The Case of the Stolen Szechuan Sauce

What's the Operating System of the Server? (Clark)

To find the operating system version of the DC01 device we need to look at the registry keys provided for us. In the provided "DC01-protected.zip" file there is the "Protected" directory. Inside this directory are several hive files, the one we are interested in here is the "software" file.

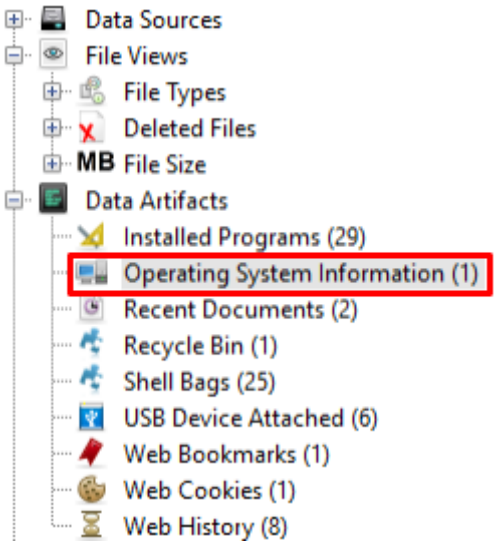
If we open up this hive in "Registry Explorer" and navigate to "Microsoft\Windows NT\CurrentVersion" we will receive the following data.

SystemRoot	RegSz	C:\Windows	00-05-12-00-00-00
SoftwareType	RegSz	System	00-00-78-F8-00-00
RegisteredOwner	RegSz	Windows User	6C-00
InstallDate	RegDword	1600361039	
CurrentVersion	RegSz	6.3	F0-00-01-00
CurrentBuild	RegSz	9600	00-00
RegisteredOrganization	RegSz		
CurrentType	RegSz	Multiprocessor Free	65-00-64-00-00-00-00-00-00-00-00-00
InstallationType	RegSz	Server	00-00-F4-E2-B7-53
EditionID	RegSz	ServerStandardEval	00-00-00-00-00-00
ProductName	RegSz	Windows Server 2012 R2 Standard Evaluation	00-00-00-00-00-00
ProductId	RegSz	00252-10000-00000-AA228	37-00-5C-00
DigitalProductId	RegBinary	A4-00-00-00-03-00-00-00-30-30-32-35-32-2D-31-3...	
DigitalProductId4	RegBinary	F8-04-00-00-04-00-00-00-30-00-30-00-30-00-30-00...	00-00-00-00
CurrentBuildNumber	RegSz	9600	36-02
BuildLab	RegSz	9600.winblue_gdr.140221-1952	00-00
BuildLabEx	RegSz	9600.17031.amd64fre.winblue_gdr.140221-1952	00-00-00-00
BuildGUID	RegSz	ffffffff-ffff-ffff-ffff-ffffffffffff	00-00
PathName	RegSz	C:\Windows	74-68-65-6E-74-00

From this, we can determine that the OS version is "Windows Server 2012 R2 Standard Evaluation". We can also see additional information like the current version, "6.3", and the current build, "9600".

What's the Operating System of the Desktop? (Clark)

Sadly the registry hive for the desktop machine is incomplete and thus doesn't contain OS information. We will use another tool, Autopsy, to figure out the OS of the desktop machine. Opening up the provided disk image for the desktop machine we can go to the "Data Artifacts" section, and then the "Operating System Information" sub-section.



From here we can access the OS information for the device, provided by Autopsy.

Type	Value
Name	DESKTOP-SDN1RPT
Domain	C137.local
Program Name	Windows 10 Enterprise Evaluation
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Path	C:\Windows

As we can see, the desktop machine is running "Windows 10 Enterprise Evaluation".

What was the local time of the Server? (Clark)

We are told at the start of the exercise that the attack took place in Colorado during MDT (UTC-6). We cannot, however, assume that all systems are properly configured. As a result, we need to individually analyze each machine for discrepancies in time zones so we can get a full view of the timeline. By opening the “system” registry hive provided in “Registry Explorer” we can navigate to “ControlSet001 > TimeZoneInformation”. There we see the following key, which reveals to use the real timezone the server was running on.

TimeZoneKeyName	Pacific Standard Time
StandardStart	Month 11, week of month 1, day of week 0,
StandardName	@tzres.dll,-212
StandardBias	0

As we can see, the server is running on PST (UTC-7). As a result, we need to make sure to adjust all time information from the server by this 1-hour difference.

Was there a breach? (Clark)

Using the provided PCAP we can show that there almost certainly was a breach.

```
2020-09-19 02:21:44.951051 194.61.24.102 10.42.85.10   RDP   117 Cookie: mstshash=Administrator, Negotiate Request
2020-09-19 02:21:44.952890 10.42.85.10   194.61.24.102 RDP    85 Negotiate Response
2020-09-19 02:21:45.173409 194.61.24.102 10.42.85.10   RDP   117 Cookie: mstshash=Administrator, Negotiate Request
2020-09-19 02:21:45.175169 10.42.85.10   194.61.24.102 RDP    85 Negotiate Response
2020-09-19 02:21:45.385206 194.61.24.102 10.42.85.10   RDP   117 Cookie: mstshash=Administrator, Negotiate Request
2020-09-19 02:21:45.387404 10.42.85.10   194.61.24.102 RDP    85 Negotiate Response
```

There was a series of roughly 100 RDP logon requests from the IP address “194.61.24.102”. These logon requests each occurred milliseconds apart, and eventually terminated when the attacker was able to gain access to the system with administrator privileges. A quick search on VirusTotal also reveals that this IP address is associated with malicious activity.

```
2020-09-19 02:22:36.664968 194.61.24.102 10.42.85.10   RDP   117 Cookie: mstshash=Administrator, Negotiate Request
2020-09-19 02:22:36.666762 10.42.85.10   194.61.24.102 RDP    85 Negotiate Response
2020-09-19 02:35:55.291953 10.42.85.10   10.42.85.115  RDP    73 Negotiate Request
```

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

The attackers performed a brute-force attack on the machine with the IP address “10.42.85.10”, the domain controller. There was no rate-limiting being performed on our end, so they were able to try hundreds of passwords a second until they got the correct one.

Was malware used? If so, what was it? If there was malware answer the following:

What process was malicious? (Clark)

The malicious process was named “coreupdater.exe”. Three main hints lead to this conclusion. Firstly, using Volatility we could access the network utilization of active processes. “coreupdater.exe” immediately stood out as communicating over the non-standard port 443.

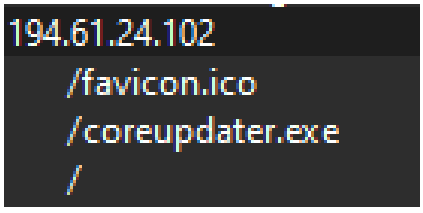
```
0x20e28d10      TCPv6   fe80::2dcf:e660:be73:d220      49155   fe80::2dcf:e660:be73:d220      62777   CLOSED  460     lsass.exe       -
0x20f52a00      TCPv6   fe80::2dcf:e660:be73:d220      135     fe80::2dcf:e660:be73:d220      62779   CLOSED  684     svchost.exe     N/A
0x20fc7590      TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0x20fffe50      TCPv4   0.0.0.0 62475   0.0.0.0 0       LISTENING       3724    spoolsv.exe     N/A
0x20fffe50      TCPv6   ::      62475   ::      0       LISTENING       3724    spoolsv.exe     N/A
```

Furthermore, a quick search for information on the “coreupdater.exe” led to malware analysis websites, such as https://www.joesandbox.com/analysis/398583/0/html, which identified the process as malicious.

Finally, attempting to extract the malicious process using Autopsy from the provided drive image results in Windows Defender immediately identifying the file as malware and removing it from the system. The file can be found in the “/Windows/System32” directory of the provided image.

What IP Address delivered the payload? (Clark)

The malicious process appears to have been downloaded from the internet using Internet Explorer. Thus we can analyze HTTP connections to see where the file was downloaded from. Using Wireshark we can do just this, navigating to “Statistics > HTTP > Requests” we can get a human-readable list of all visited URLs during the packet capture.



The attacker downloaded the malicious executable from the same IP address that was used to brute-force the system, “194.61.24.102”.

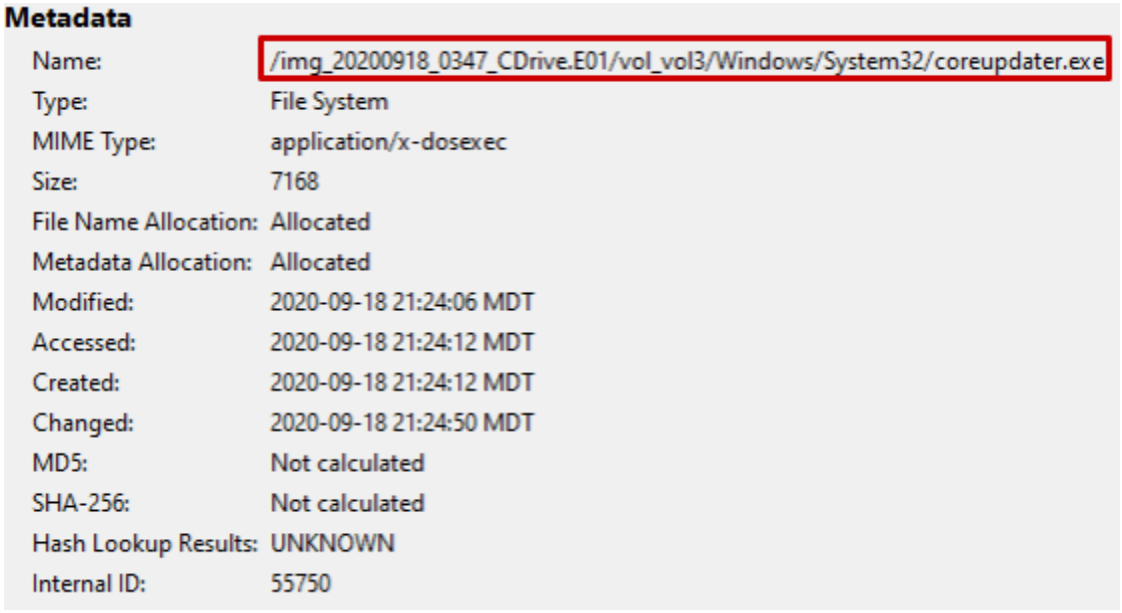
What IP Address is the malware calling to? (Clark)

The malicious process is only seen communicating with the “203.78.103.109” IP address on part 443. We discovered this, as previously mentioned, from using the “netscan” utility of Volatility on the provided memory dump.

```
0x20e28d10     TCPv6   fe80::2dcf:e660:be73:d220      49155   fe80::2dcf:e660:be73:d220      62777   CLOSED  460     lsass.exe       -
0x20f52a00     TCPv6   fe80::2dcf:e660:be73:d220      135     fe80::2dcf:e660:be73:d220      62779   CLOSED  684     svchost.exe     N/A
0x20fc7590     TCPv4   10.42.85.10     62613   203.78.103.109  443     ESTABLISHED     3644    coreupdater.ex  N/A
0x20fffe50     TCPv4   0.0.0.0 62475   0.0.0.0 0       LISTENING       3724    spoolsv.exe     N/A
0x20fffe50     TCPv6   ::      62475   ::      0       LISTENING       3724    spoolsv.exe     N/A
```

Where is this malware on disk? (Clark)

Using Autopsy we could analyze the disk image and search for the process. Using this we discovered the malware had carefully hidden itself in the System32 directory.



Metadata

Name:	/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/coreupdater.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	7168
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-09-18 21:24:06 MDT
Accessed:	2020-09-18 21:24:12 MDT
Created:	2020-09-18 21:24:12 MDT
Changed:	2020-09-18 21:24:50 MDT
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	55750

When did it first appear? (Clark)

Metadata

Name:	/img_20200918_0347_CDrive.E01/vol_vol3/Windows/System32/coreupdater.exe
Type:	File System
MIME Type:	application/x-dosexec
Size:	7168
File Name Allocation:	Allocated
Metadata Allocation:	Allocated
Modified:	2020-09-18 21:24:06 MDT
Accessed:	2020-09-18 21:24:12 MDT
Created:	2020-09-18 21:24:12 MDT
Changed:	2020-09-18 21:24:50 MDT
MD5:	Not calculated
SHA-256:	Not calculated
Hash Lookup Results:	UNKNOWN
Internal ID:	55750

According to Autopsy, the malicious “coreupdater.exe” file was created on 2020-09-18 at 21:24:06 MDT. Using Volatility’s “pslist” utility we can also figure out when the file was first run, 2020-09-19 3:56:37 UTC (2020-09-18 21:56:37 MDT).

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

Did someone move it? (Clark)

We can extract “File Explorer” history from the “$UsnJrnl_$J” file. To do this I made use of MFTECmd to extract the file to a CSV, and then used “Timeline Explorer” to view the resultant “.csv”. “coreupdater.exe” was initially installed into the “Download” folder (Entry ID 84880), but was then later moved to the “System32” folder (Entry ID 2873).

80249	☐	2020-09-19 03:24:12	coreupdater.exe	.exe	87137	2	84880
80256	☐	2020-09-19 03:24:50	coreupdater.exe	.exe	87137	2	2873

What were the capabilities of this malware? (Clark)

This Malware primarily seems to have two features: information collection and spreading. It scans any device it has gained access to and extracts hash and passwords. It also leaves open a line for command and control so the attacker can explore the system themselves and extract further files. The malware also spreads to nearby machines on the network. It utilizes stolen credentials and administrator privileges to perform this lateral movement.

Is this malware easily obtained? (Clark)

This malware appears to have been around for quite a while at this point. It has been known for almost 4 years according to VirusTotal, and if the creation date on the file is to be believed, was created almost 14 years ago.

Creation Time	2010-04-14 22:06:53 UTC
First Seen In The Wild	2020-09-18 20:24:12 UTC
First Submission	2020-09-27 13:12:13 UTC
Last Submission	2024-04-04 05:08:01 UTC
Last Analysis	2024-02-14 00:03:49 UTC

https://www.virustotal.com/gui/file/10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6/details

This virus has also popped up in numerous attacks at this point, so it is safe to say that it is fairly easy to procure the virus at this point.

Was this malware installed with persistence on any machine? (Clark)

When? (Clark)

Using “Registry Explorer” we can open the provided “system” hive and look at the “ControlSet001 > Services” key. There is a subkey for every start-up task, including our malicious “coreupdater.exe”. We can see that it was added on 2020-09-19 at 03:27:49 UTC (2020-09-18 at 21:27:49 MDT).

Where? (Clark)

As previously discussed, the malicious file is in the “System32” directory. This is further confirmed for us in “Registry Explorer” as well. See the provided screenshot from “Registry Explorer”.

What malicious IP Addresses were involved? (Aguibu)

94.61.24.102 and 203.78.103.109

Were any IP Addresses from known adversary infrastructure? (Aguibu)

Per Virustotal, 194.61.24.102 is linked to Russia and is known to be involved in RDP Brute Force attacks.

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

Around that time, 203.78.103.109 was flagged in AlienVault as associated with Meterpreter.

Did the attacker access any other systems? (Aguibu)

There's evidence in the event logs of the desktop that it was also accessed.

How? (Aguibu)

Through an RDP connection from the DC using the compromised Administrator account.

When? (Aguibu)

The listed MT time is 3:36, which is equivalent to 2:36 PST.

Did the attackers steal any data? (Aguibu)

A review of the desktop web cache (%AppData%\Microsoft\Windows\WebCache) shows that the admin account accessed the following files:

- secret_beth.txt
- szechuan_sauce.txt
- nojerry.txt
- portalgunplans.txt

When? (Aguibu)

On the 19th at 2:45 PST.

What was the network layout of the victim network? (Aguibu)

There appear to be 3 devices on the network: the domain controller with IP address 10.42.85.10, an unknown device with IP address 10.42.85.100, and the affected desktop computer with IP address 10.42.85.115