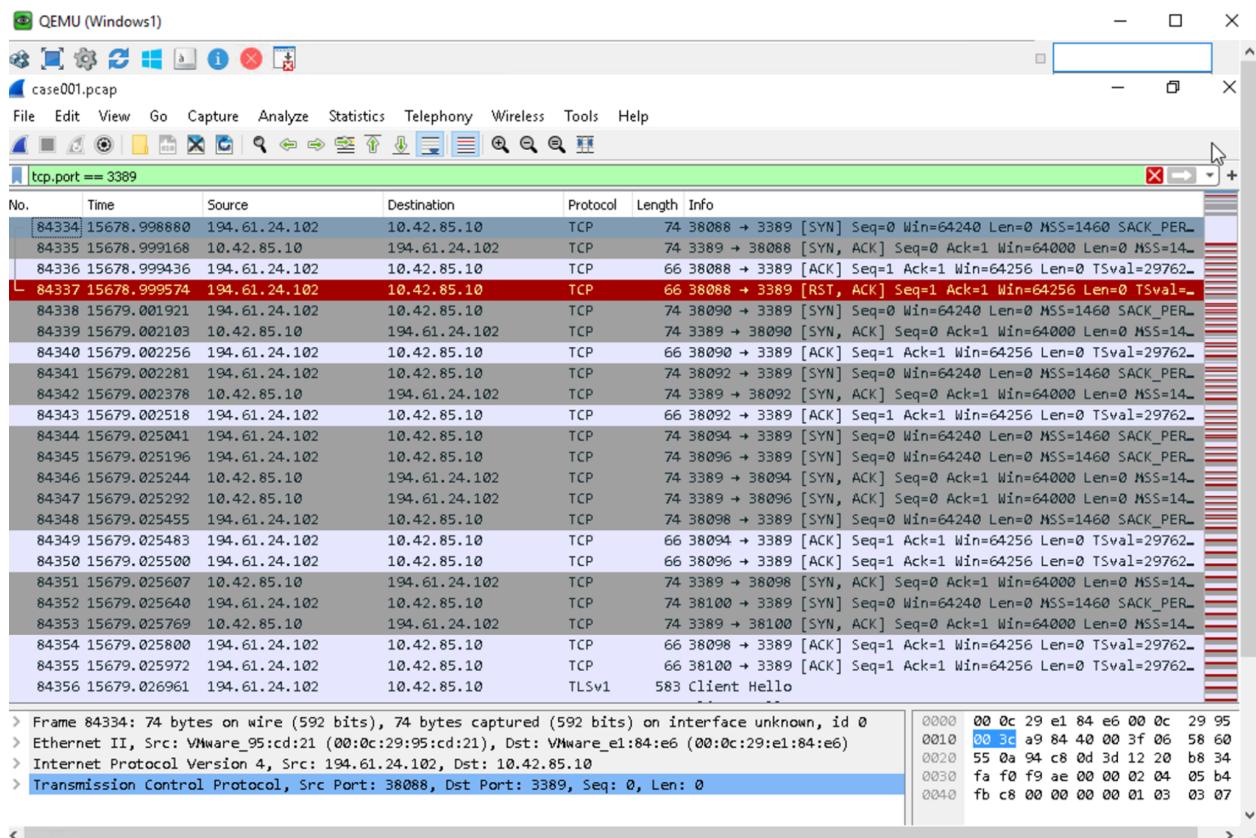
- **What process was malicious?**

The Malicious process identified during the investigation was Coreupdate.exe, which was recognized as a Metasploit Trojan. Further validation of its malicious nature was conducted by analyzing the file to examine it.



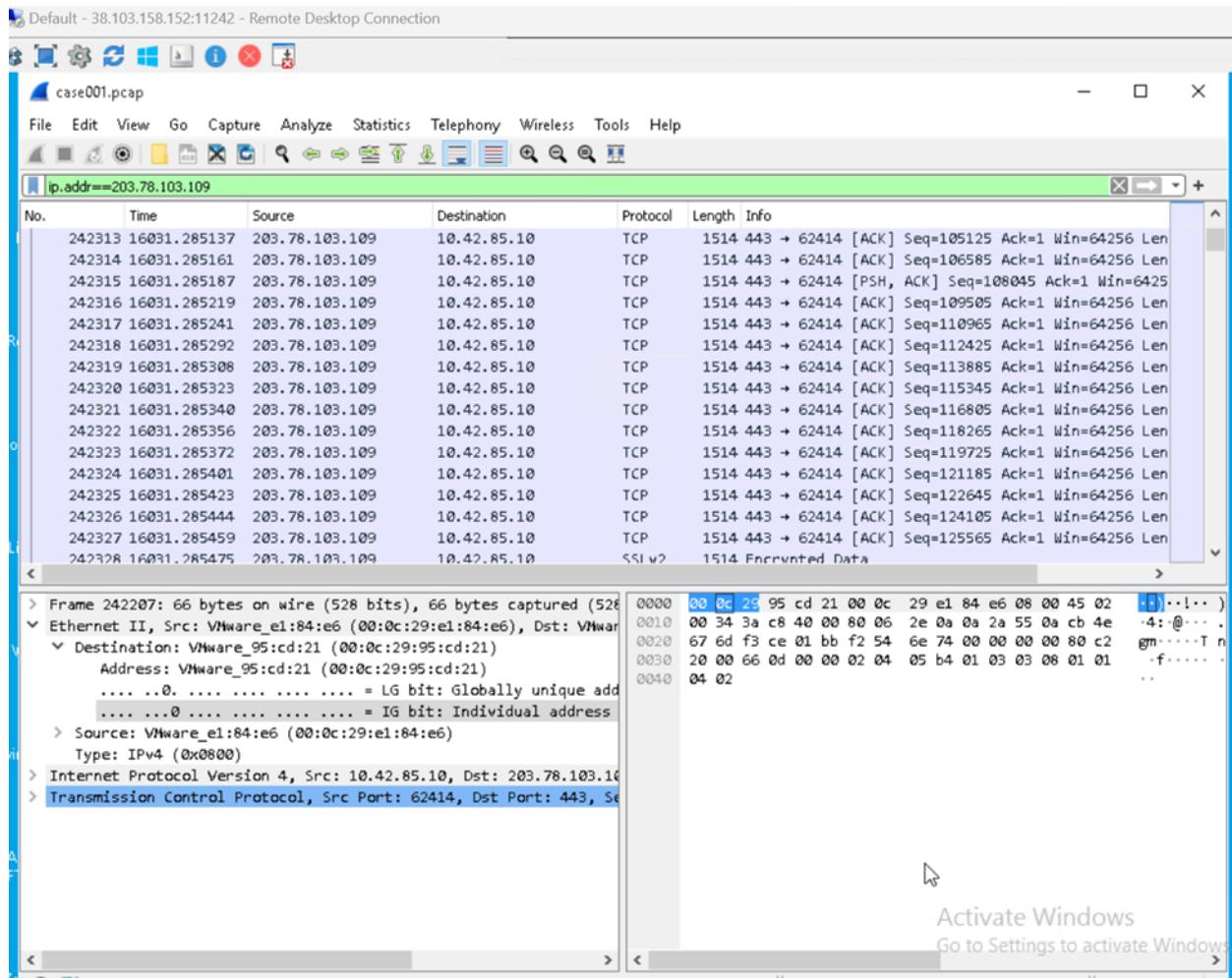
- Identify the IP Address that delivered the payload?

As observed in the packet capture data, the IP address 194.61.24.102 repeatedly initiated SYN requests targeted at the RDP port 3389, originating from a variety of source ports.



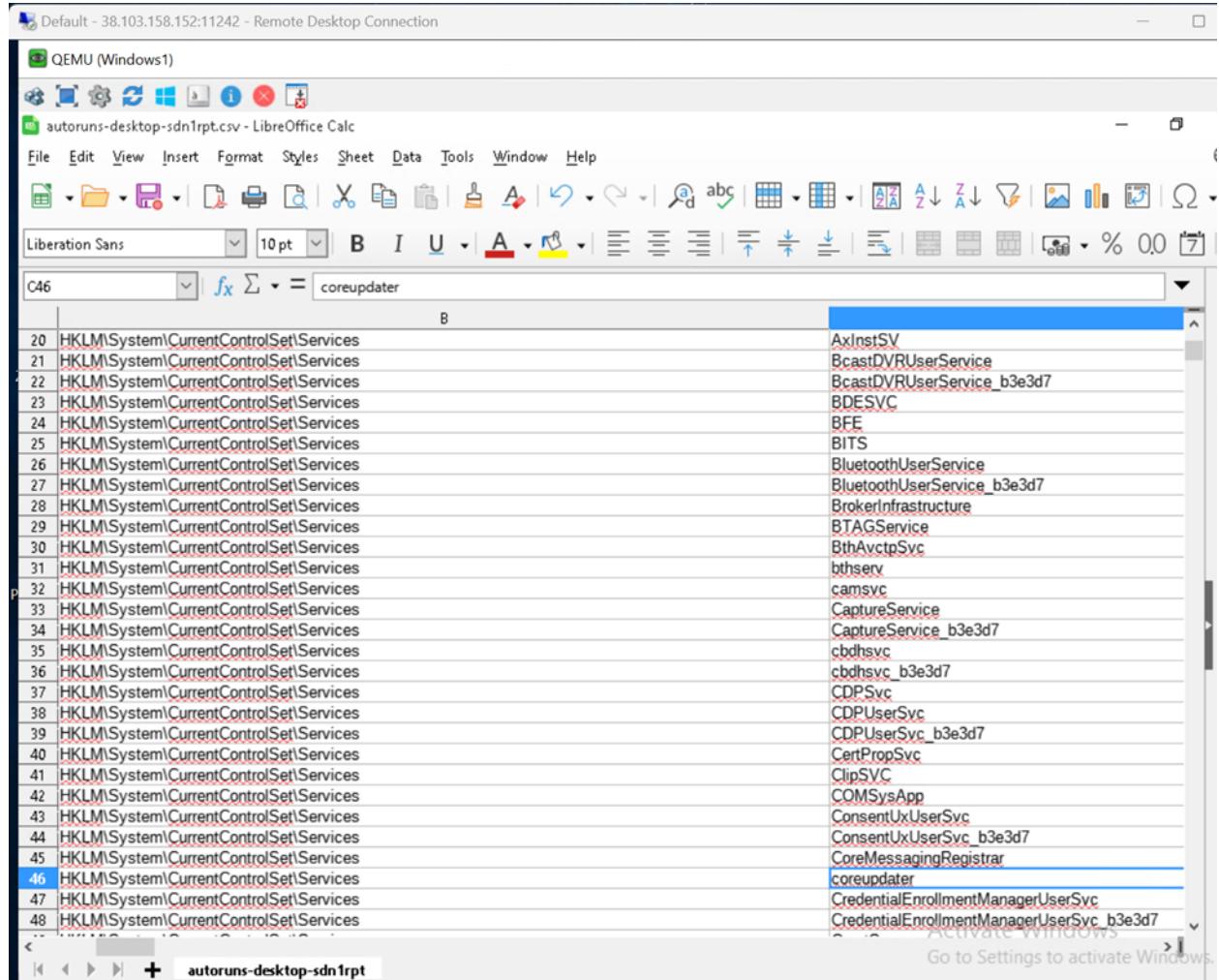
- What IP Address is the malware calling to?

In the PCAP file analysis, we noticed that the malware is establishing outgoing connections to a specific address. The most frequently contacted IP in the dataset was 203.78.103.109.



- Where is this malware on disk?

The malware is located on the disk at following file path
 C:\Windows\System32\coreupdater.exe.



Services	Path
HKLM\System\CurrentControlSet\Services	AxInstSV
HKLM\System\CurrentControlSet\Services	BcastDVRUserService
HKLM\System\CurrentControlSet\Services	BcastDVRUserService_b3e3d7
HKLM\System\CurrentControlSet\Services	BDEsvc
HKLM\System\CurrentControlSet\Services	BFE
HKLM\System\CurrentControlSet\Services	BITs
HKLM\System\CurrentControlSet\Services	BluetoothUserService
HKLM\System\CurrentControlSet\Services	BluetoothUserService_b3e3d7
HKLM\System\CurrentControlSet\Services	BrokerInfrastructure
HKLM\System\CurrentControlSet\Services	BTAGService
HKLM\System\CurrentControlSet\Services	BthAvctpSvc
HKLM\System\CurrentControlSet\Services	bthserv
HKLM\System\CurrentControlSet\Services	camsvc
HKLM\System\CurrentControlSet\Services	CaptureService
HKLM\System\CurrentControlSet\Services	CaptureService_b3e3d7
HKLM\System\CurrentControlSet\Services	cbdhsvc
HKLM\System\CurrentControlSet\Services	cbdhsvc_b3e3d7
HKLM\System\CurrentControlSet\Services	CDPSvc
HKLM\System\CurrentControlSet\Services	CDPUserSvc
HKLM\System\CurrentControlSet\Services	CDPUserSvc_b3e3d7
HKLM\System\CurrentControlSet\Services	CertPropSvc
HKLM\System\CurrentControlSet\Services	ClipSVC
HKLM\System\CurrentControlSet\Services	COMSysApp
HKLM\System\CurrentControlSet\Services	ConsentUxUserSvc
HKLM\System\CurrentControlSet\Services	ConsentUxUserSvc_b3e3d7
HKLM\System\CurrentControlSet\Services	CoreMessagingRegistrar
HKLM\System\CurrentControlSet\Services	coreupdater
HKLM\System\CurrentControlSet\Services	CredentialEnrollmentManagerUserSvc
HKLM\System\CurrentControlSet\Services	CredentialEnrollmentManagerUserSvc_b3e3d7

QEMU (Windows1)

autoruns-desktop-sdn1rpt.csv - LibreOffice Calc

File Edit View Insert Format Styles Sheet Data Tools Window Help

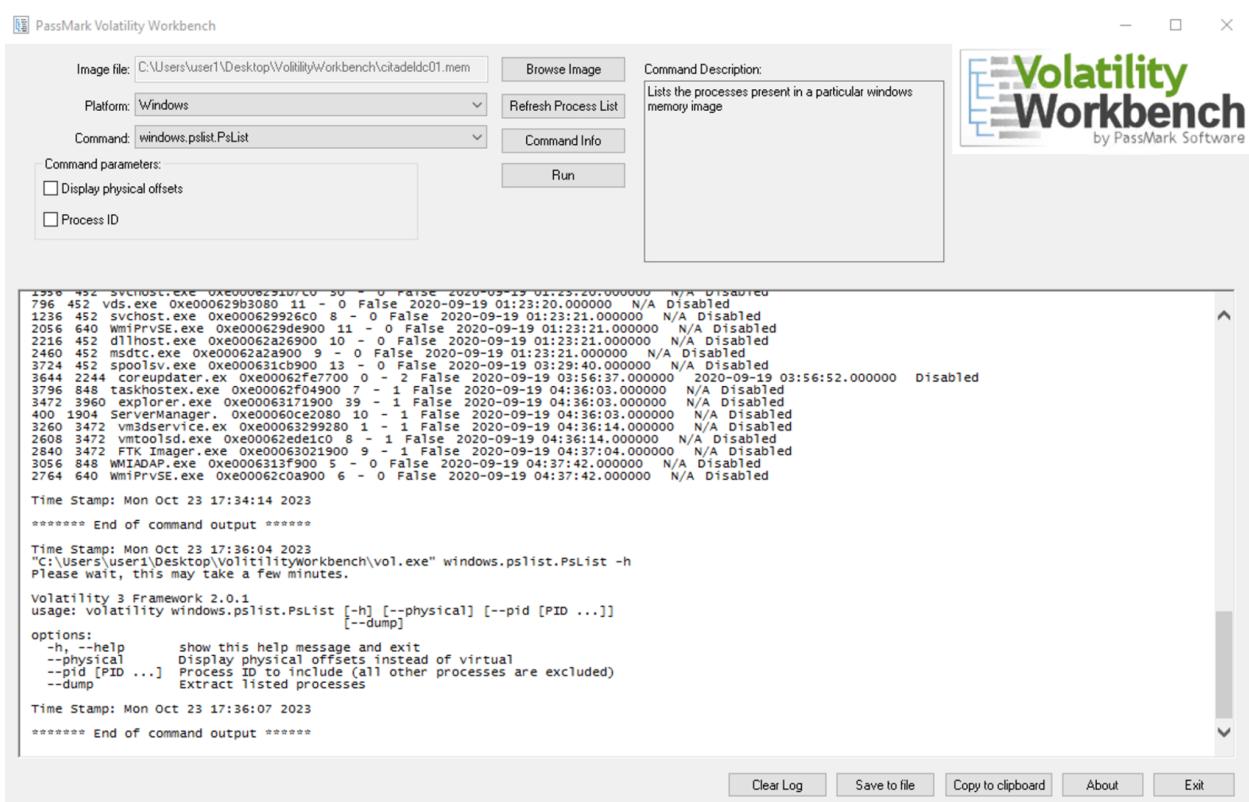
Liberation Sans 10 pt B I U A fx Σ = coreupdater

	I	J
20	Microsoft Corporation	c:\windows\system32\axinstsv.dll
21	Microsoft Corporation	c:\windows\system32\bcastdryuserservice.dll
22	Microsoft Corporation	c:\windows\system32\svchost.exe
23	Microsoft Corporation	c:\windows\system32\bdesvc.dll
24	Microsoft Corporation	c:\windows\system32\bfe.dll
25	Microsoft Corporation	c:\windows\system32\qmgr.dll
26	Microsoft Corporation	c:\windows\system32\microsoft.bluetooth.userservice.dll
27	Microsoft Corporation	c:\windows\system32\svchost.exe
28	Microsoft Corporation	c:\windows\system32\psmsrv.dll
29	Microsoft Corporation	c:\windows\system32\btagservice.dll
30	Microsoft Corporation	c:\windows\system32\bthavctpsvc.dll
31	Microsoft Corporation	c:\windows\system32\btbserv.dll
32	Microsoft Corporation	c:\windows\system32\capabilityaccessmanager.dll
33	Microsoft Corporation	c:\windows\system32\captureservice.dll
34	Microsoft Corporation	c:\windows\system32\svchost.exe
35	Microsoft Corporation	c:\windows\system32\cbdhsvc.dll
36	Microsoft Corporation	c:\windows\system32\svchost.exe
37	Microsoft Corporation	c:\windows\system32\cdpsvc.dll
38	Microsoft Corporation	c:\windows\system32\cdpusersvc.dll
39	Microsoft Corporation	c:\windows\system32\svchost.exe
40	Microsoft Corporation	c:\windows\system32\certprop.dll
41	Microsoft Corporation	c:\windows\system32\clipsvc.dll
42	Microsoft Corporation	c:\windows\system32\dllhost.exe
43	Microsoft Corporation	c:\windows\system32\consentuxclient.dll
44	Microsoft Corporation	c:\windows\system32\svchost.exe
45	Microsoft Corporation	c:\windows\system32\coremessaging.dll
46		c:\windows\system32\coreupdater.exe
47	Microsoft Corporation	c:\windows\system32\credentialenrollmentmanager.exe
48	Microsoft Corporation	c:\windows\system32\credentialenrollmentmanager.exe

autoruns-desktop-sdn1rpt

- When did it first appear?

According to Volatility Workbench, the malware (coreupdater.exe) first appeared on the disk on 202-09-19 03:56:37.



The screenshot shows the Volatility Workbench interface with the following details:

- Image file:** C:\Users\user1\Desktop\Volatility\workbench\citadeldc01.mem
- Platform:** Windows
- Command:** windows.pslist.PsList
- Command Description:** Lists the processes present in a particular windows memory image
- Command parameters:**
 - Display physical offsets
 - Process ID
- Output (Partial):**

```

1236 452 svchost.exe 0xe000629b3080 11 - 0 False 2020-09-19 01:23:20.000000 N/A Disabled
1236 452 vds.exe 0xe000629b3080 11 - 0 False 2020-09-19 01:23:20.000000 N/A Disabled
1236 452 svchost.exe 0xe000629926c 8 - 0 False 2020-09-19 01:23:21.000000 N/A Disabled
2056 640 WmiPrvSE.exe 0xe000629de900 11 - 0 False 2020-09-19 01:23:21.000000 N/A Disabled
2216 452 dlnhost.exe 0xe00062a2d900 10 - 0 False 2020-09-19 01:23:21.000000 N/A Disabled
2460 452 netdlnhost.exe 0xe00062a2d900 9 - 0 False 2020-09-19 01:23:21.000000 N/A Disabled
3724 452 spoolsv.exe 0xe000621cb900 13 - 0 False 2020-09-19 03:29:40.000000 N/A Disabled
3644 2244 coreupdater.exe 0xe00062fe7700 0 - 2 False 2020-09-19 03:56:37.000000 2020-09-19 03:56:52.000000 Disabled
3796 848 taskhostex.exe 0xe00062f04900 7 - 1 False 2020-09-19 04:36:03.000000 N/A Disabled
3472 3960 explorer.exe 0xe00063171900 39 - 1 False 2020-09-19 04:36:03.000000 N/A Disabled
400 1904 ServerManager. 0xe00060ce2080 10 - 1 False 2020-09-19 04:36:03.000000 N/A Disabled
3260 3472 vm3dservice.ex 0xe00063299280 1 - 1 False 2020-09-19 04:36:14.000000 N/A Disabled
2608 3472 spoolsd.exe 0xe00062ed1c0 8 - 1 False 2020-09-19 04:36:14.000000 N/A Disabled
2846 3472 FTKImage.exe 0xe00062e0501900 9 - 1 False 2020-09-19 04:37:44.37:04.000000 N/A Disabled
3056 848 WMIADAP.exe 0xe0006131900 5 - 0 False 2020-09-19 04:37:42.000000 N/A Disabled
2764 640 WmiPrvSE.exe 0xe00062c0a900 6 - 0 False 2020-09-19 04:37:42.000000 N/A Disabled

```
- Time Stamp:** Mon Oct 23 17:34:14 2023
- ***** End of command output *******
- Time Stamp:** Mon Oct 23 17:36:04 2023
- C:\Users\user1\Desktop\Volatility\workbench\vol.exe" windows.pslist.PsList -h**
- Please wait, this may take a few minutes.**
- Volatility 3 Framework 2.0.1**
- usage: volatility windows.pslist.PsList [-h] [--physical] [--pid [PID ...]] [--dump]**
- options:**
 - h --help show this help message and exit
 - physical Display physical offsets instead of virtual
 - pid [PID ...] Process ID to include (all other processes are excluded)
 - dump Extract listed processes
- Time Stamp:** Mon Oct 23 17:36:07 2023
- ***** End of command output *******

- **What were the capabilities of this malware?**

The malware possesses the following capabilities:

- ★ Data Exfiltration: It can steal confidential information such as passwords or trade secrets.
- ★ Remote Administration: It enables the intruder to remotely manage the compromised system through a backdoor.
- ★ Encryption and Ransom Requirement: Often seen in ransomware types, it can encode files and request payment for their release.
- ★ Lateral Movement: The malware can disseminate itself to other contacts or systems within the same network.
- ★ System Sabotage: In specific instances, the malware can deliberately disable or entirely wipe out your computing resources, resulting in substantial damage.

- **Is this malware easily obtained?**

The malicious software was detected relocating itself from the Administrator's Downloads folder to a critical system directory, namely C:\Windows\System32. Such behavior implies an attempt by the malware to conceal itself among key system files, potentially to establish long-term persistence and exert greater control over the system.

- **Was this malware installed with persistence on any machine?**

Yes, it was integrated both into the Windows registry and as a system service. Following a successful brute-force attack on the domain controller, the malware was laterally transferred into the system, embedding itself within the registry processes.

7. What malicious IP Addresses were involved?

1. Were any IP Addresses from known adversary infrastructure?

The IP addresses identified as malicious in this case were 194.61.24.102 and 203.78.103.109. Prior to the incident, 194.61.24.102 was already flagged for involvement in RDP Brute Force attacks. Meanwhile, 203.78.103.109 had a brief association with the domain happydoghappycat-th.com, which is suspected of involvement with an Advanced Persistent Threat (APT). As shown in the pictures below.

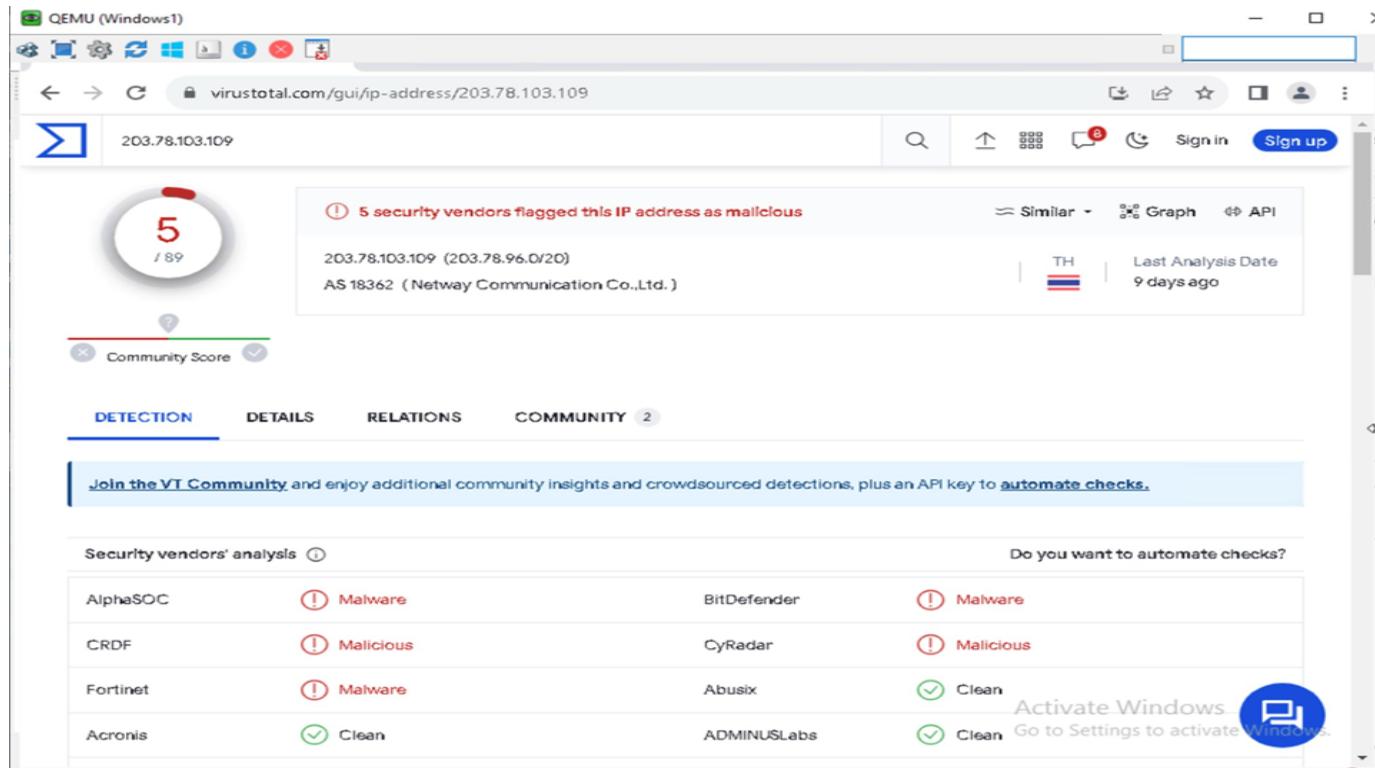
2. Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?

Only these two IP addresses participated in the attack. It is possible to see that in the pictures below.

The screenshot shows the VirusTotal analysis interface for the IP address 194.61.24.102. At the top, a message indicates "1 security vendor flagged this IP address as malicious". Below this, the IP address is listed again. To the right, there are buttons for "Similar", "Graph", and "API". Further down, the "RU" flag and "Last Analysis Date: 18 days ago" are shown. The main content area displays a "Community Score" bar and four tabs: DETECTION, DETAILS, RELATIONS, and COMMUNITY. Under the DETECTION tab, a section titled "Security vendors' analysis" lists various vendors and their findings:

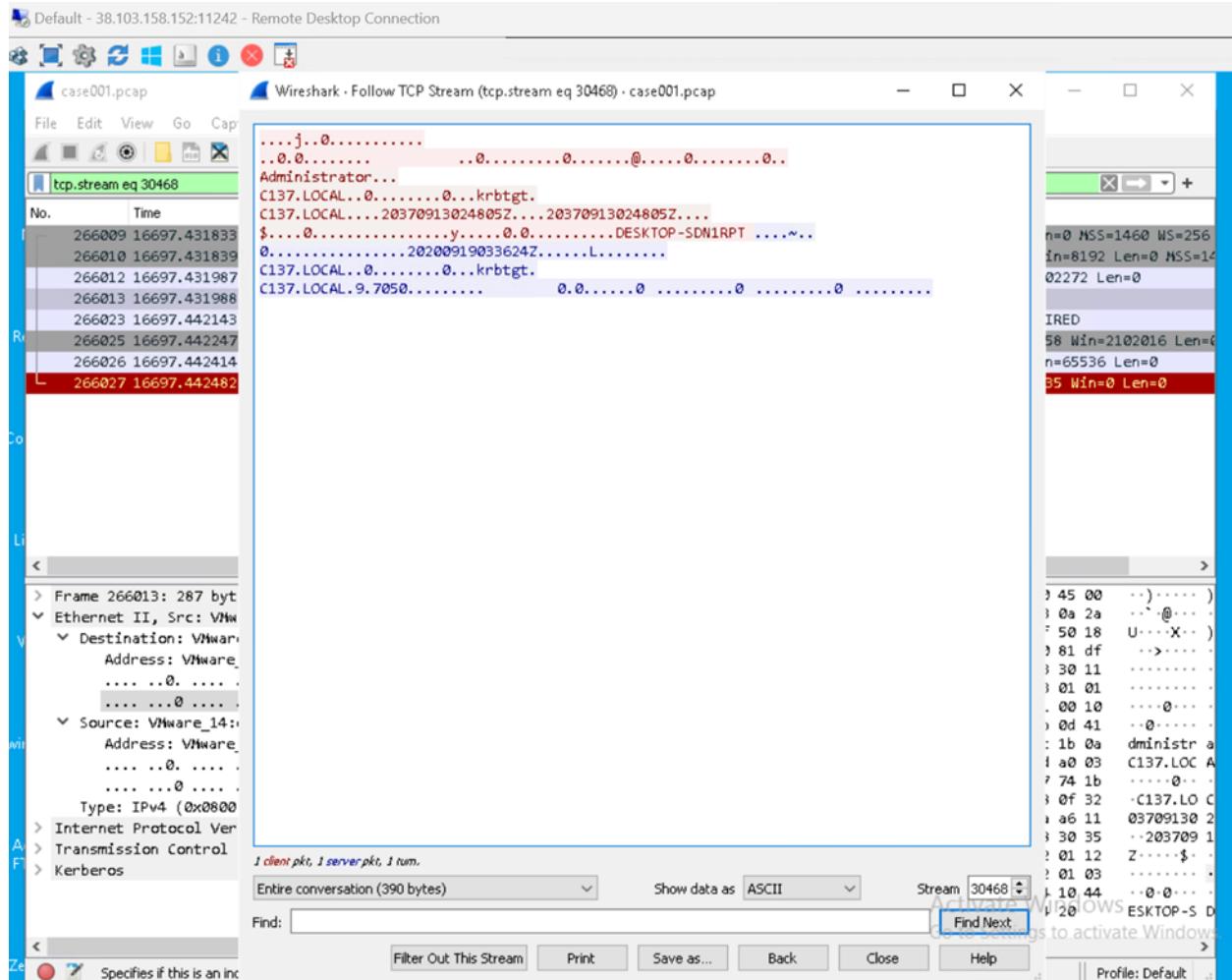
Vendor	Result
SOCRadar	Malicious
Acronis	Clean
AllLabs (MONITORAPP)	Clean
alphaMountain.ai	Clean
Abusix	Clean
ADMINUSLabs	Clean
AlienVault	Clean
Antly-AVL	Clean

On the right side of the interface, there is a "Do you want to automate checks?" section with checkboxes for each vendor. A blue button at the bottom right says "Activate Windows" and "Go to Settings to activate Windows".



8. Did the attacker access any other systems?

The intrusion successfully gained access to C137\DESKTOP-SDN1RPT\$ by leveraging Remote Desktop Protocol (RDP) from the Domain Controller (DC), utilizing the Administrator account. We discovered this behavior in the packet capture (pcap) file.



3. Did the attacker steal or access any data?

Using Autopsy, it becomes clear that the Administrator has recently engaged with every file in the "Secret" folder located in the shared file directory. It is possible to see that the file has been modified after being accessed by the attacker.

The screenshot shows the Autopsy Forensic Browser interface. On the left, the 'Data Sources' tree view is expanded to show several volumes and their contents. One volume, '20200918_0347_CDrive.E01_1', contains a 'FileShare' folder which further contains a 'Secret' folder. This 'Secret' folder is highlighted and selected. The main pane displays a 'Listing' of files within this folder. The table has columns for Name, S, C, O, Modified Time, Change Time, and Access Time. There are seven results listed:

Name	S	C	O	Modified Time	Change Time	Access Time
[current folder]				2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT	2020-09-18 23:35:06
[parent folder]				2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT	2020-09-18 23:34:18
Beth_Secret.txt	0			2020-09-18 19:35:35 EDT	2020-09-18 19:35:35 EDT	2020-09-18 19:33:54
NoJerry.txt	0			2020-09-18 18:30:24 EDT	2020-09-18 18:30:24 EDT	2020-09-18 18:29:47

The file 'Beth_Secret.txt' is currently selected. Below the table, there are tabs for Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. Under 'Data Artifacts', there are tabs for Hex, Text, Application, File Metadata, and OS Account. The 'Text' tab is selected, showing the content of the file: 'Space Beth is the real Beth'. Below this, there is a section labeled '-----METADATA-----'.

1. When?

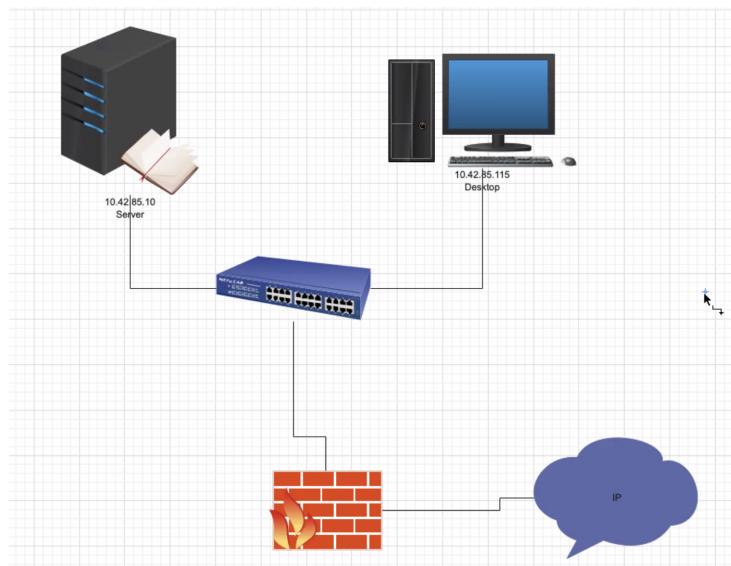
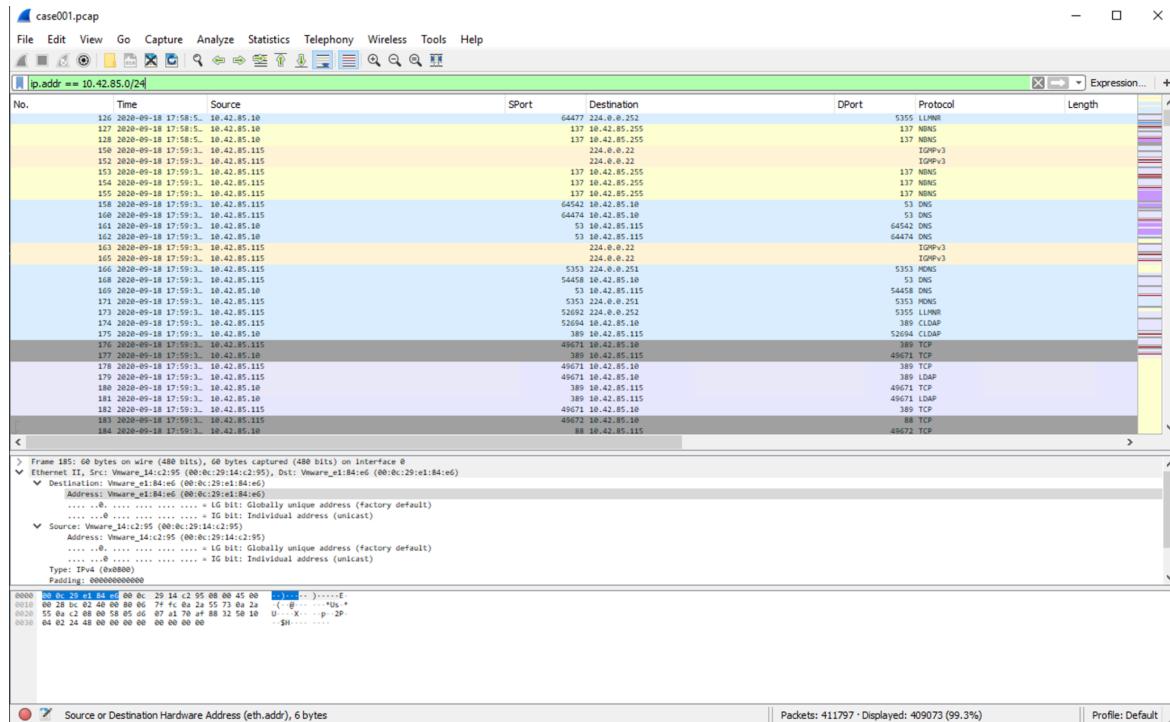
The screenshot shows the Autopsy 4.21.0 interface. The left sidebar displays a tree view of the file system, including paths like \$Extend, \$Recycle.Bin, \$Unalloc, Documents and Settings, FileShare, PerfLogs, Program Files, Program Files (x86), ProgramData, System Volume Information, Users, and Windows. The main pane shows a table titled "Listing" with 7 results for the path /img_20200918_0347_CDdrive.E01/vol_vol3/FileShare/Secret. The table includes columns for Name, S, C, O, Modified Time, Change Time, Access Time, and Create. The table lists several files: [current folder], [parent folder], Beth_Secret.txt, NoJerry.txt, PortalGunPlans.txt, SECRET_beth.txt, and Szechuan Sauce.txt. The "Szechuan Sauce.txt" file is highlighted. Below the table are tabs for Hex, Text, Application, File Metadata, OS Account, Data Artifacts, Analysis Results, Context, Annotations, and Other Occurrences. The "Text" tab is selected, showing the file content "1/1 sunflowerodium can never". At the bottom are buttons for Clear Log, Save to file, Copy to clipboard, About, and Exit.

Name	S	C	O	Modified Time	Change Time	Access Time	Create
[current folder]				2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT
[parent folder]				2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT
Beth_Secret.txt	0			2020-09-18 19:35:35 EDT	2020-09-18 19:35:35 EDT	2020-09-18 19:33:54 EDT	2020-09-18 19:33:54 EDT
NoJerry.txt	0			2020-09-18 18:30:24 EDT	2020-09-18 18:30:24 EDT	2020-09-18 18:29:47 EDT	2020-09-18 18:29:47 EDT
PortalGunPlans.txt	0			2020-09-18 18:35:35 EDT	2020-09-18 18:35:35 EDT	2020-09-18 18:33:54 EDT	2020-09-18 18:33:54 EDT
SECRET_beth.txt				2020-09-18 23:34:27 EDT	2020-09-18 23:34:27 EDT	2020-09-18 18:39:04 EDT	2020-09-18 18:39:04 EDT
Szechuan Sauce.txt	0			2020-09-18 18:38:56 EDT	2020-09-18 18:38:56 EDT	2020-09-18 18:35:43 EDT	2020-09-18 18:35:43 EDT

The picture captures the exact time that the file has been accessed and modified.

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

By this wireshark capture we can see the extensive communication between two ip addresses (server and desktop ones), and it is possible to conclude that they belong to the same network 10.42.85.0/24, as shown in the filter of the wireshark.



This diagram represents just an example of how they are connected.

Conclusion

In the face of rapidly evolving cyber threats, our investigation into the case of "The Stolen Szechuan Sauce" serves as an enlightening example of the complexities and challenges involved in digital forensic analysis. Utilizing a range of state-of-the-art forensic tools like Autopsy, FTK Imager, The Volatility Foundation, and Wireshark, we have conducted a comprehensive analysis of both a server and a desktop implicated in the cyber event under scrutiny.

Our methodical approach, framed by a series of guiding questions, allowed us to delve deep into multiple types of evidence files—disk images (E01), packet capture files (PCAP), and memory dumps. Through rigorous analysis, we confirmed a breach had occurred, identified malware and its capabilities, and traced the adversary's steps. These findings are supported by various artifacts including screenshots, logs, and network traffic data. Ensuring a robust and substantiated conclusion, this investigation underscores the vital role that thorough forensic analysis plays in demystifying complex cyber events and providing actionable intelligence for enhancing cybersecurity measures.

While our investigation has reached its intended goals, it's important to recognize that digital forensics is a continually evolving field. New methods and technologies are constantly emerging, offering both opportunities and challenges for future investigations. This project, undertaken collaboratively, not only serves as a testament to the capabilities of current forensic tools but also highlights the importance of teamwork and diverse skill sets in conducting successful cyber investigations. As cyber threats continue to advance in scale and sophistication, the lessons gleaned from this exercise will undoubtedly serve as valuable experience for tackling future cyber incidents.

References

James. (2021, March 25). *Case 001 - the stolen szechuan sauce.* DFIR Madness.

<https://dfirmadness.com/the-stolen-szechuan-sauce/>

A guide to digital forensics and cybersecurity tools.

Forensics Colleges. (2022, May 19).

<https://www.forensicscolleges.com/blog/resources/guide-digital-forensics-tools>

Wikimedia Foundation. (2023, October 15). *Windows NT.*

Wikipedia.

https://en.wikipedia.org/wiki/Windows_NT#:~:text=Windows%20NT%20is%20a%20proprietary, and%20multi%2Duser%20operating%20system.

Free Automated Malware Analysis Service - powered by Falcon Sandbox - viewing online file analysis results for "coreupdater.exe." (n.d.).

<https://www.hybrid-analysis.com/sample/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6/5f7695f4a553eb21aa0cdfe1>

VirusTotal. (n.d.). www.virustotal.com.

<https://www.virustotal.com/gui/home/search>