

DIGITAL FORENSIC

LAB:

THE STOLEN SZECHUAN

SAUCE

OVERVIEW

As part of my ongoing digital forensics training, I conducted an investigation into a simulated data breach involving the theft of a proprietary Szechuan sauce recipe. The objective was to uncover how the breach occurred, trace the attacker's activities, and identify the data exfiltration process.

Artifacts Under Investigation:

- **Disk Images:** Examined the file systems for evidence of tampering, deleted files, and forensic metadata related to the stolen recipe.
- **Memory Dumps:** Analyzed running processes, network connections, and any signs of malware persistence.
- **Network Capture Files (PCAPs):** Inspected network traffic for malicious connections, IP addresses, and exfiltration attempts.
- **Event Logs:** Focused on login events, RDP connections, and other suspicious activity timestamps to piece together the timeline.
- **Deleted Files and Metadata:** Recovered deleted data, including fragments of files that could be linked to the exfiltrated recipe.

OBJECTIVES

- What's the operating system of the server?
- What's the operating system of the desktop?
- What's the local time of the server?
- Was there a breach?
- What was the initial entry vector?
- Was malware used?
- What malicious IP Addresses were involved?
- Did the attacker access any other systems?
- What was the network layout of the victim network?
- What architecture changes should be made immediately?

- Did the attacker steal the Szechuan sauce? If so, what time?
 - Did the attacker steal or access any other sensitive files? If so what times?
 - Finally, when was the last known contact with the adversary?
- Investigation

INVESTIGATIONS

- What's the operating system of the server?

```
-----
winver v.20200525
(Software) Get Windows version & build info

ProductName           Windows Server 2012 R2 Standard Evaluation
BuildLab              9600.winblue_gdr.140221-1952
BuildLabEx            9600.17031.amd64fre.winblue_gdr.140221-1952
RegisteredOrganization
RegisteredOwner       Windows User
InstallDate           2020-09-17 16:43:59Z
```

Using RegRipper with the winver plugin, I extracted the server's operating system details. The information was located in the Registry key: HKLM\Software\Microsoft\Windows NT\CurrentVersion. This provided crucial system version and build details for the investigation.

- What's the local time of the server?

```
-----
timezone v.20200518
(System) Get TimeZoneInformation key contents

TimeZoneInformation key
ControlSet001\Control\TimeZoneInformation
LastWrite Time 2020-09-17 17:56:13Z
DaylightName -> @tzres.dll,-211
StandardName -> @tzres.dll,-212
Bias -> 480 (8 hours)
ActiveTimeBias -> 420 (7 hours)
TimeZoneKeyName-> Pacific Standard Time
-----
```

I also used RegRipper but this time with timezone plugin from the location:

HKLM\System\CurrentControlSet\Control\TimeZoneInformation\

- Was there a breach?

Yes

- What was the initial entry vector?

No.	Time	Source	Destination	Protocol	Length	Info
84320	15665.944030	194.61.24.102	10.42.85.10	TCP	58	64385 → 443 [SYN] Seq=0 Win=1024 L
84321	15665.944047	194.61.24.102	10.42.85.10	TCP	54	64385 → 80 [ACK] Seq=1 Ack=1 Win=1
84334	15678.998880	194.61.24.102	10.42.85.10	TCP	74	38088 → 3389 [SYN] Seq=0 Win=64240
84335	15678.999168	10.42.85.10	194.61.24.102	TCP	74	3389 → 38088 [SYN, ACK] Seq=0 Ack=
84336	15678.999436	194.61.24.102	10.42.85.10	TCP	66	38088 → 3389 [ACK] Seq=1 Ack=1 Win
84337	15678.999574	194.61.24.102	10.42.85.10	TCP	66	38088 → 3389 [RST, ACK] Seq=1 Ack=
84338	15679.001921	194.61.24.102	10.42.85.10	TCP	74	38090 → 3389 [SYN] Seq=0 Win=64240
84339	15679.002103	10.42.85.10	194.61.24.102	TCP	74	3389 → 38090 [SYN, ACK] Seq=0 Ack=
84340	15679.002256	194.61.24.102	10.42.85.10	TCP	66	38090 → 3389 [ACK] Seq=1 Ack=1 Win
84341	15679.002281	194.61.24.102	10.42.85.10	TCP	74	38092 → 3389 [SYN] Seq=0 Win=64240
84342	15679.002378	10.42.85.10	194.61.24.102	TCP	74	3389 → 38092 [SYN, ACK] Seq=0 Ack=
84343	15679.002518	194.61.24.102	10.42.85.10	TCP	66	38092 → 3389 [ACK] Seq=1 Ack=1 Win
84344	15679.025041	194.61.24.102	10.42.85.10	TCP	74	38094 → 3389 [SYN] Seq=0 Win=64240
84345	15679.025196	194.61.24.102	10.42.85.10	TCP	74	38096 → 3389 [SYN] Seq=0 Win=64240
84346	15679.025244	10.42.85.10	194.61.24.102	TCP	74	3389 → 38094 [SYN, ACK] Seq=0 Ack=
84347	15679.025292	10.42.85.10	194.61.24.102	TCP	74	3389 → 38096 [SYN, ACK] Seq=0 Ack=

I identified brute-forcing activity, which revealed the attacker's entry point. I filtered the network traffic using `ip.addr == 194.61.24.102` and `tcp` to isolate the relevant packets.

- Was malware used?

```

—(myenv)—(root@kali)—[/home/kali/DC01-memory]
—# vol -f citadeldc01.mem windows.pslist > processeslist.txt
3724 452 spoolsv.exe 0xe000631cb900 13 - 0 False 2020-09-19 03:29:40
.000000 UTC N/A Disabled
3644 2244 coreupdater.exe 0xe00062fe7700 0 - 2 False 2020-09-19 03:56:37
.000000 UTC 2020-09-19 03:56:52.000000 UTC Disabled

```

Yes, a Trojan malware was detected during the investigation. The process began with analyzing network traffic in Wireshark, where I identified a suspicious file within the objects. I exported this file for further analysis. Next, I generated a hash of the file and submitted it to VirusTotal, an online malware detection and threat intelligence platform. The VirusTotal scan revealed that the file was flagged as a Trojan by multiple antivirus engines,

This screenshot shows the VirusShare analysis interface for the file `coreupdater.exe`. On the left, a circular progress indicator shows a score of 65 out of 72. The main header indicates that 65 out of 72 security vendors flagged the file as malicious. The file's SHA-256 hash is `10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfd6a`. The file size is 7.00 KB, and the last analysis was performed 21 days ago. The file icon is labeled `EXE`.

Property	Value
Score	65 / 72
Vendors Flagged	65/72 security vendors
SHA-256 Hash	10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfd6a
File Name	coreupdater.exe
Size	7.00 KB
Last Analysis Date	21 days ago
File Type	EXE

192.61.24.102 delivered the payload through a get request that the malicious file was downloaded.

```
> GET /coreupdater.exe HTTP/1.1\r\n
  Accent: */*\r\n
```

The IP address the malware is calling to according to VirusTotal and also

203.78.103.109		5 / 94		18362		TH	
9212	0x20e28d10	TCPv6	fe80::2dcf:e660:be73:d220	49155	fe80::2dcf:e660:be73:d220	62777	CLOSED 460 lsass.exe -
9213	0x20f52a00	TCPv6	fe80::2dcf:e660:be73:d220	135	fe80::2dcf:e660:be73:d220	62779	CLOSED 684 svchost.exe N/A
9214	0x20fc7590	TCPv4	10.42.85.10	62613	203.78.103.109	443	ESTABLISHED 3644 coreupdater.ex N/A
9215	0x20ffffe50	TCpv4	0.0.0.0	62475	0.0.0.0	0	LISTENING 3724 spoolsv.exe N/A
9216	0x20ffffe50	TCpv6	::	62475	::	0	LISTENING 3724 spoolsv.exe N/A

Where is the malware on disk?

I identified the file path of the malware by analyzing the hierarchical structure of running processes using Volatility's pstree plugin. This plugin displays processes in a tree-like format, showing parent-child relationships. By carefully examining the process tree, I located a suspicious process and traced its file path to its location on disk. This analysis was crucial in confirming the presence of malware and understanding its execution flow within the system.

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

```

-# vol -f citadelc01.mem windows.pstree > processtree.txt
Progress:    0.00          Scanning layer_name using PdbSignatureScan
Progress:    0.00          Scanning layer_name using PdbSignatureScan
Progress:  100.00          PDB scanning finished

```

38	* 808	492	dwm.exe	0xe0060d09680	7	-	1	False	2020-09-19 01:22:40.000000	UTC	N/A	
			Device\HarddiskVolume2\Windows\System32\dwm.exe "dwm.exe" C:\Windows\System32\dwm.exe									
39	3644	2244	coreupdater.exe	0xe00602f6770	0	-	2	False	2020-09-19 03:56:37.000000	UTC	2020-09-19 03:56:52.000000	
			UTC Device\HarddiskVolume2\Windows\System32\coreupdater.exe - -									
40	3472	3960	explorer.exe	0xe00603171900	39	-	1	False	2020-09-19 04:36:03.000000	UTC	N/A	

When did it first appear?

2020-09-19 03:56:37.000000 UTC

Did someone move it?

Yes, it was moved from downloads to system32.

- What were the capabilities of this malware?

```

3724      spoolsv.exe 0x4afbf20000      0x4afbf51fff      VadS      PAGE_EXECUTE_READWRITE  50  1  Disat
fc 48 89 ce 48 81 ec 00 20 00 00 48 83 e4 f0 e8 .H..H... ..H....
cc 00 00 00 41 51 41 50 52 51 56 48 31 d2 65 48 ....AQAPRQVH1.eH
8b 52 60 48 8b 52 18 48 8b 52 20 48 8b 72 50 48 .R`H.R.H.R H.rPH
0f b7 4a 4a 4d 31 c9 48 31 c0 ac 3c 61 7c 02 2c ..JJM1.H1..<a|.,      fc 48 89 ce 48 81 ec 00 20 00
3724      spoolsv.exe 0x4afc1f0000      0x4afc25afff      VadS      PAGE_EXECUTE_READWRITE  107 1  Disat
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 01 00 00 ..... 4d 5a 90 00 03 00 00 00 04 00
3724      spoolsv.exe 0x4afc070000      0x4afc0a8fff      VadS      PAGE_EXECUTE_READWRITE  57  1  Disat
4d 5a 41 52 55 48 89 e5 48 83 ec 20 48 83 e4 f0 MZARUH..H.. H...
e8 00 00 00 00 5b 48 81 c3 b7 57 00 00 ff d3 48 .....[H...W....H
81 c3 34 b6 02 00 48 89 3b 49 89 d8 6a 04 5a ff ..4...H.;I..j.Z.
d0 00 00 00 00 00 00 00 00 00 00 00 00 f0 00 00 00 ..... 4d 5a 41 52 55 48 89 e5 48 83
3724      spoolsv.exe 0x4afc260000      0x4afc283fff      VadS      PAGE_EXECUTE_READWRITE  36  1  Disat
4d 5a 90 00 03 00 00 00 04 00 00 00 ff ff 00 00 MZ.....
b8 00 00 00 00 00 00 00 40 00 00 00 00 00 00 00 .....@.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00 00 00 00 00 00 00 00 00 00 00 00 00 e0 00 00 00 ..... 4d 5a 90 00 03 00 00 00 04 00
3472      explorer.exe 0x57700000      0x5770ffff      VadS      PAGE_EXECUTE_READWRITE  1  1  Disabled
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....

```

From the result of the malfind plugin ran against the memory dump, The MZ signature in the memory regions of spoolsv.exe and explorer.exe suggests that executable code may have been injected into these processes.

The PAGE_EXECUTE_READWRITE memory protection is highly suspicious, as this combination is commonly used by malware to execute malicious code from memory.

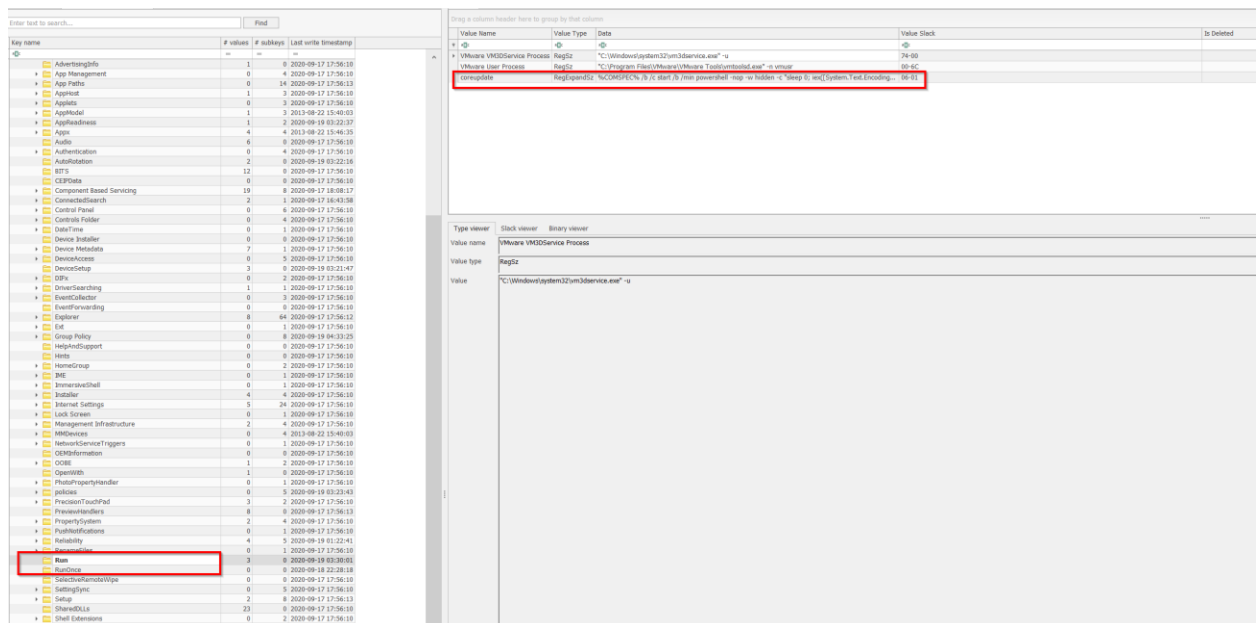
Overall, the malware is capable of the following:

1. **Code Injection:** Inject itself into legitimate processes like spoolsv.exe to evade detection.
2. **Data Exfiltration:** Steal sensitive files or data by uploading them to a command-and-control (C2) server.
3. **Keylogging:** Capture user keystrokes to harvest credentials or other confidential information.

4. **Persistence:** Install itself with mechanisms to survive reboots and maintain long-term access to the system.
5. **Remote Control:** Allow attackers to execute commands, manipulate files, and control the infected system remotely.

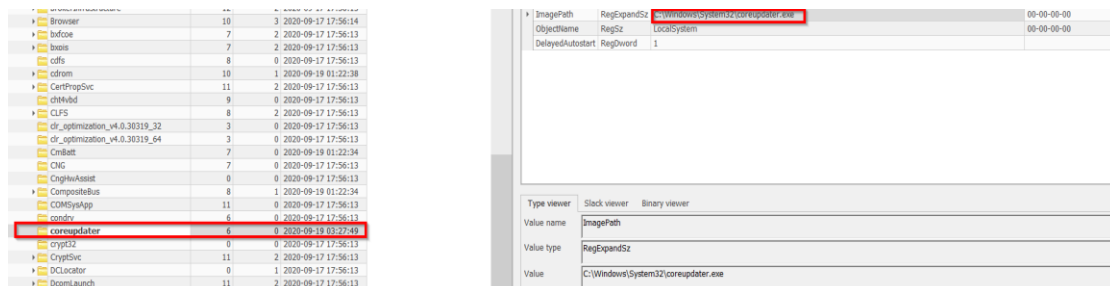
- Is this malware easily obtained?
Yes, can be obtained from meterpreter.

- Was this Malware installed with persistence?



The screenshot shows the Windows Registry Editor with the path `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WMI\Instances\WMI` selected. The right pane shows the `Value Name`, `Value Type`, `Data`, and `Value Stack` columns. The `WMI` value is highlighted in red, showing a `RegDword` type with a value of `1`. The `WMI` value is also highlighted in the left pane.

Where? && when??



The screenshot shows the Windows Registry Editor with the path `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\WMI\Instances\WMI` selected. The right pane shows the `Value Name`, `Value Type`, `Data`, and `Value Stack` columns. The `WMI` value is highlighted in red, showing a `RegDword` type with a value of `1`. The `WMI` value is also highlighted in the left pane.

- What malicious IP addresses were involved??

The IP Address 192.61.24.102 initiated the connection by RDP bruteforce attack. Also virus total confirmed the IP Address 192.61.24.102 and the Ip it is calling to 203.78.103.109 are part of known adversary infrastructure.

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

Yes according to the result below from virus total.

IP	Detections	Autonomous System	Country
104.71.214.69	0 / 94	16625	US
152.195.19.97	0 / 94	15133	US
192.168.0.23	0 / 94	-	-
192.168.0.30	0 / 94	-	-
192.168.0.34	0 / 94	-	-
192.168.0.36	0 / 94	-	-
192.168.0.38	0 / 94	-	-
192.168.0.54	0 / 94	-	-
192.168.0.8	0 / 94	-	-
192.229.211.108	0 / 94	15133	US
20.96.52.198	0 / 94	8075	US
20.99.132.105	0 / 94	8075	US
20.99.133.109	1 / 94	8075	US
20.99.184.37	2 / 94	8075	US
20.99.185.48	1 / 94	8075	US
20.99.186.246	0 / 94	8075	US
203.78.103.109	5 / 94	18362	TH
23.216.147.76	1 / 94	20940	US
23.216.81.152	0 / 94	16625	US

- Did the attacker access any other systems?

Yes, it accessed the RDP of the Domain Controller (DESKTOP-SDN1RPT) at

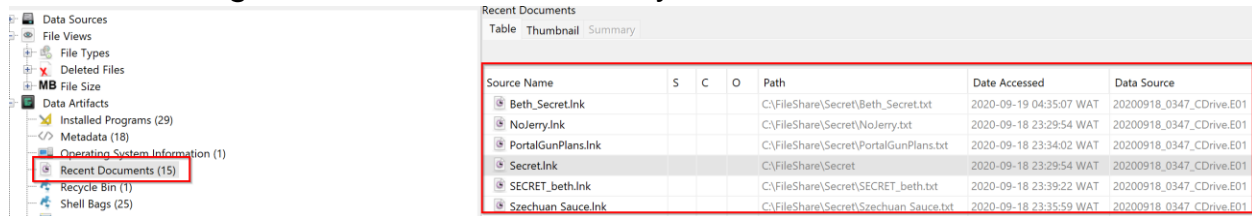
No.	Time	Source
266009	16697.431833	10.42.
266010	16697.431839	10.42.
266012	16697.431987	10.42.
266013	16697.431988	10.42.
266023	16697.442143	10.42.
266025	16697.442247	10.42.
266026	16697.442414	10.42.
266027	16697.442482	10.42.

....j..0.....	..0.0.....	..0.....0.....@.....0.....0..
Administrator...		
C137.LOCAL..0.....0...krbtgt.		
C137.LOCAL....20370913024805Z....20370913024805Z....		
\$...0.....y.....0.0.....	DESKTOP-SDN1RPT	
...0.....20200919033624Z.....L.....		
C137.LOCAL..0.....0...krbtgt.		
C137.LOCAL.9.7050.....	0.0.....0.....0.....0.....0.....	

around 02:36 UTC on the 19th of September.

Did the attacker steal or access any data?

Yes, through from recent document you can see the secret documents.



The screenshot shows a file explorer interface with a sidebar on the left containing categories like 'Data Sources', 'File Views', 'File Types', 'Deleted Files', 'MB File Size', 'Data Artifacts', 'Installed Programs (29)', 'Metadata (16)', 'Operating System Information (1)', 'Recent Documents (15)', 'Recycle Bin (1)', and 'Shell Bags (25)'. The 'Recent Documents (15)' category is selected, displaying a table of documents.

Source Name	S	C	O	Path	Date Accessed	Data Source
Beth_Secret.Ink				C:\FileShare\Secret\Beth_Secret.txt	2020-09-19 04:35:07 WAT	20200918_0347_CDrive.E01
NoJerry.Ink				C:\FileShare\Secret\NoJerry.txt	2020-09-18 23:29:54 WAT	20200918_0347_CDrive.E01
PortalGunPlans.Ink				C:\FileShare\Secret\PortalGunPlans.txt	2020-09-18 23:34:02 WAT	20200918_0347_CDrive.E01
Secret.Ink				C:\FileShare\Secret	2020-09-18 23:29:54 WAT	20200918_0347_CDrive.E01
SECRET_beth.Ink				C:\FileShare\Secret\SECRET_beth.txt	2020-09-18 23:39:22 WAT	20200918_0347_CDrive.E01
Szechuan Sauce.Ink				C:\FileShare\Secret\Szechuan Sauce.txt	2020-09-18 23:35:59 WAT	20200918_0347_CDrive.E01

- What was the network layout of the victim network?



The screenshot shows a terminal window with the following commands and output:

```
(myenv)-(root@kali)-[/home/kali]
# tcpdump -nr case001.pcap 'host 10.42' -c15
reading from file case001.pcap, link-type EN10MB (Ethernet), snapshot length 262144
17:58:07.470323 ARP, Request who-has 10.42.85.10 tell 0.0.0.0, length 46
17:58:08.469951 ARP, Request who-has 10.42.85.10 tell 0.0.0.0, length 46
17:58:09.469817 ARP, Request who-has 10.42.85.10 tell 0.0.0.0, length 46
17:58:10.470544 ARP, Request who-has 10.42.85.10 tell 10.42.85.10, length 46
17:58:10.471766 IP 10.42.85.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
17:58:10.472962 IP 10.42.85.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
17:58:10.473430 IP 10.42.85.10.64915 > 224.0.0.252.5355: UDP, length 30
17:58:10.548726 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
17:58:10.548819 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
17:58:10.548947 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
17:58:10.892100 IP 10.42.85.10.64915 > 224.0.0.252.5355: UDP, length 30
17:58:10.970259 IP 10.42.85.10 > 224.0.0.22: igmp v3 report, 1 group record(s)
17:58:11.298189 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
17:58:11.298223 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
17:58:11.298271 IP 10.42.85.10.137 > 10.42.85.255.137: UDP, length 68
```

10.42.85.0/24

- What architecture changes should be made immediately?

To enhance security, immediate architecture changes should include restricting remote desktop access to internal network connections only. External access to RDP should be blocked entirely, and any remote access should be routed through a secure VPN or a dedicated bastion host. Additionally, ensure that strong authentication mechanisms, such as multi-factor authentication (MFA), are enforced for all remote connections.

- Did the attacker steal the Szechuan sauce? If so, what time?

Case View Tools Window Help

Add Data Source Images/Videos Communications Geolocation Timeline Discovery Generate Report Close Case

Keyword Lists Keyword Search

Listing
/img_20200918_0347_CDrive.E01/vol3/Users/Administrator/AppData/Roaming/Microsoft/Windows/Recent/AutomaticDestinations/9b9cd69c1c24e2b.automaticDestinations-ms

Thumbnail Summary

6 Results

Save Table as CSV

Name	C	D	Modified Time	Change Time	Access Time	Created Time	Size	Flags(Dir)	Flags(Meta)	Known	Location
Beth_Secret.txtLink	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	750	Allocated	Allocated	unknown	/img_20200918_034
No preferred path foundLink	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	956	Allocated	Allocated	unknown	/img_20200918_034
NoJerry.txtLink	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	736	Allocated	Allocated	unknown	/img_20200918_034
PortalGunPlans.txtLink	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	759	Allocated	Allocated	unknown	/img_20200918_034
SECRET_beth.txtLink	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	750	Allocated	Allocated	unknown	/img_20200918_034
Szechuan Sauce.txtLink	0	0	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	0000-00-00 00:00:00	759	Allocated	Allocated	unknown	/img_20200918_034

Hex Text Application File Metadata OS Account Data Artifacts Analysis Results Context Annotations Other Occurrences

Result: 1 of 1 Result

Type	Value	Source(s)
Path	C:\Fileshare\Secret\SECRET_beth.txt	RecentActivity
Path ID	235337	RecentActivity
Date Accessed	0000-00-00 00:00:00	RecentActivity

Yes, the attacker did at around 22:35:43 UTC.

- Did the attacker steal or access any other sensitive file? If so, what time?

Yes, the attacker accessed the above files as seen above.