

# Forensics Report and Documentation

Case 001 The Case of the Stolen Szechuan Sauce

By: Dan Howard and Heather Fincati



The Stolen Szechuan Sauce [image courtesy of [artwork-tee](#)]

<b>Executive Summary.....</b>	<b>3</b>
<b>Questions.....</b>	<b>4</b>
1. What's the Operating System of the Server?.....	4
2. What's the Operating System of the Desktop?.....	4
3. What was the local time of the Server?.....	4
4. Was there a breach?.....	5
5. What was the initial entry vector (how did they get in)?.....	5
6. Was malware used? If so, what was it?.....	7
8. Did the attacker access any other systems?.....	13
9. What was the network layout of the victim network?.....	17
<b>References.....</b>	<b>18</b>

# Executive Summary

A digital forensics investigation was conducted to understand a cyber security incident involving the theft of confidential data. The scenario, created by [DFIR Madness](#), focused on a compromised server and desktop.

Our investigation confirmed a system breach targeting sensitive data. Evidence suggests a brute-force RDP attack, like Morty teleporting into the wrong dimension. Malicious software (coreupdater.exe) was identified lurking on both machines, downloaded from a suspicious IP address. This malware established persistence mechanisms and has functionalities for compromising security, reconnaissance, and potentially manipulating data. The attacker infiltrated the network, potentially stealing the Szechuan Sauce recipe! Further investigation is necessary to determine if the sauce was stolen and its impact on world C-137.

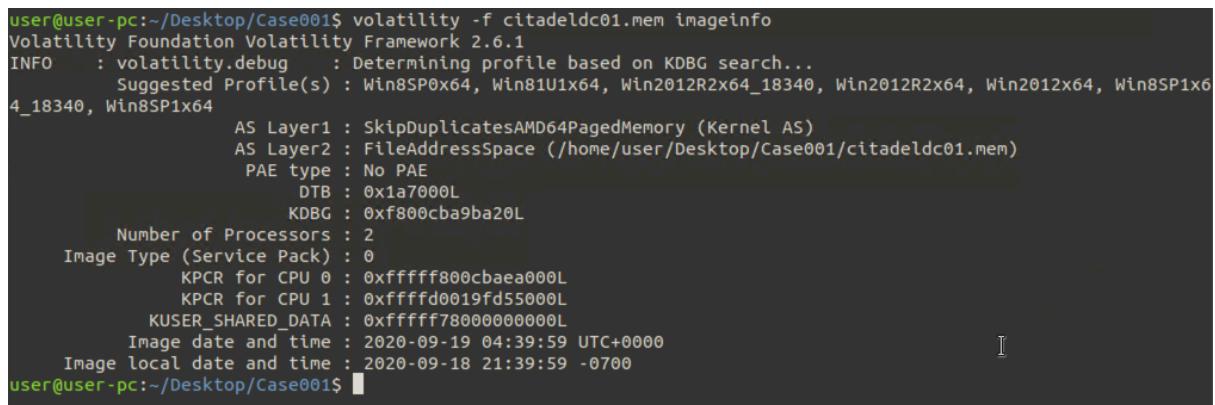
We recommend a network security assessment to identify and address RDP vulnerabilities. Additionally, implementing stronger RDP authentication methods can help prevent similar attacks in the future. This incident underscores the importance of robust cyber security measures to mitigate such risks, otherwise you might find yourself in a sticky situation, with your sauce hostage.

# Questions

## 1. What's the Operating System of the Server? (Dan and Heather)

To find the answer we used Volatility software on our Linux machine to examine the memory file citadeldc01.mem. In order to extract the information needed we used the command terminal and imputed <volatility -f citadeldc01.mem imageinfo> (Figure 1).

**Answer:** Windows Server 2012 - Win2012R2x64



```
user@user-pc:~/Desktop/Case001$ volatility -f citadeldc01.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win8SP0x64, Win81U1x64, Win2012R2x64_18340, Win2012R2x64, Win2012x64, Win8SP1x6
4_18340, Win8SP1x64
          AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
          AS Layer2 : FileAddressSpace (/home/user/Desktop/Case001/citadeldc01.mem)
          PAE type : No PAE
          DTB : 0x1a7000L
          KDBG : 0xf800cba9ba20L
          Number of Processors : 2
Image Type (Service Pack) : 0
          KPCR for CPU 0 : 0xfffff800cbaea000L
          KPCR for CPU 1 : 0xfffffd0019fd55000L
          KUSER_SHARED_DATA : 0xfffff780000000000L
          Image date and time : 2020-09-19 04:39:59 UTC+0000
          Image local date and time : 2020-09-18 21:39:59 -0700
user@user-pc:~/Desktop/Case001$
```

Figure 1

## 2. What's the Operating System of the Desktop? (Dan and Heather)

To find the answer we used Volatility software on our Linux machine to examine the memory file citadeldc01.mem. In order to extract the information needed we used the command terminal and imputed <volatility -f citadeldc01.mem imageinfo> (Figure 1)

**Answer:** Microsoft Windows Win8SP0x64, Win81U1x64

## 3. What was the local time of the Server? (Dan and Heather)

To find the answer we used Volatility software on our Linux machine to examine the memory file citadeldc01.mem. In order to extract the information needed we used the command terminal and imputed <volatility -f citadeldc01.mem imageinfo> (Figure 1)

**Answer:** 2020-09-18 21:39:59 -0700

## 4. Was there a breach? (Dan and Heather)

**Answer:** Yes. We know from the summary the recipe was stolen.

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

Wireshark was our ally during this phase, from the captures we could see how they got in and what method they used. (Figure 2)

**Answer:** Remote Desktop Brute Force

ip.src == 10.42.85.115 && ip.addr == 194.61.24.102						
No.	Time	Source	Destination	Protocol	Length	Info
3273...	16879.464364	10.42.85.115	194.61.24.102	TCP	66	50840 → 80 [SYN] Seq=
3273...	16879.464503	10.42.85.115	194.61.24.102	TCP	66	50841 → 80 [SYN] Seq=
3273...	16879.464889	10.42.85.115	194.61.24.102	TCP	60	50840 → 80 [ACK] Seq=
3273...	16879.464917	10.42.85.115	194.61.24.102	TCP	60	50841 → 80 [ACK] Seq=
→ 3273...	16879.468884	10.42.85.115	194.61.24.102	HTTP	428	GET / HTTP/1.1
3273...	16879.469960	10.42.85.115	194.61.24.102	CP	60	50840 → 80 [ACK] Seq=
3273...	16879.470115	10.42.85.115	194.61.24.102	CP	60	50840 → 80 [ACK] Seq=
3273...	16879.471155	10.42.85.115	194.61.24.102	CP	60	50840 → 80 [FIN, ACK]
3394...	16910.939638	10.42.85.115	194.61.24.102	CP	60	50841 → 80 [FIN, ACK]
3394...	16910.939892	10.42.85.115	194.61.24.102	CP	66	50864 → 80 [SYN] Seq=
3394...	16910.939946	10.42.85.115	194.61.24.102	CP	66	50865 → 80 [SYN] Seq=
3394...	16910.940090	10.42.85.115	194.61.24.102	CP	60	50841 → 80 [ACK] Seq=
3394...	16910.940179	10.42.85.115	194.61.24.102	CP	60	50864 → 80 [ACK] Seq=
3394...	16910.940361	10.42.85.115	194.61.24.102	HTTP	352	GET /coreupdater.exe
3394...	16910.940387	10.42.85.115	194.61.24.102	CP	60	50865 → 80 [ACK] Seq=
3394...	16910.941028	10.42.85.115	194.61.24.102	CP	60	50864 → 80 [ACK] Seq=
3394...	16910.941190	10.42.85.115	194.61.24.102	CP	60	50864 → 80 [ACK] Seq=
3394...	16910.941248	10.42.85.115	194.61.24.102	CP	60	50864 → 80 [ACK] Seq=
3394...	16910.942244	10.42.85.115	194.61.24.102	CP	60	50864 → 80 [FIN, ACK]
3492...	16989.371536	10.42.85.115	194.61.24.102	CP	60	50865 → 80 [FIN, ACK]
3492...	16989.372021	10.42.85.115	194.61.24.102	CP	60	50865 → 80 [ACK] Seq=
→ Frame 327363: 428 bytes on wire (3424 bits), 428 bytes captured (3424 bits) on interface eth0 Ethernet II, Src: VMware (00:0c:29:95:00:02), Dst: 194.61.24.102 (00:0c:29:95:00:01) Internet Protocol Version 4, Src: 10.42.85.115 (10.42.85.115), Dst: 194.61.24.102 (194.61.24.102) Transmission Control Protocol Hypertext Transfer Protocol						
Follow						
Copy						
(3424 bits) on interface eth0						
Protocol Preferences						
Decode As...						
Show Packet in New Window						

Figure 2

From the screenshot above (Figure 2) we right-clicked the GET request and used “Follow” protocol action which resulted in the below screenshot (Figure 3). This confirms access to the system.

```

GET / HTTP/1.1
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/70.0.3538.102 Safari/537.36 Edge/18.19041
Accept-Encoding: gzip, deflate
Host: 194.61.24.102
Connection: Keep-Alive

HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.18
Date: Sat, 19 Sep 2020 02:39:26 GMT
Content-type: text/html; charset=UTF-8
Content-Length: 228

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 3.2 Final//EN"><html>
<title>directory listing for /</title>
<body>
<h2>directory listing for /</h2>
<hr>
<ul>
<li><a href="coreupdater.exe">coreupdater.exe</a>
</ul>
<hr>
</body>
</html>

```

1 client pkt, 1 server pkt, 1 turn.

Entire conversation (757 bytes) Show data as ASCII Stream 30611

Find:  Find Next

Filter Out This Stream Print Save as... Back Close Help

Figure 3

Filtering the 192.61.24.102 IP we can determine the different packets that uploaded the coreupdater.exe file (Figure 4).

Packet	Hostname	Content Type	Size	Filename
236791	194.61.24.102	text/html	228 bytes	\
236809	194.61.24.102	text/html	195 bytes	favicon.ico
238574	194.61.24.102	application/x-msdos-program	7168 bytes	coreupdater.exe
327366	194.61.24.102	text/html	228 bytes	\
339465	194.61.24.102	application/x-msdos-program	7168 bytes	coreupdater.exe

Figure 4

## 6. Was malware used? If so, what was it? If there was malware answer the following: (Dan and Heather)

In order to find all the information below we utilized our Linux machine to get IP addresses, PID, and Ports through a netscan and pull the files out into a more easily read file with the argument netscan.out. We also entered the hash values from the autorun csv file in VirusTotal to gather the rest of the information.

### 6a. What process was malicious?

Answer: 3644 (Figure 5)

```
*****  
coreupdater.ex pid: 3644  
*****
```

Figure 5

### 6b. Identify the IP Address that delivered the payload

Searching with Ctrl+F we can search for the suspicious PID 3644 (Figures 7, 8). We notice there are two successful connection establishments through TCPv4 and the implicated IP. This was associated with the coreupdater.ex file.

Answer: 203.78.103.109 through Port 443.

```
user@user-pc:~$ volatility -f citadeldc01.mem --profile=Win2012R2x64 netscan | tee netscan.out
```

Figure 6

CLOSED	684	SVHOST.exe		ESTABLISHED	3644
9219 0x20Fc7590	TCPv4	10.42.85.10:62613			
coreupdater.ex					
9220 0x21268600	UDPV4	0.0.0.0:0	*		
1368 dns.exe		2020-0			
9221 0x21268600	UDPV6	::			
1368 dns.exe		2020-0			
9222 0x21268ec0	UDPV4	0.			
1368 dns.exe		2020-0			
9223 0x21268ec0	UDPV6	::			
1368 dns.exe		2020-0			
9224 0x21285410	UDPV4	0.			
1368 dns.exe		2020-0			
9225 0x21285ba0	UDPV4	0.			
1368 dns.exe		2020-0			
9226 0x212be560	UDPV4	0.			
1368 dns.exe		2020-0			
9227 0x212becf0	UDPV4	0.			
1368 dns.exe		2020-0			
9228 0x217fc510	UDPV4	0.			
1368 dns.exe		2020-0			
9229 0x217fccf0	UDPV4	0.			
1368 dns.exe		2020-0			
9230 0x21807880	UDPV4	0.0.0.0:0			

Figure 7

18129 0x60182590	TCPv4	10.42.85.10:62613	203.78.103.109:443	ESTABLISHED	3644
18130 0x601cd00	TCPv6	fe80::2dcf:e660:be73:d220:135	fe80::2dcf:e660:be73:d220:62779		
CLOSED	684	svchost.exe			
18131 0x60426560	UDPV4	0.			
1368 dns.exe	UDPV4	2020-0			
18132 0x60426cf0	UDPV4	0.			
1368 dns.exe	UDPV4	2020-0			
18133 0x60442410	UDPV4	0.			
1368 dns.exe	UDPV4	2020-0			
18134 0x60442ba0	UDPV4	0.			
1368 dns.exe	UDPV4	2020-0			
18135 0x604a5600	UDPV4	0.			
1368 dns.exe	UDPV4	2020-0			
18136 0x604a5600	UDPV6	::			
1368 dns.exe	UDPV6	2020-0			
18137 0x604a5ec0	UDPV4	0.			
1368 dns.exe	UDPV4	2020-0			
18138 0x604a5ec0	UDPV6	::			
1368 dns.exe	UDPV6	2020-0			
18139 0x604bc560	UDPV4	0.			
1368 dns.exe	UDPV4	2020-0			
18140 0x604bccf0	UDPV4	0.			

Figure 8

### 6c. What IP Address is the malware calling to?

**Answer:** 10.42.85.10 through port 62613 (Figures 7, 8)

### 6d. Where is this malware on disk?

**Answer:** C:\Windows\System32\coreupdater.exe (Figure 9)

path: C:\Windows\system32\dwm.exe					
0xfffffe00062fe7700:coreupdater.exe	3644	2244	0	-----	2020-09-19 03:56:37 UTC+0000
audit: \Device\HarddiskVolume1\Windows\System32\coreupdater.exe					
0xfffffe00060ce2080:ServerManager.	400	1904	10	0	2020-09-19 04:36:03 UTC+0000
audit: \Device\HarddiskVolume2\Windows\System32\ServerManager.exe					
cmd.					

Figure 9

### 6e. When did it first appear?

**Answer:** Sat, Sept 19, 2020 at 2:39:26 GMT (Figure 10)

```
HTTP/1.0 200 OK
Server: SimpleHTTP/0.6 Python/2.7.18
Date: Sat, 19 Sep 2020 02:39:26 GMT
Content-type: text/html; charset=UTF-8
Content-Length: 228
```

Figure 10

### 6f. Did someone move it?

**Answer:** We can see that it was moved the admin downloads into the Windows\System32 directory. (Figures 11, 12, 13, 14)

2020-09-19 03:24:12		coreupdater.exe	.exe	87137	FileCreate	1	84880
2020-09-19 03:24:12		coreupdater.exe	.exe	87137	FileCreate Close	1	84880
2020-09-19 03:24:12		coreupdater.exe	.exe	87137	FileDelete Close	1	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	FileCreate	2	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	FileCreate Close	2	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	DataTruncation	2	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	DataTruncation Close	2	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	DataExtend	2	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	DataOverwrite DataExtend	2	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	DataOverwrite DataExtend Basic...	2	84880
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	DataOverwrite DataExtend Basic...	2	84880
2020-09-19 03:24:12		coreupdater[1].exe	.exe	76711	FileDelete Close	12	87050
2020-09-19 03:24:12		coreupdater.exe.2424urv.partial	.partial	87137	RenameOldName	2	84880
2020-09-19 03:24:12		coreupdater.exe	.exe	87137	RenameNewName	2	84880
2020-09-19 03:24:12		coreupdater.exe	.exe	87137	RenameNewName Close	2	84880
2020-09-19 03:24:50		coreupdater.exe	.exe	87137	RenameOldName	2	84880

Figure 11

Line	Tag	Update Timestamp	Parent Path	Name	Extension	Entry Number	Update Reasons	Sequence Number	P
=	[ ]	=	[ ]	[ ]	[ ]	=	84880 [ ]	=	*
16019	[ ]	2020-09-17 16:46:26		Downloads		84880	ObjectIdChange Close	1	
16018	[ ]	2020-09-17 16:46:26		Downloads		84880	ObjectIdChange	1	
15873	[ ]	2020-09-17 16:46:25		Downloads		84880	BasicInfoChange Close	1	
15872	[ ]	2020-09-17 16:46:25		Downloads		84880	BasicInfoChange	1	
14883	[ ]	2020-09-17 16:46:16		Downloads		84880	BasicInfoChange Close	1	
14882	[ ]	2020-09-17 16:46:16		Downloads		84880	BasicInfoChange	1	
14881	[ ]	2020-09-17 16:46:16		Downloads		84880	BasicInfoChange Close	1	
14880	[ ]	2020-09-17 16:46:16		Downloads		84880	BasicInfoChange	1	
14182	[ ]	2020-09-17 16:46:15		Downloads		84880	SecurityChange BasicInfoChange...	1	
14181	[ ]	2020-09-17 16:46:15		Downloads		84880	SecurityChange BasicInfoChange	1	
14180	[ ]	2020-09-17 16:46:15		Downloads		84880	SecurityChange	1	
14179	[ ]	2020-09-17 16:46:15		Downloads		84880	FileCreate Close	1	
14178	[ ]	2020-09-17 16:46:15		Downloads		84880	FileCreate	1	

Figure 12

2020-09-19 03:40:42		coreupdater.exe	.exe	26213	RenameNewName	4	3254
2020-09-19 03:40:42		coreupdater.exe	.exe	26213	RenameNewName Close	4	3254
2020-09-19 03:40:42		coreupdater.exe	.exe	26213	SecurityChange	4	3254
2020-09-19 03:40:42		coreupdater.exe	.exe	26213	SecurityChange Clo...	4	3254
2020-09-19 03:40:49		coreupdater.exe	.exe	26213	StreamChange	4	3254
2020-09-19 03:40:49		coreupdater.exe	.exe	26213	StreamChange Close	4	3254

Figure 13

Drag a column header here to group by that column							Enter text to search...	Find
Line	Tag	Update Timestamp	Parent Path	Name	Extension	Entry Number	Update Reasons	Sequence N
35946	[ ]	2020-09-19 03:40:42		System32		3254 [ ]	3254 ObjectIdChange	=

Figure 14

## 6g. What were the capabilities of this malware?

**Answer:** This malware is capable of defence evasion, discovery of victim environment, command and control protocols, anti-static analysis, and micro-data manipulation (Figure 15).

The screenshot shows a dark-themed interface for a dynamic analysis sandbox. At the top, a warning message reads: "The sandbox Lastline flags this file as: MALWARE TROJAN". Below this, under "MITRE ATT&CK Tactics and Techniques", there are three expanded categories: "Defense Evasion" (TA0005), "Discovery" (TA0007), and "Command and Control" (TA0011). Under "Malware Behavior Catalog Tree", there are three expanded categories: "Anti-Static Analysis" (OB0002), "Defense Evasion" (OB0005), and "Data" (OB0004).

Figure 15

## 6h. Is this malware easily obtained?

**Answer:** Yes, it is available through metasploit, shelma, and rozena. This can be seen on the VirusTotal page when viewing the coreupdater.exe hash.

## 6i. Was this malware installed with persistence on any machine?

**Answer:** The malware created a service to run on startup on both the DC (Figure 16) and Desktop (Figure 17) as well as a registry key on both systems.

CITADEL-DC01.C137.local	2020-09-19 04:39:59	7045	Name: AccessData Driver	StartType: demand start
CITADEL-DC01.C137.local	2020-09-19 03:56:55	7045	Name: pmhrio	StartType: demand start
CITADEL-DC01.C137.local	2020-09-19 03:44:29	7045	Name: mszhao	StartType: demand start
CITADEL-DC01.C137.local	2020-09-19 03:27:49	7045	Name: coreupdater	StartType: auto start
CITADEL-DC01.C137.local	2020-09-19 03:25:44	7045	Name: outmgo	StartType: demand start

Figure 16 - DC

DESKTOP-SDN1RPT.C137.local	2020-09-19 05:10:38	7045	Name: AccessData Driver	StartType: demand start
DESKTOP-SDN1RPT.C137.local	2020-09-19 05:08:59	7045	Name: WPD File System driver	StartType: demand start
DESKTOP-SDN1RPT.C137.local	2020-09-19 03:43:14	7045	Name: nehgye	StartType: demand start
DESKTOP-SDN1RPT.C137.local	2020-09-19 03:42:42	7045	Name: coreupdater	StartType: auto start
DESKTOP-SDN1RPT	2020-09-18 05:54:01	7045	Name: VMware Snapshot Provider	StartType: demand start

Figure 17 - Desktop

### 6i.1. When?

**Answer:** The installation of the service, "coreupdater", first occurred on the DC at 2:27:49(Figure 16) and at 2:42:42 on DESKTOP-SDN1RPT. (Figure 17)

## 6i.2. Where?

**Answer:** Inside System32 and on the Desktop (Figures 18, 19, 20, 21)

This screenshot shows a list of processes created. The title bar says "Process and service actions". The list includes:

- %SAMPLEPATH%\10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6.exe
- %SAMPLEPATH%\file.exe
- C:\Users\Elijah\AppData\Local\Temp\10f3b92002bb98467334161cf85d0be9a0c1cfda6.exe
- C:\Windows\System32\wuapihost.exe

Figure 18

This screenshot shows a list of shell commands run. The title bar says "Shell Commands". The list includes:

- "%SAMPLEPATH%\10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6.exe"
- "%SAMPLEPATH%\file.exe"
- C:\Users\Elijah\AppData\Local\Temp\10f3b92002bb98467334161cf85d0be9a0c1cfda6.exe
- C:\Windows\System32\wuapihost.exe -Embedding

Figure 19

This screenshot shows a list of processes terminated. The title bar says "Processes Terminated". The list includes:

- %SAMPLEPATH%\10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6.exe
- %SAMPLEPATH%\file.exe
- %windir%\System32\svchost.exe -k WerSvcGroup
- C:\Windows\System32\wuapihost.exe
- wmiadap.exe /F /T /R

Figure 20

Processes Tree			
2236 - %windir%\System32\svchost.exe -k WerSvcGroup			
2564 - C:\Users\Elijah\AppData\Local\Temp\10f3b92002bb98467334161cf85d0be9a0c1cfda6.exe			
2596 - %SAMPLEPATH%			
2896 - wmiadap.exe /F /T /R			
2940 - %windir%\system32\wbem\wmiprvse.exe			
3528 - %WINDIR%\explorer.exe			
4060 - %SAMPLEPATH%\10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6.exe			
6656 - 'C:\Users\user\Desktop\program.exe'			

Figure 21

## 7. What malicious IP Addresses were involved? (Dan and Heather)

**Answer:** Yes

### 7a. Were any IP Addresses from known adversary infrastructure?

**Answer:** Yes. 203.78.103.109 has been compromised with suspicious communications files (Figure 22). These files have been flagged by multiple threat detection companies. 194.61.254.102 has been known to have been a hostile IP. The IP has been associated with RDP Brute Force attacks as noted by VirusTotal (Figures 23, 24).

Communicating Files (11) ⓘ			
Scanned	Detections	Type	Name
2024-02-14	62 / 71	Win32 EXE	coreupdater.exe
2023-07-31	32 / 59	Powershell	test.ps1
2023-12-18	25 / 59	Text	testps1.ps1
2023-03-31	20 / 59	Powershell	decode.ps1
2021-09-09	19 / 58	unknown	file2
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
2023-03-31	32 / 59	Powershell	powershell.ps1

Figure 22

Files Referring (50) ⓘ			
Scanned	Detections	Type	Name
2024-02-29	2 / 57	Network capture	case001.pcap

Figure 23

```

HTTP Requests
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMy%2BghUNoZ7OrUETfACEAilzVJfGSR
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMy%2BghUNoZ7OrUETfACEAilzVJfGSR
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMy%2BghUNoZ7OrUETfACEA8sEMibB
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAtb9ltp%2FvQi
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMy%2BghUNoZ7OrUETfACEA8sEMibB
+ GET
+ http://ocsp.msocsp.com/MFQwUjBQME4wTDAJBgUrDgMCGgUABBSIGkp%2Fv9GUvNUu1EP06Tu7%2BChyAQukZ47RGw9V5xCdyo010%2FrzEqXLNoCEAADTV
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAtb9ltp%2FvQi
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ50obx%2Fh0Ztl%2Bz8SiPi7wEWVxDlQUTiJUIBiV5uNu5g%2F6%2BrkS7QYXjkCEAqvpsXKY8
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBTBL0V27RVZ7LBduom%2FnYB45SPUEwQU5Z1ZMIJHWMy%2BghUNoZ7OrUETfACEAilzVJfGSR
+ GET
+ http://ocsp.digicert.com/MFEwTzBNMEswSTAJBgUrDgMCGgUABBSAUQYBMq2awn1Rh6Doh%2FsBYgFV7gQUA95QNVbRTLtm8KPiGxvDI7I90VUCEAH9o%2BtuynX

```

Figure 24

## 7b. Are these pieces of adversary infrastructure involved in other attacks around the time of the attack?

**Answer:** Yes, as we can see from the following screenshot the hash value has been flagged as compromised by 62/71 vendors on AlienVault. The coreupdater.exe has been recognized by several anti-malware detection companies in multiple attacks. AlienVault is still receiving updates, even as recently as 2 days ago, regarding this hash (Figure 25).

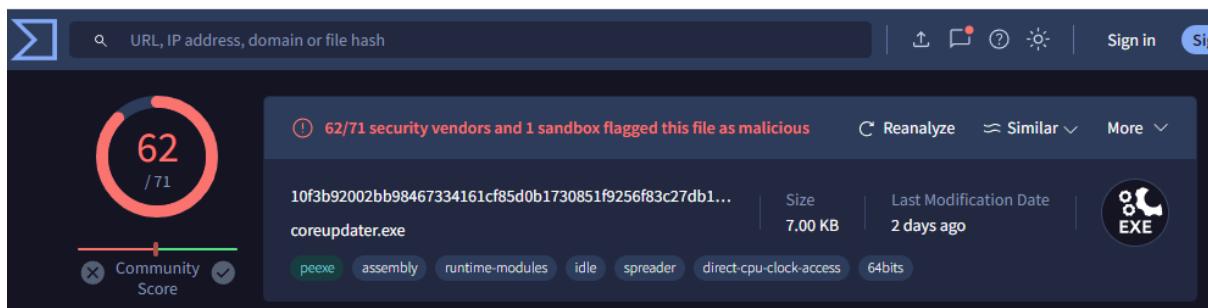


Figure 25

## 8. Did the attacker access any other systems? (Dan and Heather)

**Answer:** Yes, other systems were accessed.

## 8a. How?

**Answer:** As we can see from the following screenshot and mentioned before, the coreupdate.exe has the ability to write itself to other portions of the system (Figure 26). The attack was able to gain access to DESKTOP-SDN1RPT.C137.local via RDP from the DC using the admin account. The pcap has revealed an RDP connection after initial access (Figure 27). This connection between malicious IP and the victim address is integral for finding the answer to what has happened.

DESKTOP-SDN1RPT.C137.local	2020-09-19 03:36:24	4624	DESKTOP-SDN1RPT (10.42.85.10)	Target: C137\Administrator	LogonType 10
----------------------------	---------------------	------	-------------------------------	----------------------------	--------------

Figure 26

766794 2020-09-19 02:36:25.637848	10.42.85.10 10.42.85.115 TCP	66 389 → 50706 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
766800 2020-09-19 02:36:25.638290	10.42.85.10 10.42.85.115 TCP	1514 389 → 50706 [ACK] Seq=1 Ack=351 Win=65536 Len=1460 [TCP segment of a reassemble
766801 2020-09-19 02:36:25.638291	10.42.85.10 10.42.85.115 LDAP	1208 searchResEntry(37) "<ROOT>"   searchResDone(37) success [2 results]
766805 2020-09-19 02:36:25.639241	10.42.85.10 10.42.85.115 TCP	60 389 → 50706 [ACK] Seq=2615 Ack=2184 Win=65536 Len=0
766806 2020-09-19 02:36:25.639762	10.42.85.10 10.42.85.115 LDAP	264 bindResponse(39) success
766808 2020-09-19 02:36:25.646090	10.42.85.10 10.42.85.115 LDAP	496 SASL GSS-API Integrity: searchResEntry(40) "DC=C137,DC=local" searchResRef(40)
766810 2020-09-19 02:36:25.647966	10.42.85.10 10.42.85.115 TCP	66 389 → 50707 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460 WS=256 SACK_PERM=1
766814 2020-09-19 02:36:25.650111	10.42.85.10 10.42.85.115 TCP	60 389 → 50707 [ACK] Seq=1 Ack=1908 Win=65536 Len=0
766816 2020-09-19 02:36:25.650582	10.42.85.10 10.42.85.115 LDAP	264 bindResponse(43) success
766818 2020-09-19 02:36:25.651271	10.42.85.10 10.42.85.115 LDAP	206 SASL GSS-API Integrity: searchResEntry(44) "<ROOT>" searchResDone(44) success
766820 2020-09-19 02:36:25.651742	10.42.85.10 10.42.85.115 LDAP	200 SASL GSS-API Integrity: searchResEntry(45) "CN=Default-First-Site-Name,CN=Sites
766822 2020-09-19 02:36:25.652201	10.42.85.10 10.42.85.115 LDAP	108 SASL GSS-API Integrity: searchResDone(46) success [2 results]
766921 2020-09-19 02:36:25.964745	10.42.85.10 10.42.85.115 TCP	60 389 → 50707 [ACK] Seq=509 Ack=2300 Win=65280 Len=0
766922 2020-09-19 02:36:25.964746	10.42.85.10 10.42.85.115 TCP	60 389 → 50707 [RST, ACK] Seq=509 Ack=2300 Win=0 Len=0
766950 2020-09-19 02:36:26.062182	10.42.85.10 10.42.85.115 TCP	60 389 → 50706 [RST, ACK] Seq=3321 Ack=2962 Win=0 Len=0

Figure 27

## 8b. When?

**Answer:** The attacker was able to gain remote access through the RDP protocol using an admin account (Figure 28) on the 19th at 2:36 (Figures 28, 29). This allowed the attacker access into the system to then start performing reconnaissance. The coreupdater.exe has a timestamp noting September 19, 2020 at 3:56:37 UTC+0000 (Figure 29). This backs up the theory of the coreupdater.exe performing actions on our system. We know access to the HKLM\SOFTWARE\ hives started as early as 2:43 (Figure 30). We can then begin to explore what information is accessed, when, and what was done with it.

DESKTOP-SDN1RPT.C137.local	2020-09-19 03:36:24	4624	DESKTOP-SDN1RPT (10.42.85.10)	Target: C137\Administrator	LogonType 10
----------------------------	---------------------	------	-------------------------------	----------------------------	--------------

Figure 28

```

path: C:\Windows\system32\dwm.exe
0xfffffe000062fe7700:coreupdater.exe 3644 2244 0 ----- 2020-09-19 03:56:37 UTC+0000
audit: \Device\HddiskVolume1\Windows\System32\coreupdater.exe
0xfffffe000060ce2080:ServerManager. 400 1904 10 0 2020-09-19 04:36:03 UTC+0000
audit: \Device\HddiskVolume2\Windows\System32\ServerManager.exe
cmd.

```

Figure 29

A	B	C	D	E	F		
1	Time	Entry Location	Entry	Enabled	Category	Profile	Description
872	10/23/1937 2:43 AM	HKEY_SOFTWARE\Microsoft\Windows\CurrentVersion\Run\	coreupdater.exe	enabled	Logon	System-wide	Windows PowerShell

Figure 30

## 8c. Did the attacker steal or access any data?

**Answer:** Yes

### 8c.1. When?

**Answer:** By going through the Hive files, again, we can get insight to where the attacker looked into the system.

- We can check for recently accessed files with MRU, which arranges the most recently used files at the top of the list.
- We can see that the admin accessed the “Secret” folder in the “FileShare” directory.
- Within the Desktop portion of the search we also notice there is a new zip called “loot” as well as the previously seen “Secret” zip files in the FileShare directory (Figures 31, 32).

Parent Path	File Name	Extension	Created@x10	Last Modified@x10
\recent	lnk	.lnk	=	=
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	PortalGunPlans.lnk	.lnk	2020-09-18 22:34:02	2020-09-19 03:32:0
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	NoJerry.lnk	.lnk	2020-09-18 22:29:54	2020-09-19 03:31:5
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Secret.lnk	.lnk	2020-09-18 22:29:54	2020-09-19 03:35:0
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Szechuan Sauce.lnk	.lnk	2020-09-18 22:35:59	2020-09-19 03:32:2
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	SECRET_beth.lnk	.lnk	2020-09-18 22:39:22	2020-09-19 03:32:1
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Beth_Secret.lnk	.lnk	2020-09-19 03:35:07	2020-09-19 03:35:0

Figure 31

Parent Path	File Name	Extension	Created@x10	Last Modified@x10
\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	.lnk	.lnk	=	=
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	My Social Security Number.lnk	.lnk	2020-09-19 03:45:34	2020-09-19 03:45:3
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Plans.lnk	.lnk	2020-09-19 03:45:39	2020-09-19 03:45:3
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Portal_gun.lnk	.lnk	2020-09-19 03:45:54	2020-09-19 03:45:5
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Documents.lnk	.lnk	2020-09-19 03:45:34	2020-09-19 03:45:5
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	loot.lnk	.lnk	2020-09-19 03:46:18	2020-09-19 03:46:1
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Thoughts.lnk	.lnk	2020-09-19 03:47:39	2020-09-19 03:47:3
.\Users\Administrator\AppData\Roaming\Microsoft\Windows\Recent	Desktop.lnk	.lnk	2020-09-19 03:47:39	2020-09-19 03:47:3

Figure 32

Zipped files are also important to note. This is because it makes the extraction of information easier and faster for attackers.

Looking more into these files we can confirm that they were created by the recently accessed, compromised admin account. This is a step to finding out that something was actually stolen (Figures 33, 34).

Name	Extension	Entry Number	Seq...	Paren...	... Parent...	Upd...	Update Timestamp	Update Reasons
Secret.zip	.zip	87102	2	86963	7	903...	2020-09-19 03:34:18	FileDelete Close
Secret.zip	.zip	87102	2	86963	7	902...	2020-09-19 03:32:39	SecurityChange RenameNewName
Secret.zip	.zip	87102	2	86963	7	902...	2020-09-19 03:32:39	SecurityChange RenameNewName
Secret.zip	.zip	87101	2	86963	7	902...	2020-09-19 03:32:39	RenameOldName
Secret.zip	.zip	87101	2	86963	7	902...	2020-09-19 03:32:39	FileCreate Close
Secret.zip	.zip	87101	2	86963	7	902...	2020-09-19 03:32:39	FileCreate

Figure 33

Name	Extension	Entry Number	Sequenc...	Parent E...	Pare...	Pa...	Update Seq...	Update Timestamp	Update Reasons
loot.zip	.zip	87470	2	88824	2	26375072	2020-09-19 03:47:09	FileDelete Close	
loot.zip	.zip	87470	2	88824	2	26372080	2020-09-19 03:46:18	ObjectIdChange Close	
loot.zip	.zip	87470	2	88824	2	26372000	2020-09-19 03:46:18	ObjectIdChange	
loot.zip	.zip	87470	2	88824	2	26371920	2020-09-19 03:46:18	RenameNewName Close	
loot.zip	.zip	87470	2	88824	2	26371840	2020-09-19 03:46:18	RenameNewName	

Figure 34

We can then trace these files to find out when the attacker actually got the files out of the system. This is the point of the final file movement before extraction (Figures 35, 36).

Figure 35

FileSize	Type	Flags	AccessCount	SyncTime	CreationTime	ExpiryTime	ModifiedTime	AccessedTime	PostCheckTime	SyncCount	ExemptionDelta	Url
0	2097153	0	2	19/09/2020 3:15:00 AM	0	15/10/2020 3:15:00 AM	19/09/2020 3:15:00 AM	19/09/2020 3:15:00 AM	0	0	0	Visited: Administrator@file:///C:/FileShare/Secret/NoLery.txt
0	2097153	0	5	18/09/2020 10:32:18 PM	0	14/10/2020 10:32:18 PM	18/09/2020 10:32:18 PM	18/09/2020 10:32:18 PM	0	0	0	Visited: Administrator@res://C:/Windows/system32/mmcndmgr.dll
0	2097153	0	2	19/09/2020 3:32:02 AM	0	15/10/2020 3:32:02 AM	19/09/2020 3:32:02 AM	19/09/2020 3:32:02 AM	0	0	0	Visited: Administrator@file:///C:/FileShare/Secret/PortalGunPlans.t
0	2097153	0	2	19/09/2020 3:32:21 AM	0	15/10/2020 3:32:21 AM	19/09/2020 3:32:21 AM	19/09/2020 3:32:21 AM	0	0	0	Visited: Administrator@file:///C:/FileShare/Secret/Szechuan%20Sa
0	2097153	0	2	19/09/2020 3:32:13 AM	0	15/10/2020 3:32:13 AM	19/09/2020 3:32:13 AM	19/09/2020 3:32:13 AM	0	0	0	Visited: Administrator@file:///C:/FileShare/Secret/SECRET_bethbt
0	2097153	0	2	19/09/2020 3:23:01 AM	0	15/10/2020 3:23:01 AM	19/09/2020 3:23:01 AM	19/09/2020 3:23:01 AM	0	0	0	Visited: Administrator@res://setup/dl/HardAdmin.htm
0	2097153	0	2	19/09/2020 3:23:41 AM	0	15/10/2020 3:23:41 AM	19/09/2020 3:23:41 AM	19/09/2020 3:23:41 AM	0	0	0	Visited: Administrator@http://194.61.24.102/
0	2097153	0	1	19/09/2020 3:23:41 AM	0	15/10/2020 3:23:41 AM	19/09/2020 3:23:41 AM	19/09/2020 3:23:41 AM	0	1	0	Visited: Administrator@http://194.61.24.102/favicon.ico
0	2097153	0	1	19/09/2020 3:35:07 AM	0	15/10/2020 3:27:58 AM	19/09/2020 3:35:07 AM	19/09/2020 3:35:07 AM	0	1	0	Visited: Administrator@file:///C:/FileShare/Secret/Beth_Secret.b

Figure 36

## **9. What was the network layout of the victim network? (Dan and Heather)**

**Answer:** Microsoft Windows 8 - Win8SPOx64, Win81U1x64

Windows Server - Win2012R2x64 (Figure 37)

```
user@user-pc:~/Desktop/Case001$ volatility -f citadeldc01.mem imageinfo
Volatility Foundation Volatility Framework 2.6.1
INFO    : volatility.debug      : Determining profile based on KDBG search...
          Suggested Profile(s) : Win8SP0x64, Win8U1x64, Win2012R2x64_18340, Win2012R2x64, Win2012x64, Win8SP1x6
4_18340, Win8SP1x64
          AS Layer1 : SkipDuplicatesAMD64PagedMemory (Kernel AS)
          AS Layer2 : FileAddressSpace (/home/user/Desktop/Case001/citadeldc01.mem)
          PAE type : No PAE
          DTB   : 0x1a7000L
          KDBG  : 0xf800cba9ba20L
Number of Processors : 2
Image Type (Service Pack) : 0
          KPCR for CPU 0 : 0xfffffff800cbaea000L
          KPCR for CPU 1 : 0xfffffd0019fd55000L
          KUSER_SHARED_DATA : 0xfffffff78000000000L
Image date and time : 2020-09-19 04:39:59 UTC+0000
Image local date and time : 2020-09-18 21:39:59 -0700
user@user-pc:~/Desktop/Case001$
```

Figure 37

# References

1. Volatility is an open-source memory forensics tool  
<https://volatilityfoundation.org/>
2. Wireshark is an open-source network scanning tool  
<https://www.wireshark.org/>
3. VirusTotal is an online services used to analyzes suspicious files and URLs to detect types of Malware or malicious software  
<https://www.virustotal.com/gui/file/9af8a2d9ca5d904b9ca6696016b2a794ef7eb97693ccca22df2a367305d31b88>
4. Metasploit is a Framework used to determine the source of malware.  
<https://www.metasploit.com>
5. AlienVault is an online free resource for identifying whether a hash, website, or file is safe to use or malware.  
<https://www.alienvault.com>

