# The Stolen Szechuan Sauce
# Forensics Report and Documentation

Zehra Nur Ozer - Jean Guerrier

July 2024

# Table of Contents

# Foreword

**Jean Guerrier** and **Zehra Nur Ozer** collaborated on this report. We worked together on all sections, conducting multiple Zoom meetings to complete the assignment. While the study and findings presented in this report were achieved through our joint efforts, **Zehra Nur Ozer** developed and presented the report itself**.**

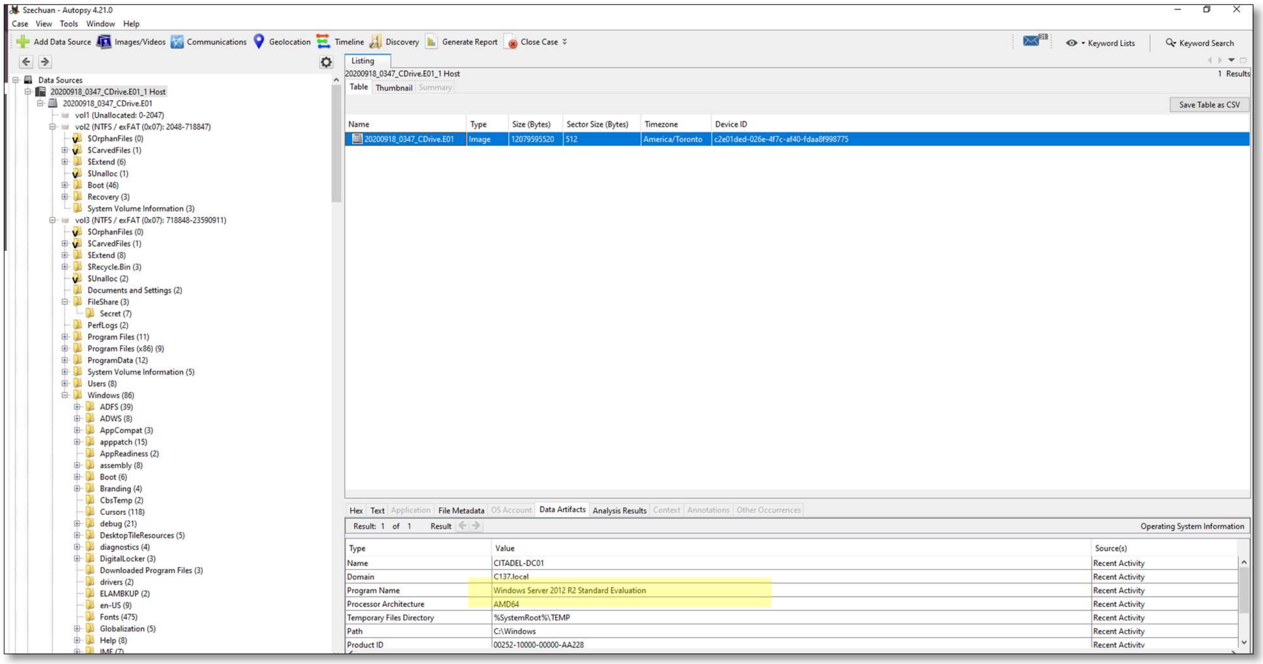
# Introduction

This report details the forensic investigation of Case 001 – The Stolen Szechuan Sauce. The investigation was conducted by analyzing various artifacts provided by DFIR Madness to determine the nature and scope of the breach.
To obtain the results, a VM Sift box, Autopsy, Registry Explorer, Volatility3, and FTK Imager were used. The report is constructed in a question-and-answer format, and the findings and screenshots have been developed from the documents provided on the website dfirmadness.com. Jean Guerrier

# Questions and Answers

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

**Windows Server 2012**
We examined the system information from the DC01 Disk Image using Autopsy.



20200918_0347_CDrive.E01_1 Host — 1 Results

| Name | Type | Size (Bytes) | Sector Size (Bytes) | Timezone | Device ID |
|---|---|---|---|---|---|
| 20200918_0347_CDrive.E01 | Image | 12079595520 | 512 | America/Toronto | c2e01ded-026e-4f7c-af40-fdaa8f998775 |

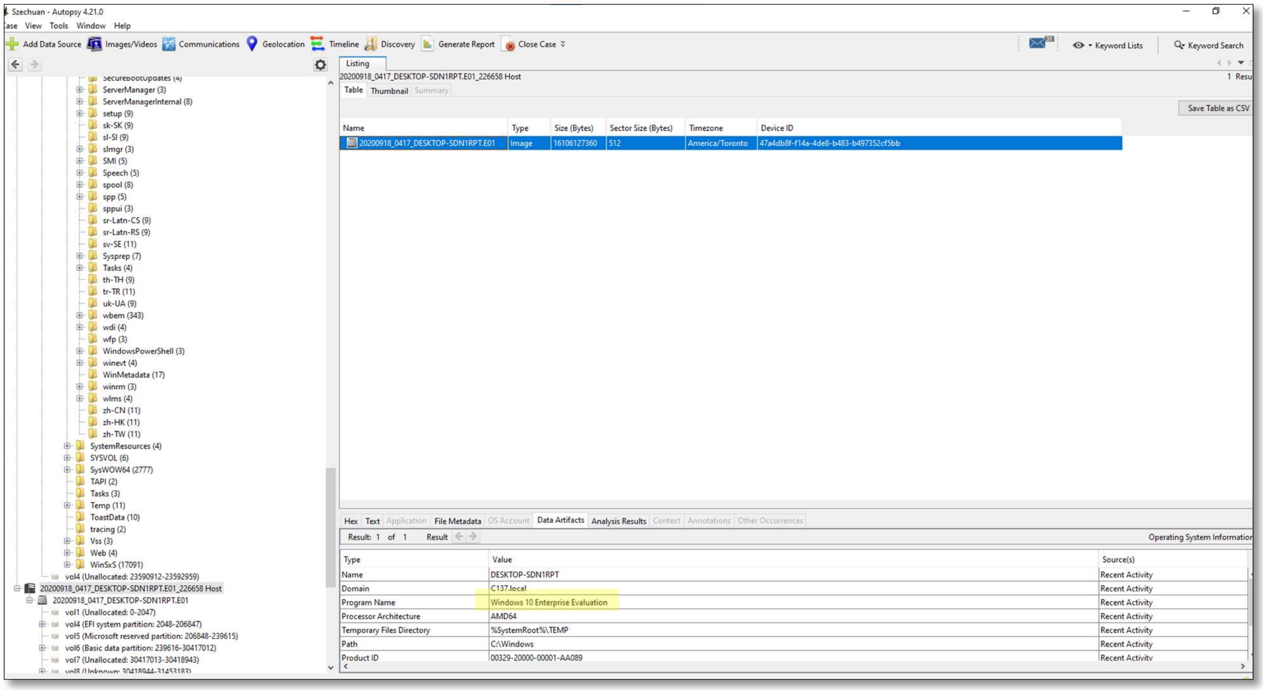
Result: 1 of 1 Result — Operating System Information

| Type | Value | Source(s) |
|---|---|---|
| Name | CITADEL-DC01 | Recent Activity |
| Domain | C137.local | Recent Activity |
| Program Name | Windows Server 2012 R2 Standard Evaluation | Recent Activity |
| Processor Architecture | AMD64 | Recent Activity |
| Temporary Files Directory | %SystemRoot%\TEMP | Recent Activity |
| Path | C:\Windows | Recent Activity |
| Product ID | 00252-10000-00000-AA228 | Recent Activity |

## 2. What’s the Operating System of the Desktop?

**Windows 10**

We checked the system details from the Desktop Disk Image using Autopsy.



```
SecureBootUpdates (4)
ServerManager (3)
ServerManagerInternal (8)
setup (9)
sk-SK (9)
sl-SI (9)
slmgr (3)
SMI (5)
Speech (5)
spool (8)
spp (5)
sppui (3)
sr-Latn-CS (9)
sr-Latn-RS (9)
sv-SE (11)
Sysprep (7)
Tasks (4)
th-TH (9)
tr-TR (11)
uk-UA (9)
wbem (343)
wdi (4)
wfp (3)
WindowsPowerShell (3)
winevt (4)
WinMetadata (17)
winrm (3)
wlms (4)
zh-CN (11)
zh-HK (11)
zh-TW (11)
SystemResources (4)
SYSVOL (6)
SysWOW64 (2777)
TAPI (2)
Tasks (3)
Temp (11)
ToastData (10)
tracing (2)
Vss (3)
Web (4)
WinSxS (17091)
vol4 (Unallocated: 23590912-23592959)
20200918_0417_DESKTOP-SDN1RPT.E01_226658 Host
20200918_0417_DESKTOP-SDN1RPT.E01
vol1 (Unallocated: 0-2047)
vol4 (EFI system partition: 2048-206847)
vol5 (Microsoft reserved partition: 206848-239615)
vol6 (Basic data partition: 239616-30417012)
vol7 (Unallocated: 30417013-30418943)
vol8 (Unknown: 30418944-31453183)
```

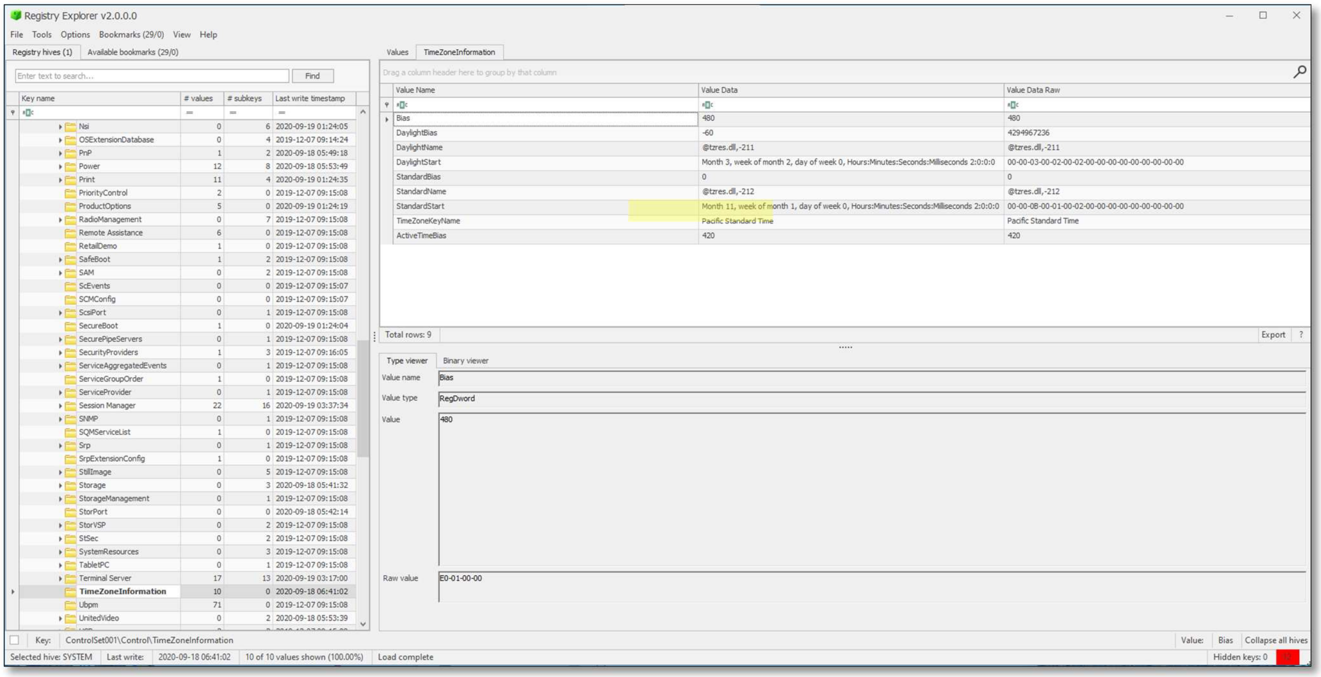
20200918_0417_DESKTOP-SDN1RPT.E01_226658 Host

| Name | Type | Size (Bytes) | Sector Size (Bytes) | Timezone | Device ID |
|---|---|---|---|---|---|
| 20200918_0417_DESKTOP-SDN1RPT.E01 | Image | 16106127360 | 512 | America/Toronto | 47a4db8f-f14a-4de8-b483-b497352cf5bb |

| Type | Value | Source(s) |
|---|---|---|
| Name | DESKTOP-SDN1RPT | Recent Activity |
| Domain | C137.local | Recent Activity |
| Program Name | Windows 10 Enterprise Evaluation | Recent Activity |
| Processor Architecture | AMD64 | Recent Activity |
| Temporary Files Directory | %SystemRoot%\TEMP | Recent Activity |
| Path | C:\Windows | Recent Activity |
| Product ID | 00329-20000-00001-AA089 | Recent Activity |

## 3. What was the local time of the Server?

**Pacific Standard Time**
We downloaded “Registry Explorer” from Eric Zimmerman’s website to find the time zone information.



Registry Explorer v2.0.0.0
File Tools Options Bookmarks (29/0) View Help
Registry hives (1)
Available bookmarks (29/0)
Enter text to search...
Find
Values
TimeZoneInformation
Drag a column header here to group by that column

| Key name | # values | # subkeys | Last write timestamp |
|---|---|---|---|
| Nsi | 0 | 6 | 2020-09-19 01:24:05 |
| OSExtensionDatabase | 0 | 4 | 2019-12-07 09:14:24 |
| PnP | 1 | 2 | 2020-09-18 05:49:18 |
| Power | 12 | 8 | 2020-09-18 05:53:49 |
| Print | 11 | 4 | 2020-09-19 01:24:35 |
| PriorityControl | 2 | 0 | 2019-12-07 09:15:08 |
| ProductOptions | 5 | 0 | 2020-09-19 01:24:19 |
| RadioManagement | 0 | 7 | 2019-12-07 09:15:08 |
| Remote Assistance | 6 | 0 | 2019-12-07 09:15:08 |
| RetailDemo | 1 | 0 | 2019-12-07 09:15:08 |
| SafeBoot | 1 | 2 | 2019-12-07 09:15:08 |
| SAM | 0 | 2 | 2019-12-07 09:15:08 |
| ScEvents | 0 | 0 | 2019-12-07 09:15:07 |
| SCMConfig | 0 | 0 | 2019-12-07 09:15:07 |
| ScsiPort | 0 | 1 | 2019-12-07 09:15:08 |
| SecureBoot | 1 | 0 | 2020-09-19 01:24:04 |
| SecurePipeServers | 0 | 1 | 2019-12-07 09:15:08 |
| SecurityProviders | 1 | 3 | 2019-12-07 09:16:05 |
| ServiceAggregatedEvents | 0 | 1 | 2019-12-07 09:15:08 |
| ServiceGroupOrder | 1 | 0 | 2019-12-07 09:15:08 |
| ServiceProvider | 0 | 1 | 2019-12-07 09:15:08 |
| Session Manager | 22 | 16 | 2020-09-19 03:37:34 |
| SNMP | 0 | 1 | 2019-12-07 09:15:08 |
| SQMServiceList | 1 | 0 | 2019-12-07 09:15:08 |
| Srp | 0 | 1 | 2019-12-07 09:15:08 |
| SrpExtensionConfig | 1 | 0 | 2019-12-07 09:15:08 |
| StillImage | 0 | 5 | 2019-12-07 09:15:08 |
| Storage | 0 | 3 | 2020-09-18 05:41:32 |
| StorageManagement | 0 | 1 | 2019-12-07 09:15:08 |
| StorPort | 0 | 0 | 2020-09-18 05:42:14 |
| StorVSP | 0 | 2 | 2019-12-07 09:15:08 |
| StSec | 0 | 2 | 2019-12-07 09:15:08 |
| SystemResources | 0 | 3 | 2019-12-07 09:15:08 |
| TabletPC | 0 | 1 | 2019-12-07 09:15:08 |
| Terminal Server | 17 | 13 | 2020-09-19 03:17:00 |
| **TimeZoneInformation** | 10 | 0 | 2020-09-18 06:41:02 |
| Ubpm | 71 | 0 | 2019-12-07 09:15:08 |
| UnitedVideo | 0 | 2 | 2020-09-18 05:53:39 |

| Value Name | Value Data | Value Data Raw |
|---|---|---|
| Bias | 480 | 480 |
| DaylightBias | -60 | 4294967236 |
| DaylightName | @tzres.dll,-211 | @tzres.dll,-211 |
| DaylightStart | Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0 | 00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00 |
| StandardBias | 0 | 0 |
| StandardName | @tzres.dll,-212 | @tzres.dll,-212 |
| StandardStart | Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0 | 00-00-0B-00-01-00-02-00-00-00-00-00-00-00-00-00 |
| TimeZoneKeyName | Pacific Standard Time | Pacific Standard Time |
| ActiveTimeBias | 420 | 420 |

Total rows: 9

Value name: Bias
Value type: RegDword
Value: 480
Raw value: E0-01-00-00

Key: ControlSet001\Control\TimeZoneInformation

Selected hive: SYSTEM | Last write: 2020-09-18 06:41:02 | 10 of 10 values shown (100.00%) | Load complete

Value: Bias | Collapse all hives | Hidden keys: 0

## 4. Was there a breach?

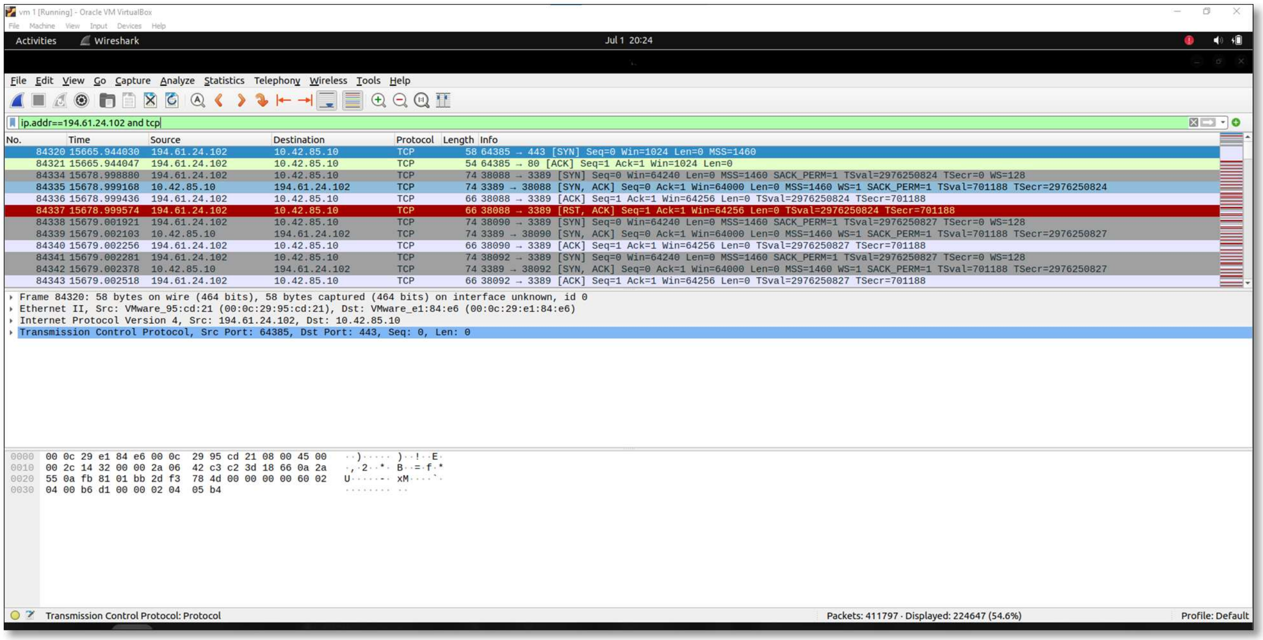
**Yes**
Evidence of unauthorized access was found in the logs and network captures.

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

**RDP Brute Force**

We analyzed the security logs and identified repeated failed login attempts followed by a successful login. Wireshark was used to examine it.

The command **ip.addr==194.61.24.102 and TCP** have been used.


vm 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
Jul 1 20:24
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
Profile: Default

```
ip.addr==194.61.24.102 and tcp
```

```
No.   Time            Source          Destination     Protocol Length Info
84320 15665.944030    194.61.24.102   10.42.85.10     TCP      58 64385 → 443 [SYN] Seq=0 Win=1024 Len=0 MSS=1460
84321 15665.944047    194.61.24.102   10.42.85.10     TCP      54 64385 → 80 [ACK] Seq=1 Ack=1 Win=1024 Len=0
84334 15678.998880    194.61.24.102   10.42.85.10     TCP      74 38088 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2976250824 TSecr=0 WS=128
84335 15678.999168    10.42.85.10     194.61.24.102   TCP      74 3389 → 38088 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1 TSval=701188 TSecr=2976250824
84336 15678.999436    194.61.24.102   10.42.85.10     TCP      66 38088 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2976250824 TSecr=701188
84337 15678.999574    194.61.24.102   10.42.85.10     TCP      66 38088 → 3389 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2976250824 TSecr=701188
84338 15679.001921    194.61.24.102   10.42.85.10     TCP      74 38090 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2976250827 TSecr=0 WS=128
84339 15679.002103    10.42.85.10     194.61.24.102   TCP      74 3389 → 38090 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1 TSval=701188 TSecr=2976250827
84340 15679.002256    194.61.24.102   10.42.85.10     TCP      66 38090 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2976250827 TSecr=701188
84341 15679.002281    194.61.24.102   10.42.85.10     TCP      74 38092 → 3389 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1 TSval=2976250827 TSecr=0 WS=128
84342 15679.002378    10.42.85.10     194.61.24.102   TCP      74 3389 → 38092 [SYN, ACK] Seq=0 Ack=1 Win=64000 Len=0 MSS=1460 WS=1 SACK_PERM=1 TSval=701188 TSecr=2976250827
84343 15679.002518    194.61.24.102   10.42.85.10     TCP      66 38092 → 3389 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=2976250827 TSecr=701188
```

```
› Frame 84320: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface unknown, id 0
› Ethernet II, Src: VMware_95:cd:21 (00:0c:29:95:cd:21), Dst: VMware_e1:84:e6 (00:0c:29:e1:84:e6)
› Internet Protocol Version 4, Src: 194.61.24.102, Dst: 10.42.85.10
› Transmission Control Protocol, Src Port: 64385, Dst Port: 443, Seq: 0, Len: 0
```

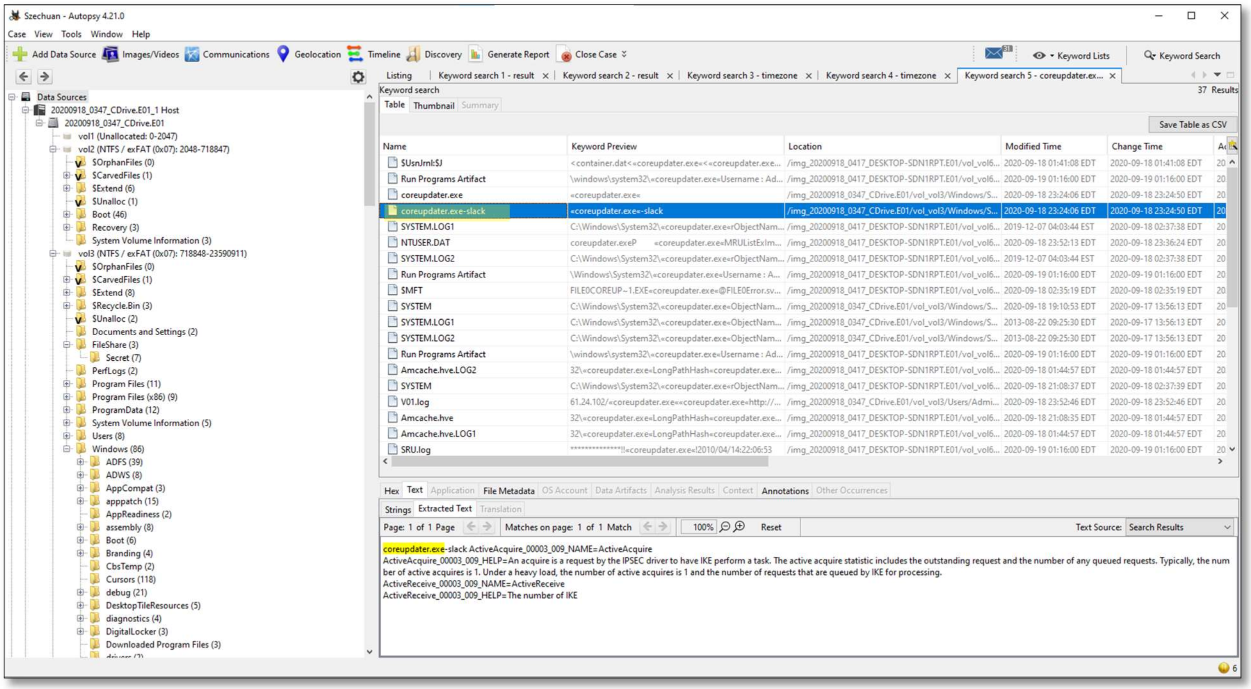
```
0000  00 0c 29 e1 84 e6 00 0c  29 95 cd 21 08 00 45 00   ··)·····)··!··E·
0010  00 2c 14 32 00 00 2a 06  42 c3 c2 3d 18 66 0a 2a   ·,·2··*·B··=·f·*
0020  55 0a fb 81 01 bb 2d f3  78 4d 00 00 00 00 60 02   U·····-·xM····`·
0030  04 00 b6 d1 00 00 02 04  05 b4                     ··········
```

```
Transmission Control Protocol: Protocol          Packets: 411797 · Displayed: 224647 (54.6%)
```

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

**Yes, coreupdater**

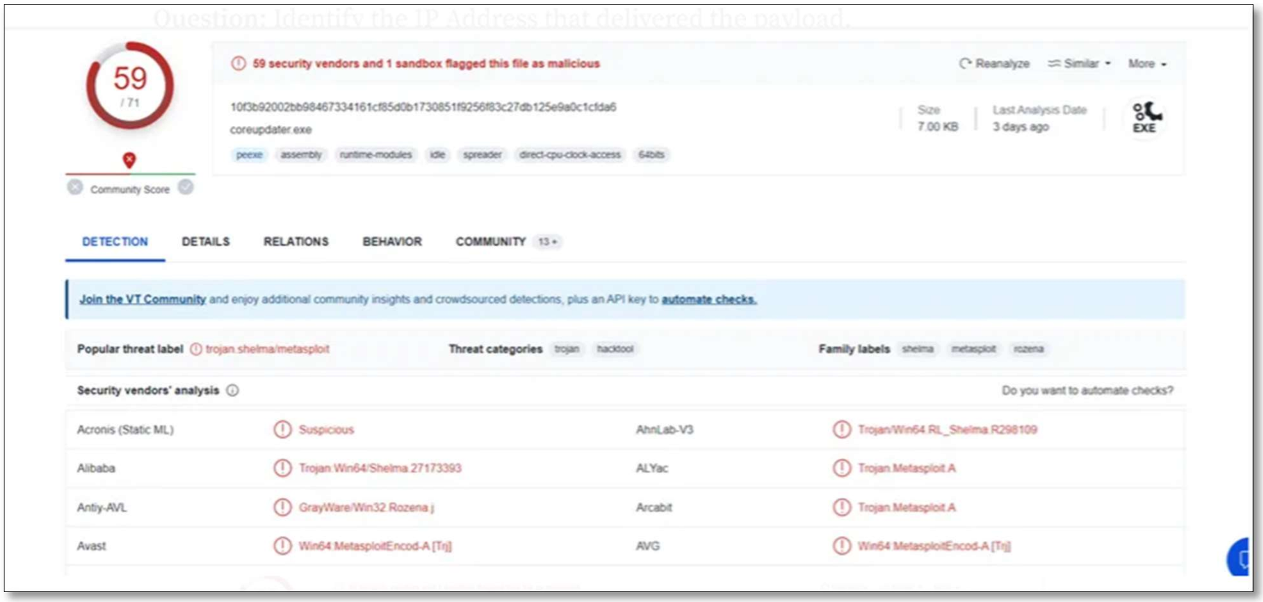
We identified malicious processes and files during memory analysis and disk examination. We used the keyword search for well-known malware names.



| Name | Keyword Preview | Location | Modified Time | Change Time | Ac |
|---|---|---|---|---|---|
| $UsnJrnl:$J | <container.dat<«coreupdater.exe«<«coreupdater.exe... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 01:41:08 EDT | 2020-09-18 01:41:08 EDT | 20 |
| Run Programs Artifact | \windows\system32\«coreupdater.exe«Username : Ad... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-19 01:16:00 EDT | 2020-09-19 01:16:00 EDT | 20 |
| coreupdater.exe | «coreupdater.exe« | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2020-09-18 23:24:06 EDT | 2020-09-18 23:24:50 EDT | 20 |
| coreupdater.exe-slack | «coreupdater.exe«-slack | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2020-09-18 23:24:06 EDT | 2020-09-18 23:24:50 EDT | 20 |
| SYSTEM.LOG1 | C:\Windows\System32\«coreupdater.exe«rObjectNam... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2019-12-07 04:03:44 EST | 2020-09-18 02:37:38 EDT | 20 |
| NTUSER.DAT | coreupdater.exeP «coreupdater.exe«MRUListExIm... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 23:52:13 EDT | 2020-09-18 23:36:24 EDT | 20 |
| SYSTEM.LOG2 | C:\Windows\System32\«coreupdater.exe«rObjectNam... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2019-12-07 04:03:44 EST | 2020-09-18 02:37:38 EDT | 20 |
| Run Programs Artifact | \Windows\System32\«coreupdater.exe«Username : A... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-19 01:16:00 EDT | 2020-09-19 01:16:00 EDT | 20 |
| $MFT | FILE0COREUP~1.EXE«coreupdater.exe«@FILE0Error.sv... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 02:35:19 EDT | 2020-09-18 02:35:19 EDT | 20 |
| SYSTEM | C:\Windows\System32\«coreupdater.exe«ObjectNam... | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2020-09-18 19:10:53 EDT | 2020-09-17 13:56:13 EDT | 20 |
| SYSTEM.LOG1 | C:\Windows\System32\«coreupdater.exe«ObjectNam... | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2013-08-22 09:25:30 EDT | 2020-09-17 13:56:13 EDT | 20 |
| SYSTEM.LOG2 | C:\Windows\System32\«coreupdater.exe«ObjectNam... | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2013-08-22 09:25:30 EDT | 2020-09-17 13:56:13 EDT | 20 |
| Run Programs Artifact | \windows\system32\«coreupdater.exe«Username : Ad... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-19 01:16:00 EDT | 2020-09-19 01:16:00 EDT | 20 |
| Amcache.hve.LOG2 | 32\«coreupdater.exe«LongPathHash«coreupdater.exe... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 01:44:57 EDT | 2020-09-18 01:44:57 EDT | 20 |
| SYSTEM | C:\Windows\System32\«coreupdater.exe«rObjectNam... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 21:08:37 EDT | 2020-09-18 02:37:39 EDT | 20 |
| V01.log | 61.24.102/«coreupdater.exe««coreupdater.exe«http://... | /img_20200918_0347_CDrive.E01/vol_vol3/Users/Admi... | 2020-09-18 23:52:46 EDT | 2020-09-18 23:52:46 EDT | 20 |
| Amcache.hve | 32\«coreupdater.exe«LongPathHash«coreupdater.exe... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 21:08:35 EDT | 2020-09-18 01:44:57 EDT | 20 |
| Amcache.hve.LOG1 | 32\«coreupdater.exe«LongPathHash«coreupdater.exe... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 01:44:57 EDT | 2020-09-18 01:44:57 EDT | 20 |
| SRU.log | **************!!«coreupdater.exe«!2010/04/14:22:06:53 | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-19 01:16:00 EDT | 2020-09-19 01:16:00 EDT | 20 |

```
coreupdater.exe-slack ActiveAcquire_00003_009_NAME=ActiveAcquire
ActiveAcquire_00003_009_HELP=An acquire is a request by the IPSEC driver to have IKE perform a task. The active acquire statistic includes the outstanding request and the number of any queued requests. Typically, the num
ber of active acquires is 1. Under a heavy load, the number of active acquires is 1 and the number of requests that are queued by IKE for processing.
ActiveReceive_00003_009_NAME=ActiveReceive
ActiveReceive_00003_009_HELP=The number of IKE
```

Please note that we are also aware that the hash value for coreupdater.exe was identified as malicious. The screenshot below shows the malicious percentage of coreupdater.exe. Lalwani (2023)



Question: Identify the IP Address that delivered the payload.

59 security vendors and 1 sandbox flagged this file as malicious

10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

coreupdater.exe

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  Do you want to automate checks?

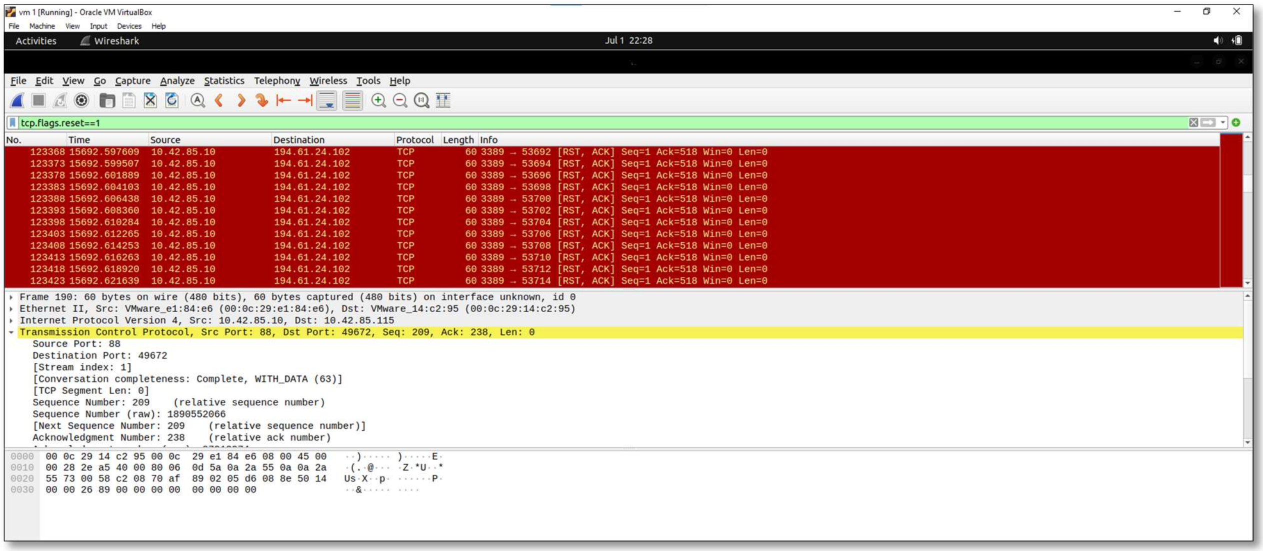
| | | | |
|---|---|---|---|
| Acronis (Static ML) | Suspicious | AhnLab-V3 | Trojan/Win64.RL_Shelma.R298109 |
| Alibaba | Trojan:Win64/Shelma.27173393 | ALYac | Trojan.Metasploit.A |
| Antiy-AVL | GrayWare/Win32.Rozena.j | Arcabit | Trojan.Metasploit.A |
| Avast | Win64:MetasploitEncod-A [Trj] | AVG | Win64:MetasploitEncod-A [Trj] |

*Figure 1by Lalwani (2023*

## 7. What process was malicious?

**coreupdater was the initial process.**

Identified during the memory analysis and verified with process execution logs.
The filter shows the packet list only for the TCP SYN packets, allowing you to focus on initiating TCP connections on your network.


vm 1 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
Activities
Wireshark
Jul 1 22:28
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

```
tcp.flags.reset==1
```

```
No.           Time          Source          Destination      Protocol  Length Info
  123368 15692.597609  10.42.85.10     194.61.24.102    TCP       60 3389 → 53692 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123373 15692.599507  10.42.85.10     194.61.24.102    TCP       60 3389 → 53694 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123378 15692.601889  10.42.85.10     194.61.24.102    TCP       60 3389 → 53696 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123383 15692.604103  10.42.85.10     194.61.24.102    TCP       60 3389 → 53698 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123388 15692.606438  10.42.85.10     194.61.24.102    TCP       60 3389 → 53700 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123393 15692.608360  10.42.85.10     194.61.24.102    TCP       60 3389 → 53702 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123398 15692.610284  10.42.85.10     194.61.24.102    TCP       60 3389 → 53704 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123403 15692.612265  10.42.85.10     194.61.24.102    TCP       60 3389 → 53706 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123408 15692.614253  10.42.85.10     194.61.24.102    TCP       60 3389 → 53708 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123413 15692.616263  10.42.85.10     194.61.24.102    TCP       60 3389 → 53710 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123418 15692.618920  10.42.85.10     194.61.24.102    TCP       60 3389 → 53712 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
  123423 15692.621639  10.42.85.10     194.61.24.102    TCP       60 3389 → 53714 [RST, ACK] Seq=1 Ack=518 Win=0 Len=0
```

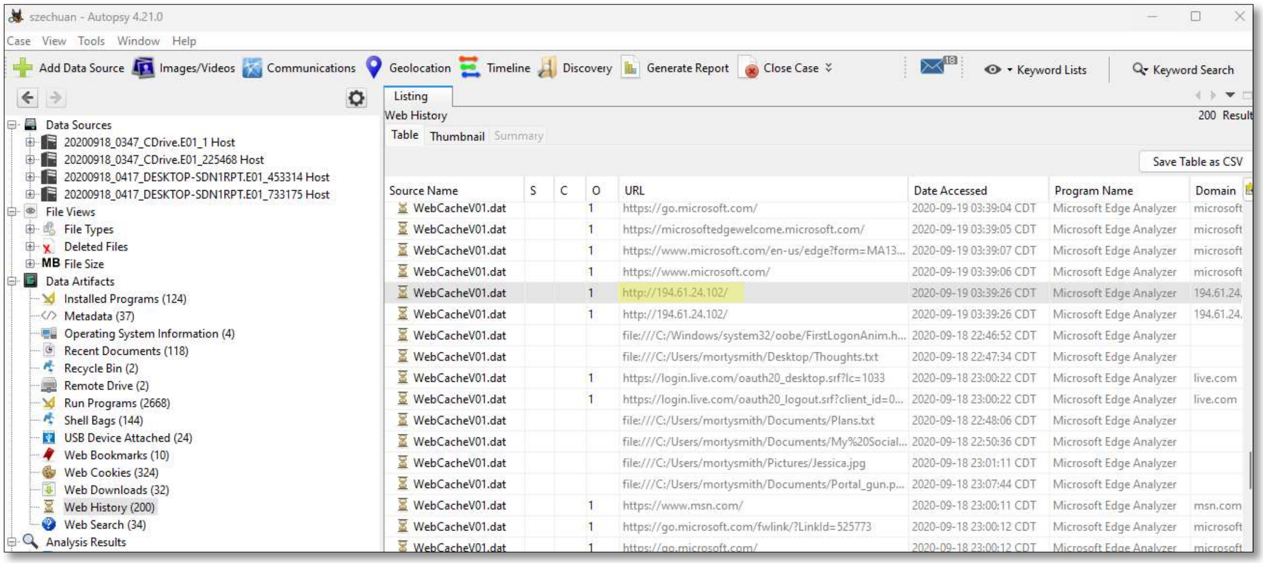
```
› Frame 190: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface unknown, id 0
› Ethernet II, Src: VMware_e1:84:e6 (00:0c:29:e1:84:e6), Dst: VMware_14:c2:95 (00:0c:29:14:c2:95)
› Internet Protocol Version 4, Src: 10.42.85.10, Dst: 10.42.85.115
˅ Transmission Control Protocol, Src Port: 88, Dst Port: 49672, Seq: 209, Ack: 238, Len: 0
    Source Port: 88
    Destination Port: 49672
    [Stream index: 1]
    [Conversation completeness: Complete, WITH_DATA (63)]
    [TCP Segment Len: 0]
    Sequence Number: 209    (relative sequence number)
    Sequence Number (raw): 1890552066
    [Next Sequence Number: 209    (relative sequence number)]
    Acknowledgment Number: 238    (relative ack number)
```

```
0000  00 0c 29 14 c2 95 00 0c  29 e1 84 e6 08 00 45 00   ··)·····)·····E·
0010  00 28 2e a5 40 00 80 06  0d 5a 0a 2a 55 0a 0a 2a   ·(.·@····Z·*U··*
0020  55 73 00 58 c2 08 70 af  89 02 05 d6 08 8e 50 14   Us·X··p·······P·
0030  00 00 26 89 00 00 00 00  00 00 00 00               ··&·········
```

## 8. Identify the IP Address that delivered the payload.

**194.61.24.102**

Analysis of network captures and system logs.



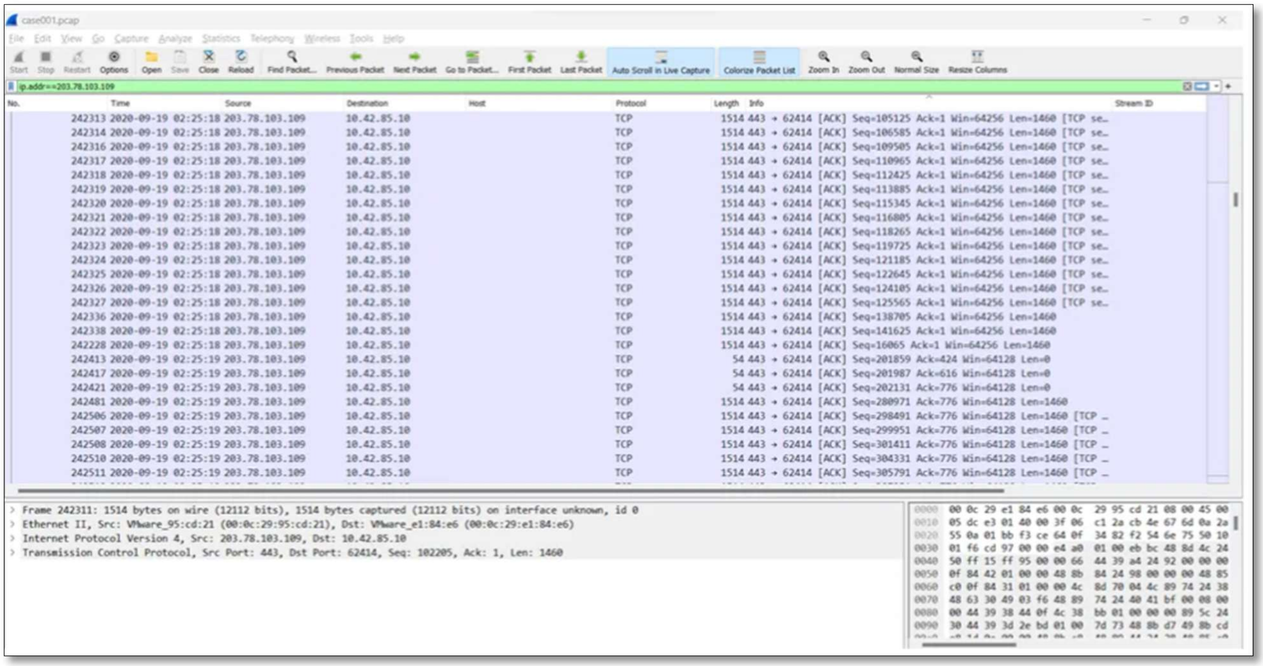
| Source Name | S | C | O | URL | Date Accessed | Program Name | Domain |
|---|---|---|---|---|---|---|---|
| WebCacheV01.dat | | | 1 | https://go.microsoft.com/ | 2020-09-19 03:39:04 CDT | Microsoft Edge Analyzer | microsoft |
| WebCacheV01.dat | | | 1 | https://microsoftedgewelcome.microsoft.com/ | 2020-09-19 03:39:05 CDT | Microsoft Edge Analyzer | microsoft |
| WebCacheV01.dat | | | 1 | https://www.microsoft.com/en-us/edge?form=MA13... | 2020-09-19 03:39:07 CDT | Microsoft Edge Analyzer | microsoft |
| WebCacheV01.dat | | | 1 | https://www.microsoft.com/ | 2020-09-19 03:39:06 CDT | Microsoft Edge Analyzer | microsoft |
| WebCacheV01.dat | | | 1 | http://194.61.24.102/ | 2020-09-19 03:39:26 CDT | Microsoft Edge Analyzer | 194.61.24. |
| WebCacheV01.dat | | | 1 | http://194.61.24.102/ | 2020-09-19 03:39:26 CDT | Microsoft Edge Analyzer | 194.61.24. |
| WebCacheV01.dat | | | | file:///C:/Windows/system32/oobe/FirstLogonAnim.h... | 2020-09-18 22:46:52 CDT | Microsoft Edge Analyzer | |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Desktop/Thoughts.txt | 2020-09-18 22:47:34 CDT | Microsoft Edge Analyzer | |
| WebCacheV01.dat | | | 1 | https://login.live.com/oauth20_desktop.srf?lc=1033 | 2020-09-18 23:00:22 CDT | Microsoft Edge Analyzer | live.com |
| WebCacheV01.dat | | | 1 | https://login.live.com/oauth20_logout.srf?client_id=0... | 2020-09-18 23:00:22 CDT | Microsoft Edge Analyzer | live.com |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Documents/Plans.txt | 2020-09-18 22:48:06 CDT | Microsoft Edge Analyzer | |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Documents/My%20Social... | 2020-09-18 22:50:36 CDT | Microsoft Edge Analyzer | |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Pictures/Jessica.jpg | 2020-09-18 23:01:11 CDT | Microsoft Edge Analyzer | |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Documents/Portal_gun.p... | 2020-09-18 23:07:44 CDT | Microsoft Edge Analyzer | |
| WebCacheV01.dat | | | 1 | https://www.msn.com/ | 2020-09-18 23:00:11 CDT | Microsoft Edge Analyzer | msn.com |
| WebCacheV01.dat | | | 1 | https://go.microsoft.com/fwlink/?LinkId=525773 | 2020-09-18 23:00:12 CDT | Microsoft Edge Analyzer | microsoft |
| WebCacheV01.dat | | | 1 | https://go.microsoft.com/ | 2020-09-18 23:00:12 CDT | Microsoft Edge Analyzer | microsoft |

## 9. What IP Address is the malware calling to?

**203.78.103.109**

We reviewed outbound network connections in the PCAP file.

203.78.103.109 is the IP Address that the malware is calling. We verified this by looking into the VirusTotal > Relations Tab and noticed 6 IP addresses associated with it. Then, we looked into case001.pcap file and observed that the most called IP Address was 203.78.103.109. Lalwani (2023)



```
ip.addr==203.78.103.109
```

```
No.           Time                Source          Destination      Host        Protocol   Length Info                                                                       Stream ID
      242313 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=105125 Ack=1 Win=64256 Len=1460 [TCP se…
      242314 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=106585 Ack=1 Win=64256 Len=1460 [TCP se…
      242316 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=109505 Ack=1 Win=64256 Len=1460 [TCP se…
      242317 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=110965 Ack=1 Win=64256 Len=1460 [TCP se…
      242318 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=112425 Ack=1 Win=64256 Len=1460 [TCP se…
      242319 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=113885 Ack=1 Win=64256 Len=1460 [TCP se…
      242320 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=115345 Ack=1 Win=64256 Len=1460 [TCP se…
      242321 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=116805 Ack=1 Win=64256 Len=1460 [TCP se…
      242322 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=118265 Ack=1 Win=64256 Len=1460 [TCP se…
      242323 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=119725 Ack=1 Win=64256 Len=1460 [TCP se…
      242324 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=121185 Ack=1 Win=64256 Len=1460 [TCP se…
      242325 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=122645 Ack=1 Win=64256 Len=1460 [TCP se…
      242326 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=124105 Ack=1 Win=64256 Len=1460 [TCP se…
      242327 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=125565 Ack=1 Win=64256 Len=1460 [TCP se…
      242336 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=138705 Ack=1 Win=64256 Len=1460
      242338 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=141625 Ack=1 Win=64256 Len=1460
      242228 2020-09-19 02:25:18 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=16065 Ack=1 Win=64256 Len=1460
      242413 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP          54 443 → 62414 [ACK] Seq=201859 Ack=424 Win=64128 Len=0
      242417 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP          54 443 → 62414 [ACK] Seq=201987 Ack=616 Win=64128 Len=0
      242421 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP          54 443 → 62414 [ACK] Seq=202131 Ack=776 Win=64128 Len=0
      242481 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=280971 Ack=776 Win=64128 Len=1460
      242506 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=298491 Ack=776 Win=64128 Len=1460 [TCP …
      242507 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=299951 Ack=776 Win=64128 Len=1460 [TCP …
      242508 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=301411 Ack=776 Win=64128 Len=1460 [TCP …
      242510 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=304331 Ack=776 Win=64128 Len=1460 [TCP …
      242511 2020-09-19 02:25:19 203.78.103.109  10.42.85.10                  TCP        1514 443 → 62414 [ACK] Seq=305791 Ack=776 Win=64128 Len=1460 [TCP …
```

```
> Frame 242311: 1514 bytes on wire (12112 bits), 1514 bytes captured (12112 bits) on interface unknown, id 0
> Ethernet II, Src: VMware_95:cd:21 (00:0c:29:95:cd:21), Dst: VMware_e1:84:e6 (00:0c:29:e1:84:e6)
> Internet Protocol Version 4, Src: 203.78.103.109, Dst: 10.42.85.10
> Transmission Control Protocol, Src Port: 443, Dst Port: 62414, Seq: 102205, Ack: 1, Len: 1460
```

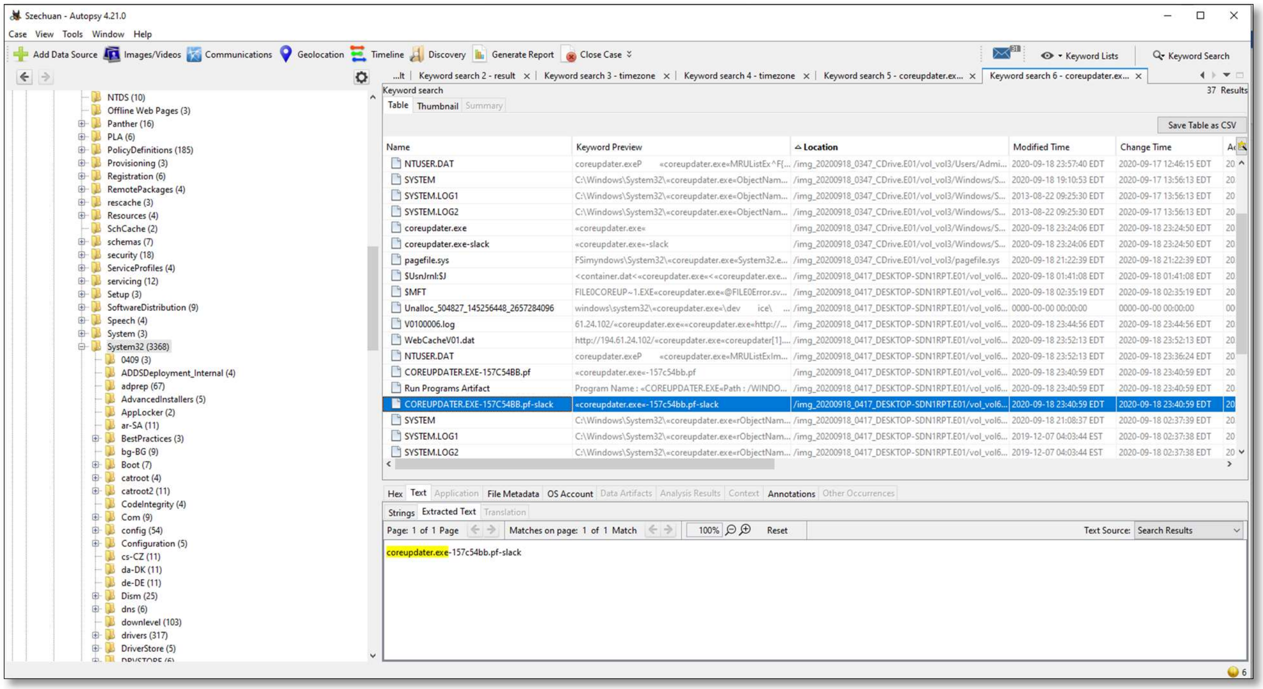
```
0000  00 0c 29 e1 84 e6 00 0c  29 95 cd 21 08 00 45 00
0010  05 dc e3 01 40 00 3f 06  c1 2a cb 4e 67 6d 0a 2a
0020  55 0a 01 bb f3 ce 64 0f  34 82 f2 54 6e 75 50 10
0030  01 f6 cd 97 00 00 e4 a0  01 00 eb bc 48 8d 4c 24
0040  50 ff 15 ff 95 00 00 66  44 39 a4 24 92 00 00 00
0050  0f 84 42 01 00 00 48 8b  84 24 98 00 00 00 48 85
0060  c0 0f 84 31 01 00 00 4c  8d 70 04 4c 89 74 24 38
0070  48 63 30 49 03 f6 48 89  74 24 40 41 bf 00 08 00
0080  00 44 39 38 44 0f 4c 38  bb 01 00 00 00 89 5c 24
0090  30 44 39 3d 2e bd 01 00  7d 73 48 8b d7 49 8b cd
```

*Figure 2 by Lalwani (2023)*

## 10. Where is this malware on disk?

**C:\Windows\System32\coreupdate.exe**

File path identified during disk analysis.



Szechuan - Autopsy 4.21.0

Keyword search 6 - coreupdater.ex...

Keyword search — 37 Results

| Name | Keyword Preview | Location | Modified Time | Change Time | Ac |
|---|---|---|---|---|---|
| NTUSER.DAT | coreupdater.exeP «coreupdater.exe«MRUListEx^F{... | /img_20200918_0347_CDrive.E01/vol_vol3/Users/Admi... | 2020-09-18 23:57:40 EDT | 2020-09-17 12:46:15 EDT | 20 |
| SYSTEM | C:\Windows\System32\«coreupdater.exe«ObjectNam... | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2020-09-18 19:10:53 EDT | 2020-09-17 13:56:13 EDT | 20 |
| SYSTEM.LOG1 | C:\Windows\System32\«coreupdater.exe«ObjectNam... | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2013-08-22 09:25:30 EDT | 2020-09-17 13:56:13 EDT | 20 |
| SYSTEM.LOG2 | C:\Windows\System32\«coreupdater.exe«ObjectNam... | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2013-08-22 09:25:30 EDT | 2020-09-17 13:56:13 EDT | 20 |
| coreupdater.exe | «coreupdater.exe« | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2020-09-18 23:24:06 EDT | 2020-09-18 23:24:50 EDT | 20 |
| coreupdater.exe-slack | «coreupdater.exe«-slack | /img_20200918_0347_CDrive.E01/vol_vol3/Windows/S... | 2020-09-18 23:24:06 EDT | 2020-09-18 23:24:50 EDT | 20 |
| pagefile.sys | FSimyndows\System32\«coreupdater.exe«System32.e... | /img_20200918_0347_CDrive.E01/vol_vol3/pagefile.sys | 2020-09-18 21:22:39 EDT | 2020-09-18 21:22:39 EDT | 20 |
| $UsnJrnl:$J | <container.dat<«coreupdater.exe«<«coreupdater.exe... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 01:41:08 EDT | 2020-09-18 01:41:08 EDT | 20 |
| $MFT | FILE0COREUP~1.EXE«coreupdater.exe«@FILE0Error.sv... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 02:35:19 EDT | 2020-09-18 02:35:19 EDT | 20 |
| Unalloc_504827_145256448_2657284096 | windows\system32\«coreupdater.exe«\dev ice\ ... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 0000-00-00 00:00:00 | 0000-00-00 00:00:00 | 00 |
| V0100006.log | 61.24.102/«coreupdater.exe««coreupdater.exe«http://... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 23:44:56 EDT | 2020-09-18 23:44:56 EDT | 20 |
| WebCacheV01.dat | http://194.61.24.102/«coreupdater.exe«coreupdater[1].... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 23:52:13 EDT | 2020-09-18 23:52:13 EDT | 20 |
| NTUSER.DAT | coreupdater.exeP «coreupdater.exe«MRUListExIm... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 23:52:13 EDT | 2020-09-18 23:36:24 EDT | 20 |
| COREUPDATER.EXE-157C54BB.pf | «coreupdater.exe«-157c54bb.pf | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 23:40:59 EDT | 2020-09-18 23:40:59 EDT | 20 |
| Run Programs Artifact | Program Name : «COREUPDATER.EXE«Path : /WINDO... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 23:40:59 EDT | 2020-09-18 23:40:59 EDT | 20 |
| COREUPDATER.EXE-157C54BB.pf-slack | «coreupdater.exe«-157c54bb.pf-slack | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 23:40:59 EDT | 2020-09-18 23:40:59 EDT | 20 |
| SYSTEM | C:\Windows\System32\«coreupdater.exe«rObjectNam... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2020-09-18 21:08:37 EDT | 2020-09-18 02:37:39 EDT | 20 |
| SYSTEM.LOG1 | C:\Windows\System32\«coreupdater.exe«rObjectNam... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2019-12-07 04:03:44 EST | 2020-09-18 02:37:38 EDT | 20 |
| SYSTEM.LOG2 | C:\Windows\System32\«coreupdater.exe«rObjectNam... | /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6... | 2019-12-07 04:03:44 EST | 2020-09-18 02:37:38 EDT | 20 |

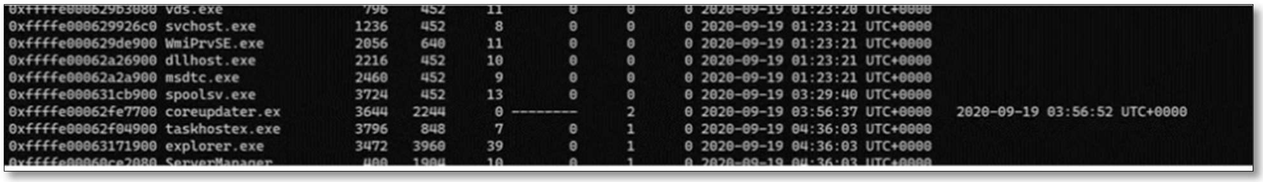
Page: 1 of 1 Page — Matches on page: 1 of 1 Match — 100% — Text Source: Search Results

coreupdater.exe-157c54bb.pf-slack

## 11. When did it first appear?

**It first appeared on 2020–09–19 03:56:52 UTC+0000**

Timeline analysis using the Super Timeline and cross-referencing with system logs.



```
0xffffe0006293080 vds.exe          796    452    11        0    0    0 2020-09-19 01:23:20 UTC+0000
0xffffe000629926c0 svchost.exe      1236   452     8        0    0    0 2020-09-19 01:23:21 UTC+0000
0xffffe000629de900 WmiPrvSE.exe     2056   640    11        0    0    0 2020-09-19 01:23:21 UTC+0000
0xffffe00062a26900 dllhost.exe      2216   452    10        0    0    0 2020-09-19 01:23:21 UTC+0000
0xffffe00062a2a900 msdtc.exe        2460   452     9        0    0    0 2020-09-19 01:23:21 UTC+0000
0xffffe000631cb900 spoolsv.exe      3724   452    13        0    0    0 2020-09-19 03:29:40 UTC+0000
0xffffe00062fe7700 coreupdater.ex   3644   2244    0 --------    2    0 2020-09-19 03:56:37 UTC+0000   2020-09-19 03:56:52 UTC+0000
0xffffe00062f04900 taskhostex.exe   3796   848     7        0    1    0 2020-09-19 04:36:03 UTC+0000
0xffffe00063171900 explorer.exe     3472   3960   39        0    1    0 2020-09-19 04:36:03 UTC+0000
0xffffe00060ce2080 ServerManager    400    1904   10        0    1    0 2020-09-19 04:36:03 UTC+0000
```

## 12. Did someone move it?

**Yes, from the Administrator's Downloads folder to C:\Windows\System32.**

File movement is tracked through filesystem changes and timestamps.

## 13. What were the capabilities of this malware?

**The malware is capable of process migration, credential theft, keylogging, screen scraping, and many other functionalities.**

Analysis of the malware sample using reverse engineering tools and documentation review.

## 14. Is this malware easily obtained?

**Yes, the harmful program was found in the Administrator's Download area in C:\Windows\System32, which is very important.**

## 15. Was this malware installed with persistence on any machine?

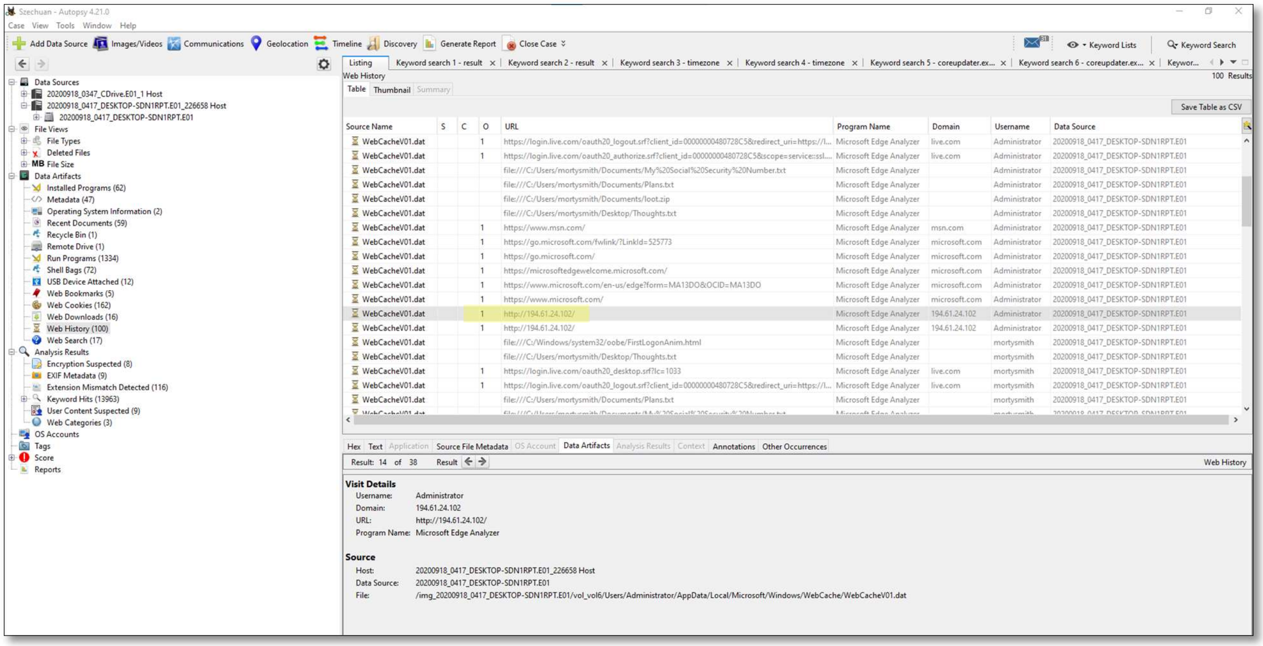
**Yes, both in the registry and as a service.**
Persistence mechanisms were identified during registry and services analysis.

## 16. What malicious IP Addresses were involved?

**194.61.24.102 and 203.78.103.109**
Network traffic analysis and cross-referencing with threat intelligence sources.

## 17. Were any IP Addresses from known adversary infrastructure?

**Yes, 194.61.24.102 was tracked as a hostile IP involved in RDP Brute Force attacks. 203.78.103.109 was linked to happydoghappycat-th.com, suspected in APT activities.**
Checked against threat intelligence databases.



Web History

100 Results

| Source Name | S | C | O | URL | Program Name | Domain | Username | Data Source |
|---|---|---|---|---|---|---|---|---|
| WebCacheV01.dat | | | 1 | https://login.live.com/oauth20_logout.srf?client_id=0000000480728C5&redirect_uri=https://l... | Microsoft Edge Analyzer | live.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://login.live.com/oauth20_authorize.srf?client_id=0000000480728C5&scope=service::ssl.... | Microsoft Edge Analyzer | live.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Documents/My%20Social%20Security%20Number.txt | Microsoft Edge Analyzer | | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Documents/Plans.txt | Microsoft Edge Analyzer | | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Documents/loot.zip | Microsoft Edge Analyzer | | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Desktop/Thoughts.txt | Microsoft Edge Analyzer | | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://www.msn.com/ | Microsoft Edge Analyzer | msn.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://go.microsoft.com/fwlink/?LinkId=525773 | Microsoft Edge Analyzer | microsoft.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://go.microsoft.com/ | Microsoft Edge Analyzer | microsoft.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://microsoftedgewelcome.microsoft.com/ | Microsoft Edge Analyzer | microsoft.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://www.microsoft.com/en-us/edge?form=MA13DO&OCID=MA13DO | Microsoft Edge Analyzer | microsoft.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://www.microsoft.com/ | Microsoft Edge Analyzer | microsoft.com | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | http://194.61.24.102/ | Microsoft Edge Analyzer | 194.61.24.102 | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | http://194.61.24.102/ | Microsoft Edge Analyzer | 194.61.24.102 | Administrator | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | | file:///C:/Windows/system32/oobe/FirstLogonAnim.html | Microsoft Edge Analyzer | | mortysmith | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Desktop/Thoughts.txt | Microsoft Edge Analyzer | | mortysmith | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://login.live.com/oauth20_desktop.srf?lc=1033 | Microsoft Edge Analyzer | live.com | mortysmith | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | 1 | https://login.live.com/oauth20_logout.srf?client_id=0000000480728C5&redirect_uri=https://l... | Microsoft Edge Analyzer | live.com | mortysmith | 20200918_0417_DESKTOP-SDN1RPT.E01 |
| WebCacheV01.dat | | | | file:///C:/Users/mortysmith/Documents/Plans.txt | Microsoft Edge Analyzer | | mortysmith | 20200918_0417_DESKTOP-SDN1RPT.E01 |

Result: 14 of 38 Result

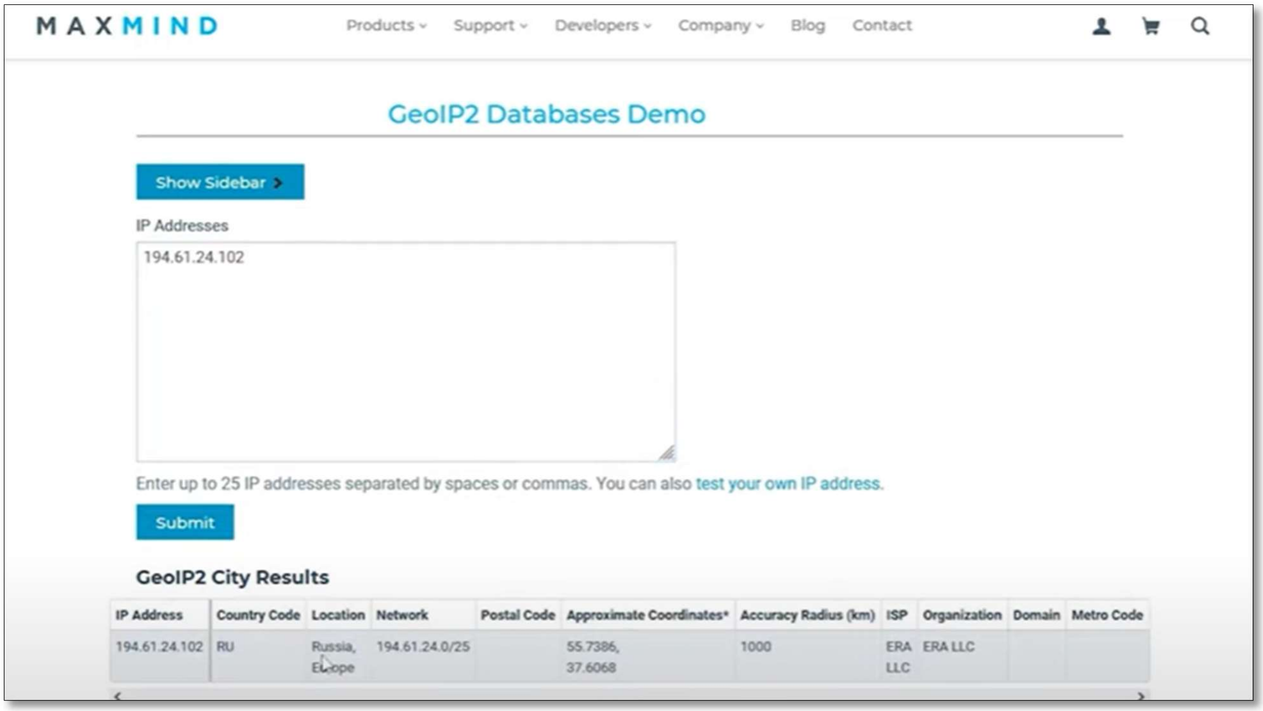
Web History

**Visit Details**

Username: Administrator
Domain: 194.61.24.102
URL: http://194.61.24.102/
Program Name: Microsoft Edge Analyzer

**Source**

Host: 20200918_0417_DESKTOP-SDN1RPT.E01_226658 Host
Data Source: 20200918_0417_DESKTOP-SDN1RPT.E01
File: /img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6/Users/Administrator/AppData/Local/Microsoft/Windows/WebCache/WebCacheV01.dat



GeoIP2 Databases Demo

IP Addresses

194.61.24.102

Enter up to 25 IP addresses separated by spaces or commas. You can also test your own IP address.

GeoIP2 City Results

| IP Address | Country Code | Location | Network | Postal Code | Approximate Coordinates* | Accuracy Radius (km) | ISP | Organization | Domain | Metro Code |
|---|---|---|---|---|---|---|---|---|---|---|
| 194.61.24.102 | RU | Russia, Europe | 194.61.24.0/25 | | 55.7386, 37.6068 | 1000 | ERA LLC | ERA LLC | | |

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

**Yes**

Correlated with incident reports and threat intelligence feeds.

## 19. Did the attacker access any other systems?

**Yes, the Desktop machine, Desktop-SDN1RPT.**

Traced RDP sessions from the Domain Controller to the Desktop machine.

**Brute Forced the password for the Administrator account on the DC, then used RDP to access the Desktop machine—analysis of login attempts and RDP session logs.**

## 20. Did the attacker steal or access any data?

**Yes**

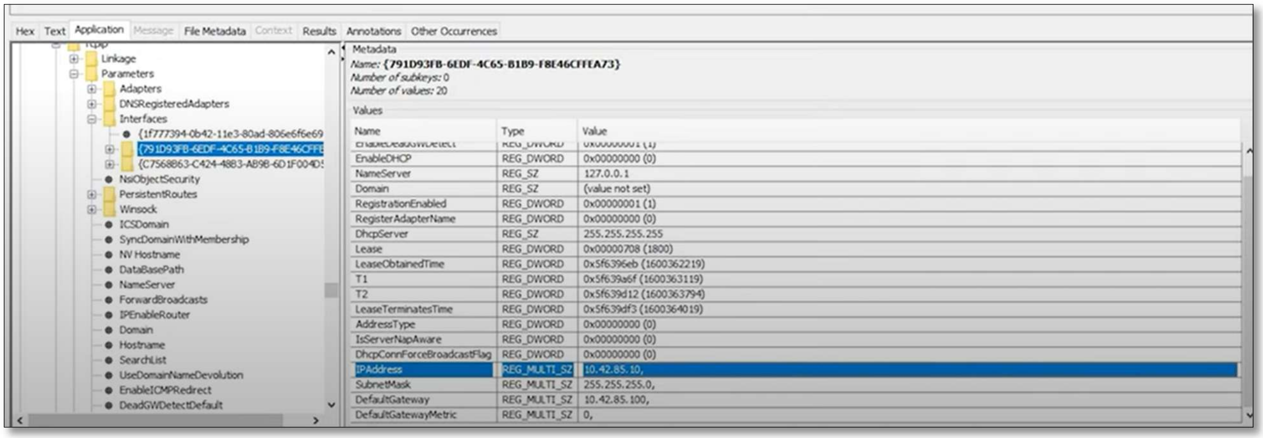
Examination of file access logs and data exfiltration evidence.

Secret.zip was exfiltrated at 02:31; loot.zip was exfiltrated at 02:48.

Detailed timeline and file transfer logs analysis.

## 21. What was the network layout of the victim network?

**Two hosts in 10.42.85.0/24. DC: 10.42.85.10; User: 10.42.85.115**



Metadata
*Name:* **{791D93FB-6EDF-4C65-B1B9-F8E46CFFEA73}**
*Number of subkeys:* 0
*Number of values:* 20

Values

| Name | Type | Value |
|---|---|---|
| EnableDeadGWDetect | REG_DWORD | 0x00000001 (1) |
| EnableDHCP | REG_DWORD | 0x00000000 (0) |
| NameServer | REG_SZ | 127.0.0.1 |
| Domain | REG_SZ | (value not set) |
| RegistrationEnabled | REG_DWORD | 0x00000001 (1) |
| RegisterAdapterName | REG_DWORD | 0x00000000 (0) |
| DhcpServer | REG_SZ | 255.255.255.255 |
| Lease | REG_DWORD | 0x00000708 (1800) |
| LeaseObtainedTime | REG_DWORD | 0x5f6396eb (1600362219) |
| T1 | REG_DWORD | 0x5f639a6f (1600363119) |
| T2 | REG_DWORD | 0x5f639d12 (1600363794) |
| LeaseTerminatesTime | REG_DWORD | 0x5f639df3 (1600364019) |
| AddressType | REG_DWORD | 0x00000000 (0) |
| IsServerNapAware | REG_DWORD | 0x00000000 (0) |
| DhcpConnForceBroadcastFlag | REG_DWORD | 0x00000000 (0) |
| IPAddress | REG_MULTI_SZ | 10.42.85.10, |
| SubnetMask | REG_MULTI_SZ | 255.255.255.0, |
| DefaultGateway | REG_MULTI_SZ | 10.42.85.100, |
| DefaultGatewayMetric | REG_MULTI_SZ | 0, |

*Figure 3by (The Jesters Castle, 2021)*

# Conclusion

We have responded to the critical questions that have been raised to complete this forensic study. Through forensic analysis and the use of various tools, we identified and documented the details of the breach, including the entry vector, malware used, and actions taken by the attacker.

# References

AlzetteInfoSec. (2024, March 28). *STREAM 2022-01-31 [BLUE TEAM] DFIR Madness Case 001 The Stolen Szechuan Sauce PCAP* [Video]. YouTube. https://www.youtube.com/watch?v=REHaqLwWYG8

*chatgpt*. (2024, July 1). Chatgpt.

*https://www.scribbr.com/*. (2024, July 1). https://www.scribbr.com/.

John Hammond. (2023, April 21). *Quick forensics of Windows Event Logs (DeepBlueCLI)* [Video]. YouTube. https://www.youtube.com/watch?v=G8XjSO_eshc

Lalwani, T. (2023, August 24). Case of the stolen Szechuan sauce - Tanvi Lalwani - Medium. *Medium*. https://medium.com/@tanvilalwani5/case-of-the-stolen-szechuan-sauce-bd440e5c2a6d

The Jesters Castle. (2021, October 25). *Rick & Morty Digital Forensics: Disk Images* [Video]. YouTube. https://www.youtube.com/watch?v=FYSyxTIXYhI