CASE 001
THE STOLEN SZECHUAN SAUCE

By Andrew Mendis

Table of Contents

Table of Contents

Executive Summary

The following report outlines the results and findings from the Stolen Szechuan Sauce Case. A number of tools were used for the purposes of the investigation. The tools consist of the following; FTKImager, volatility, and Autopsy. The investigation found evidence of a breach which was done through an RDP brute force attack. After the successful breach a payload was created using metasploit and subsequently deployed and executed onto the system. An administrator account was compromised, a number of files were exfiltrated, and persistence was established on the computer. The malware is capable of many functions which will be detailed in the report below. The report will outline the many vulnerabilities in the organization which lead to this breach, a timeline of the events, and recommend changes to prevent further breaches from happening.

Methodology

Evidence & Data

Disk Images

DC01-E01.zip - Disk image of “CITADEL-DC01” the domain controller.

DESKTOP-E01.zip - Disk image of “DESKTOP-SDN1RPT” the workstation computer.

Memory Captures

DC01-memory.zip - Memory Capture for the domain controller “CITADEL-DC01”

DESKTOP-SDN1RPT-memory.zip - Memory Capture for the domain controller “DESKTOP-SDN1RPT”

Files

SOFTWARE_Clean - Software hive for the two systems. Has a separate file with the same name for each in different directories.

SYSTEM_clean - Software hive for the two systems. Has a separate file with the same name for each in different directories.

Security.evtx - Security events log file for the two systems. Has a separate file with the same name for each in different directories.

System.evtx - System events log file for the two systems. Has a separate file with the same name for each in different directories.

WebCache.dat - File containing the cached items from Internet Explorer and Microsoft Edge. Has information regarding web history and file downloads. Has a separate file with the same name for each in different directories.

$UsnJrnl:$J - Log file for file activity. Shows a history of when files were accessed, modified, created, and deleted. Important for creating a timeline of file activity when

advanced logging hasn't been enabled on a system. Has a separate file with the same name for each in different directories.

Tools & Programs

Access Data FTK Imager

FTK Imager provides the mounting and access of the Disk Images. Through the imager I'll be able to gain access to valuable artifacts such as registry hives, and documents with ease.

Autopsy

Autopsy is a powerful and useful tool which scans and indexes the files in the Disk Images from our evidence. Once the scan is finished it will provide hashes of the individual files and detail things such as creation time, last access time, modified times, and many more properties. This will help give a high level overview of events and aid in creating a timeline of the events that took place in the systems and network. Having this kind of insight will help understand how the breach happened and gain insight to subsequently fix the vulnerabilities.

IE10Analyzer

This tool allows us to analyze the WebCache file for Internet Explorer and Microsoft Edge. giving us insight into the history of webpages visited and files downloaded.

MFTEcmd

Allows the conversion of the UsnJrnl file into a CSV table making it more readable.

PowerShell

Powershell allows us to download Eric Zimmerman's tools, and hash evidence to verify their integrity against the given hash list.

Registry Explorer

Registry Hives will be opened here for investigation. The program helps us view contents in the registry to gather valuable insight into what happened to the systems. It provides a user-friendly

interface to explore the values in the hives, helping to extract information and correlate it towards the accuracy of the timeline of events that happened.

VirusTotal

VirusTotal will provide a comprehensive cross-analysis between antivirus/antimalware providers to check the reputation of a file or its hash.

Volatility

Volatility provides analysis of memory captures. It's another powerful tool that gives us insight into what processes were running and what open connections they had. The tool will also allow us to extract running programs and analyze them with other tools.

Verifying Integrity of Evidence

Before starting work on the case, the initial step is to verify the integrity of the evidence. The client had provided MD5 hashes for the evidence which was used as reference to validate the integrity of the files once copies were received. Below are the MD5 values that were hashed post intake.

Server Disk Image

Client Provided Hash ↴

```
MD5 E57FC636E833C5F1AB58DFACE873BBDE    DC01-E01.zip
```

Locally Produced Hash ↴

```
PS C:\Users\Aeschylus> Get-FileHash X:\Downloads\browser\DC01-E01.zip -Algorithm md5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             E57FC636E833C5F1AB58DFACE873BBDE                                       X:\Downloads\browser\DC01-E01.zip
```

Server Memory Capture

Client Provided Hash ↴

Y

```
MD5 64A4E2CB47138084A5C2878066B2D7B1   DC01-memory.zip
```

Locally Produced Hash ↴

```
PS C:\Users\Aeschylus> Get-FileHash X:\Downloads\browser\DC01-memory.zip -Algorithm md5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             64A4E2CB47138084A5C2878066B2D7B1                                       X:\Downloads\browser\DC01-memor...
```

Workstation Disk Image

Client Provided Hash ↴

```
MD5 71C5C3509331F472ABCDF81EB6EFFF07   DESKTOP-E01.zip
```

Locally Produced Hash ↴

```
PS C:\Users\Aeschylus> Get-FileHash X:\Downloads\browser\DESKTOP-E01.zip -Algorithm md5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             71C5C3509331F472ABCDF81EB6EFFF07                                       X:\Downloads\browser\DESKTOP-E...
```

Workstation Memory Capture

Client Provided Hash ↴

```
MD5 CF31E2635C77811AAA1BB04A92A721E2   DESKTOP-SDN1RPT-memory.zip
```

Locally Produced Hash ↴

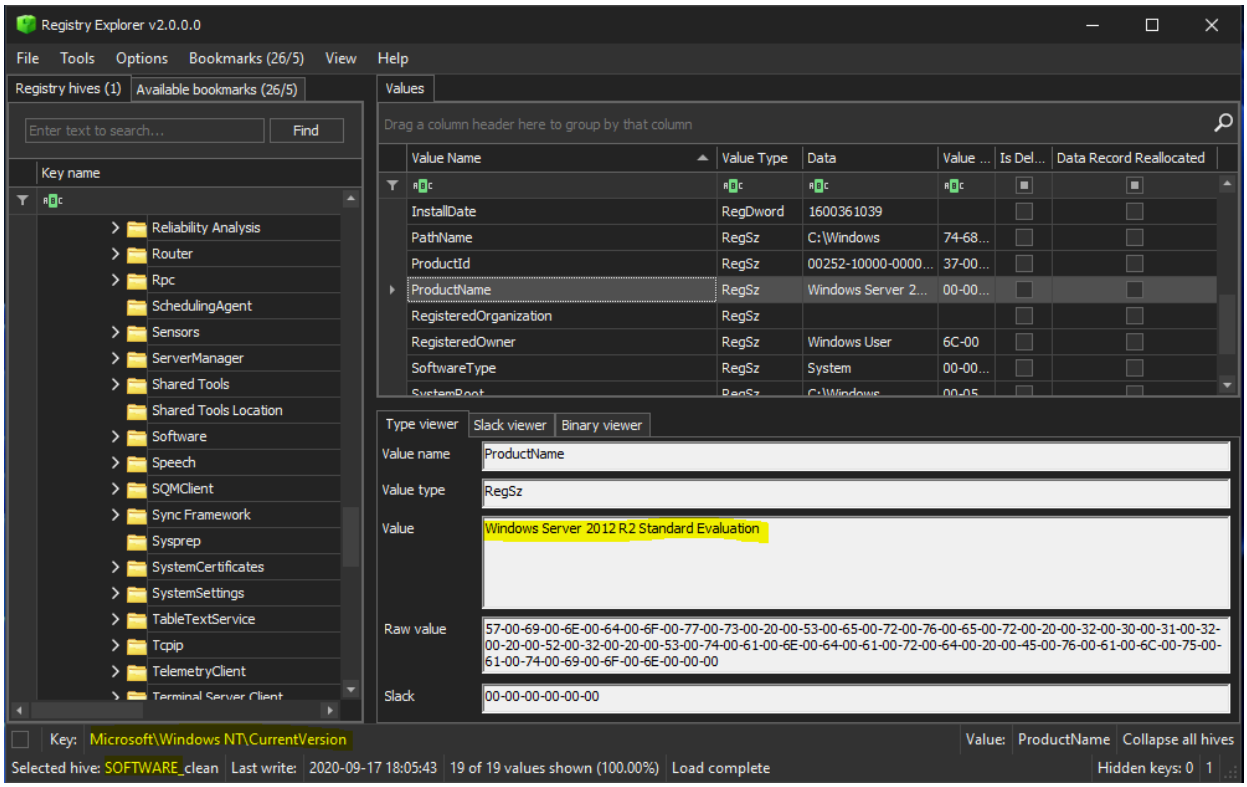
```
PS C:\Users\Aeschylus> Get-FileHash X:\Downloads\browser\DESKTOP-SDN1RPT-memory.zip -Algorithm md5

Algorithm       Hash                                                                   Path
---------       ----                                                                   ----
MD5             CF31E2635C77811AAA1BB04A92A721E2                                       X:\Downloads\browser\DESKTOP-SD...
```

Investigation

Q1: What's the Operating System of the Server?

A1: Windows Server 2012 R2 Standard Evaluation

Using FTK Imager we can first mount the image of the server to view the SOFTWARE registry hive. Once mounted, we navigate to HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion where the data for the ProductName value tells us what OS the server is running.

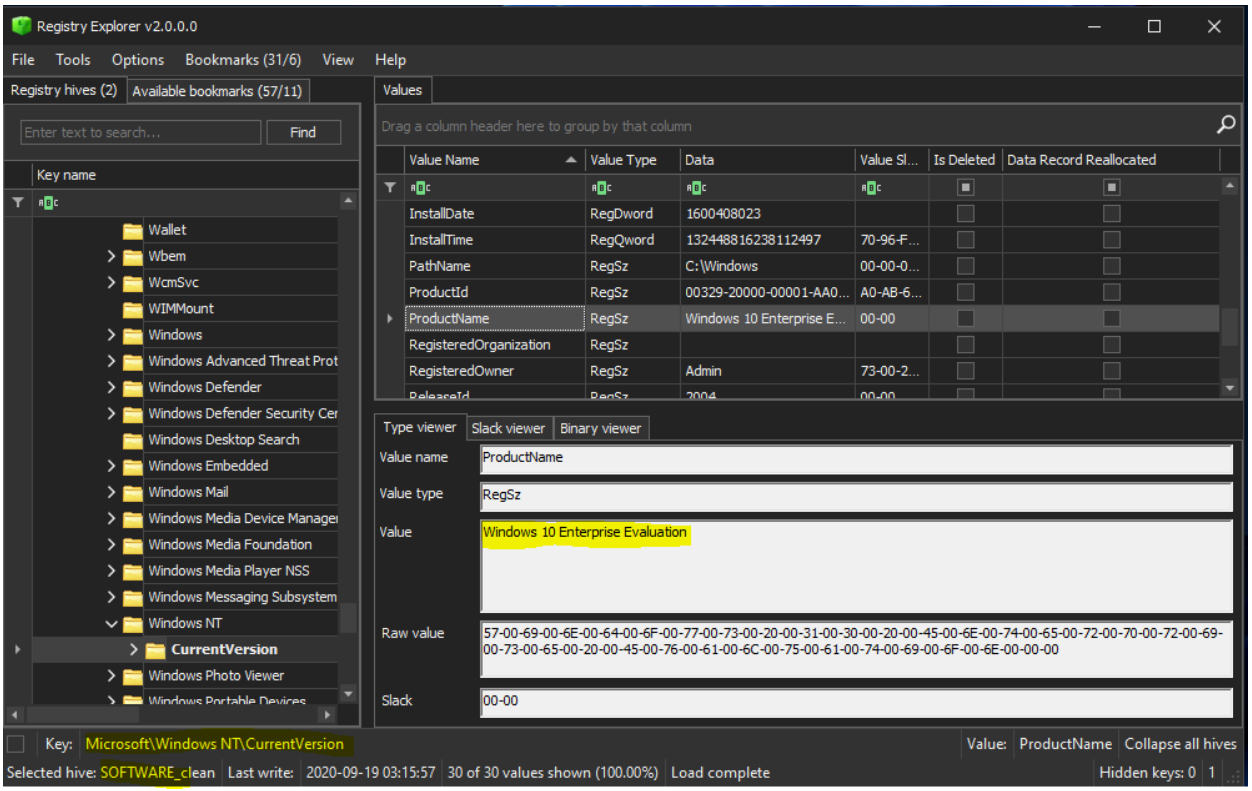


Q2: What's the Operating System of the Desktop?

A2: Windows 10 Enterprise Evaluation

Using FTK Imager we can first mount the image of the desktop to retrieve the SOFTWARE registry hive. Once that's done, we navigate to HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion where the data for the ProductName value tells us what OS the desktop is running.

1



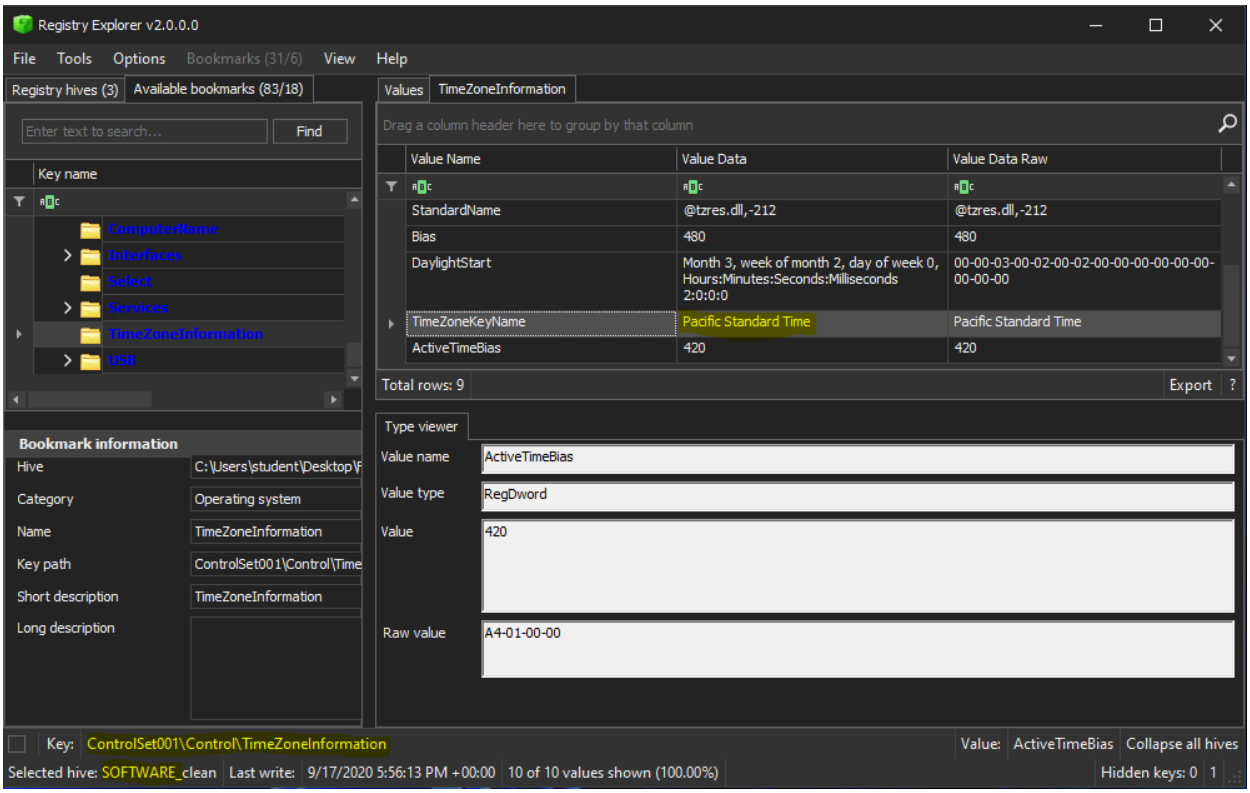
Q3: What was the local time of the Server?

A3: Pacific Standard Time

Like with the previous questions we use FTK Imager to first mount the image of the server. Afterwards we retrieve the SOFTWARE registry hive. Once that's done, we navigate to

HKLM\SOFTWARE\ControlSet001\Control\TimeZoneInformation where the data for the TimeZoneKeyName value tells us what the local time zone is on the server.

1



Q4: Was there a breach?

A4: Yes

Q5: What was the initial entry vector (how did they get in)?

A5: Bruteforce Attack via RDP

Looking through the security logs we can see that there were multiple failed login attempts originating from a computer called ‘kali’. All trying to attempt to login via a network type connection (Logon Type 3) using the account ‘Administrator’. After many failed attempts they login

successfully using either Terminal Services or an RDP Connection (Logon Type 10) originating from '194.61.24.102'. The first picture below shows the repeated attempts to login via the **Administrator** account. The first entry is a false positive. It was normal user behaviour, as they logged in with correct credentials after the one bad attempt. The brute force attack started at 20:21:25 PST on 18/09/2020, and after 96 attempts they were able to successfully login at 20:21:48 PM PST.

1

Level	Date and Time	Event ID	Source	Task Category
Information	18/09/2020 12:13:43 AM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:25 PM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:25 PM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:26 PM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:26 PM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:26 PM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:26 PM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:27 PM	4625	Microsoft Windows security auditing.	Logon
Information	18/09/2020 11:21:27 PM	4625	Microsoft Windows security auditing.	Logon

2

An account failed to log on.

Subject:
- Security ID: NULL SID
- Account Name: -
- Account Domain: -
- Logon ID: 0x0

Logon Type: 3

Account For Which Logon Failed:
- Security ID: NULL SID
- Account Name: Administrator
- Account Domain:

Failure Information:
- Failure Reason: Unknown user name or bad password.
- Status: 0xC000006D
- Sub Status: 0xC000006A

Process Information:
- Caller Process ID: 0x0
- Caller Process Name: -

Network Information:
- Workstation Name: kali
- Source Network Address: -
- Source Port: -

Detailed Authentication Information:
- Logon Process: NtLmSsp
- Authentication Package: NTLM
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

An account was successfully logged on.

Subject:
- Security ID: SYSTEM
- Account Name: CITADEL-DC01$
- Account Domain: C137
- Logon ID: 0x3E7

Logon Type: 10

Impersonation Level: Impersonation

New Logon:
- Security ID: S-1-5-21-2232410529-1445159330-2725690660-500
- Account Name: Administrator
- Account Domain: C137
- Logon ID: 0x510986
- Logon GUID: {71334fab-9dc8-3b83-5cf0-7392d7ef15f2}

Process Information:
- Process ID: 0x4c4
- Process Name: C:\Windows\System32\winlogon.exe

Network Information:
- Workstation Name: CITADEL-DC01
- Source Network Address: 194.61.24.102
- Source Port: 0

Detailed Authentication Information:
- Logon Process: User32
- Authentication Package: Negotiate
- Transited Services: -
- Package Name (NTLM only): -
- Key Length: 0

Q6.1: Was malware used? If so, what was it? Yes coreupdater.exe

A6.1: What process was malicious?

Using the PsList module in **Volatility** “coreupdater.exe* was found *(Table #1)*. It didn’t seem like a normal windows process or service. Using the “cmdline” module *(Table #2)* in volatility, a check was made to see if it was recently executed and if so what program or process executed it. Not much information was provided other than that it could have been executed from a directory that’s part of the PATH system variable. Afterwards a process dump was run against the PID of the process to get the executable *(Table #3)* to run further analysis. The hash was submitted to Virus total and returned with an 87% positive result *(Table #4)*.

1

```
PS C:\Users\student\Desktop\VolatilityWorkbench> .\vol.exe -f .\citadeldc01.mem windows.pslist.PsList
Volatility 3 Framework 2.7.0
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
324     316     csrss.exe       0xe000602c2080  8       -       0       False   2020-09-19 01:22:39.000000
404     316     wininit.exe     0xe000602cc900  1       -       0       False   2020-09-19 01:22:40.000000
412     396     csrss.exe       0xe000602c1900  10      -       1       False   2020-09-19 01:22:40.000000
452     404     services.exe    0xe00060c11080  5       -       0       False   2020-09-19 01:22:40.000000
460     404     lsass.exe       0xe00060c0e080  31      -       0       False   2020-09-19 01:22:40.000000
492     396     winlogon.exe    0xe00060c2a080  4       -       1       False   2020-09-19 01:22:40.000000
640     452     svchost.exe     0xe00060c84900  8       -       0       False   2020-09-19 01:22:40.000000
684     452     svchost.exe     0xe00060c9a700  6       -       0       False   2020-09-19 01:22:40.000000
800     452     svchost.exe     0xe00060ca3900  12      -       0       False   2020-09-19 01:22:40.000000
808     492     dwm.exe 0xe00060d09680  7       -       1       False   2020-09-19 01:22:40.000000      N/A
848     452     svchost.exe     0xe00060d1e080  39      -       0       False   2020-09-19 01:22:41.000000
928     452     svchost.exe     0xe00060d5d500  16      -       0       False   2020-09-19 01:22:41.000000
1000    452     svchost.exe     0xe00060da2080  18      -       0       False   2020-09-19 01:22:41.000000
668     452     svchost.exe     0xe00060e09900  16      -       0       False   2020-09-19 01:22:41.000000
1292    452     Microsoft.Acti  0xe00060f73900  9       -       0       False   2020-09-19 01:22:57.000000
1332    452     dfsrs.exe       0xe00060fe1900  16      -       0       False   2020-09-19 01:22:57.000000
1368    452     dns.exe 0xe00060ff3080  16      -       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
1556    452     VGAuthService.  0xe000614aa200  2       -       0       False   2020-09-19 01:22:57.000000
1600    452     vmtoolsd.exe    0xe00061a30900  9       -       0       False   2020-09-19 01:22:57.000000
1644    452     wlms.exe        0xe00061a9a800  2       -       0       False   2020-09-19 01:22:57.000000
1660    452     dfssvc.exe      0xe00061a9b2c0  11      -       0       False   2020-09-19 01:22:57.000000
1956    452     svchost.exe     0xe0006291b7c0  30      -       0       False   2020-09-19 01:23:20.000000
796     452     vds.exe 0xe000629b3080  11      -       0       False   2020-09-19 01:23:20.000000      N/A
1236    452     svchost.exe     0xe000629926c0  8       -       0       False   2020-09-19 01:23:21.000000
2056    640     WmiPrvSE.exe    0xe000629de900  11      -       0       False   2020-09-19 01:23:21.000000
2216    452     dllhost.exe     0xe00062a26900  10      -       0       False   2020-09-19 01:23:21.000000
2460    452     msdtc.exe       0xe00062a2a900  9       -       0       False   2020-09-19 01:23:21.000000
3724    452     spoolsv.exe     0xe000631cb900  13      -       0       False   2020-09-19 03:29:40.000000
3644    2244    coreupdater.ex  0xe00062fe7700  0       -       2       False   2020-09-19 03:56:37.000000
3796    848     taskhostex.exe  0xe00062f04900  7       -       1       False   2020-09-19 04:36:03.000000
3472    3960    explorer.exe    0xe00063171900  39      -       1       False   2020-09-19 04:36:03.000000
400     1904    ServerManager.  0xe00060ce2080  10      -       1       False   2020-09-19 04:36:03.000000
3260    3472    vm3dservice.ex  0xe00063299280  1       -       1       False   2020-09-19 04:36:14.000000
2608    3472    vmtoolsd.exe    0xe00062ede1c0  8       -       1       False   2020-09-19 04:36:14.000000
2840    3472    FTK Imager.exe  0xe00063021900  9       -       1       False   2020-09-19 04:37:04.000000
3056    848     WMIADAP.exe     0xe0006313f900  5       -       0       False   2020-09-19 04:37:42.000000
2764    640     WmiPrvSE.exe    0xe00062c0a900  6       -       0       False   2020-09-19 04:37:42.000000
```

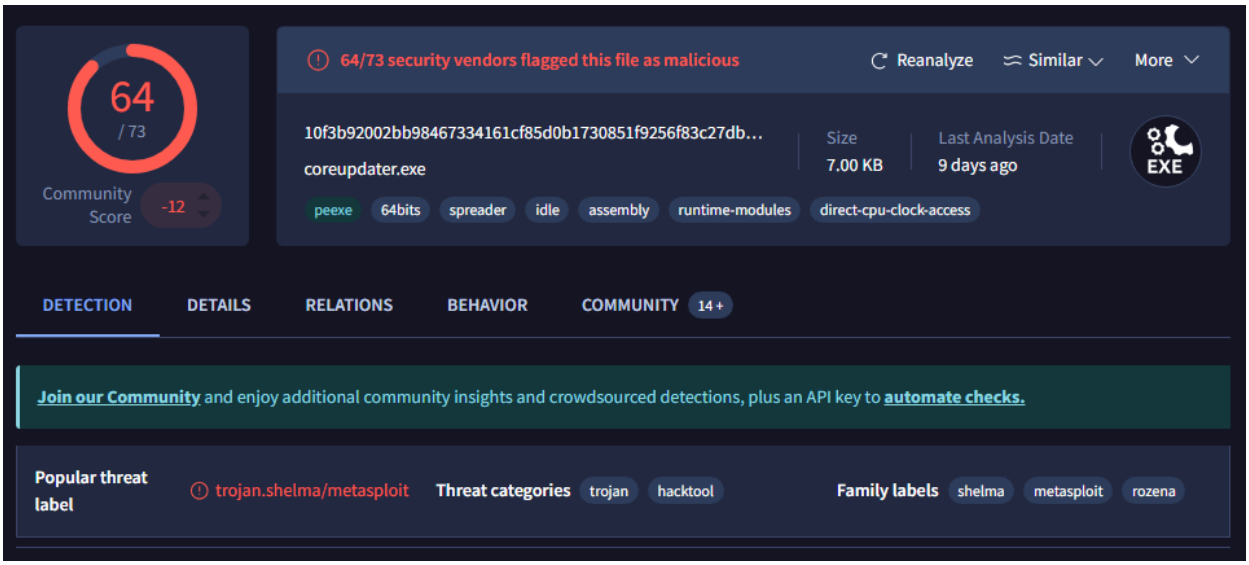
2

```
dllhost.exe pid:   2216
Command line : C:\Windows\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}
**********************************************************************
msdtc.exe pid:   2460
Command line : C:\Windows\System32\msdtc.exe
**********************************************************************
spoolsv.exe pid:   3724
Command line : C:\Windows\System32\spoolsv.exe
**********************************************************************
coreupdater.ex pid:   3644
**********************************************************************
taskhostex.exe pid:   3796
Command line : taskhostex.exe
**********************************************************************
explorer.exe pid:   3472
Command line : C:\Windows\Explorer.EXE
**********************************************************************
```

3

```
PS C:\Users\student\Downloads\vol3\volatility3> python vol.py -f .\citadeldc01.mem windows.dumpfiles --pid 3644
Volatility 3 Framework 2.11.0
Progress:  100.00               PDB scanning finished
Cache   FileObject      FileName        Result
```

4



Q6.2: Identify the IP Address that delivered the payload.

A6.2: 194.61.24.102

We can make a good assumption that the source of the file was from the same IP (194.61.24.102) as the source of the RDP connection from Q4.1. We know from the VirusTotal results that the payload was created using metasploit, and the source machine's hostname is kali. Kali is known for penetration testing and usually comes with metasploit pre-installed.

1	An account was successfully logged on. Subject: Security ID: SYSTEM Account Name: CITADEL-DC01$ Account Domain: C137 Logon ID: 0x3E7 Logon Type: 10 Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2232410529-1445159330-2725690660-500 Account Name: Administrator Account Domain: C137 Logon ID: 0x510986 Logon GUID: {71334fab-9dc8-3b83-5cf0-7392d7ef15f2} Process Information: Process ID: 0x4c4 Process Name: C:\Windows\System32\winlogon.exe Network Information: Workstation Name: CITADEL-DC01 Source Network Address: 194.61.24.102 Source Port: 0 Detailed Authentication Information: Logon Process: User32 Authentication Package: Negotiate Transited Services: - Package Name (NTLM only): - Key Length: 0

CITADEL-DC01

Q6.3: What IP Address is the malware calling to?

A6.3: 203.78.103.109

Further analysis revealed that the malware has an open socket. Using the NetStat module in volatility, it showed the following result *(Table #1)*. The malware seems to be active and communicating with the foreign address “203.78.103.109”. The virus total results *(Table #3)* show that the IP address has a history of communications involving the “coreupdater.exe” executable. It also has other IP addresses associated that also have a history of malware *(Table #3)*.

1

```
PS C:\Users\student\Desktop\volatility3> python vol.py -f .\citadeldc01.mem windows.netstat
Volatility 3 Framework 2.11.0
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
0xe00062a31270  TCPv6   fe80::2dcf:e660:be73:d220       49182   fe80::2dcf:e660:be73:d220       389     ESTABLISHED
0xe0006103c4f0  TCPv6   fe80::2dcf:e660:be73:d220       49174   fe80::2dcf:e660:be73:d220       49155   ESTABLISHED
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
```

1

Categories

alphaMountain.ai	Malicious (alphaMountain.ai)

History

First Submission	2020-09-04 01:31:13 UTC
Last Submission	2024-09-22 03:50:04 UTC
Last Analysis	2024-09-22 03:50:04 UTC

HTTP Response

Final URL

http://203.78.103.109/

Communicating Files (12)

Scanned	Detections	Type	Name
2024-11-01	65 / 72	Win32 EXE	coreupdater.exe
2024-04-11	30 / 58	Powershell	test.ps1
2023-12-18	25 / 59	Text	testps1.ps1
2024-04-10	26 / 60	Text	decode.ps1
2021-09-09	19 / 58	unknown	file2
2024-07-19	31 / 64	Powershell	function pLBA {.txt
2021-10-07	30 / 58	Powershell	steg2.txt
2023-03-06	27 / 59	JavaScript	2.ps1
2023-03-06	27 / 59	Powershell	script.ps1
2023-12-14	55 / 72	Win32 EXE	file.None.0xffffe00062b10010.img

2

IP Traffic

- TCP 203.78.103.109:443
- UDP 192.168.0.34:137
- TCP 20.99.132.105:443
- TCP 23.216.147.76:443
- TCP 20.99.133.109:443
- UDP a83f:8110:0:0:b89d:2800:0:0:53
- TCP 192.229.211.108:80
- UDP a83f:8110:0:0:1400:1400:2800:3800:53
- TCP 20.96.52.198:443
- TCP 20.99.184.37:443
- UDP a83f:8110:0:0:100:0:1800:0:53
- UDP 192.168.0.30:137
- UDP a83f:8110:1800:0:0:0:0:200:53
- UDP a83f:8110:8b8e:e001:0:ff15:c0bc:200:53
- UDP a83f:8110:3500:6400:3000:6600:3900:3500:53
- UDP 192.168.0.38:137
- TCP 23.216.81.152:80 (www.microsoft.com)
- TCP 20.99.186.246:443
- TCP 23.64.157.53:443
- TCP 20.99.185.48:443
- UDP 192.168.0.54:137
- UDP 192.168.0.8:137
- UDP a83f:8110:84cd:ffff:3003:d471:84cd:ffff:53
- TCP 104.71.214.69:80 (www.microsoft.com)
- UDP 192.168.0.23:137
- UDP a83f:8110:0:0:1400:0:0:0:53
- TCP 52.185.73.156:443

Q6.4: Where is this malware on disk?

A6.4: System32 folder

Running the PsTree module shows that it was executed from the System32 directory.

1

```
PS C:\Users\student\Desktop\VolatilityWorkbench> .\vol.exe -f .\citadeldc01.mem windows.pstree.PsTree | findstr -i coreupdater.exe
3644ress224400.0coreupdater.ex  0xe00062fe7700in0shed  -       2       False   2020-09-19 03:56:37.000000      2020-09-19 03:56:52.000000      \Device\HarddiskVolume2\Windows\System32\coreupdater.exe
```

↘ ↙

```
\Device\HarddiskVolume2\Windows\System32\coreupdater.exe
```

Q6.5: When did it first appear?

A6.5: It first appeared at 20:24:12 PST on the system

By analyzing the WebCache.dat file using IE10Analyzer we can conclude that the file was first downloaded to the Administrator's Downloads folder at 20:24:12 PST.

1

History(M)_Recovered | iecompatua(M)_Recovered | MSHist012020091820200919(M)_... | iecompat(M)_Recovered | **iedownload(M)**

	EntryId	AccessedTime	DownloadPath
☐	1	2020-09-19 08:24:12	http://194.61.24.102/application/x-msdos-programC:\Users\Administrator\AppData\Local\Microsoft\Windows\INetCache\IE\CLE9U4I5\coreupdater[1].exehttp://194.61.24.102/coreupdater.exeC:\Users\Administrator\Downloads\coreupdater.exe

↘ ↙

ter.exeC:\Users\Administrator\Downloads\coreupdater.exe

Q6.6: Did someone move it?

A6.6: Yes, to C:\Windows\System32\

Using Autopsy we can confirm its only current location on the system by doing a search and asking to view the file in its source.

1

Listing | Keyword search 2 - coreupdater.ex... | Keyword search 3 - pacific | Keyword search 4 - f60163ce-2b8d-...

/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32 — 3368 Results

Table | Thumbnail | Summary

Save Table as CSV

Name	S	C	O	...	Change Time	Access Time	Created Time	Size	Flags(Dir)	F
convert.exe			1	...	2020-09-17 12:48:36 EDT	2013-08-22 07:32:40 EDT	2013-08-22 07:32:40 EDT	19968	Allocated	A
CoreMmRes.dll			1	...	2020-09-17 12:50:03 EDT	2013-08-22 07:45:04 EDT	2013-08-22 07:45:04 EDT	15360	Allocated	A
coreupdater.exe	!		1	...	2020-09-18 23:24:50 EDT	2020-09-18 23:24:12 EDT	2020-09-18 23:24:12 EDT	7168	Allocated	A
correngine.dll			1	...	2020-09-17 12:48:36 EDT	2013-08-22 07:00:26 EDT	2013-08-22 07:00:26 EDT	82432	Allocated	A
CredentialUIBroker.exe			1	...	2020-09-17 12:48:36 EDT	2013-08-22 07:16:45 EDT	2013-08-22 07:16:45 EDT	37264	Allocated	A
credssp.dll			1	...	2020-09-17 12:48:36 EDT	2013-08-22 06:01:38 EDT	2013-08-22 06:01:38 EDT	21504	Allocated	A

Q6.7: What were the capabilities of this malware?

A6.7: Many

The malware is a metasploit payload. Depending on how the module/payload was created it can have a number of capabilities. Below in *(Table #1)* you'll find some of its detected techniques and capabilities from Falcon Sandbox analysis on Hybrid Analysis' website. From the results shown we can assume it has the following capabilities; Persistence, Privilege Escalation, Credential Access, Discovery, and Command and Control. These are just the known and detected features of the payload. There could be more that the sandbox/software did not have a chance to detect due to test duration.

1

MITRE ATT&CK™ Techniques Detection

Persistence

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1179	Hooking	• Persistence • Privilege Escalation • Credential Access	Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Learn more		• Installs hooks/patches the running process	

Privilege Escalation

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1179	Hooking	• Persistence • Privilege Escalation • Credential Access	Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Learn more		• Installs hooks/patches the running process	

Credential Access

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1179	Hooking	• Persistence • Privilege Escalation • Credential Access	Windows processes often leverage application programming interface (API) functions to perform tasks that require reusable system resources. Learn more		• Installs hooks/patches the running process	

Discovery

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1046	Network Service Scanning	• Discovery	Adversaries may attempt to get a listing of services running on remote hosts, including those that may be vulnerable to remote software exploitation. Learn more		• Detected increased number of ARP broadcast requests (network device lookup)	
T1016	System Network Configuration Discovery	• Discovery	Adversaries will likely look for details about the network configuration and settings of systems they access or through information discovery of remote systems. Learn more	• Detected a large number of ARP broadcast requests (network device lookup)		
T1012	Query Registry	• Discovery	Adversaries may interact with the Windows Registry to gather information about the system, configuration, and installed software. Learn more		• Monitors specific registry key for changes	

Command and Control

ATT&CK ID	Name	Tactics	Description	Malicious Indicators	Suspicious Indicators	Informative Indicators
T1043	Commonly Used Port	• Command and Control	Adversaries may communicate over a commonly used port to bypass firewalls or network detection systems and to blend with normal network activity to avoid more detailed inspection. Learn more		• Sends traffic on typical HTTP outbound port, but without HTTP header	

Q6.8: Is this malware easily obtained?

A6.8: Yes

Metasploit is a free to use open-source application used by penetration testers and the like. It comes preinstalled on some linux distributions and has comprehensive documentation made for it. It has a large community base and users willing to do a deep dive can be creating and deploying payloads on systems in a short amount of time.

Q6.9: Was this malware installed with persistence on any machine?

A6.9: Yes

A6.9.1 & 6.9.2: When? & Where?

The malware was installed on both machines and set up persistence through registry entries and setting itself up as a service. The service is set to start-up automatically. As shown in *(Table #1)* for the Server & *(Table #2)* for the Workstation the services were installed at 2020-09-18 20:27:49 (20:27:49 PST) for the Server & 2020-09-18 (08:42:42 PST) for the Workstation. The registry keys were also installed at the same time as the services for each respectively as shown in *(Table #3)* for the Server & *(Table #4)* for the Workstation.

1

Name	Description	Display Name	Start Mode	Service Type	Name Key Last Write	Parameters K...	Group	Image Path	Service DLL	Required Privile...
COMSysApp	@comres.dll,-948	@comres.dll,-947	Manual	Win32OwnProc...	2020-09-17 17:56:13			%SystemRoot%\system32\dllhost.exe /Processid:{02D4B3F1-FD88-11D1-960D-00805FC79235}		SeAssignPrimaryTokenPrivilege SeAuditPrivilege SeChangeNotifyPrivilege SeCreateGlobalPrivilege SeDebugPrivilege SeImpersonatePrivilege SeIncreaseQuotaPrivilege
condrv		Console Driver	Manual	KernelDriver	2020-09-17 17:56:13		Base	System32\drivers\condrv.sys		
coreupdater			Automatic	Win32OwnProc...	2020-09-19 03:27:49			C:\Windows\System32\coreupdater.exe		
crypt32			Disabled	Adapter	2020-09-17 17:56:13					
CryptSvc	@%SystemRoot%\system32\cryptsvc.dll,-1002	@%SystemRoot%\system32\cryptsvc.dll,-1001	Automatic	Win32SharePro...	2020-09-17 17:56:13	2020-09-17 1...		%SystemRoot%\system32\svchost.exe -k NetworkService	%SystemRoot%\system32\cryptsvc.dll	SeChangeNotifyPrivilege SeCreateGlobalPrivilege SeImpersonatePrivilege
DCLocator			Disabled	Adapter	2020-09-17 17:56:13					

2

Name	Description	Display Name	Start Mode	Service Type	Name Key Last Write	Parameters K...	Group	Image Path	Service DLL	Required Privileg...
ConsentUxUserSvc_b3e3d7	@%SystemRoot%\system32\ConsentUxClient.dll,-101	ConsentUX_b3e3d7	Manual	224	2020-09-19 05:08:15			C:\Windows\system32\svchost.exe -k DevicesFlow		
CoreMessagingRegistrar	@%SystemRoot%\system32\coremessaging.dll,-2	@%SystemRoot%\system32\coremessaging.dll,-1	Automatic	Win32SharePro...	2019-12-07 09:15:07	2019-12-07 0...		%SystemRoot%\system32\svchost.exe -k LocalServiceNoNetwork -p	%SystemRoot%\system32\coremessaging.dll	
CoreUI			Disabled	Adapter	2019-12-07 09:15:07					
coreupdater			Automatic	Win32OwnProc...	2020-09-19 03:42:42			C:\Windows\System32\coreupdater.exe		
CredentialEnrollmentManagerUserSvc	@%SystemRoot%\system32\CredentialEnrollmentManager.exe,-101	@%SystemRoot%\system32\CredentialEnrollmentManager.exe,-100	Manual	80	2019-12-07 09:15:07			%SystemRoot%\system32\CredentialEnrollmentManager.exe		
CredentialEnrollmentManagerUserSvc_b3e3d7	@%SystemRoot%\system32\CredentialEnrollmentManager.exe,-101	CredentialEnrollmentManagerUserSvc_b3e3d7	Manual	208	2020-09-19 05:08:15			C:\Windows\system32\CredentialEnrollmentManager.exe		

3

System Number of events: 60,189

Filtered: Log: file://X:\documents\lhl\VMShares\Forensics Project\ForensicsProject\Citadel\logs\System.evtx; Source: ; Event ID: 7045. Number of

Level	Date and Time	Source	Event ID	Task Category
Information	17/09/2020 1:51:41 PM	Service Control ...	7045	None
Information	18/09/2020 11:25:44 PM	Service Control ...	7045	None
Information	18/09/2020 11:27:49 PM	Service Control ...	7045	None

Event 7045, Service Control Manager

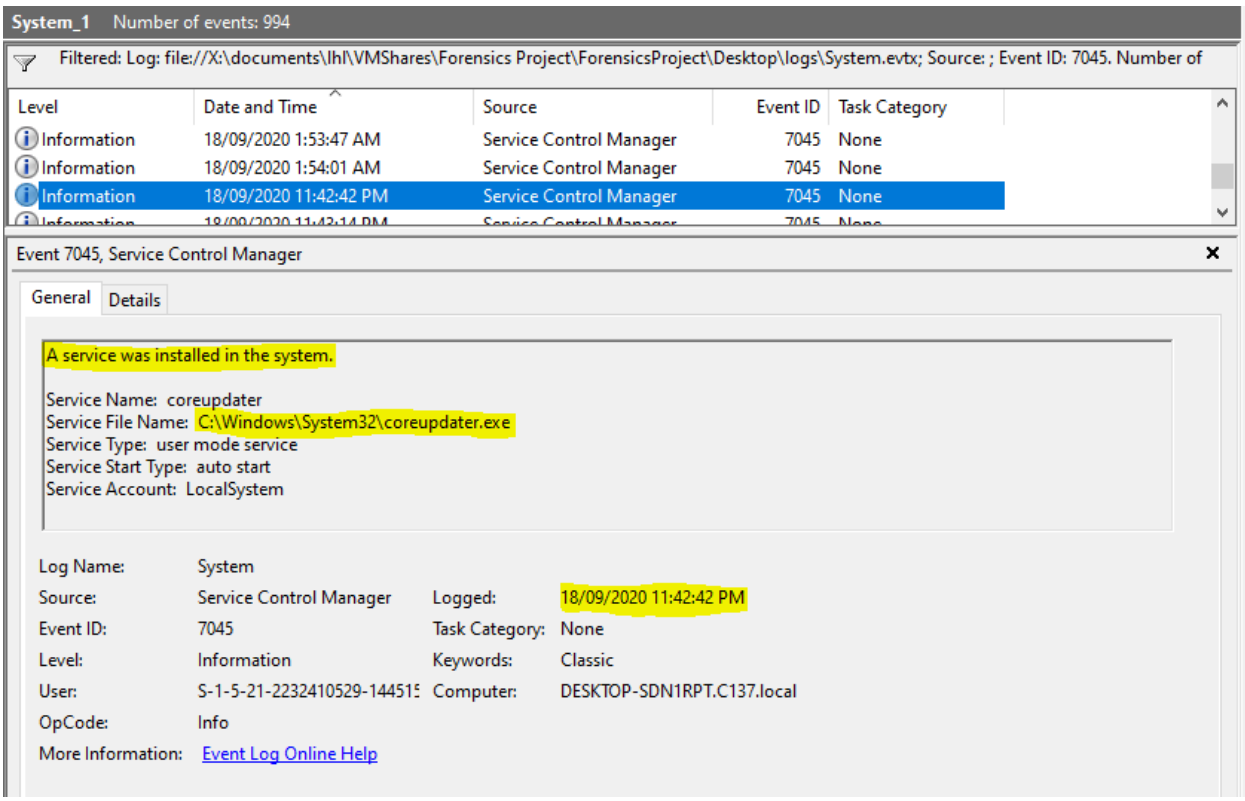
General Details

A service was installed in the system.

Service Name: coreupdater
Service File Name: C:\Windows\System32\coreupdater.exe
Service Type: user mode service
Service Start Type: auto start
Service Account: LocalSystem

Log Name:	System		
Source:	Service Control Manager	Logged:	18/09/2020 11:27:49 PM
Event ID:	7045	Task Category:	None
Level:	Information	Keywords:	Classic
User:	S-1-5-21-2232410529-144515	Computer:	CITADEL-DC01.C137.local
OpCode:	Info		
More Information:	Event Log Online Help		

4



Q7: What malicious IP Addresses were involved?

A: 194.61.24.102 & 203.78.103.109

Q7.2: Were any IP Addresses from known adversary infrastructure?

A7.2: Yes

1

Associated Artifacts for 203.78.103.109

Domain	Threat Level	Positives	Last Resolved	Reference
ns1.happydoghappycat-th.com	-	-	09/07/2020 13:10:15	Report
happydoghappycat-th.com	-	-	08/27/2020 03:03:35	Report
ns1.browneypetworld.com	-	-	08/27/2020 13:09:01	Report
ns1.pppethome.com	-	-	08/27/2020 13:53:56	Report
webmail.happydoghappycat-th.com	-	-	08/27/2020 03:03:44	Report

Q7.3: Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?

A7.3: Yes

Hybrid analysis shows that 203.78.103.109 has been involved in 7 attacks in total in the past. It has been used for a variety of types of attacks.

1

Search results for *203.78.103.109*

Download all DNS Requests (CSV) | Download all Contacted Hosts (CSV)

Timestamp	Input		Threat level	Analysis Summary
August 24th 2024 22:04:48 (UTC)	**shellcode.exe** PE32+ executable (GUI) x86-64, for MS Windows 4909528cd5fca04c25b4a6d12e3679b3df555d1461486f52ff69669200c11a23	Sample (1KiB)	malicious	Threat Score: 100/100 AV Detection: **64%** ShellCode.Metasploit.Marte Matched **34** Indicators
January 25th 2024 11:26:41 (UTC)	**malicious_script.ps1** ASCII text, with very long lines 24ad5f0cfdf8b0457ce01f3b1dcfff47f0077b85e00edbdd230f66494b494444	Sample (2.7KiB)	malicious	Threat Score: 100/100 AV Detection: **43%** PwShell.Rozena.3.Generic Matched **102** Indicators #backdoor #empire
December 29th 2023 12:47:41 (UTC)	**file.None.0xffffe00062b10010.img** PE32+ executable (GUI) x86-64, for MS Windows ac34816de24c334dc69234ac0410aa48c9026b579671ab46a08308a589fd2d7f	Sample (10KiB)	malicious	Threat Score: 100/100 AV Detection: **78%** Malware Matched **34** Indicators Show Similar Samples
March 26th 2023 10:27:03 (UTC)	**download.ps1** ASCII text, with very long lines, with no line terminators 14f8d42dc50f98ef0f5263da5c118ea8f93bf77994c66b7fc405f1050ec99d57	Sample (2.4KiB)	ambiguous	AV Detection: **25%** PowerShell/Agent.WO trojan Matched **59** Indicators
October 30th 2022 02:30:42 (UTC)	**coreupdater.exe** PE32+ executable (GUI) x86-64, for MS Windows 10f3b92002bb9846733416 1cf85d0b173085 1f9256f83c27db125e9a0c1cfda6	Sample (7KiB)	malicious	Threat Score: 100/100 AV Detection: **85%** Malware Matched **21** Indicators Show Similar Samples
April 11th 2021 12:26:48 (UTC)	**http://203.78.103.109/**		no specific threat	AV Detection: **Marked as clean** Matched **19** Indicators
October 2nd 2020 02:52:36 (UTC)	**coreupdater.exe** PE32+ executable (GUI) x86-64, for MS Windows 10f3b92002bb9846733416 1cf85d0b173085 1f9256f83c27db125e9a0c1cfda6	Sample (7KiB)	malicious	Threat Score: 97/100 AV Detection: **85%** Malware Matched **16** Indicators Show Similar Samples

Q8: Did the attacker access any other systems?

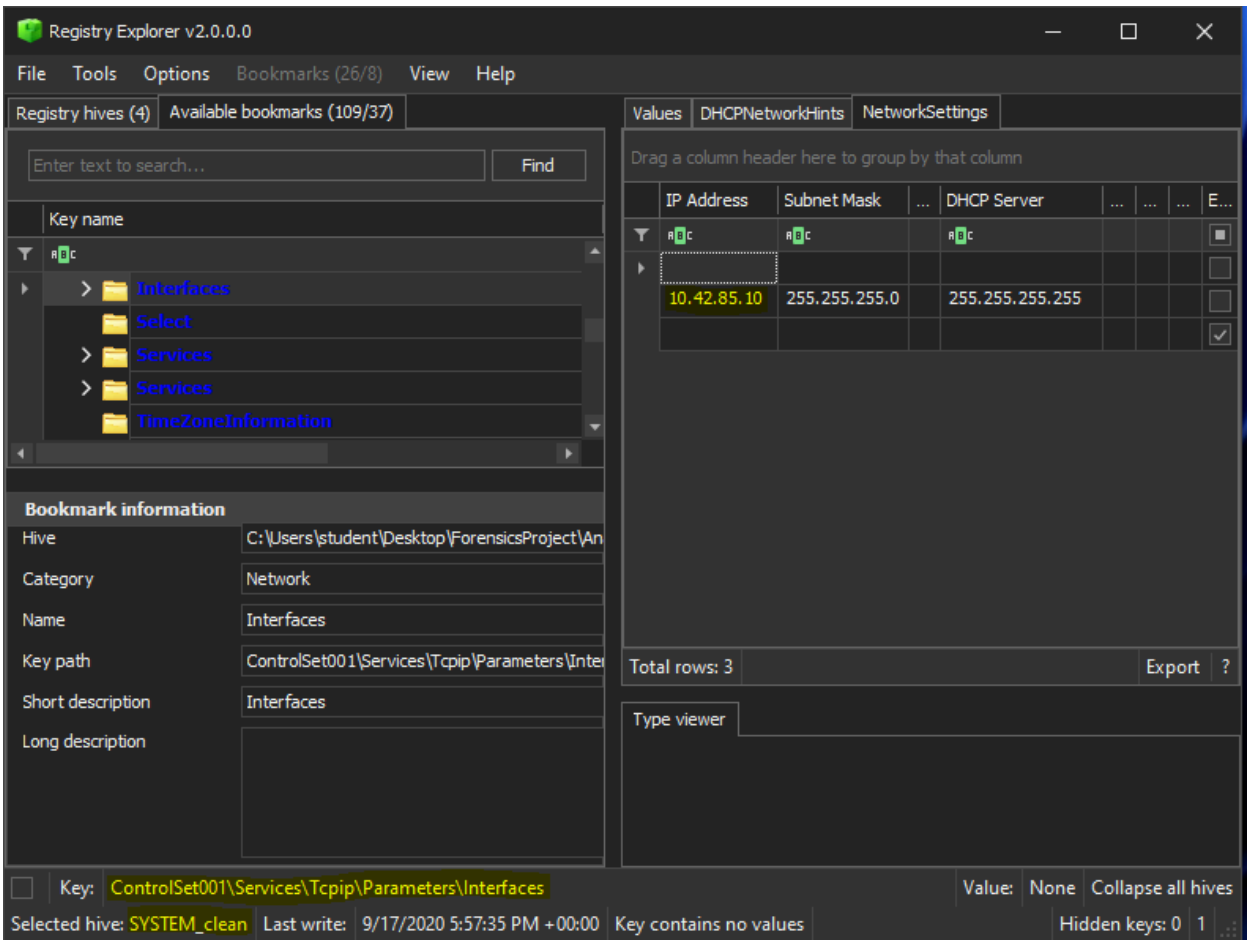
A8: Yes

Q8.2: How?

A8.2: Via RDP

Since the attacker has the credentials for the Administrator account on the domain, they can login using RDP over the local network to other devices on the domain with ease. Below *(Table #1)* you will find the attacker logged in to the workstation using the Administrator account on 18/09/2020 at 20:36:24 PST via RDP (Logon Type 10). They logged in via the server as evidenced in *(Table #2)*. The originating IP address is the same as the DC server's local IP.

1	An account was successfully logged on. Subject: Security ID: SYSTEM Account Name: DESKTOP-SDN1RPT$ Account Domain: C137 Logon ID: 0x3E7 Logon Information: Logon Type: 10 Restricted Admin Mode: No Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-21-2232410529-1445159330-2725690660-500 Account Name: Administrator Account Domain: C137 Logon ID: 0x857E73 Linked Logon ID: 0x0 Network Account Name: - Network Account Domain: - Logon GUID: {ab9dbb59-4c14-68c0-0eef-6c7ac9d540fd} Process Information: Process ID: 0x1c0 Process Name: C:\Windows\System32\svchost.exe Network Information: Workstation Name: DESKTOP-SDN1RPT Source Network Address: 10.42.85.10 Source Port: 0 Log Name: Security Source: Microsoft Windows security Logged: 18/09/2020 11:36:24 PM Event ID: 4624 Task Category: Logon Level: Information Keywords: Audit Success User: N/A Computer: DESKTOP-SDN1RPT.C137.local OpCode: Info

2	

Q8.3: When?

A8.3: On 18/09/2020 at 20:36:24 PST

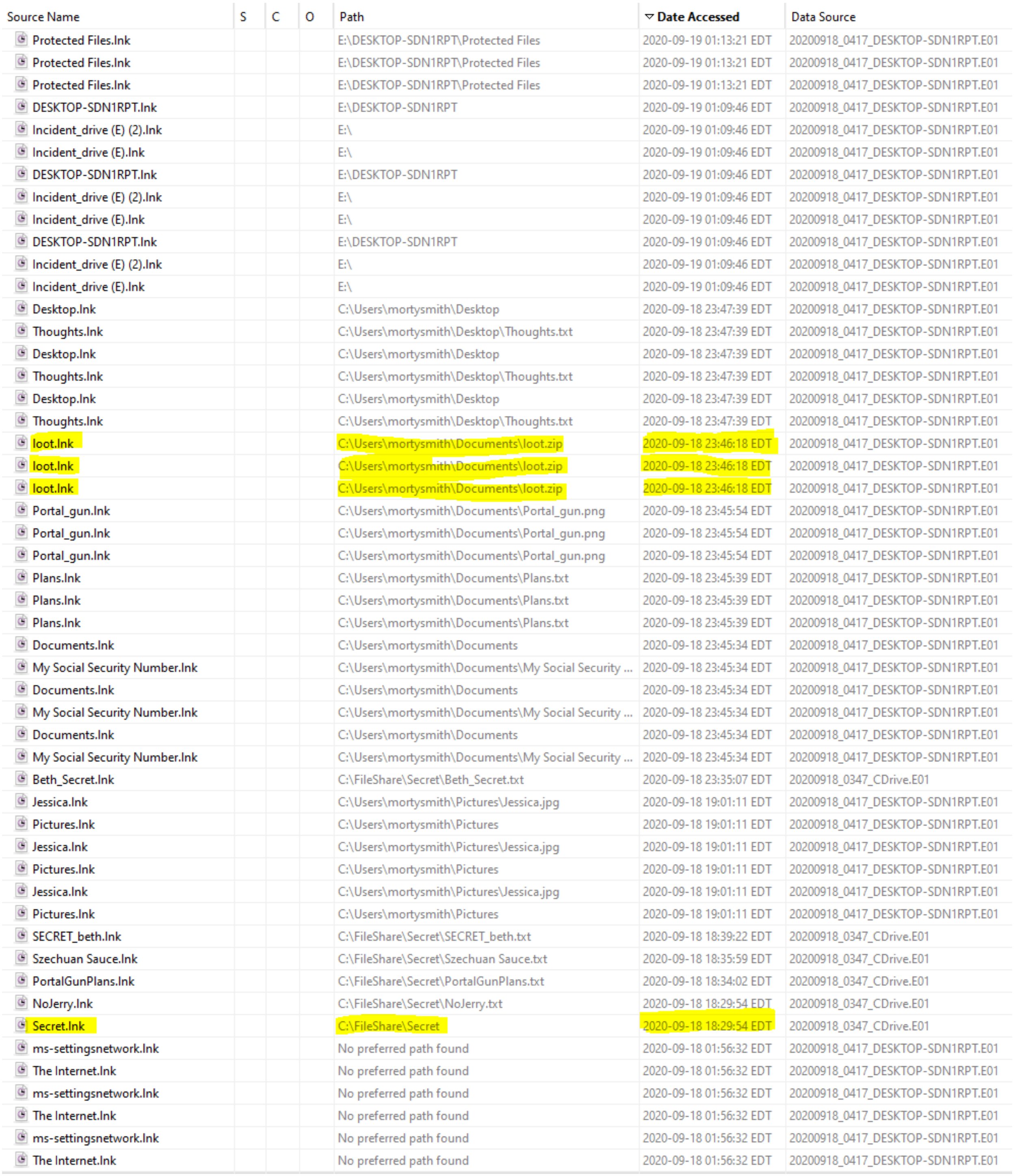
The attacker logged in to the workstation using the Administrator account on 18/09/2020 at 20:36:24 PST via RDP (Logon Type 10) as was shown in *(Table #1)* above.

Q8.4: Did the attacker steal or access any data? If so, when?

A8.4: Yes

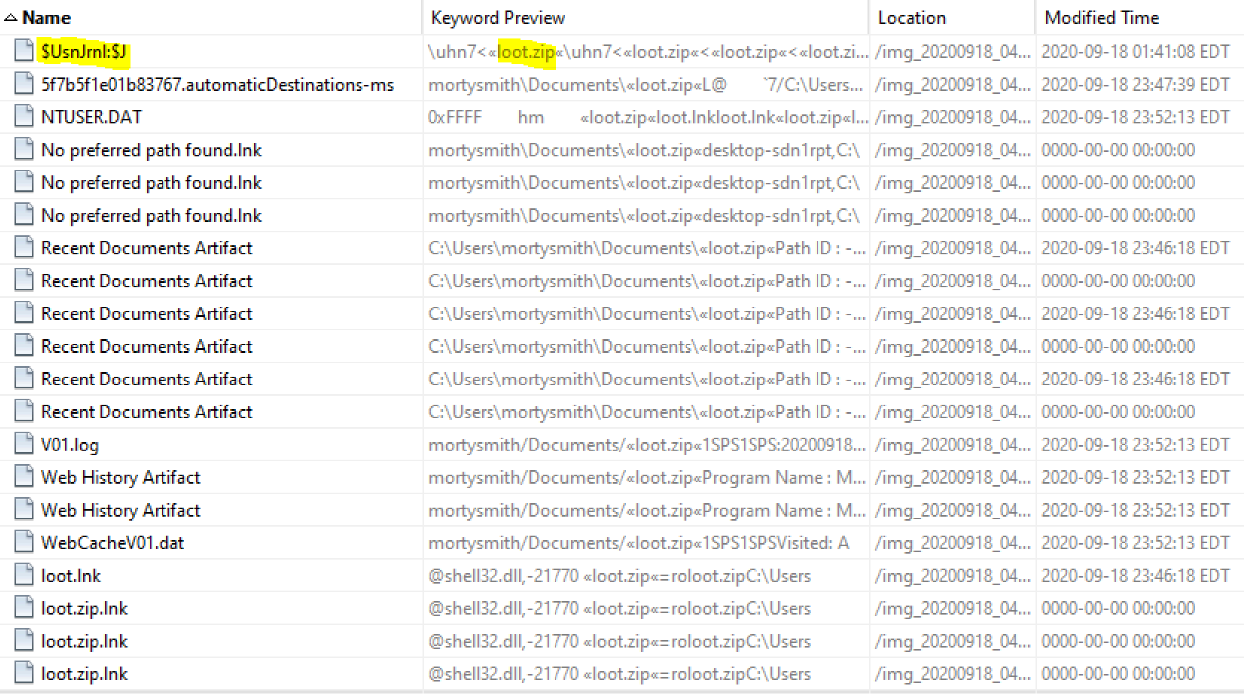
Autopsy shows us the most recently interacted with files on the systems. We can see some suspicious activity from the Administrator user after the compromise had happened. The attacker accessed a number of files in the Desktop, Documents, and Pictures folders of the user 'mortysmith' on the Desktop Device (DESKTOP-SDN1RPT). The attacker also accessed a FileShare called 'Secret' on the Server (CITADEL-DC01). It looks like the files on the Desktop were compressed into a zip file called 'loot.zip' and the contents of the fileshare on the server compressed into a file called 'Secret.zip'. A list of the most recently interacted files between the Desktop and Server are shown below in *(Table #1).* The recent and suspicious file called loot.zip was nowhere to be found. At which point I started to inspect the $UsnJrnl file as Autopsy showed an entry in it while searching for 'loot.zip' as shown in *(Table #2)*. Using MFTECmd.exe the journals on both devices were parsed and exported into CSV tables. The entries indicate that upon the creation of loot.zip and Secret.zip files they were immediately deleted. We can suspect that before deletion the files were exfiltrated as archiving multiple files into one makes it easier for attackers to download files as one. We can make an educated judgment that 'loot.zip' was exfiltrated approximately at 20:46:XX PST before deletion *(Table #4)* and 'Secret.zip' was exfiltrated approximately at 20:32XX PST before deletion as shown in *(Table #5)* in their own respective $UsnJrnl entries.

1



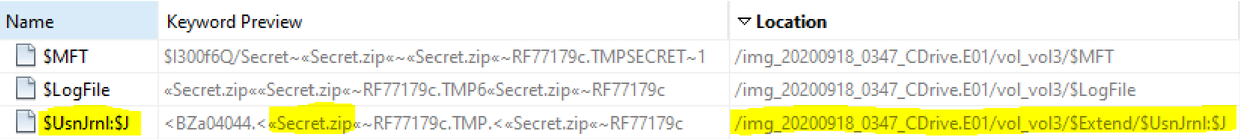
Source Name	S	C	O	Path	▽ Date Accessed	Data Source
Protected Files.lnk				E:\DESKTOP-SDN1RPT\Protected Files	2020-09-19 01:13:21 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Protected Files.lnk				E:\DESKTOP-SDN1RPT\Protected Files	2020-09-19 01:13:21 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Protected Files.lnk				E:\DESKTOP-SDN1RPT\Protected Files	2020-09-19 01:13:21 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
DESKTOP-SDN1RPT.lnk				E:\DESKTOP-SDN1RPT	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Incident_drive (E) (2).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Incident_drive (E).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
DESKTOP-SDN1RPT.lnk				E:\DESKTOP-SDN1RPT	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Incident_drive (E) (2).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Incident_drive (E).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
DESKTOP-SDN1RPT.lnk				E:\DESKTOP-SDN1RPT	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Incident_drive (E) (2).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Incident_drive (E).lnk				E:\	2020-09-19 01:09:46 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Desktop.lnk				C:\Users\mortysmith\Desktop	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Thoughts.lnk				C:\Users\mortysmith\Desktop\Thoughts.txt	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Desktop.lnk				C:\Users\mortysmith\Desktop	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Thoughts.lnk				C:\Users\mortysmith\Desktop\Thoughts.txt	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Desktop.lnk				C:\Users\mortysmith\Desktop	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Thoughts.lnk				C:\Users\mortysmith\Desktop\Thoughts.txt	2020-09-18 23:47:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
loot.lnk				C:\Users\mortysmith\Documents\loot.zip	2020-09-18 23:46:18 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
loot.lnk				C:\Users\mortysmith\Documents\loot.zip	2020-09-18 23:46:18 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
loot.lnk				C:\Users\mortysmith\Documents\loot.zip	2020-09-18 23:46:18 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Portal_gun.lnk				C:\Users\mortysmith\Documents\Portal_gun.png	2020-09-18 23:45:54 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Portal_gun.lnk				C:\Users\mortysmith\Documents\Portal_gun.png	2020-09-18 23:45:54 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Portal_gun.lnk				C:\Users\mortysmith\Documents\Portal_gun.png	2020-09-18 23:45:54 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Plans.lnk				C:\Users\mortysmith\Documents\Plans.txt	2020-09-18 23:45:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Plans.lnk				C:\Users\mortysmith\Documents\Plans.txt	2020-09-18 23:45:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Plans.lnk				C:\Users\mortysmith\Documents\Plans.txt	2020-09-18 23:45:39 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Documents.lnk				C:\Users\mortysmith\Documents	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
My Social Security Number.lnk				C:\Users\mortysmith\Documents\My Social Security ...	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Documents.lnk				C:\Users\mortysmith\Documents	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
My Social Security Number.lnk				C:\Users\mortysmith\Documents\My Social Security ...	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Documents.lnk				C:\Users\mortysmith\Documents	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
My Social Security Number.lnk				C:\Users\mortysmith\Documents\My Social Security ...	2020-09-18 23:45:34 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Beth_Secret.lnk				C:\FileShare\Secret\Beth_Secret.txt	2020-09-18 23:35:07 EDT	20200918_0347_CDrive.E01
Jessica.lnk				C:\Users\mortysmith\Pictures\Jessica.jpg	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Pictures.lnk				C:\Users\mortysmith\Pictures	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Jessica.lnk				C:\Users\mortysmith\Pictures\Jessica.jpg	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Pictures.lnk				C:\Users\mortysmith\Pictures	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Jessica.lnk				C:\Users\mortysmith\Pictures\Jessica.jpg	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
Pictures.lnk				C:\Users\mortysmith\Pictures	2020-09-18 19:01:11 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
SECRET_beth.lnk				C:\FileShare\Secret\SECRET_beth.txt	2020-09-18 18:39:22 EDT	20200918_0347_CDrive.E01
Szechuan Sauce.lnk				C:\FileShare\Secret\Szechuan Sauce.txt	2020-09-18 18:35:59 EDT	20200918_0347_CDrive.E01
PortalGunPlans.lnk				C:\FileShare\Secret\PortalGunPlans.txt	2020-09-18 18:34:02 EDT	20200918_0347_CDrive.E01
NoJerry.lnk				C:\FileShare\Secret\NoJerry.txt	2020-09-18 18:29:54 EDT	20200918_0347_CDrive.E01
Secret.lnk				C:\FileShare\Secret	2020-09-18 18:29:54 EDT	20200918_0347_CDrive.E01
ms-settingsnetwork.lnk				No preferred path found	2020-09-18 01:56:32 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
The Internet.lnk				No preferred path found	2020-09-18 01:56:32 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
ms-settingsnetwork.lnk				No preferred path found	2020-09-18 01:56:32 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
The Internet.lnk				No preferred path found	2020-09-18 01:56:32 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
ms-settingsnetwork.lnk				No preferred path found	2020-09-18 01:56:32 EDT	20200918_0417_DESKTOP-SDN1RPT.E01
The Internet.lnk				No preferred path found	2020-09-18 01:56:32 EDT	20200918_0417_DESKTOP-SDN1RPT.E01

2



Name	Keyword Preview	Location	Modified Time
$UsnJrnl:$J	\uhn7<«loot.zip«\uhn7<«loot.zip«<«loot.zip«<«loot.zi...	/img_20200918_04...	2020-09-18 01:41:08 EDT
5f7b5f1e01b83767.automaticDestinations-ms	mortysmith\Documents\«loot.zip«L@ `7/C:\Users...	/img_20200918_04...	2020-09-18 23:47:39 EDT
NTUSER.DAT	0xFFFF hm «loot.zip«loot.lnkloot.lnk«loot.zip«l...	/img_20200918_04...	2020-09-18 23:52:13 EDT
No preferred path found.lnk	mortysmith\Documents\«loot.zip«desktop-sdn1rpt,C:\	/img_20200918_04...	0000-00-00 00:00:00
No preferred path found.lnk	mortysmith\Documents\«loot.zip«desktop-sdn1rpt,C:\	/img_20200918_04...	0000-00-00 00:00:00
No preferred path found.lnk	mortysmith\Documents\«loot.zip«desktop-sdn1rpt,C:\	/img_20200918_04...	0000-00-00 00:00:00
Recent Documents Artifact	C:\Users\mortysmith\Documents\«loot.zip«Path ID : -...	/img_20200918_04...	2020-09-18 23:46:18 EDT
Recent Documents Artifact	C:\Users\mortysmith\Documents\«loot.zip«Path ID : -...	/img_20200918_04...	0000-00-00 00:00:00
Recent Documents Artifact	C:\Users\mortysmith\Documents\«loot.zip«Path ID : -...	/img_20200918_04...	2020-09-18 23:46:18 EDT
Recent Documents Artifact	C:\Users\mortysmith\Documents\«loot.zip«Path ID : -...	/img_20200918_04...	0000-00-00 00:00:00
Recent Documents Artifact	C:\Users\mortysmith\Documents\«loot.zip«Path ID : -...	/img_20200918_04...	2020-09-18 23:46:18 EDT
Recent Documents Artifact	C:\Users\mortysmith\Documents\«loot.zip«Path ID : -...	/img_20200918_04...	0000-00-00 00:00:00
V01.log	mortysmith/Documents/«loot.zip«1SPS1SPS:20200918...	/img_20200918_04...	2020-09-18 23:52:13 EDT
Web History Artifact	mortysmith/Documents/«loot.zip«Program Name : M...	/img_20200918_04...	2020-09-18 23:52:13 EDT
Web History Artifact	mortysmith/Documents/«loot.zip«Program Name : M...	/img_20200918_04...	2020-09-18 23:52:13 EDT
WebCacheV01.dat	mortysmith/Documents/«loot.zip«1SPS1SPSVisited: A	/img_20200918_04...	2020-09-18 23:52:13 EDT
loot.lnk	@shell32.dll,-21770 «loot.zip«=roloot.zipC:\Users	/img_20200918_04...	2020-09-18 23:46:18 EDT
loot.zip.lnk	@shell32.dll,-21770 «loot.zip«=roloot.zipC:\Users	/img_20200918_04...	0000-00-00 00:00:00
loot.zip.lnk	@shell32.dll,-21770 «loot.zip«=roloot.zipC:\Users	/img_20200918_04...	0000-00-00 00:00:00
loot.zip.lnk	@shell32.dll,-21770 «loot.zip«=roloot.zipC:\Users	/img_20200918_04...	0000-00-00 00:00:00

3



Name	Keyword Preview	Location
$MFT	$I300f6Q/Secret~«Secret.zip«~«Secret.zip«~RF77179c.TMPSECRET~1	/img_20200918_0347_CDrive.E01/vol_vol3/$MFT
$LogFile	«Secret.zip««Secret.zip«~RF77179c.TMP6«Secret.zip«~RF77179c	/img_20200918_0347_CDrive.E01/vol_vol3/$LogFile
$UsnJrnl:$J	<BZa04044.<«Secret.zip«~RF77179c.TMP.<«Secret.zip«~RF77179c	/img_20200918_0347_CDrive.E01/vol_vol3/$Extend/$UsnJrnl:$J

4	loot.zip	2020-09-19 3:46:18	RenameNewName	.zip
	loot.zip	2020-09-19 3:46:18	RenameNewName|Close	.zip
	loot.zip	2020-09-19 3:46:18	ObjectIdChange	.zip
	loot.zip	2020-09-19 3:46:18	ObjectIdChange|Close	.zip
	loot.lnk	2020-09-19 3:46:18	FileCreate	.lnk
	loot.lnk	2020-09-19 3:46:18	DataExtend|FileCreate	.lnk
	loot.lnk	2020-09-19 3:46:18	DataExtend|FileCreate|Close	.lnk
	5f7b5f1e01b83767.automaticDestinations-ms	2020-09-19 3:46:18	DataExtend	.automaticDestin
	5f7b5f1e01b83767.automaticDestinations-ms	2020-09-19 3:46:18	DataOverwrite|DataExtend	.automaticDestin
	5f7b5f1e01b83767.automaticDestinations-ms	2020-09-19 3:46:18	DataOverwrite|DataExtend|Close	.automaticDestin
	V01.chk	2020-09-19 3:46:23	DataOverwrite	.chk
	V01.chk	2020-09-19 3:46:23	DataOverwrite|Close	.chk
	Microsoft-Windows-SettingSync%4Debug.evtx	2020-09-19 3:46:25	DataOverwrite	.evtx
	SEARCHPROTOCOLHOST.EXE-69C456C3.pf	2020-09-19 3:46:26	DataTruncation	.pf
	SEARCHPROTOCOLHOST.EXE-69C456C3.pf	2020-09-19 3:46:26	DataExtend|DataTruncation	.pf
	SEARCHPROTOCOLHOST.EXE-69C456C3.pf	2020-09-19 3:46:26	DataExtend|DataTruncation|Close	.pf
	V01.chk	2020-09-19 3:46:41	DataOverwrite	.chk
	V01.chk	2020-09-19 3:46:41	DataOverwrite|Close	.chk
	SVCHOST.EXE-6A249820.pf	2020-09-19 3:46:53	DataTruncation	.pf
	SVCHOST.EXE-6A249820.pf	2020-09-19 3:46:53	DataExtend|DataTruncation	.pf
	SVCHOST.EXE-6A249820.pf	2020-09-19 3:46:53	DataExtend|DataTruncation|Close	.pf
	VSSVC.EXE-6C8F0C66.pf	2020-09-19 3:46:53	DataTruncation	.pf
	VSSVC.EXE-6C8F0C66.pf	2020-09-19 3:46:53	DataExtend|DataTruncation	.pf
	VSSVC.EXE-6C8F0C66.pf	2020-09-19 3:46:53	DataExtend|DataTruncation|Close	.pf
	80237EE4964FC9C409AAF55BF996A292_E503E	2020-09-19 3:46:59	DataOverwrite	
	80237EE4964FC9C409AAF55BF996A292_E503E	2020-09-19 3:46:59	DataOverwrite|Close	
	AUDIODG.EXE-AB22E9A6.pf	2020-09-19 3:47:09	DataTruncation	.pf
	AUDIODG.EXE-AB22E9A6.pf	2020-09-19 3:47:09	DataExtend|DataTruncation	.pf
	loot.zip	2020-09-19 3:47:10	FileDelete|Close	.zip

5	Secret.zip	2020-09-19 3:32:39	FileCreate	.zip
	BZa04044	2020-09-19 3:32:39	FileCreate	
	BZa04044	2020-09-19 3:32:39	DataExtend|FileCreate	
	BZa04044	2020-09-19 3:32:39	DataOverwrite|DataExtend|FileCreate	
	BZa04044	2020-09-19 3:32:39	DataOverwrite|DataExtend|FileCreate|Close	
	Secret.zip	2020-09-19 3:32:39	FileCreate|Close	.zip
	BZa04044	2020-09-19 3:32:39	SecurityChange	
	Secret.zip~RF77179c.TMP	2020-09-19 3:32:39	FileCreate	.TMP
	Secret.zip~RF77179c.TMP	2020-09-19 3:32:39	FileCreate|Close	.TMP
	Secret.zip~RF77179c.TMP	2020-09-19 3:32:39	FileDelete|Close	.TMP
	Secret.zip	2020-09-19 3:32:39	RenameOldName	.zip
	Secret.zip~RF77179c.TMP	2020-09-19 3:32:39	RenameNewName	.TMP
	BZa04044	2020-09-19 3:32:39	SecurityChange|RenameOldName	
	Secret.zip	2020-09-19 3:32:39	SecurityChange|RenameNewName	.zip
	Secret.zip~RF77179c.TMP	2020-09-19 3:32:39	RenameNewName|Close	.TMP
	Secret.zip	2020-09-19 3:32:39	SecurityChange|RenameNewName|Cl	.zip
	Secret.zip~RF77179c.TMP	2020-09-19 3:32:39	FileDelete|Close	.TMP

•
•
•
•

DRIVERS	2020-09-19 3:33:55	BasicInfoChange	
DRIVERS	2020-09-19 3:33:55	BasicInfoChange|Close	
Secret.zip	2020-09-19 3:34:18	FileDelete|Close	.zip
$IU2L112.txt	2020-09-19 3:34:27	FileCreate	.txt

Q9: What was the network layout of the victim network?

A9: The network layout is quite simple; the network 10.42.85.0/24 has two devices in it. CITADEL-DC01 has the IP address 10.42.85.10 and DESKTOP-SDN1RPT has the IP address 10.42.85.115.

Looking at the interfaces key we can see the details for the network configuration on each machine. *(Table #1)* shows the network configuration for CITADEL-DC01 & *(Table #2)* shows the network configuration for DESKTOP-SDN1RPT. *(Table #2)* shows a diagram visualizing the information from these two entries into a network diagram.l

1

Registry Explorer v2.0.0.0

File Tools Options Bookmarks (0/0) View Help

Registry hives (3) | Available bookmarks (88/25)

Enter text to search... Find

Key name

- Windows
- Windows
- AppCompatCache
- ComputerName
- Interfaces
  - {1f777394-0b42-11e3-80ad-806e6f6e6963}
  - {791D93FB-6EDF-4C65-B1B9-F8E46CFFEA73}
  - {C7568B63-C424-48B3-AB9B-6D1F004D5AFC}
- Select
- Services
- Services
- TimeZoneInformation
- USB

Bookmark information

Hive
Category
Name
Key path
Short description
Long description

Values

Drag a column header here to group by that column

Value Name	Value Type	Data
AddressType	RegDword	0
DefaultGateway	RegMultiSz	10.42.85.100
DefaultGatewayMetric	RegMultiSz	0
DhcpConnForceBroadcastFlag	RegDword	0
DhcpServer	RegSz	255.255.255.255
Domain	RegSz	
EnableDeadGWDetect	RegDword	1
EnableDHCP	RegDword	0
IPAddress	RegMultiSz	10.42.85.10
IsServerNapAware	RegDword	0
Lease	RegDword	1800
LeaseObtainedTime	RegDword	1600362219
LeaseTerminatesTime	RegDword	1600364019
NameServer	RegSz	127.0.0.1
RegisterAdapterName	RegDword	0
RegistrationEnabled	RegDword	1
SubnetMask	RegMultiSz	255.255.255.0
T1	RegDword	1600363119
T2	RegDword	1600363794

Type viewer | Binary viewer

Value name: AddressType

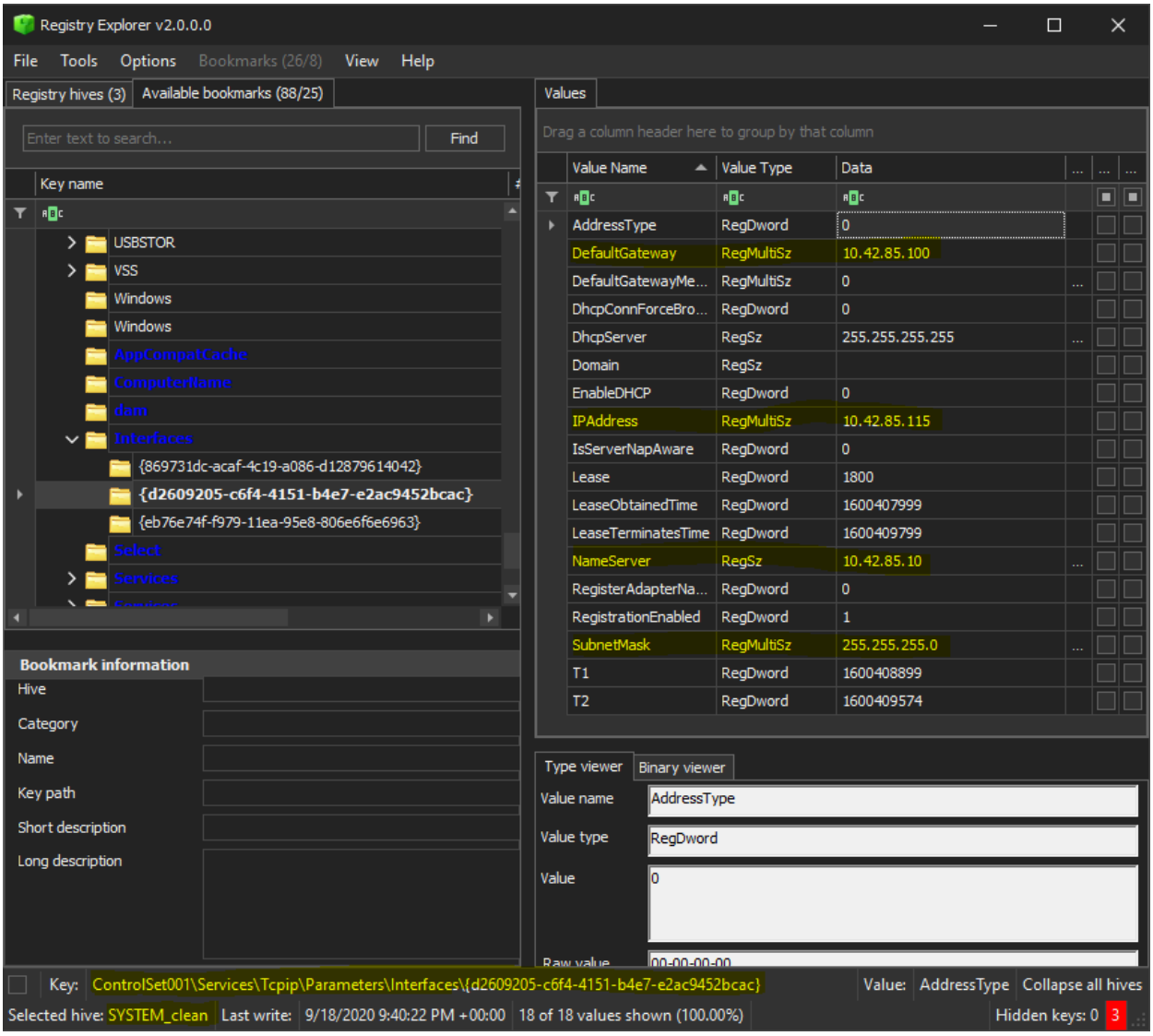
Value type: RegDword

Value: 0

Raw value: 00-00-00-00

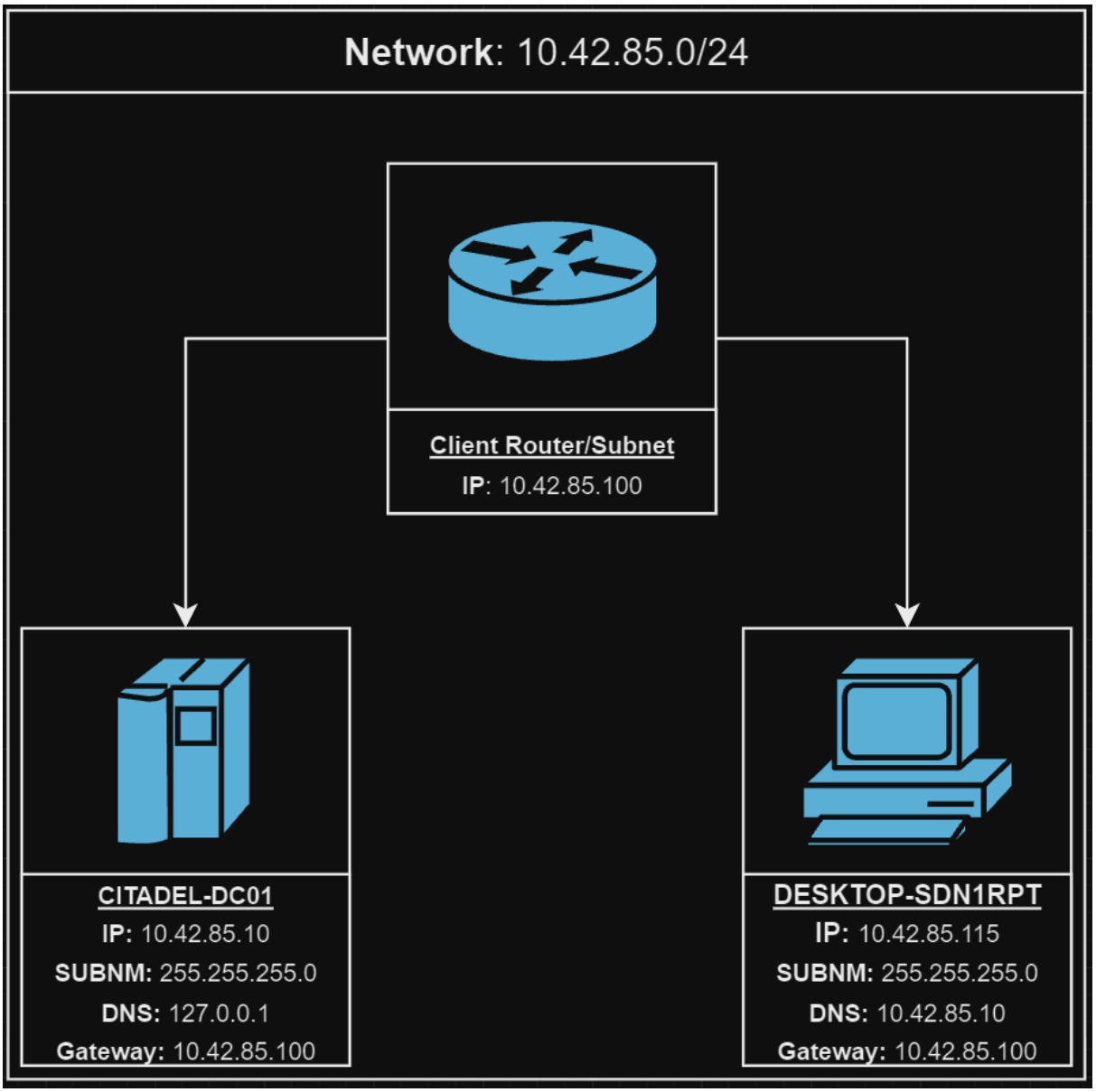
Key: ControlSet001\Services\Tcpip\Parameters\Interfaces\{791D93FB-6EDF-4C65-B1B9-F8E46CFFEA73} Value: AddressType Collapse all hives

Selected hive: SYSTEM_clean Last write: 9/17/2020 5:57:16 PM +00:00 20 of 20 values shown (100.00%) Hidden keys: 0 3

2	

Registry Explorer v2.0.0.0
File Tools Options Bookmarks (26/8) View Help
Registry hives (3) Available bookmarks (88/25)
Enter text to search... Find
Key name
USBSTOR
VSS
Windows
Windows
AppCompatCache
ComputerName
dam
Interfaces
{869731dc-acaf-4c19-a086-d12879614042}
{d2609205-c6f4-4151-b4e7-e2ac9452bcac}
{eb76e74f-f979-11ea-95e8-806e6f6e6963}
Select
Services
Bookmark information
Hive
Category
Name
Key path
Short description
Long description
Values
Drag a column header here to group by that column
Value Name Value Type Data
AddressType RegDword 0
DefaultGateway RegMultiSz 10.42.85.100
DefaultGatewayMe... RegMultiSz 0
DhcpConnForceBro... RegDword 0
DhcpServer RegSz 255.255.255.255
Domain RegSz
EnableDHCP RegDword 0
IPAddress RegMultiSz 10.42.85.115
IsServerNapAware RegDword 0
Lease RegDword 1800
LeaseObtainedTime RegDword 1600407999
LeaseTerminatesTime RegDword 1600409799
NameServer RegSz 10.42.85.10
RegisterAdapterNa... RegDword 0
RegistrationEnabled RegDword 1
SubnetMask RegMultiSz 255.255.255.0
T1 RegDword 1600408899
T2 RegDword 1600409574
Type viewer Binary viewer
Value name AddressType
Value type RegDword
Value 0
Raw value 00-00-00-00
Key: ControlSet001\Services\Tcpip\Parameters\Interfaces\{d2609205-c6f4-4151-b4e7-e2ac9452bcac}
Value: AddressType Collapse all hives
Selected hive: SYSTEM_clean Last write: 9/18/2020 9:40:22 PM +00:00 18 of 18 values shown (100.00%)
Hidden keys: 0 3

3



Timeline

Date + Time	Event
18/09/2020 20:21:25 PM PST	Attacker starts bruteforce attack on CITADEL-DC01

18/09/2020 20:21:48 PM PST	Attacker succeeds in bruteforce attack
18/09/2020 20:24:12 PST	Payload downloaded into the Administrators Downloads folder
18/09/2020 20:24:12 PST	Malware was moved to the *\System32 folder
↕	Malware was executed
18/09/2020 20:27:49 PST	Persistence was established via registry key entry and autostart service
18/09/2020 20:32XX PST	‘Secret.zip’ was exfiltrated
18/09/2020 20:36:24 PST	Moved laterally to DESKTOP-SDN1RPT via RDP connection
18/09/2020 20:40:01 PST	Payload downloaded into the Administrators Downloads folder
↕	Malware was executed
18/09/2020 20:42:42 PST	Persistence was established via registry key entry and autostart service
18/09/2020 20:46:XX PST	loot.zip’ was exfiltrated

Recommendations

Disable RDP Port 3389

The events that occurred happened due to RDP being enabled over the internet. Should RDP be needed it should only be used locally. Blocking port 3389 on the firewall removes the threat of anyone attempting this from outside the network all together.

Stronger Password Policy

The brute force attack took less than 1 minute to be successful. This indicates that the user “Administrator’ had a weak password. An implementation of a password policy would help prolong a subsequent attack or make the attacker give up altogether due to time constraints.

2FA for RDP/Domain Login

Enabling 2FA would essentially nullify brute force attacks in the future given that the attacker doesn't have the second authentication method. This would in general strengthen the overall security posture of the organization.

Install/Enable IPS System

Having an IPS system would have automatically blocked this type of attack.

CITATIONS

Labs, Fsp. (n.d.). *Process tracking with Event Log Explorer*. Event Log Explorer blog. https://eventlogxp.com/blog/process-tracking-with-event-log-explorer/

Moaistory. (n.d.). *Moaistory/IE10Analyzer: Http://moaistory.blogspot.com/2016/08/ie10analyzer.html*. GitHub. https://github.com/moaistory/IE10Analyzer

Payload module. Payload Module - an overview | ScienceDirect Topics. (n.d.). https://www.sciencedirect.com/topics/computer-science/payload-module

Summerson, C., & Lewis, N. (2023, November 29). *How to edit your system path for easy command line access in windows*. How. https://www.howtogeek.com/118594/how-to-edit-your-system-path-for-easy-command-line-access/

USNJRNL forensics extraction for Efficient Investigation | Otorio. (n.d.-a). https://www.otorio.com/resources/usnjrnl-extraction-for-efficient-investigation/

Vinaypamnani-Msft. (n.d.). *4624(s) an account was successfully logged on. - windows 10*. 4624(S) An account was successfully logged on. - Windows 10 | Microsoft Learn. https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/event-4624

Volatility filescan – eyehatemalwares. (n.d.-b). https://www.eyehatemalwares.com/digital-forensics/memory-analysis/volatility-filescan/

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

How payloads work. Metasploit Documentation Penetration Testing Software, Pen Testing Security. (n.d.).
https://docs.metasploit.com/docs/using-metasploit/basics/how-payloads-work.html

Event ID 4625 without source IP. Server Fault.
https://serverfault.com/questions/683837/event-id-4625-without-source-ip

How to know when a file was deleted in a NTFS filesystem?. Information Security Stack Exchange.
https://security.stackexchange.com/questions/61166/how-to-know-when-a-file-was-deleted-in-a-ntfs-filesystem

What is the WebCache folder in AppData/Local/Microsoft/Windows/ Windows 10. Super User.
https://superuser.com/questions/1600395/what-is-the-webcache-folder-in-appdata-local-microsoft-windows-windows-10