Forensics Report and Documentation
Case 001 - The Stolen Szechuan Sauce

Prepared by: Anastasiya Gruneva
Date: February 19th, 2025

Table of Contents

Executive Summary

This report documents the findings of a forensic investigation into Case 001, known as "The Stolen Szechuan Sauce," involving a breach of a server and desktop system within a victim's network. The incident was caused by a successful brute-force attack exploiting weak RDP credentials, leading to the installation of malware and lateral movement across the network.

The affected systems included a Windows Server 2012 R2 and a Windows 10 Enterprise desktop, both of which were compromised with a remote access Trojan (RAT), known as coreupdater.exe. The initial malware delivery was traced to the IP address 194.61.24.102, with the malware establishing connections to a command and control (C2) server at IP address 203.78.103.209. The malware was capable of various malicious actions, including credential theft, keylogging, and persistence via registry modifications, ensuring it remained active on both systems after reboot.

Through comprehensive forensic tools like Volatility, FTK Imager, Wireshark, and VirusTotal, the investigation revealed that the malware was moved and installed on the system, initially residing in the Downloads folder before being relocated to the System32 directory. The attack resulted in unauthorized access to both the server and the desktop, with lateral movement facilitated by RDP.

Key indicators of compromise (IOCs) included the malware’s persistence in the system registry, suspicious network traffic, and multiple RDP requests linked to the attacker’s infrastructure. The compromised network layout was minimal, comprising two hosts within the 10.42.85.0/24 subnet: the server at 10.42.85.10 and the desktop at 10.42.85.115.

This report outlines critical insights into the breach, highlighting the methods and tools used by the attacker, the malware's capabilities, and the overall impact on the victim's network security. The findings emphasize the importance of strong authentication protocols, continuous monitoring for unusual network activity, and prompt remediation efforts to mitigate such threats in the future.

Investigation

Tools used

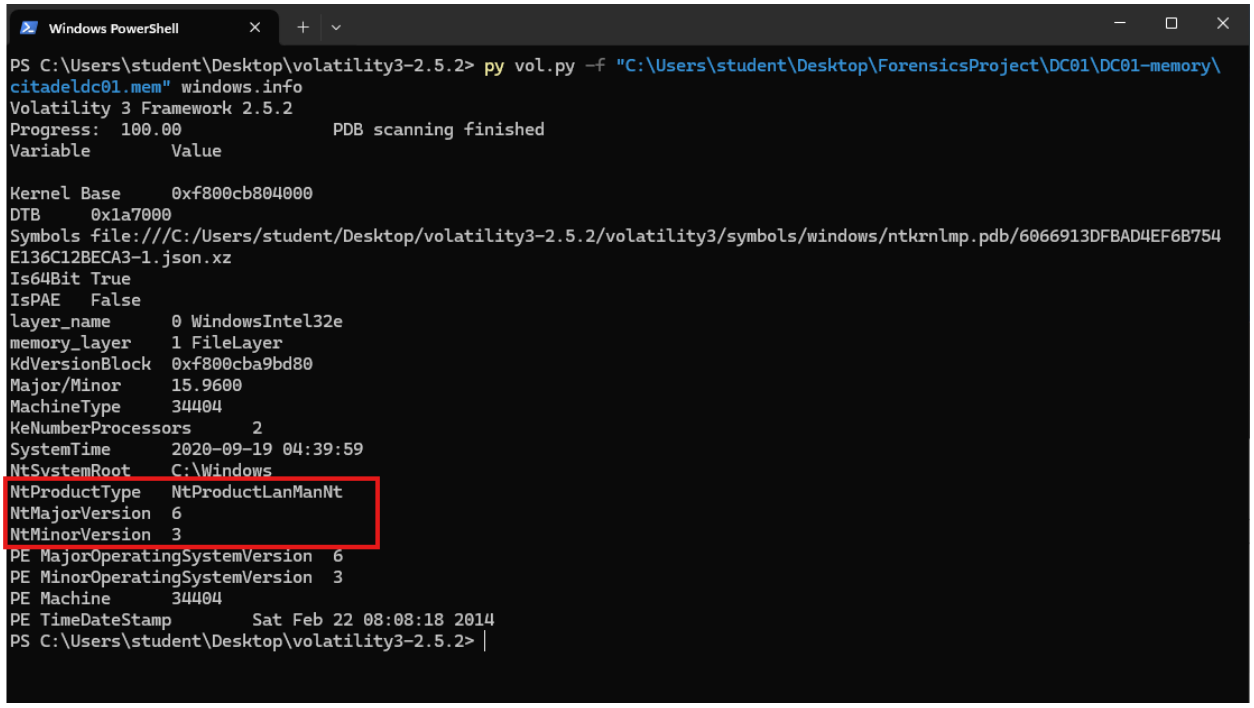
Volatility 3-2.5.2
FTK Imager 4.7.1.2
Registry Explorer v2.0.0.0
Wireshark
VirusTotal
TimeLine Explorer v2.0.0.1

Answers to case questions

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

Answer: Windows Server 2012 R2

The server OS version was identified using Volatility 3's "windows.info" plugin, which extracted details like major and minor OS versions (Pearson, 2021).



```
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\
citadeldc01.mem" windows.info
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Variable        Value

Kernel Base     0xf800cb804000
DTB     0x1a7000
Symbols file:///C:/Users/student/Desktop/volatility3-2.5.2/volatility3/symbols/windows/ntkrnlmp.pdb/6066913DFBAD4EF6B754
E136C12BECA3-1.json.xz
Is64Bit True
IsPAE   False
layer_name      0 WindowsIntel32e
memory_layer    1 FileLayer
KdVersionBlock  0xf800cba9bd80
Major/Minor     15.9600
MachineType     34404
KeNumberProcessors      2
SystemTime      2020-09-19 04:39:59
NtSystemRoot    C:\Windows
NtProductType   NtProductLanManNt
NtMajorVersion  6
NtMinorVersion  3
PE MajorOperatingSystemVersion  6
PE MinorOperatingSystemVersion  3
PE Machine      34404
PE TimeDateStamp        Sat Feb 22 08:08:18 2014
PS C:\Users\student\Desktop\volatility3-2.5.2>
```

Figure 1. Volatility 3 Windows Info

The OS version information is in these fields:

- NtMajorVersion: 6
- NtMinorVersion: 3

So, our memory dump is from a Windows 8.1 system.

- NtProductLanManNt → This means the system is likely a Windows Server edition.

So, our memory dump is from Windows Server 2012 R2, which is based on Windows 8.1 (*Operating System Version - Win32 Apps*, 2021).

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

Answer: Windows 10 Enterprise Evaluation

The desktop OS version was identified using FTK Imager and Registry Explorer.

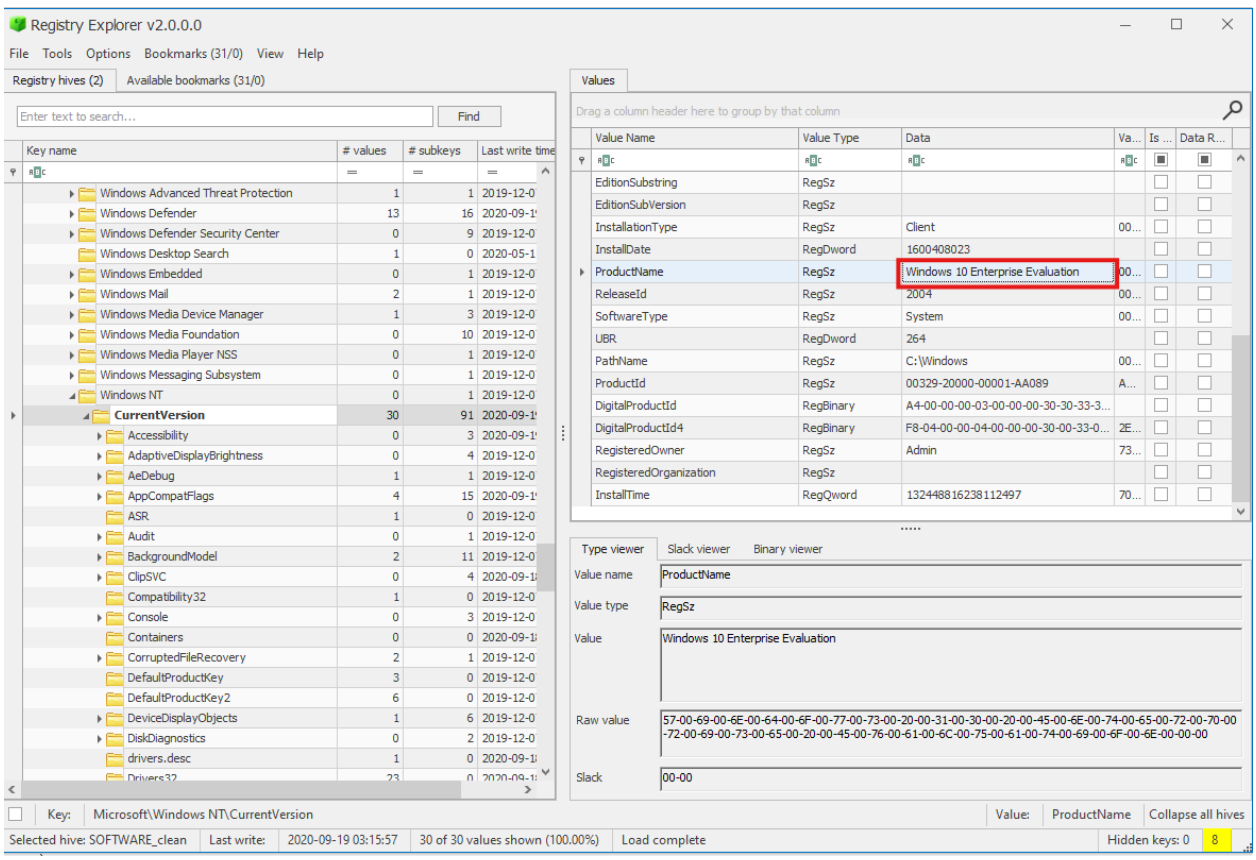


Figure 2. Desktop OS Version (Software hive)

Steps for extracting OS Version from a disk image using Registry Explorer:

1. Loaded the Desktop E01 file into FTK Imager.

2. Navigated to: Basic data partition → NONAME → root → Windows → System32 → config to locate the registry files.
3. Exported the SOFTWARE hive, which contains system configuration and installed software details.
4. Imported the SOFTWARE hive into Registry Explorer v2.0 for examination.
5. Accessed SOFTWARE → Microsoft → Windows NT → CurrentVersion to retrieve OS version and system details.

3. What was the local time of the Server?

Answer: According to the project notes, the time zone is MST (UTC -6). However, based on the information in the System hive on the server, the time zone is set to PST (UTC -8). It is possible that the server's time zone was changed.

To find the server's local time:

- Exported the System hive using FTK Imager and opened it in Registry Explorer.
- Navigated to the location: SYSTEM\CurrentControlSet\Control\TimeZoneInformation to retrieve the server's local time zone information.

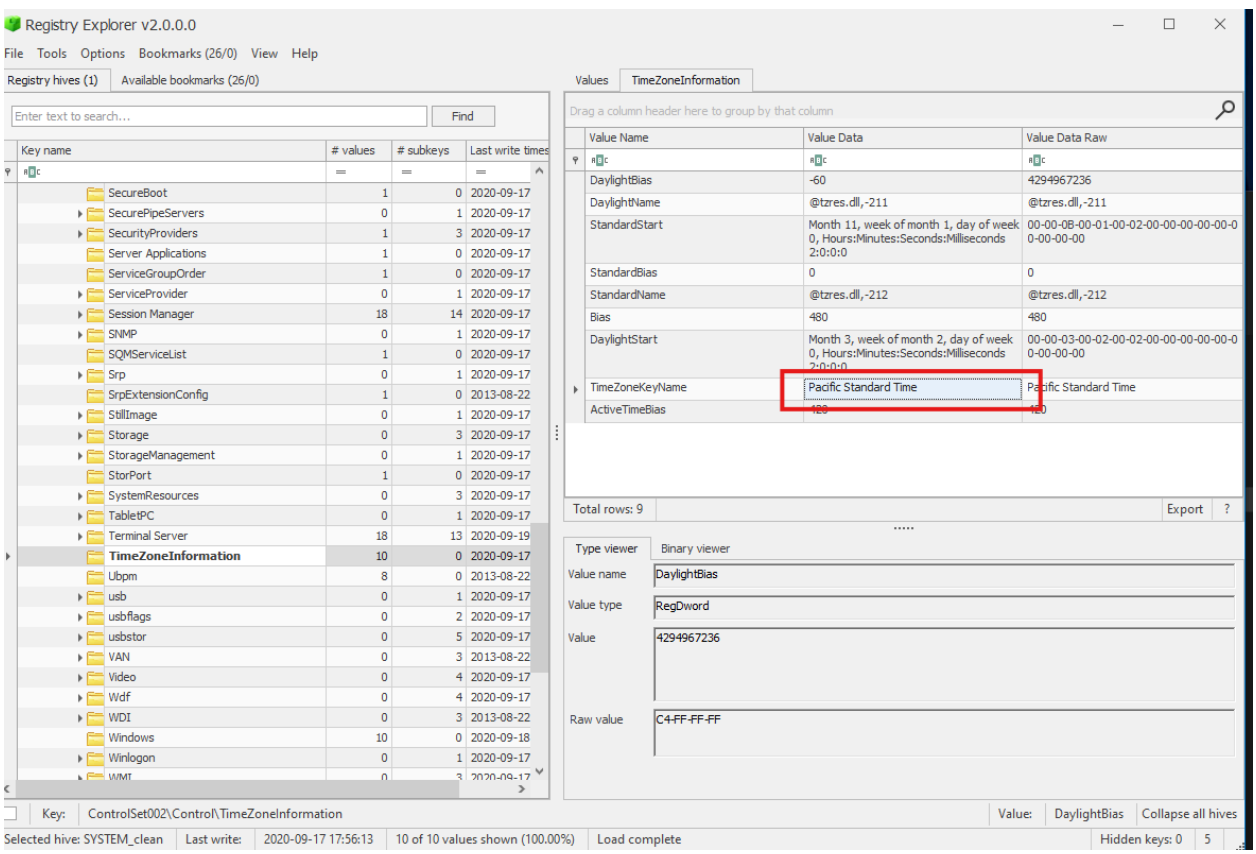


Figure 3. The Server's Time Zone (System Hive)

However, according to the project notes, the incident occurred in Colorado in September, which places the local time at UTC -6 (James, 2020). This suggests the server's time zone might have been changed. Keep this in mind when analyzing the output from various tools.

4. Was there a breach?

Answer: Yes, there was a breach. As stated in the project case, "the FBI contacted him. They found his recently-developed Szechuan sauce recipe on the dark web" (James, 2020). Additionally, malware was detected, which further supports the occurrence of a breach.

Upon examining the server's memory using Volatility 3, specifically the "pslist" plugin, a suspicious process was detected. Coreupdater.exe is activated and then almost immediately turns itself off. Coreupdater.exe is not a standard Windows system process, which suggests it could be suspicious, especially if it starts and terminates quickly.

```
Windows PowerShell
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.pslist
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime        File output

4       0       System  0xe0005f273040  98      -       N/A     False   2020-09-19 01:22:38.000000      N/A     Disabled
204     4       smss.exe        0xe00060354900  2       -       N/A     False   2020-09-19 01:22:38.000000      N/A     Disabled
324     316     csrss.exe       0xe000602c2080  8       -       0       False   2020-09-19 01:22:39.000000      N/A     Disabled
404     316     wininit.exe     0xe000602cc900  1       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
412     396     csrss.exe       0xe000602c1900  10      -       1       False   2020-09-19 01:22:40.000000      N/A     Disabled
452     404     services.exe    0xe00060c11080  5       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
460     404     lsass.exe       0xe00060c0e080  31      -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
492     396     winlogon.exe    0xe00060c2a080  4       -       1       False   2020-09-19 01:22:40.000000      N/A     Disabled
640     452     svchost.exe     0xe00060c84900  8       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
684     452     svchost.exe     0xe00060c9a700  6       -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
800     452     svchost.exe     0xe00060ca3900  12      -       0       False   2020-09-19 01:22:40.000000      N/A     Disabled
808     492     dwm.exe 0xe00060d09680  7       -       1       False   2020-09-19 01:22:40.000000      N/A     Disabled
848     452     svchost.exe     0xe00060d1e080  39      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
928     452     svchost.exe     0xe00060d5d500  16      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
1000    452     svchost.exe     0xe00060da2080  18      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
668     452     svchost.exe     0xe00060e09900  16      -       0       False   2020-09-19 01:22:41.000000      N/A     Disabled
1292    452     Microsoft.Acti  0xe00060f73900  9       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1332    452     dfsrs.exe       0xe00060fe1900  16      -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1368    452     dns.exe 0xe00060ff3080  16      -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1392    452     ismserv.exe     0xe00060ff7900  6       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1556    452     VGAuthService.  0xe000614aa200  2       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1600    452     vmtoolsd.exe    0xe00061a30900  9       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1644    452     wlms.exe        0xe00061a9a800  2       -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1660    452     dfssvc.exe      0xe00061a9b2c0  11      -       0       False   2020-09-19 01:22:57.000000      N/A     Disabled
1956    452     svchost.exe     0xe0006291b7c0  30      -       0       False   2020-09-19 01:23:20.000000      N/A     Disabled
796     452     vds.exe 0xe000629b3080  11      -       0       False   2020-09-19 01:23:20.000000      N/A     Disabled
1236    452     svchost.exe     0xe000629926c0  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     dllhost.exe     0xe00062a26900  10      -       0       False   2020-09-19 01:23:21.000000      N/A     Disabled
2460    452     msdtc.exe       0xe00062a2a900  9       -       0       False   2020-09-19 01:23:21.000000      N/A     Disabled
2724    452     spoolsv.exe     0xe000631cb900  13      -       0       False   2020-09-19 03:39:40.000000      N/A     Disabled
3644    2244    coreupdater.ex  0xe00062fe7700  0       -       2       False   2020-09-19 03:56:37.000000      2020-09-19 03:56:52.000000      Disabled
3736    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    vmtoolsd.exe    0xe00062ede1c0  8       -       1       False   2020-09-19 04:36:14.000000      N/A     Disabled
2840    3472    FTK Imager.exe  0xe00063021900  9       -       1       False   2020-09-19 04:37:04.000000      N/A     Disabled
3056    848     WMIADAP.exe     0xe0006313f900  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
PS C:\Users\student\Desktop\volatility3-2.5.2>
```

Figure 4. Suspicious Process Detection in Server Memory Using Volatility 3 (pslist)

A quick search confirmed that Coreupdater.exe is associated with malware. Various cybersecurity reports indicate that this executable has been linked to suspicious activities, including unauthorized system modifications and potential data exfiltration.

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

Answer: Brute-force attack

To find the IP addresses of the server and desktop, Volatility 3's “netstat” plugin is used to analyze network connections from a memory dump. The output provides details on Local IP Addresses (assigned to the system), Foreign IP Addresses (external connections), ports, and process IDs (PIDs). By examining the Local Address column, the system’s assigned IP can be identified.

```
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\Desktop\DESKTOP-SDN1RPT-memo
ry\DESKTOP-SDN1RPT.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xbe8e78d5c460  TCPv4   10.42.85.115    50966   13.107.21.200   443     ESTABLISHED     -       -       N/A
```

Figure 5. Volatility 3 Netstat Output Showing Desktop Local IP

```
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe00063266d10  TCPv6   fe80::2dcf:e660:be73:d220       62777   fe80::2dcf:e660:be73:d220       49155   CLOSED  460     lsass.exe       -
0xe00062a31270  TCPv6   fe80::2dcf:e660:be73:d220       49182   fe80::2dcf:e660:be73:d220       389     ESTABLISHED     1332    dfsrs.exe       N/A
0xe0006103c4f0  TCPv6   fe80::2dcf:e660:be73:d220       49174   fe80::2dcf:e660:be73:d220       49155   ESTABLISHED     1660    dfssvc.exe      N/A
0xe000610d0640  TCPv6   ::1     49161   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A
0xe000631c7590  TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0xe0006102d010  TCPv6   ::1     49160   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A
```

Figure 6. Volatility 3 Netstat Output Showing Server Local IP

As shown on Figures 5 and 6:

- Desktop IP address: 10.42.85.115
- Server IP address: 10.42.85.10

A quick search in the PCAP file using Wireshark revealed a foreign IP address associated with a malicious file named “coreupdater”.

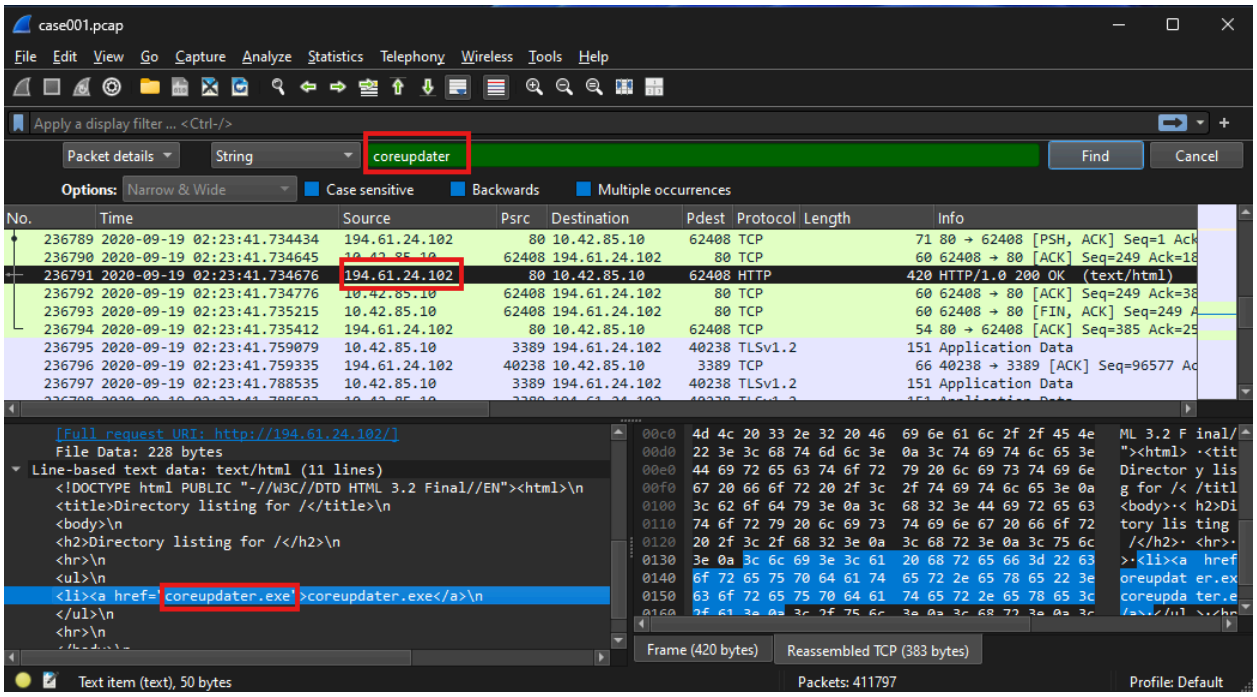


Figure 7. Foreign IP Address Associated with Coreupdater Identified in PCAP File

As shown on Figure 7, foreign IP address 194.61.24.102 is connected to the server via HTTP protocol.

We also observed a large number of RDP requests associated with this IP address in the PCAP file using Wireshark.

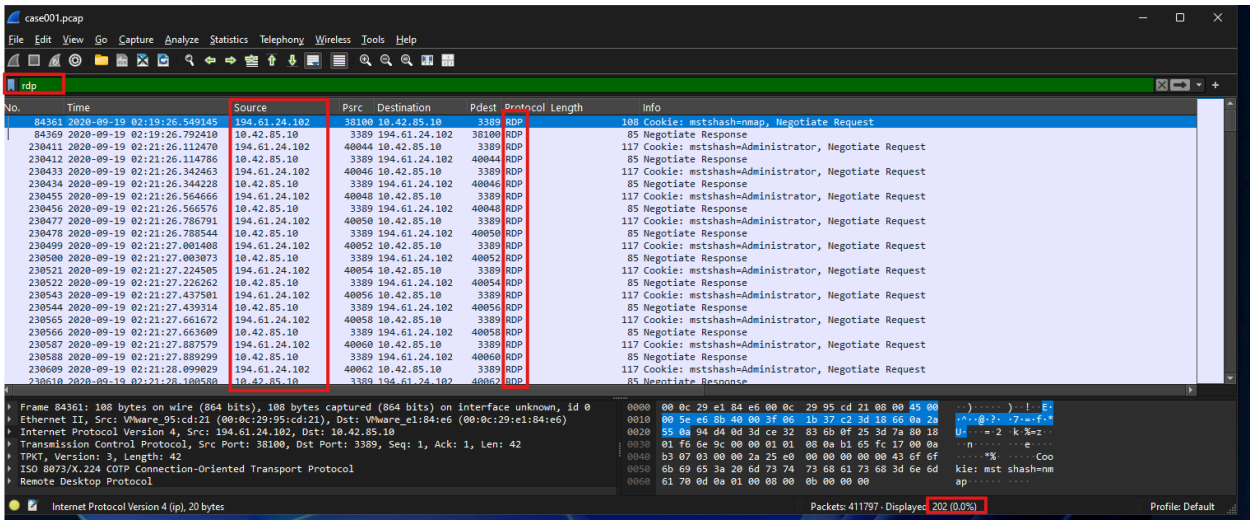


Figure 8. RDP Requests Associated with Malicious IP Address Identified in PCAP File.

The large number of RDP requests associated with this IP address is a clear indication of a brute-force attack. Brute-force attacks are commonly characterized by multiple

rapid login attempts with different password combinations in an attempt to gain unauthorized access to a system (*Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®*, n.d.).

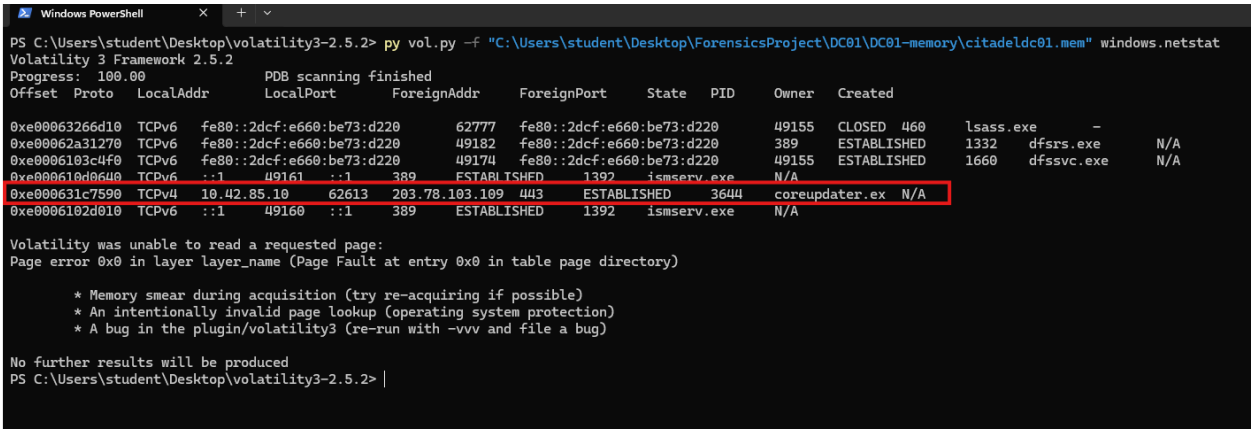
6. Was malware used? If so, what was it?

Answer: yes, see details below

6.1. What process was malicious?

Answer: coreupdater.exe and spoolsv.exe

Upon examining the server's memory using Volatility 3, specifically the "netstat" plugin, we observed that the "Coreudater" process made a connection. The analysis revealed the local and foreign IP addresses and ports.



```
Windows PowerShell
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" windows.netstat
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
Offset  Proto   LocalAddr       LocalPort       ForeignAddr     ForeignPort     State   PID     Owner   Created

0xe00063266d10  TCPv6   fe80::2dcf:e660:be73:d220       62777   fe80::2dcf:e660:be73:d220       49155   CLOSED  460     lsass.exe       -
0xe00062a31270  TCPv6   fe80::2dcf:e660:be73:d220       49182   fe80::2dcf:e660:be73:d220       389     ESTABLISHED     1332    dfsrs.exe       N/A
0xe0006103c4f0  TCPv6   fe80::2dcf:e660:be73:d220       49174   fe80::2dcf:e660:be73:d220       49155   ESTABLISHED     1660    dfssvc.exe      N/A
0xe000610d0640  TCPv6   ::1     49161   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A
0xe000631c7590  TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0xe0006102d010  TCPv6   ::1     49160   ::1     389     ESTABLISHED     1392    ismserv.exe     N/A

Volatility was unable to read a requested page:
Page error 0x0 in layer layer_name (Page Fault at entry 0x0 in table page directory)

        * Memory smear during acquisition (try re-acquiring if possible)
        * An intentionally invalid page lookup (operating system protection)
        * A bug in the plugin/volatility3 (re-run with -vvv and file a bug)

No further results will be produced
PS C:\Users\student\Desktop\volatility3-2.5.2>
```

Figure 9. Network Connections Analyzed with Volatility 3's 'netstat' Plugin

This analysis reveals that coreupdater.exe established a connection to the foreign IP address 203.78.103.209. A quick search on VirusTotal indicates that this IP address is associated with malicious activities (VirusTotal, n.d.). It could be a Command and Control (C2) server (*Cyber Kill Chain®*, n.d.).

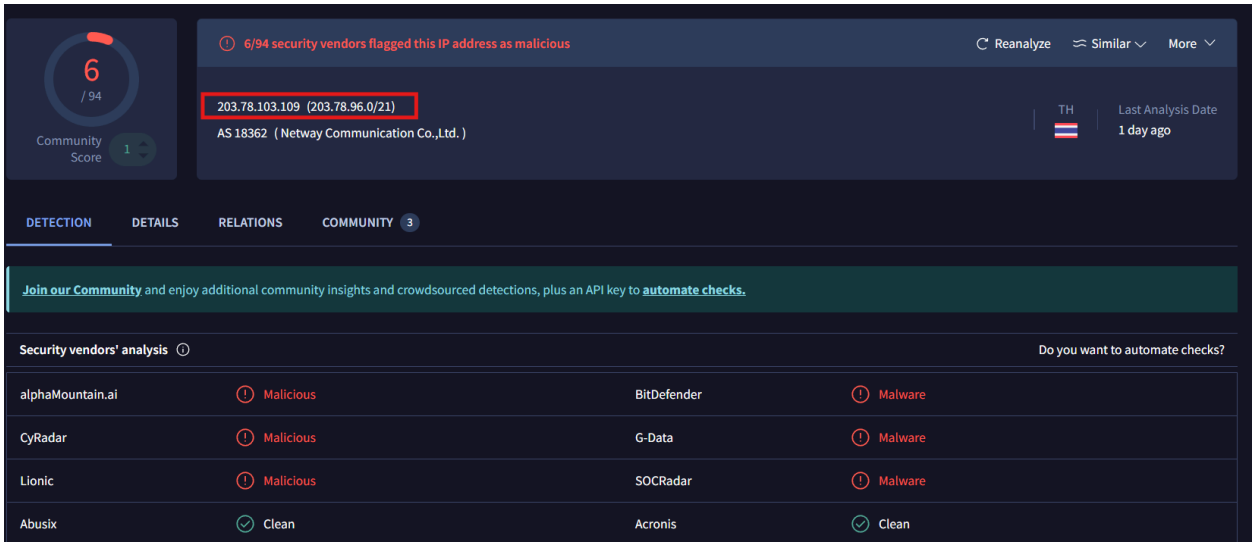


Figure 10. VirusTotal search results

Volatility 3 “malfind” plugin helps identify malicious processes.

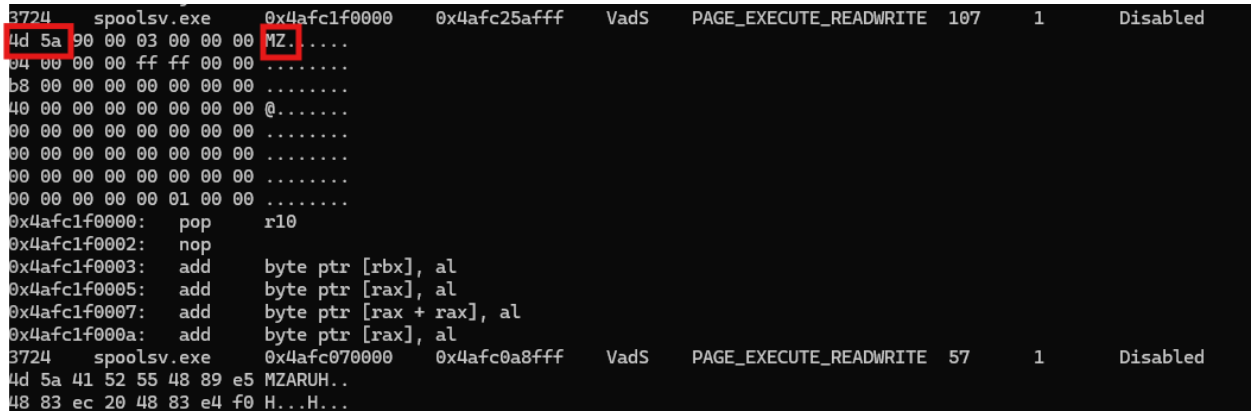


Figure 11.Output of the 'malfind' Plugin in Volatility 3.

The assembly code under analysis appears to be injected into a process. Finding an "MZ" signature in the hex dump of the injected code is a strong indicator of a portable executable file (James, 2020).

Process 3724 exhibits suspicious behavior. It contains the magic hex numbers for "MZ," which indicate a portable executable. This strongly suggests injected code.

We have confirmed that Spoolsv.exe (PID 3724) is exhibiting malicious behavior, with injected code. A quick Google search reveals that Spoolsv.exe is typically a legitimate Windows Printer Spooling service, which should run from C:\Windows\System32 (*Introduction to Spooler Components - Windows Drivers*, 2024).

```
PS C:\Users\student\Desktop\volatility3-2.5.2> py vol.py -f "C:\Users\student\Desktop\ForensicsProject\DC01\DC01-memory\citadeldc01.mem" -
o "C:\Users\student\Desktop\ForensicsProject\investigation" windows.pstree
Volatility 3 Framework 2.5.2
Progress:  100.00               PDB scanning finished
PID     PPID    ImageFileName   Offset(V)       Threads Handles SessionId       Wow64   CreateTime      ExitTime

4       0       System  0xe0005f273040  98      -       N/A     False   2020-09-19 01:22:38.000000      N/A
* 204   4       smss.exe        0xe00060354900  2       -       N/A     False   2020-09-19 01:22:38.000000      N/A
324     316     csrss.exe       0xe000602c2080  8       -       0       False   2020-09-19 01:22:39.000000      N/A
404     316     wininit.exe     0xe000602cc900  1       -       0       False   2020-09-19 01:22:40.000000      N/A
* 460   404     lsass.exe       0xe00060c0e080  31      -       0       False   2020-09-19 01:22:40.000000      N/A
* 452   404     services.exe    0xe00060c11080  5       -       0       False   2020-09-19 01:22:40.000000      N/A
** 640  452     svchost.exe     0xe00060c84900  8       -       0       False   2020-09-19 01:22:40.000000      N/A
*** 2056        640     WmiPrvSE.exe    0xe000629de900  11      -       0       False   2020-09-19 01:23:21.000000      N/A
*** 2764        640     WmiPrvSE.exe    0xe00062c0a900  6       -       0       False   2020-09-19 04:37:42.000000      N/A
** 1292 452     Microsoft.Acti  0xe00060f73900  9       -       0       False   2020-09-19 01:22:57.000000      N/A
** 3724 452     spoolsv.exe     0xe000631cb900  13      -       0       False   2020-09-19 03:29:40.000000      N/A
** 1556 452     VGAuthService.  0xe000614aa200  2       -       0       False   2020-09-19 01:22:57.000000      N/A
** 796  452     vds.exe 0xe000629b3080  11      -       0       False   2020-09-19 01:23:20.000000      N/A
** 668  452     svchost.exe     0xe00060e09900  16      -       0       False   2020-09-19 01:22:41.000000      N/A
** 2460 452     msdtc.exe       0xe00062a2a900  9       -       0       False   2020-09-19 01:23:21.000000      N/A
** 800  452     svchost.exe     0xe00060ca3900  12      -       0       False   2020-09-19 01:22:40.000000      N/A
** 928  452     svchost.exe     0xe00060d5d500  16      -       0       False   2020-09-19 01:22:41.000000      N/A
** 1956 452     svchost.exe     0xe0006291b7c0  30      -       0       False   2020-09-19 01:23:20.000000      N/A
** 2216 452     dllhost.exe     0xe00062a26900  10      -       0       False   2020-09-19 01:23:21.000000      N/A
** 684  452     svchost.exe     0xe00060c9a700  6       -       0       False   2020-09-19 01:22:40.000000      N/A
** 1332 452     dfsrs.exe       0xe00060fe1900  16      -       0       False   2020-09-19 01:22:57.000000      N/A
** 1600 452     vmtoolsd.exe    0xe00061a30900  9       -       0       False   2020-09-19 01:22:57.000000      N/A
** 848  452     svchost.exe     0xe00060d1e080  39      -       0       False   2020-09-19 01:22:41.000000      N/A
*** 3056        848     WMIADAP.exe     0xe0006313f900  5       -       0       False   2020-09-19 04:37:42.000000      N/A
*** 3796        848     taskhostex.exe  0xe00062f04900  7       -       1       False   2020-09-19 04:36:03.000000      N/A
** 1236 452     svchost.exe     0xe000629926c0  8       -       0       False   2020-09-19 01:23:21.000000      N/A
** 1368 452     dns.exe 0xe00060ff3080  16      -       0       False   2020-09-19 01:22:57.000000      N/A
** 1000 452     svchost.exe     0xe00060da2080  18      -       0       False   2020-09-19 01:22:41.000000      N/A
** 1644 452     wlms.exe        0xe00061a9a800  2       -       0       False   2020-09-19 01:22:57.000000      N/A
** 1392 452     ismserv.exe     0xe00060ff7900  6       -       0       False   2020-09-19 01:22:57.000000      N/A
** 1660 452     dfssvc.exe      0xe00061a9b2c0  11      -       0       False   2020-09-19 01:22:57.000000      N/A
412     396     csrss.exe       0xe000602c1900  10      -       1       False   2020-09-19 01:22:40.000000      N/A
492     396     winlogon.exe    0xe00060c2a080  4       -       1       False   2020-09-19 01:22:40.000000      N/A
* 808   492     dwm.exe 0xe00060d09680  7       -       1       False   2020-09-19 01:22:40.000000      N/A
3644    2244    coreupdater.ex  0xe00062fe7700  0       -       2       False   2020-09-19 03:56:37.000000      2020-09-19 03:56:52.000000

3472    3960    explorer.exe    0xe00063171900  39      -       1       False   2020-09-19 04:36:03.000000      N/A
* 2608  3472    vmtoolsd.exe    0xe00062ede1c0  8       -       1       False   2020-09-19 04:36:14.000000      N/A
* 2840  3472    FTK Imager.exe  0xe00063021900  9       -       1       False   2020-09-19 04:37:04.000000      N/A
* 3260  3472    vm3dservice.ex  0xe00063299280  1       -       1       False   2020-09-19 04:36:14.000000      N/A
400     1904    ServerManager.  0xe00060ce2080  10      -       1       False   2020-09-19 04:36:03.000000      N/A
PS C:\Users\student\Desktop\volatility3-2.5.2>
```

Figure 12.Output of the 'pstree' Plugin in Volatility 3.

6.2. Identify the IP Address that delivered the payload.

Answer: 194.61.24.102

This IP address was recorded in a PCAP file.

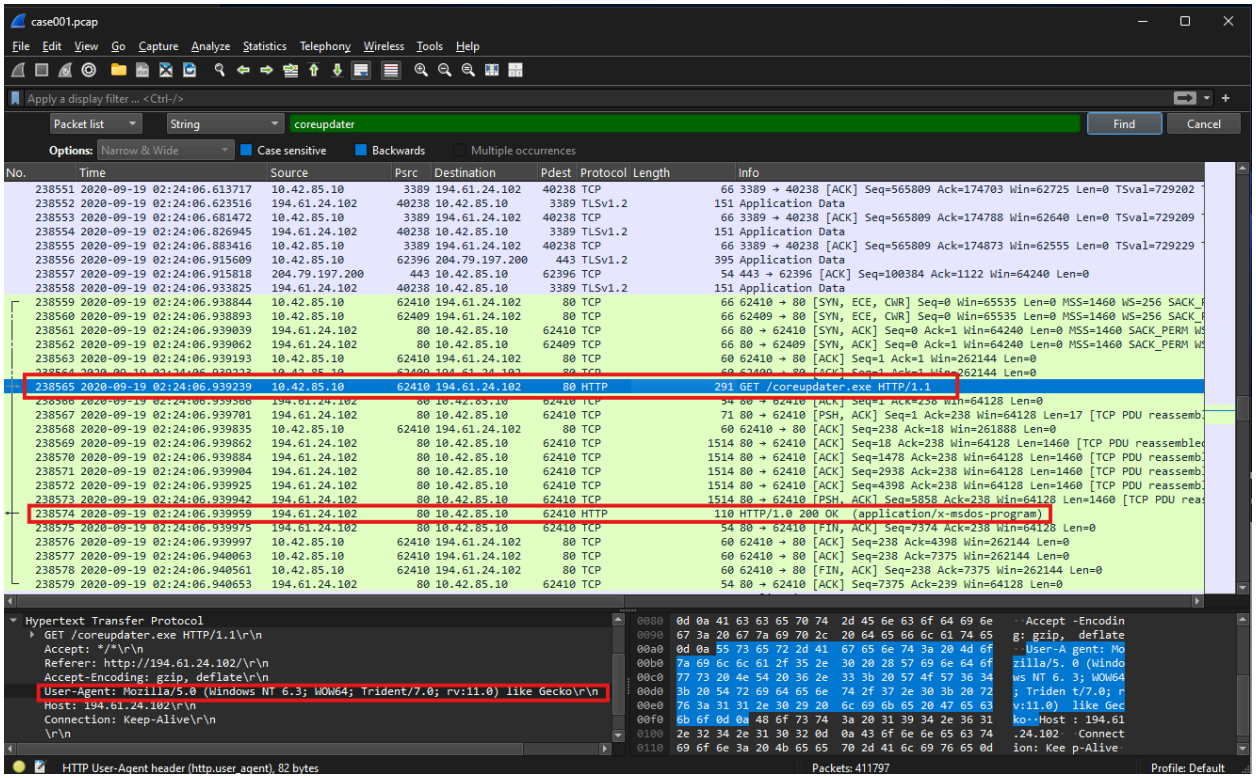


Figure 13. Network Traffic Capturing coreupdater.exe Download

In an HTTP communication captured by Wireshark, the line GET /coreupdater.exe HTTP/1.1 represents an HTTP GET request. This method is used by a client to request a specific resource from a server. In this case, the client is attempting to retrieve the file coreupdater.exe from the server's root directory (*GET - HTTP | MDN*, 2024).

The accompanying User-Agent header: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko provides information about the client's software and operating environment. This User-Agent string suggests that the request originated from Internet Explorer 11 on a Windows 8.1 system (User Agents, n.d.).

The PCAP file also reveals that the IP address 194.61.24.102 responded to the HTTP GET request by delivering coreupdater.exe, indicating a successful file transfer.

6.3. What IP Address is the malware calling to?

Answer: 203.78.103.209

Figure 9 illustrates the network connection initiated by coreupdater.exe, including the destination IP address.

6.4. Where is this malware on disk?

Answer: C:\Windows\System32

Malware was found at Windows\System32\coreupdater.exe for both server and desktop.

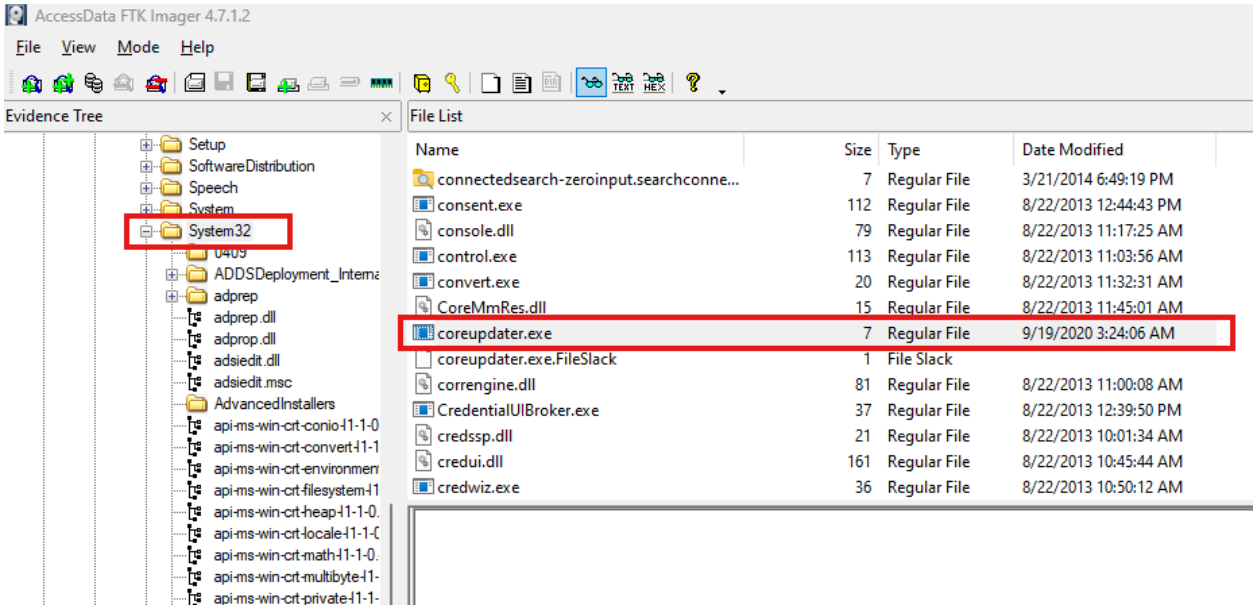


Figure 14. Coreupdater.exe location

6.5. When did it first appear?

Answer: 2020-09-19 02:24:06

Figure 13 indicates a successful file transfer on the server 2020-09-19 02:24:06.

6.6. Did someone move it?

Answer: Yes, from .C:\Users\Administrator\Downloads to C:\Windows\System32

A forensic examination of the USN Journal reveals records of file movements within the system (*Fsutil Usn*, 2024).

Timeline Explorer v2.0.0.1

File Tools Tabs View Help

20250216213912_MFTECmd_$MFT_Output.csv | 20250216213913_MFTECmd_$J_Output.csv

Drag a column header here to group by that column

coreupdater

Line	Tag	Update Timestamp	Parent Path	Name
80203		2020-09-19 03:24:06	.\PathUnknown\Directory with ID 0x0001540A-00000001	coreupdater[1].exe
80235		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe
80236		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe
80237		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe
80238		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80239		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80240		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80241		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80242		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80243		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80244		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80245		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80246		2020-09-19 03:24:12	.\PathUnknown\Directory with ID 0x0001540A-00000001	coreupdater[1].exe
80247		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe.2424urv.partial
80248		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe
80249		2020-09-19 03:24:12	.\Users\Administrator\Downloads	coreupdater.exe
80255		2020-09-19 03:24:50	.\Users\Administrator\Downloads	coreupdater.exe
80256		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe
80257		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe
80258		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe
80259		2020-09-19 03:24:50	.\Windows\System32	coreupdater.exe

C:\Users\student\Desktop\EricZimmerman Tools\USN_Analysis\20250216213913_MFTECmd_$J_Output.csv | Total lines 82,085 | Visible lines 23 | Open files: 2 | Search

Figure 15. Previous coreupdater.exe Path Identified via USN Journal Analysis

6.7. What were the capabilities of this malware?

Answer: Remote Access Trojan.

The hash value of coreupdater.exe was extracted using FTK Imager, and a VirusTotal search revealed detailed information about the malware.

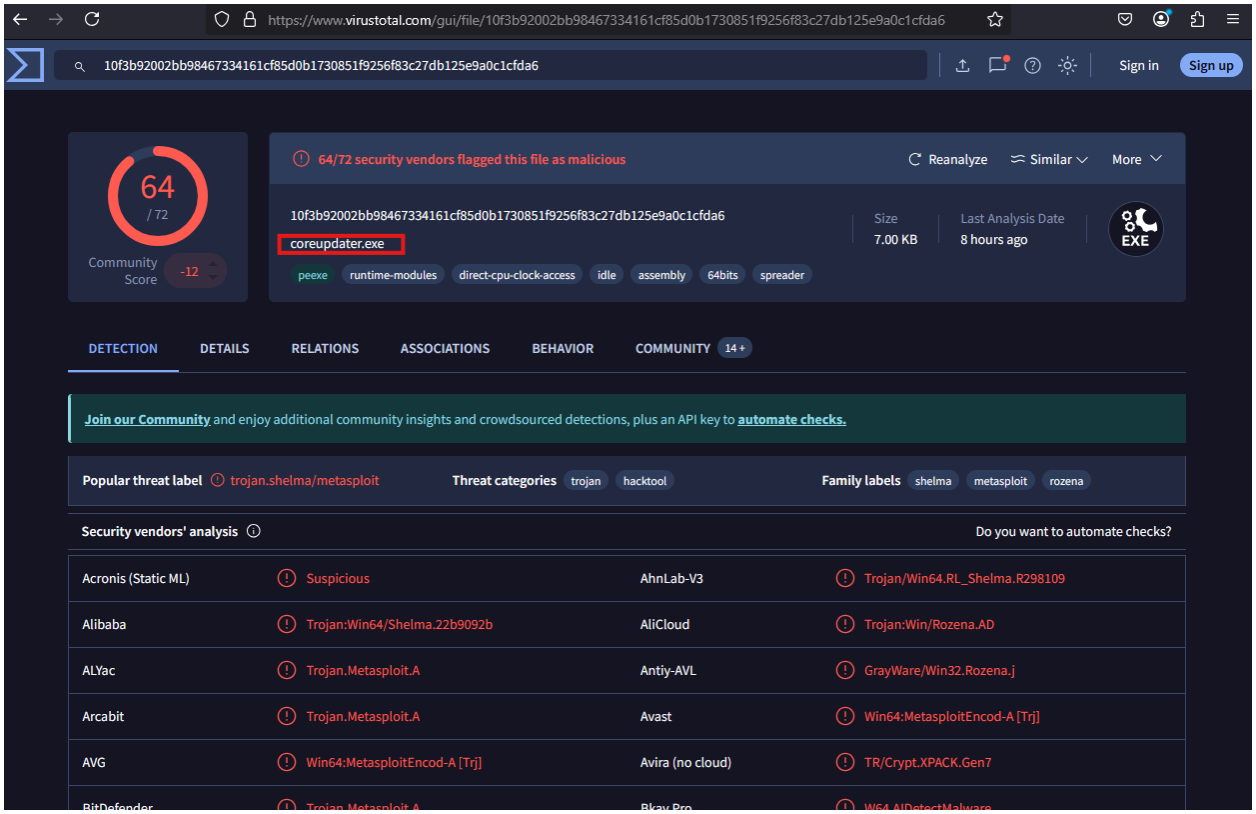


Figure 16. Information about coreupdater.exe on virustotal.com

Key Findings from VirusTotal Analysis:

1. Detected as Malware:
    - Multiple antivirus engines flagged it as malicious.
    - Possible classifications: Trojan, Backdoor, or Stealer.
2. Network Activity:
    - The behavior report may show connections to external servers (C2 communication).
    - If it downloads or uploads data, it might be used for data exfiltration.
3. Registry Modifications:
    - Some malware adds registry keys to persist after reboot.
4. File System Activity:
    - If it creates, modifies, or deletes system files, it could be part of a dropper (installing more malware).
5. Process Injection:
    - If it injects itself into other processes (e.g., explorer.exe or svchost.exe), it might be hiding from detection.

6.8. Is this malware easily obtained?

Answer: yes.

Part of this malware originates from the Metasploit Framework, a widely used penetration testing tool designed for cybersecurity professionals. While Metasploit is intended for ethical hacking and security assessments, cybercriminals often exploit it for malicious purposes (Metasploit - Penetration Testing Tool, n.d.).

6.9. Was this malware installed with persistence on any machine?

Answer: Yes, on both machines - server and desktop.

The malware employs persistence techniques to ensure it executes upon system startup. This is commonly achieved through:

- Modifying registry keys to automatically launch the malicious executable.
- Installing itself in directories like AppData, the Startup folder, or configuring scheduled tasks to execute on boot (*Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®*, 2018).

One of the most frequently targeted registry locations is:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Suspicious values in this key may indicate an unauthorized program set to execute upon login.

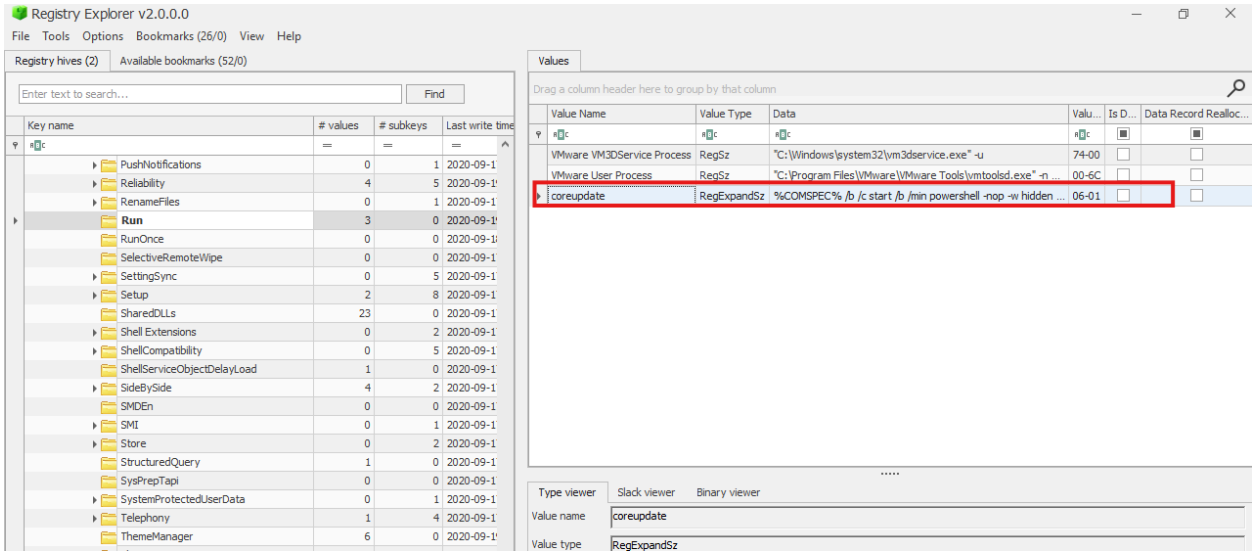


Figure 17. Evidence of Malware Persistence in Windows Registry on Server

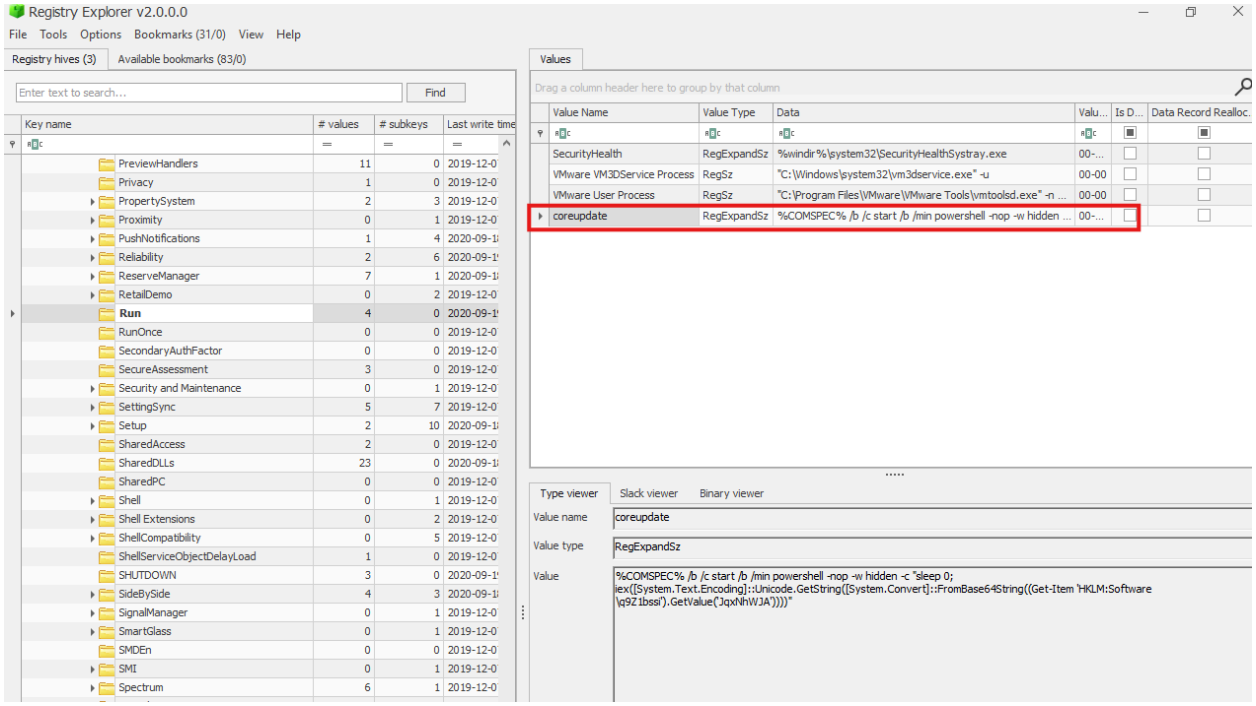


Figure 18. Evidence of Malware Persistence in Windows Registry on Desktop

If coreupdater.exe is listed there, it's trying to persist after reboot (*Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-Technique T1547.001 - Enterprise | MITRE ATT&CK®*, n.d.).

In addition to modifying registry keys for startup execution, the malware may also create a persistent service entry in:

HKLM\SYSTEM\CurrentControlSet\Services\

This method ensures that the malicious process runs continuously, even after system reboots (*Create or Modify System Process: Windows Service, Sub-Technique T1543.003 - Enterprise | MITRE ATT&CK®*, 2020).

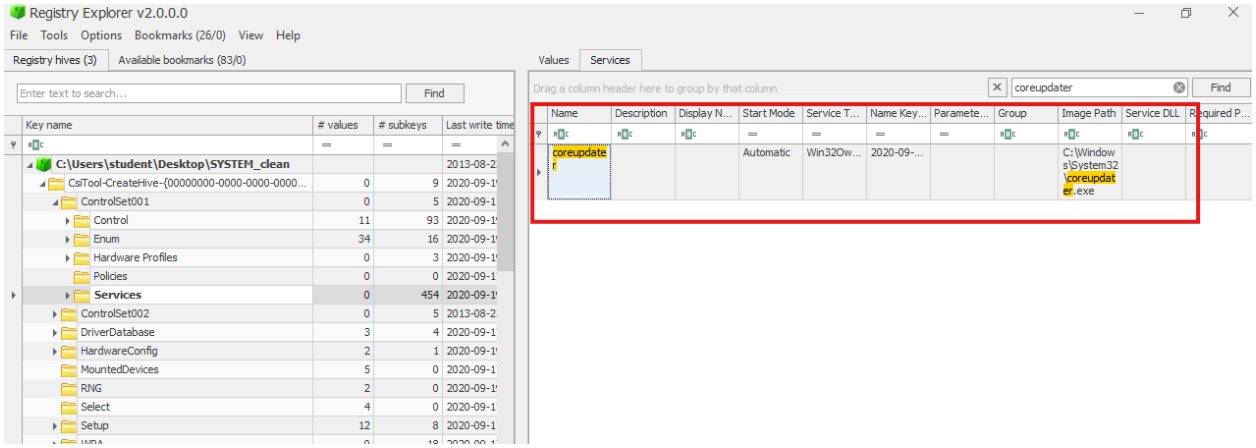


Figure 19. Malware Persistence Using Windows Service Registry Key on Server

7. What malicious IP Addresses were involved?

Answer: 194.61.24.102 (delivered malware, the attacker's IP address), 203.78.103.209 (IP address malware calling to, C2 server)

Upon investigating the IP addresses involved:

- 194.61.24.102: This IP address has been associated with malicious activities, including spam attacks on 110 websites, with the most recent activity recorded on October 12, 2020 (CleanTalk, n.d.). Additionally, it has been identified as a high-risk IP, likely involved in fraudulent behavior and malicious activities (IPQS, n.d.).
- 203.78.103.209: A few vendors on VirusTotal marked this IP as malicious (VirusTotal, n.d.).

8. Did the attacker access any other systems?

Answer: yes, the attacker gained access to the Desktop from the compromised Server.

The presence of the known adversary Command and Control (C2) IPv4 address 203.78.103.109 in the memory of DESKTOP-SDN1RPT indicates a strong likelihood that this system was also compromised. This IP address was previously linked to malware found on the Domain Controller (Citadel-DC01), suggesting that the same malware was installed on DESKTOP-SDN1RPT. Given this evidence, it is probable that this system was actively communicating with the adversary's infrastructure.

The attacker gained access to the Desktop from the compromised Server by establishing a Remote Desktop Protocol (RDP) connection.

Evidence:

- The Server IP initiated an RDP session with the Desktop IP on 2020-09-19 at 02:35:55.
- This activity suggests lateral movement, where the attacker leveraged the compromised server to access another system within the network.

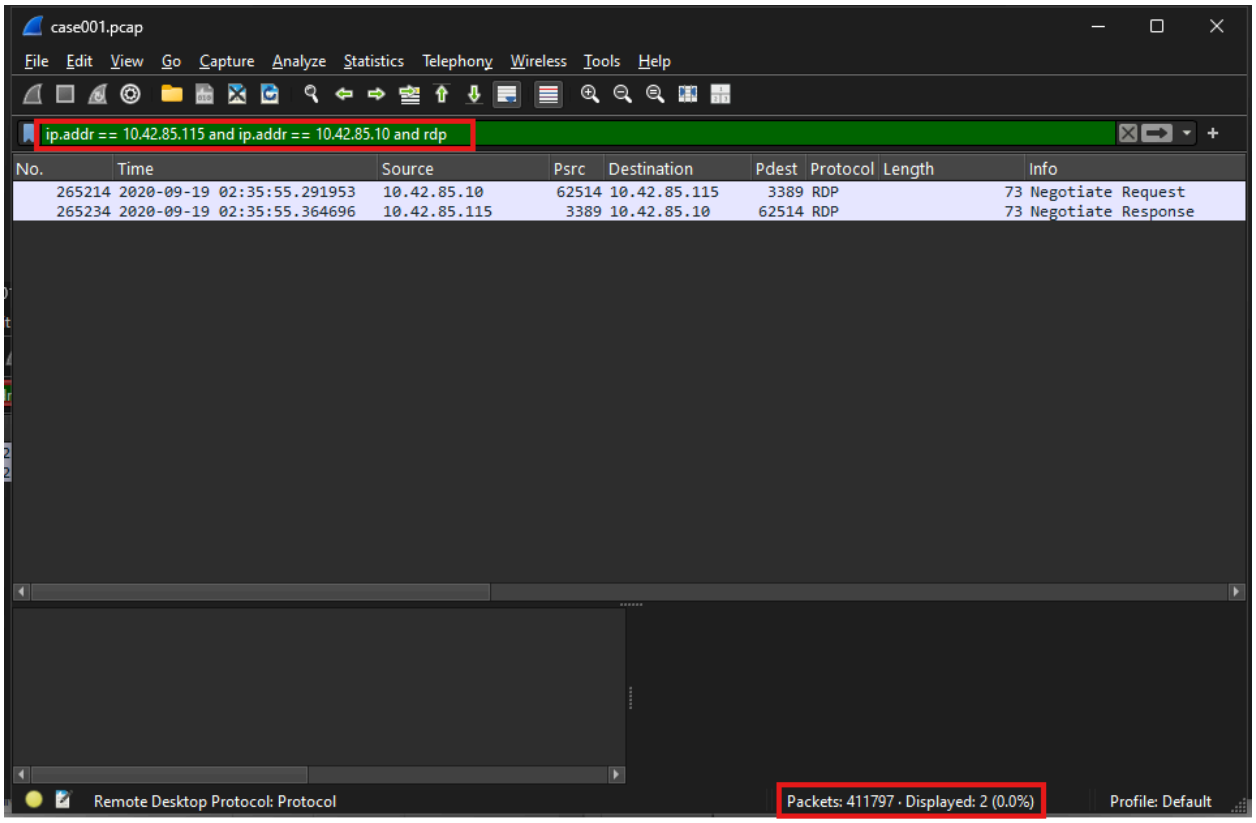


Figure 20. RDP Connection Identified between Server and Desktop During Breach

A solitary RDP connection was identified in the entire .pcap file, making it an anomalous network event during the time of the breach. This deviation from normal activity suggests potential unauthorized access and may indicate lateral movement by the attacker.

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

Answer: Two hosts on 10.42.85.0/24. Server 10.42.85.10 and Desktop 10.42.85.115.

References

Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Sub-technique T1547.001 - Enterprise | MITRE ATT&CK®. (n.d.). MITRE ATT&CK®. Retrieved February 19, 2025, from https://attack.mitre.org/techniques/T1547/001/

Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®. (n.d.). MITRE ATT&CK®. Retrieved February 18, 2025, from https://attack.mitre.org/techniques/T1110/

CleanTalk. (n.d.). Anti-Spam Plugins for WordPress, Joomla, Drupal, and any other websites. Retrieved February 19, 2025, from https://cleantalk.org

Create or Modify System Process: Windows Service, Sub-technique T1543.003 - Enterprise | MITRE ATT&CK®. (2020, January 17). MITRE ATT&CK®. Retrieved February 19, 2025, from https://attack.mitre.org/techniques/T1543/003/

Cyber Kill Chain®. (n.d.). Lockheed Martin. Retrieved February 18, 2025, from https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

fsutil usn. (2024, November 1). Microsoft Learn. Retrieved February 18, 2025, from https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/fsutil-usn

GET - HTTP | MDN. (2024, September 12). MDN Web Docs. Retrieved February 18, 2025, from https://developer.mozilla.org/en-US/docs/Web/HTTP/Methods/GET

Introduction to Spooler Components - Windows drivers. (2024, September 27). Microsoft Learn. Retrieved February 18, 2025, from https://learn.microsoft.com/en-us/windows-hardware/drivers/print/introduction-to-spooler-components

IPQS. (n.d.). *Proxy Detection Test | Detect Proxies With Our IP Lookup*. Retrieved February 19, 2025, from https://www.ipqualityscore.com/free-ip-lookup-proxy-vpn-test

James. (2020, September 21). *The Case of the Stolen Szechuan Sauce*. https://dfirmadness.com/the-stolen-szechuan-sauce/

James. (2020, September 27). *Case 001 Memory Analysis*. DFIR Madness. https://dfirmadness.com/case-001-memory-analysis/

Metasploit - Penetration Testing Tool. (n.d.). Rapid7. Retrieved February 18, 2025, from https://www.rapid7.com/products/metasploit/

Operating System Version - Win32 apps. (2021, November 5). Microsoft Learn. Retrieved February 18, 2025, from https://learn.microsoft.com/en-us/windows/win32/sysinfo/operating-system-version

Pearson, A. (2021, May 10). *Volatility 3 CheatSheet - onfvpBlog [Ashley Pearson]*. onfvp [Ashley Pearson]. Retrieved February 18, 2025, from https://blog.onfvp.com/post/volatility-cheatsheet/

Persistence, Tactic TA0003 - Enterprise | MITRE ATT&CK®. (2018, October 17). MITRE ATT&CK®. Retrieved February 19, 2025, from https://attack.mitre.org/tactics/TA0003/

User Agents. (n.d.). Retrieved February 18, 2025, from https://user-agents.net/string/mozilla-5-0-windows-nt-6-3-wow64-trident-7-0-rv-11-0-like-gecko-ig9qmujg-04

VirusTotal. (n.d.). Retrieved February 18, 2025, from https://www.virustotal.com/