Forensic Investigation Project - Case 001 – The Stolen Szechuan Sauce

Alex Dods and Bahja Hagielmi

Table of Contents:

Executive Summary:

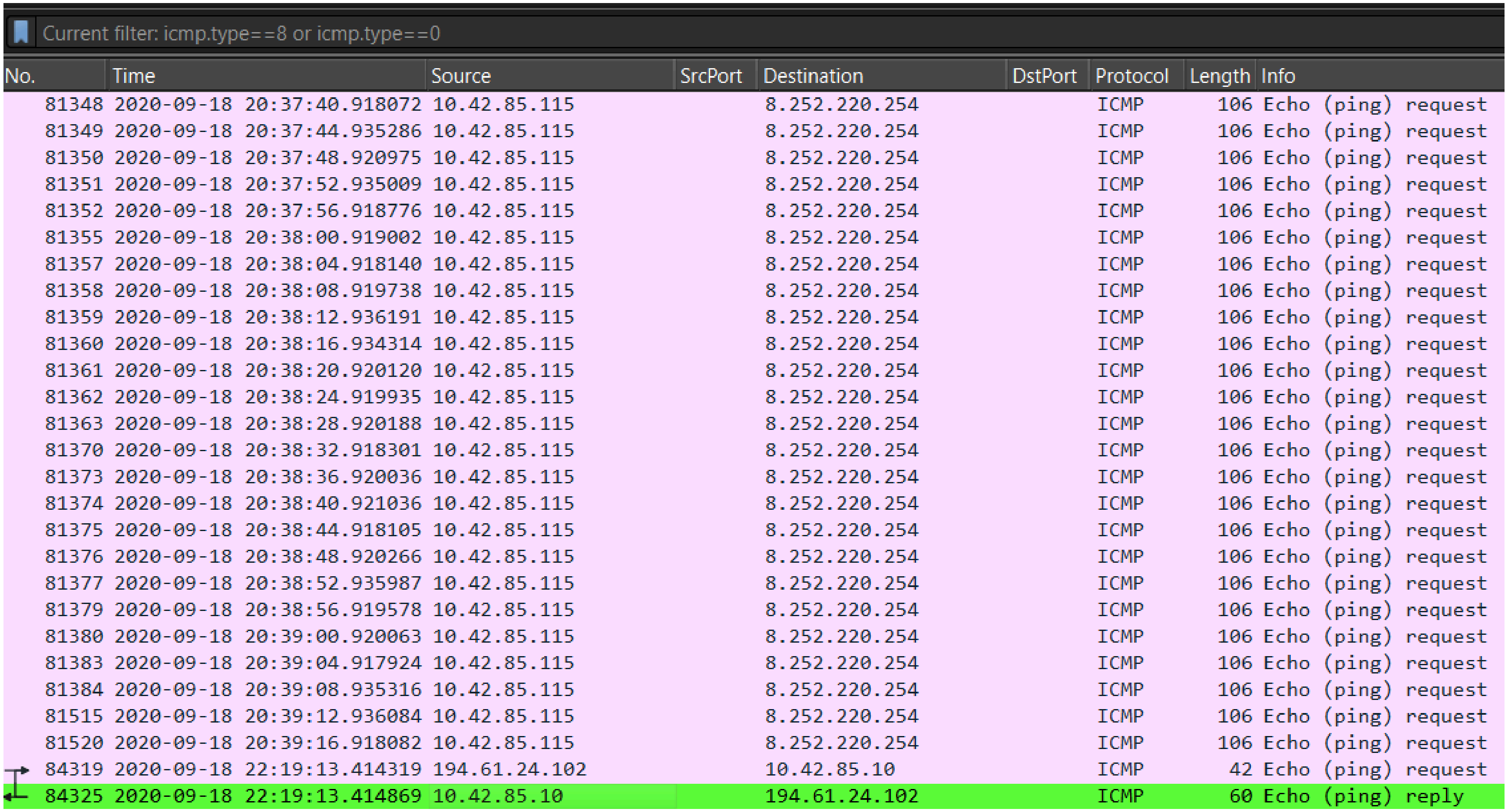
We have been asked to review the test case: “The Case of the Stolen Szechuan Sauce” on difrmadness.com. This report will review the given source materials for the project, and perform forensic analysis with documented proofs. An analysis of the attack will be made, and recommendations for upgrading the victim’s system in order to prevent further breaches of this nature are also provided, along with technique citations from the MITRE ATT&CK Enterprise Matrix and a brief explanation of the tools used.

Traffic Analysis:

A Wireshark capture of the network traffic at the time of the incident in question was provided for review and analysis; it will also contain an analysis of the attacker’s techniques, mapped to the MITRE ATT&CK Enterprise Matrix[1].

Ping Sweeps:

By employing the filter “*icmp.type==8 or icmp.type==0*” without quotes on the capture file, we can pair down the results to the ping requests and responses. This filters the results to the traffic which has either an Echo (ICMP Type Number 8) or Echo Reply (ICMP Type Number 0)[2]; the results are shown below:



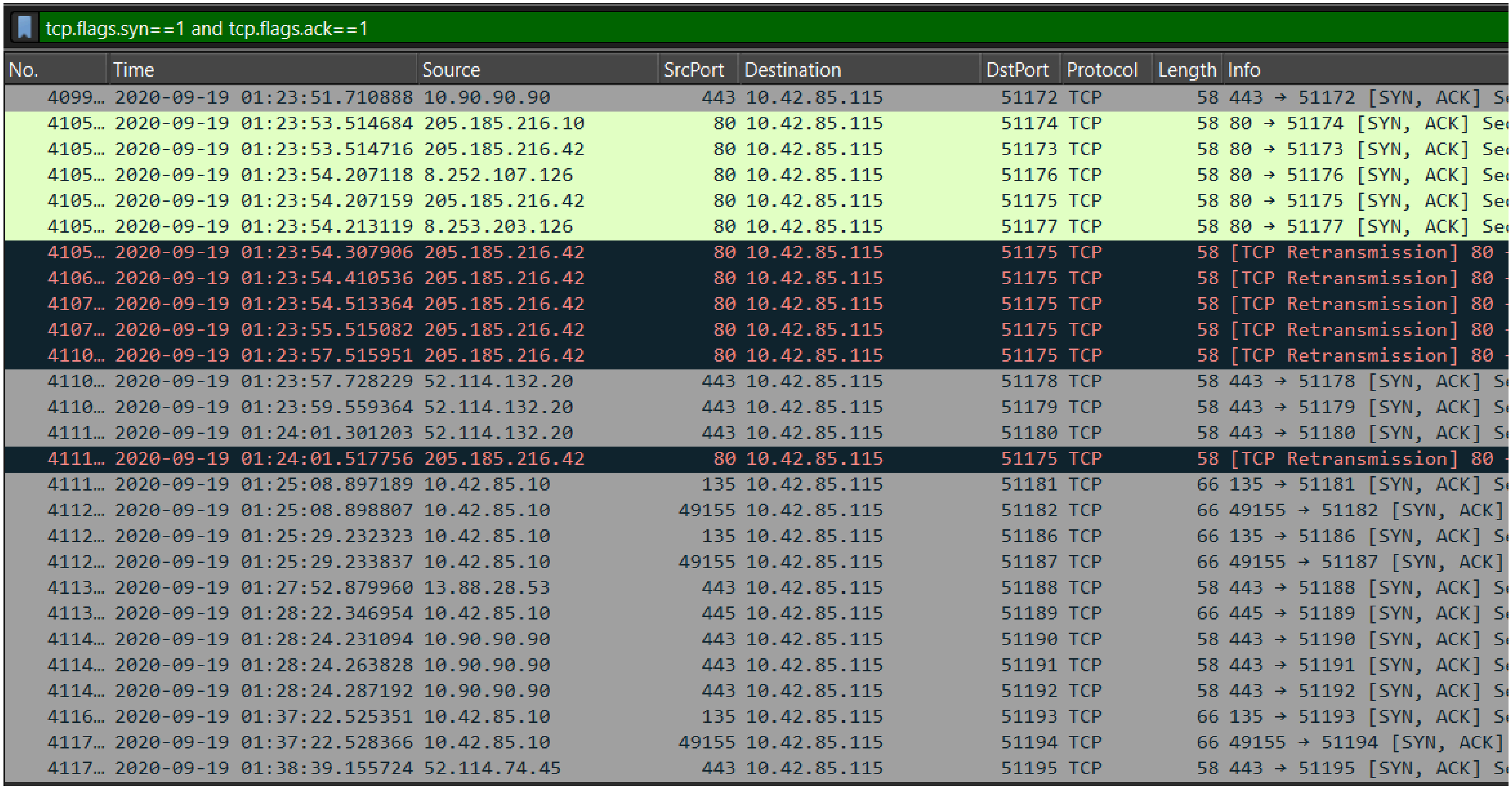
Current filter: icmp.type==8 or icmp.type==0

No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Length	Info
81348	2020-09-18 20:37:40.918072	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81349	2020-09-18 20:37:44.935286	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81350	2020-09-18 20:37:48.920975	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81351	2020-09-18 20:37:52.935009	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81352	2020-09-18 20:37:56.918776	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81355	2020-09-18 20:38:00.919002	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81357	2020-09-18 20:38:04.918140	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81358	2020-09-18 20:38:08.919738	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81359	2020-09-18 20:38:12.936191	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81360	2020-09-18 20:38:16.934314	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81361	2020-09-18 20:38:20.920120	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81362	2020-09-18 20:38:24.919935	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81363	2020-09-18 20:38:28.920188	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81370	2020-09-18 20:38:32.918301	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81373	2020-09-18 20:38:36.920036	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81374	2020-09-18 20:38:40.921036	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81375	2020-09-18 20:38:44.918105	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81376	2020-09-18 20:38:48.920266	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81377	2020-09-18 20:38:52.935987	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81379	2020-09-18 20:38:56.919578	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81380	2020-09-18 20:39:00.920063	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81383	2020-09-18 20:39:04.917924	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81384	2020-09-18 20:39:08.935316	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81515	2020-09-18 20:39:12.936084	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
81520	2020-09-18 20:39:16.918082	10.42.85.115		8.252.220.254		ICMP	106	Echo (ping) request
84319	2020-09-18 22:19:13.414319	194.61.24.102		10.42.85.10		ICMP	42	Echo (ping) request
84325	2020-09-18 22:19:13.414869	10.42.85.10		194.61.24.102		ICMP	60	Echo (ping) reply

The above image shows multiple ping requests from the IP address **8.252.220.254**, which start at *UTC 2020-09-19 00:34:48* and end at UTC 202-09-19 00:39:16. Later, at *UTC 2020-09-19 2:19:13*, the machine receives a ping from the IP address **194.61.24.102**, to which the machine sends back an Echo(ping) reply. This is an example of Active Scanning, a Reconnaissance technique as described in the Mitre ATT&CK Enterprise Matrix: "*Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP.*"[3]

SYN Scan:

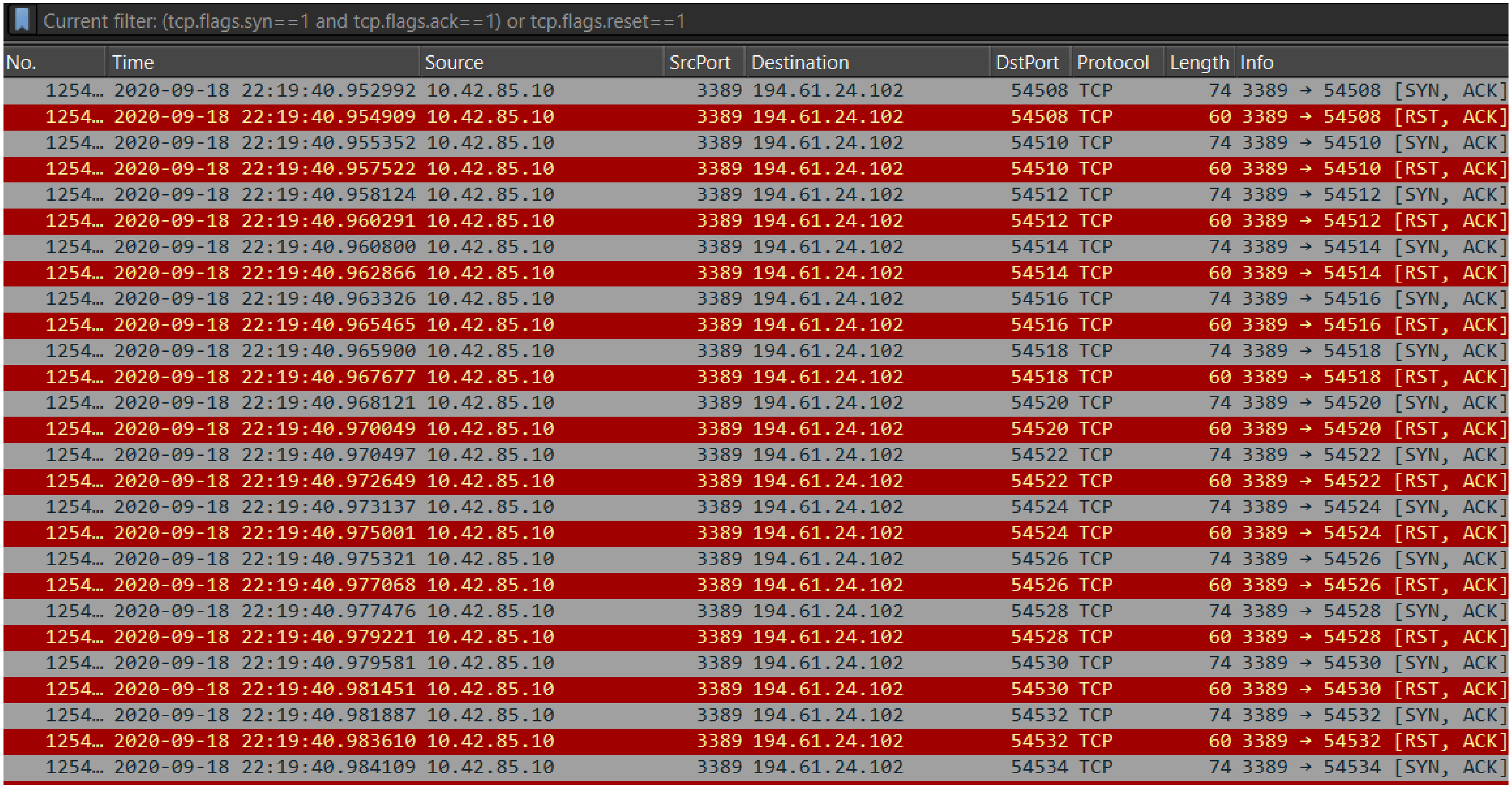
By employing the filter “*tcp.flags.syn==1 and tcp.flags.ack==1*” without quotes on the capture file, we can pair down the results to packets that have SYN and ACK flags on. From the previous filtering of the traffic, this confirms the suspicion of a malicious actor scanning the system; this new filtering of the data will allow us to see if anyone was attempting to connect to the network.



tcp.flags.syn==1 and tcp.flags.ack==1

No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Length	Info
4099…	2020-09-19 01:23:51.710888	10.90.90.90	443	10.42.85.115	51172	TCP	58	443 → 51172 [SYN, ACK] S
4105…	2020-09-19 01:23:53.514684	205.185.216.10	80	10.42.85.115	51174	TCP	58	80 → 51174 [SYN, ACK] Se
4105…	2020-09-19 01:23:53.514716	205.185.216.42	80	10.42.85.115	51173	TCP	58	80 → 51173 [SYN, ACK] Se
4105…	2020-09-19 01:23:54.207118	8.252.107.126	80	10.42.85.115	51176	TCP	58	80 → 51176 [SYN, ACK] Se
4105…	2020-09-19 01:23:54.207159	205.185.216.42	80	10.42.85.115	51175	TCP	58	80 → 51175 [SYN, ACK] Se
4105…	2020-09-19 01:23:54.213119	8.253.203.126	80	10.42.85.115	51177	TCP	58	80 → 51177 [SYN, ACK] Se
4105…	2020-09-19 01:23:54.307906	205.185.216.42	80	10.42.85.115	51175	TCP	58	[TCP Retransmission] 80
4106…	2020-09-19 01:23:54.410536	205.185.216.42	80	10.42.85.115	51175	TCP	58	[TCP Retransmission] 80
4107…	2020-09-19 01:23:54.513364	205.185.216.42	80	10.42.85.115	51175	TCP	58	[TCP Retransmission] 80
4107…	2020-09-19 01:23:55.515082	205.185.216.42	80	10.42.85.115	51175	TCP	58	[TCP Retransmission] 80
4110…	2020-09-19 01:23:57.515951	205.185.216.42	80	10.42.85.115	51175	TCP	58	[TCP Retransmission] 80
4110…	2020-09-19 01:23:57.728229	52.114.132.20	443	10.42.85.115	51178	TCP	58	443 → 51178 [SYN, ACK] S
4110…	2020-09-19 01:23:59.559364	52.114.132.20	443	10.42.85.115	51179	TCP	58	443 → 51179 [SYN, ACK] S
4111…	2020-09-19 01:24:01.301203	52.114.132.20	443	10.42.85.115	51180	TCP	58	443 → 51180 [SYN, ACK] S
4111…	2020-09-19 01:24:01.517756	205.185.216.42	80	10.42.85.115	51175	TCP	58	[TCP Retransmission] 80
4111…	2020-09-19 01:25:08.897189	10.42.85.10	135	10.42.85.115	51181	TCP	66	135 → 51181 [SYN, ACK] S
4112…	2020-09-19 01:25:08.898807	10.42.85.10	49155	10.42.85.115	51182	TCP	66	49155 → 51182 [SYN, ACK]
4112…	2020-09-19 01:25:29.232323	10.42.85.10	135	10.42.85.115	51186	TCP	66	135 → 51186 [SYN, ACK] S
4112…	2020-09-19 01:25:29.233837	10.42.85.10	49155	10.42.85.115	51187	TCP	66	49155 → 51187 [SYN, ACK]
4113…	2020-09-19 01:27:52.879960	13.88.28.53	443	10.42.85.115	51188	TCP	58	443 → 51188 [SYN, ACK] S
4113…	2020-09-19 01:28:22.346954	10.42.85.10	445	10.42.85.115	51189	TCP	66	445 → 51189 [SYN, ACK] S
4114…	2020-09-19 01:28:24.231094	10.90.90.90	443	10.42.85.115	51190	TCP	58	443 → 51190 [SYN, ACK] S
4114…	2020-09-19 01:28:24.263828	10.90.90.90	443	10.42.85.115	51191	TCP	58	443 → 51191 [SYN, ACK] S
4114…	2020-09-19 01:28:24.287192	10.90.90.90	443	10.42.85.115	51192	TCP	58	443 → 51192 [SYN, ACK] S
4116…	2020-09-19 01:37:22.525351	10.42.85.10	135	10.42.85.115	51193	TCP	66	135 → 51193 [SYN, ACK] S
4117…	2020-09-19 01:37:22.528366	10.42.85.10	49155	10.42.85.115	51194	TCP	66	49155 → 51194 [SYN, ACK]
4117…	2020-09-19 01:38:39.155724	52.114.74.45	443	10.42.85.115	51195	TCP	58	443 → 51195 [SYN, ACK] S

By further refinding the filter to “*(tcp.flags.syn==1 and tcp.flags.ack==1) or tcp.flags.reset==1*” without quotes, we are able to see a pattern consistent with SYN scanning techniques emerge; the results are shown below:



Current filter: (tcp.flags.syn==1 and tcp.flags.ack==1) or tcp.flags.reset==1

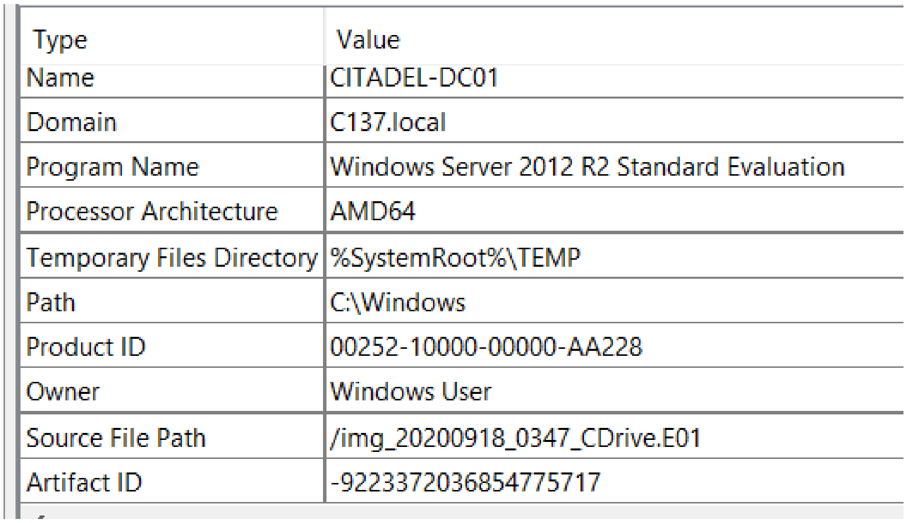
No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Length	Info
1254…	2020-09-18 22:19:40.952992	10.42.85.10	3389	194.61.24.102	54508	TCP	74	3389 → 54508 [SYN, ACK]
1254…	2020-09-18 22:19:40.954909	10.42.85.10	3389	194.61.24.102	54508	TCP	60	3389 → 54508 [RST, ACK]
1254…	2020-09-18 22:19:40.955352	10.42.85.10	3389	194.61.24.102	54510	TCP	74	3389 → 54510 [SYN, ACK]
1254…	2020-09-18 22:19:40.957522	10.42.85.10	3389	194.61.24.102	54510	TCP	60	3389 → 54510 [RST, ACK]
1254…	2020-09-18 22:19:40.958124	10.42.85.10	3389	194.61.24.102	54512	TCP	74	3389 → 54512 [SYN, ACK]
1254…	2020-09-18 22:19:40.960291	10.42.85.10	3389	194.61.24.102	54512	TCP	60	3389 → 54512 [RST, ACK]
1254…	2020-09-18 22:19:40.960800	10.42.85.10	3389	194.61.24.102	54514	TCP	74	3389 → 54514 [SYN, ACK]
1254…	2020-09-18 22:19:40.962866	10.42.85.10	3389	194.61.24.102	54514	TCP	60	3389 → 54514 [RST, ACK]
1254…	2020-09-18 22:19:40.963326	10.42.85.10	3389	194.61.24.102	54516	TCP	74	3389 → 54516 [SYN, ACK]
1254…	2020-09-18 22:19:40.965465	10.42.85.10	3389	194.61.24.102	54516	TCP	60	3389 → 54516 [RST, ACK]
1254…	2020-09-18 22:19:40.965900	10.42.85.10	3389	194.61.24.102	54518	TCP	74	3389 → 54518 [SYN, ACK]
1254…	2020-09-18 22:19:40.967677	10.42.85.10	3389	194.61.24.102	54518	TCP	60	3389 → 54518 [RST, ACK]
1254…	2020-09-18 22:19:40.968121	10.42.85.10	3389	194.61.24.102	54520	TCP	74	3389 → 54520 [SYN, ACK]
1254…	2020-09-18 22:19:40.970049	10.42.85.10	3389	194.61.24.102	54520	TCP	60	3389 → 54520 [RST, ACK]
1254…	2020-09-18 22:19:40.970497	10.42.85.10	3389	194.61.24.102	54522	TCP	74	3389 → 54522 [SYN, ACK]
1254…	2020-09-18 22:19:40.972649	10.42.85.10	3389	194.61.24.102	54522	TCP	60	3389 → 54522 [RST, ACK]
1254…	2020-09-18 22:19:40.973137	10.42.85.10	3389	194.61.24.102	54524	TCP	74	3389 → 54524 [SYN, ACK]
1254…	2020-09-18 22:19:40.975001	10.42.85.10	3389	194.61.24.102	54524	TCP	60	3389 → 54524 [RST, ACK]
1254…	2020-09-18 22:19:40.975321	10.42.85.10	3389	194.61.24.102	54526	TCP	74	3389 → 54526 [SYN, ACK]
1254…	2020-09-18 22:19:40.977068	10.42.85.10	3389	194.61.24.102	54526	TCP	60	3389 → 54526 [RST, ACK]
1254…	2020-09-18 22:19:40.977476	10.42.85.10	3389	194.61.24.102	54528	TCP	74	3389 → 54528 [SYN, ACK]
1254…	2020-09-18 22:19:40.979221	10.42.85.10	3389	194.61.24.102	54528	TCP	60	3389 → 54528 [RST, ACK]
1254…	2020-09-18 22:19:40.979581	10.42.85.10	3389	194.61.24.102	54530	TCP	74	3389 → 54530 [SYN, ACK]
1254…	2020-09-18 22:19:40.981451	10.42.85.10	3389	194.61.24.102	54530	TCP	60	3389 → 54530 [RST, ACK]
1254…	2020-09-18 22:19:40.981887	10.42.85.10	3389	194.61.24.102	54532	TCP	74	3389 → 54532 [SYN, ACK]
1254…	2020-09-18 22:19:40.983610	10.42.85.10	3389	194.61.24.102	54532	TCP	60	3389 → 54532 [RST, ACK]
1254…	2020-09-18 22:19:40.984109	10.42.85.10	3389	194.61.24.102	54534	TCP	74	3389 → 54534 [SYN, ACK]

As can be seen above, the gray SYN/ACK packets are followed up by the red RST/ACK packets, showing a chain of Synchronization and Acknowledgement requests, followed up by a Reset packet from the attacker's client. Consequently, the server assumes there's been a communications error and the client has not established a connection; the open port remains open and vulnerable to exploitation. This is another example of Active Scanning, a Reconnaissance technique as described in the Mitre ATT&CK Enterprise Matrix:"*Adversaries may perform different forms of active scanning depending on what information they seek to gather. These scans can also be performed in various ways, including using native features of network protocols such as ICMP*."[3]

Analysis Findings:

What’s the Operating System of the Server?

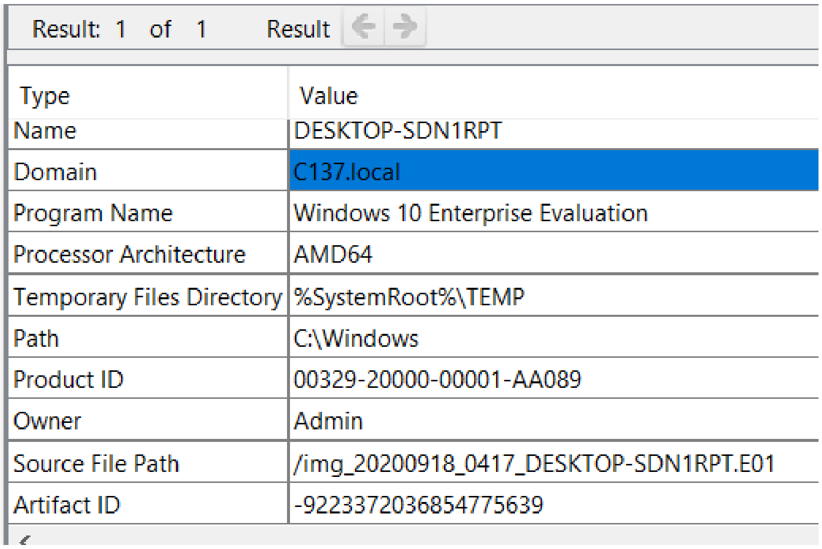
Loading the .E01 file into the Autopsy digital forensics tool, we are able to see the Operating System Information under the Data Artifacts header; the operating system on the Desktop image is ***Windows Server 2012 R2 Standard Evaluation***.



Type	Value
Name	CITADEL-DC01
Domain	C137.local
Program Name	Windows Server 2012 R2 Standard Evaluation
Processor Architecture	AMD64
Temporary Files Directory	%SystemRoot%\TEMP
Path	C:\Windows
Product ID	00252-10000-00000-AA228
Owner	Windows User
Source File Path	/img_20200918_0347_CDrive.E01
Artifact ID	-9223372036854775717

What’s the Operating System of the Desktop?

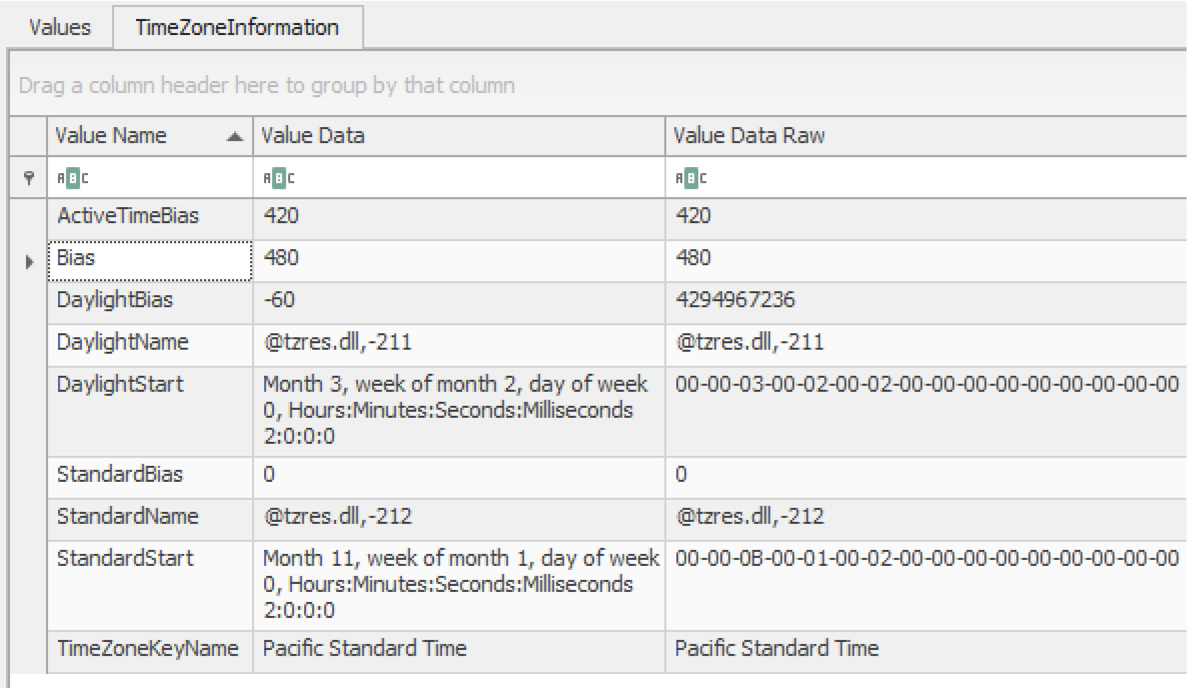
Loading the .E01 file into the Autopsy digital forensics tool, we are able to see the Operating System Information under the Data Artifacts header; the operating system on the Desktop image is ***Windows 10 Enterprise Evaluation***.



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
Product ID	00329-20000-00001-AA089
Owner	Admin
Source File Path	/img_20200918_0417_DESKTOP-SDN1RPT.E01
Artifact ID	-9223372036854775639

What was the local time of the Server?

Exploring the registry keys located at *ROOT\Controlset001\Control\TimeZoneInformation*, we are able to verify that the server's local time zone is the ***Pacific Standard Time Zone***.



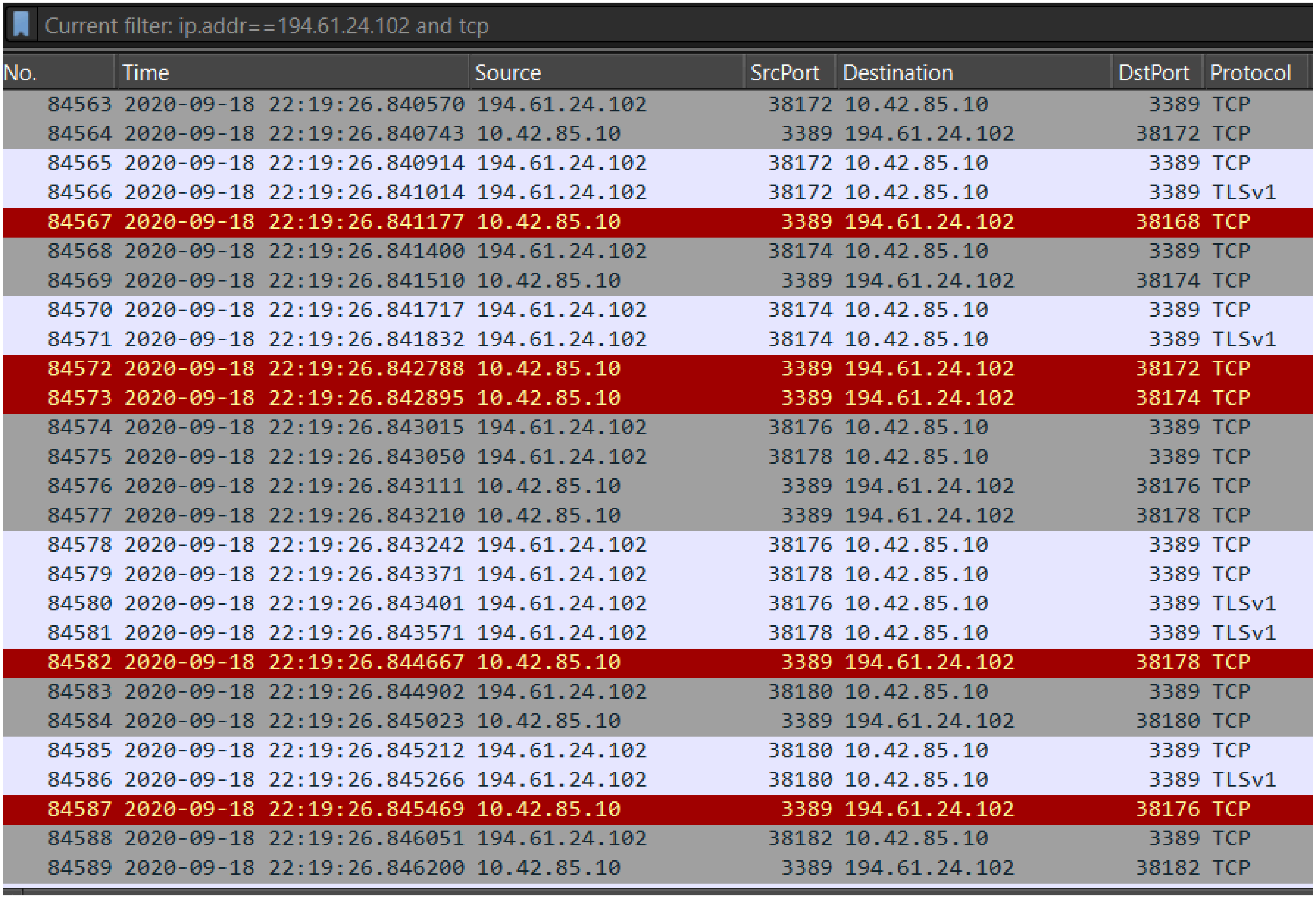
Value Name	Value Data	Value Data Raw
ActiveTimeBias	420	420
Bias	480	480
DaylightBias	-60	4294967236
DaylightName	@tzres.dll,-211	@tzres.dll,-211
DaylightStart	Month 3, week of month 2, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-03-00-02-00-02-00-00-00-00-00-00-00-00-00
StandardBias	0	0
StandardName	@tzres.dll,-212	@tzres.dll,-212
StandardStart	Month 11, week of month 1, day of week 0, Hours:Minutes:Seconds:Milliseconds 2:0:0:0	00-00-0B-00-01-00-02-00-00-00-00-00-00-00-00-00
TimeZoneKeyName	Pacific Standard Time	Pacific Standard Time

Was there a breach?

Yes; the proof shall be provided below in further detail.

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

The initial entry vector was the result of a ***RDP Brute Force attack***; the SYN Scan above indicates its presence, and it is further confirmed by reviewing the tcp traffic from the requesting connection with the following filter "*ip.addr==194.61.24.102 and tcp*" without quotes. The connections are all towards the destination port 3389, which is reserved for the Microsoft WBT Server, which handles connections for the Remote Desktop Protocol (RDP)[4]. This serves as an example of Exploit Public-Facing Application, an Initial Access technique as described in the Mitre ATT&CK Enterprise Matrix: "*Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.*"[5]



Current filter: ip.addr==194.61.24.102 and tcp

No.	Time	Source	SrcPort	Destination	DstPort	Protocol
84563	2020-09-18 22:19:26.840570	194.61.24.102	38172	10.42.85.10	3389	TCP
84564	2020-09-18 22:19:26.840743	10.42.85.10	3389	194.61.24.102	38172	TCP
84565	2020-09-18 22:19:26.840914	194.61.24.102	38172	10.42.85.10	3389	TCP
84566	2020-09-18 22:19:26.841014	194.61.24.102	38172	10.42.85.10	3389	TLSv1
84567	2020-09-18 22:19:26.841177	10.42.85.10	3389	194.61.24.102	38168	TCP
84568	2020-09-18 22:19:26.841400	194.61.24.102	38174	10.42.85.10	3389	TCP
84569	2020-09-18 22:19:26.841510	10.42.85.10	3389	194.61.24.102	38174	TCP
84570	2020-09-18 22:19:26.841717	194.61.24.102	38174	10.42.85.10	3389	TCP
84571	2020-09-18 22:19:26.841832	194.61.24.102	38174	10.42.85.10	3389	TLSv1
84572	2020-09-18 22:19:26.842788	10.42.85.10	3389	194.61.24.102	38172	TCP
84573	2020-09-18 22:19:26.842895	10.42.85.10	3389	194.61.24.102	38174	TCP
84574	2020-09-18 22:19:26.843015	194.61.24.102	38176	10.42.85.10	3389	TCP
84575	2020-09-18 22:19:26.843050	194.61.24.102	38178	10.42.85.10	3389	TCP
84576	2020-09-18 22:19:26.843111	10.42.85.10	3389	194.61.24.102	38176	TCP
84577	2020-09-18 22:19:26.843210	10.42.85.10	3389	194.61.24.102	38178	TCP
84578	2020-09-18 22:19:26.843242	194.61.24.102	38176	10.42.85.10	3389	TCP
84579	2020-09-18 22:19:26.843371	194.61.24.102	38178	10.42.85.10	3389	TCP
84580	2020-09-18 22:19:26.843401	194.61.24.102	38176	10.42.85.10	3389	TLSv1
84581	2020-09-18 22:19:26.843571	194.61.24.102	38178	10.42.85.10	3389	TLSv1
84582	2020-09-18 22:19:26.844667	10.42.85.10	3389	194.61.24.102	38178	TCP
84583	2020-09-18 22:19:26.844902	194.61.24.102	38180	10.42.85.10	3389	TCP
84584	2020-09-18 22:19:26.845023	10.42.85.10	3389	194.61.24.102	38180	TCP
84585	2020-09-18 22:19:26.845212	194.61.24.102	38180	10.42.85.10	3389	TCP
84586	2020-09-18 22:19:26.845266	194.61.24.102	38180	10.42.85.10	3389	TLSv1
84587	2020-09-18 22:19:26.845469	10.42.85.10	3389	194.61.24.102	38176	TCP
84588	2020-09-18 22:19:26.846051	194.61.24.102	38182	10.42.85.10	3389	TCP
84589	2020-09-18 22:19:26.846200	10.42.85.10	3389	194.61.24.102	38182	TCP

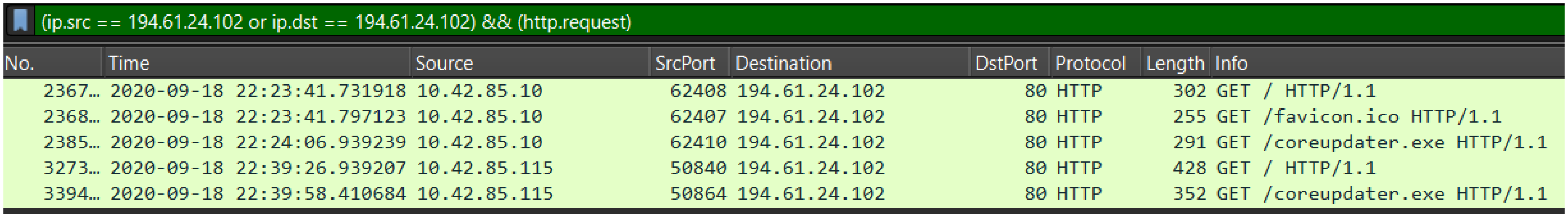
Was malware used? If so, what was it?

Yes, Malware was used; ***coreupdater.exe*** was hiding the trojan ***Metasploit***.

What process was malicious?

The malicious process was named ***coreupdater.exe*** By refining the data in the pcap file, we can determine and locate the http request to GET the file in the network traffic capture; using the filter *(ip.src == 194.61.24.102 or ip.dst == 194.61.24.102) && (http.request)*, we are shown the following information

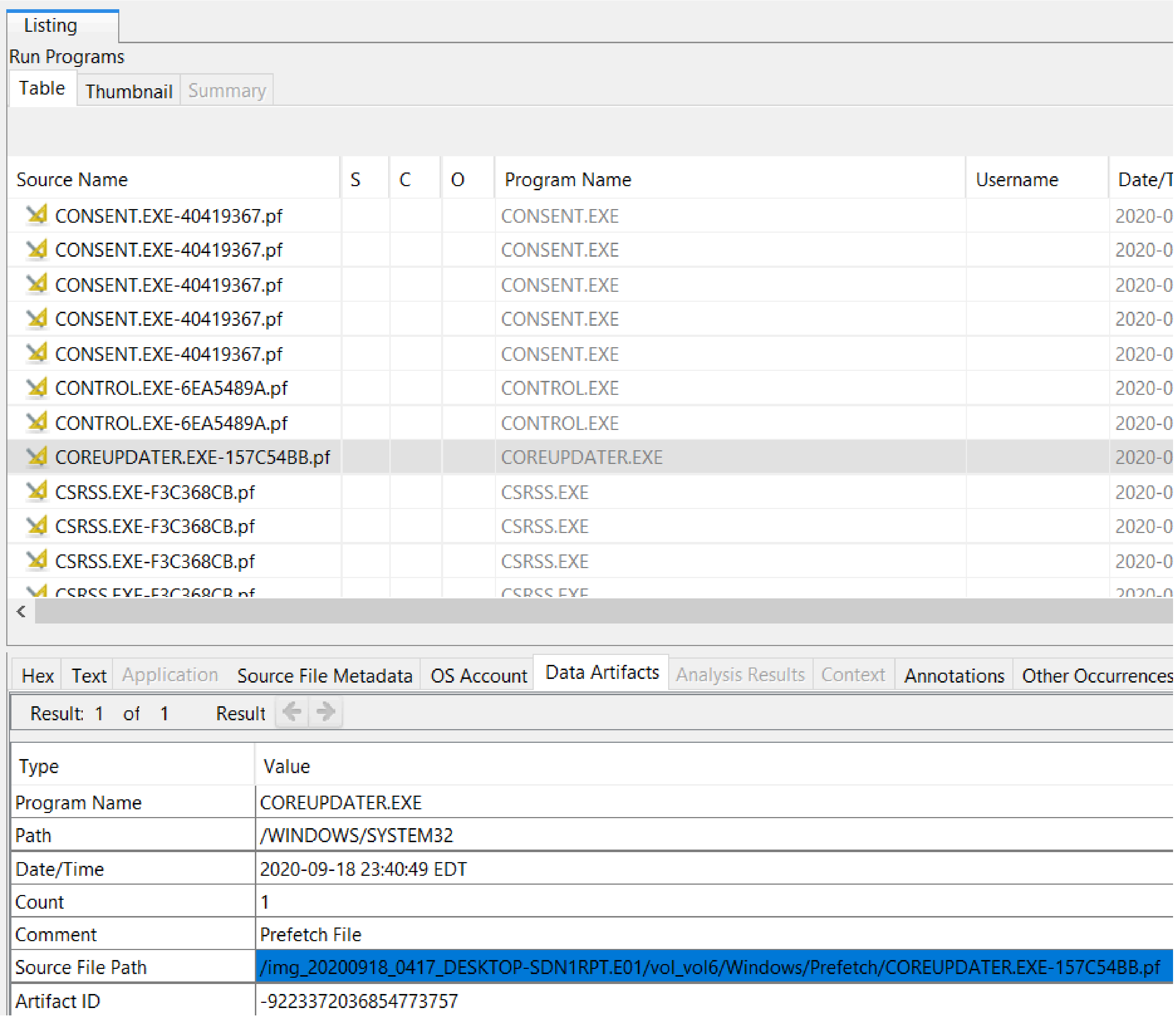
:



(ip.src == 194.61.24.102 or ip.dst == 194.61.24.102) && (http.request)

No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Length	Info
2367…	2020-09-18 22:23:41.731918	10.42.85.10	62408	194.61.24.102	80	HTTP	302	GET / HTTP/1.1
2368…	2020-09-18 22:23:41.797123	10.42.85.10	62407	194.61.24.102	80	HTTP	255	GET /favicon.ico HTTP/1.1
2385…	2020-09-18 22:24:06.939239	10.42.85.10	62410	194.61.24.102	80	HTTP	291	GET /coreupdater.exe HTTP/1.1
3273…	2020-09-18 22:39:26.939207	10.42.85.115	50840	194.61.24.102	80	HTTP	428	GET / HTTP/1.1
3394…	2020-09-18 22:39:58.410684	10.42.85.115	50864	194.61.24.102	80	HTTP	352	GET /coreupdater.exe HTTP/1.1

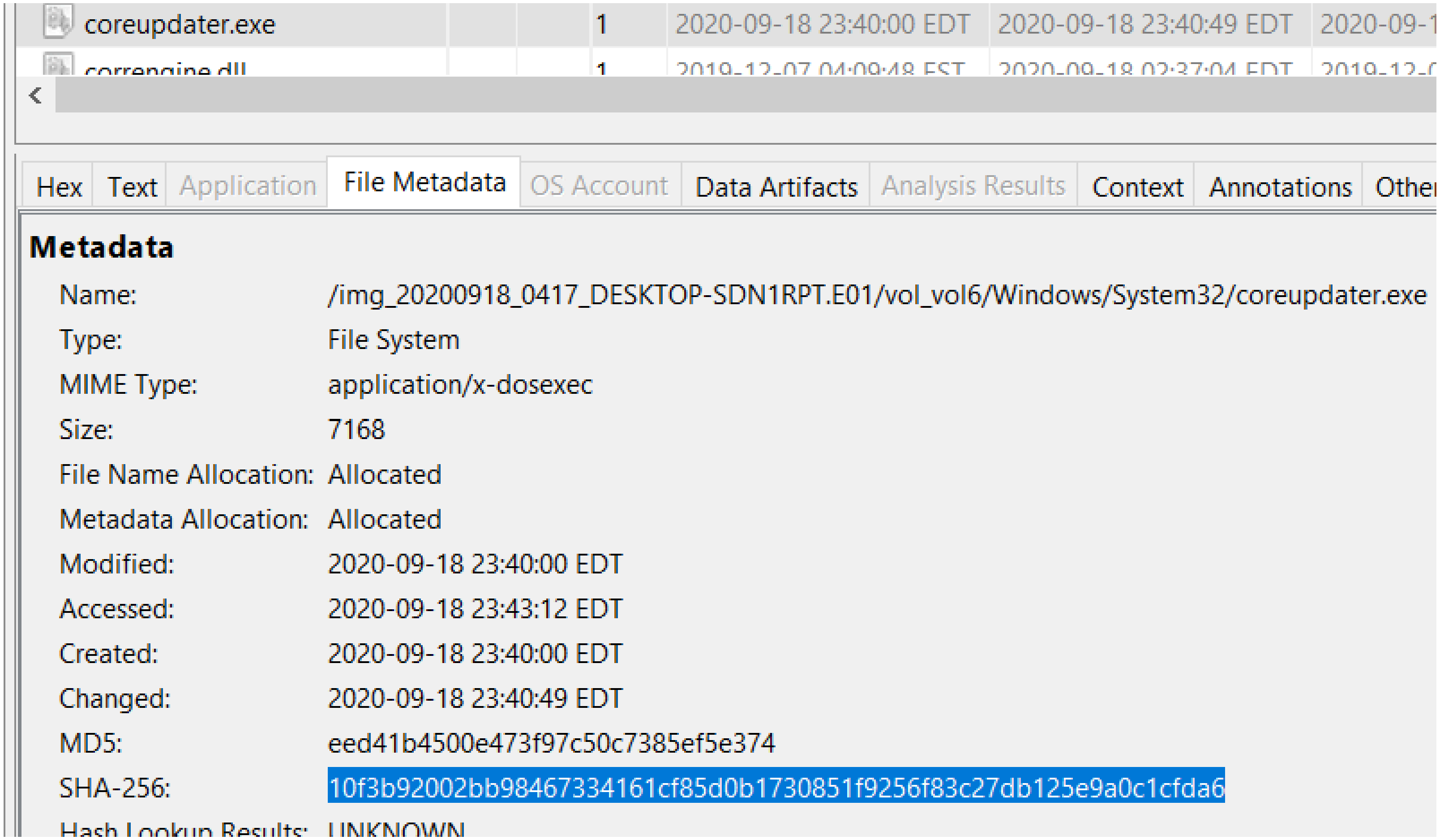
Investigating these traffic items, we can see that the file ***coreupdater.exe*** was sent from the known malicious actor IP address 194.61.24.102. Now knowing the filename, we can return to the Autopsy tool to search for the file. Byu searching for ***coreupdater.exe*** in the Run Programs section of the Data Artifacts, we can parse the data manually to search for the prefetch file related to the malicious executable. The Data Artifacts tab of the Prefetch file for ***coreupdater.exe*** lists the path to the program as "*/WINDOWS/SYSTEM32*", and the Source File Path of "*/img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6/Windows/Prefetch/COREUPDATER.EXE-157C54BB.pf*" allows us to know that the *Windows* folder is located on volume 6 of the Data Sources, as shown below.



Source Name	S	C	O	Program Name	Username	Date/T
CONSENT.EXE-40419367.pf				CONSENT.EXE		2020-0
CONSENT.EXE-40419367.pf				CONSENT.EXE		2020-0
CONSENT.EXE-40419367.pf				CONSENT.EXE		2020-0
CONSENT.EXE-40419367.pf				CONSENT.EXE		2020-0
CONSENT.EXE-40419367.pf				CONSENT.EXE		2020-0
CONTROL.EXE-6EA5489A.pf				CONTROL.EXE		2020-0
CONTROL.EXE-6EA5489A.pf				CONTROL.EXE		2020-0
COREUPDATER.EXE-157C54BB.pf				COREUPDATER.EXE		2020-0
CSRSS.EXE-F3C368CB.pf				CSRSS.EXE		2020-0
CSRSS.EXE-F3C368CB.pf				CSRSS.EXE		2020-0
CSRSS.EXE-F3C368CB.pf				CSRSS.EXE		2020-0
CSRSS.EXE-F3C368CB.pf				CSRSS.EXE		2020-0

Type	Value
Program Name	COREUPDATER.EXE
Path	/WINDOWS/SYSTEM32
Date/Time	2020-09-18 23:40:49 EDT
Count	1
Comment	Prefetch File
Source File Path	/img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6/Windows/Prefetch/COREUPDATER.EXE-157C54BB.pf
Artifact ID	-9223372036854773757

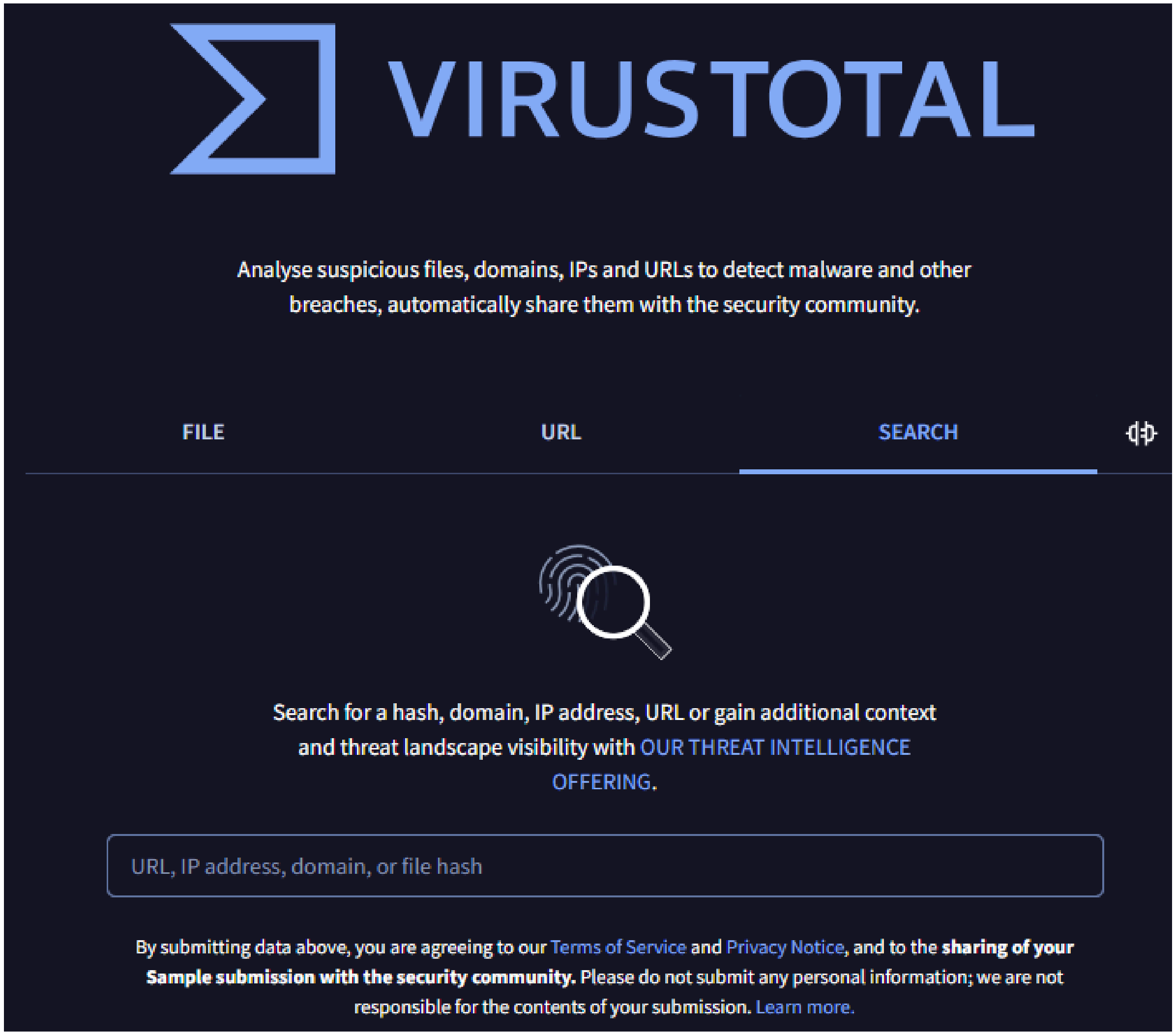
Navigating to the Data Sources tab, and accessing vol6, we are able to Navigate to the /Windows/System32 folder, where we can find the actual executable ***coreupdater.exe***. Selecting the file, we can review the File Metadata tab for the executable, and copy the SHA-256 hash from the tab, *10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6*, pasting the string into VirusTotal's lookup tool



coreupdater.exe			1	2020-09-18 23:40:00 EDT	2020-09-18 23:40:49 EDT	2020-09-1
correngine.dll			1	2019-12-07 04:09:48 EST	2020-09-18 02:37:04 EDT	2019-12-(

Metadata

Name:	/img_20200918_0417_DESKTOP-SDN1RPT.E01/vol_vol6/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 23:40:00 EDT
Accessed:	2020-09-18 23:43:12 EDT
Created:	2020-09-18 23:40:00 EDT
Changed:	2020-09-18 23:40:49 EDT
MD5:	eed41b4500e473f97c50c7385ef5e374
SHA-256:	10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6
Hash Lookup Results:	UNKNOWN



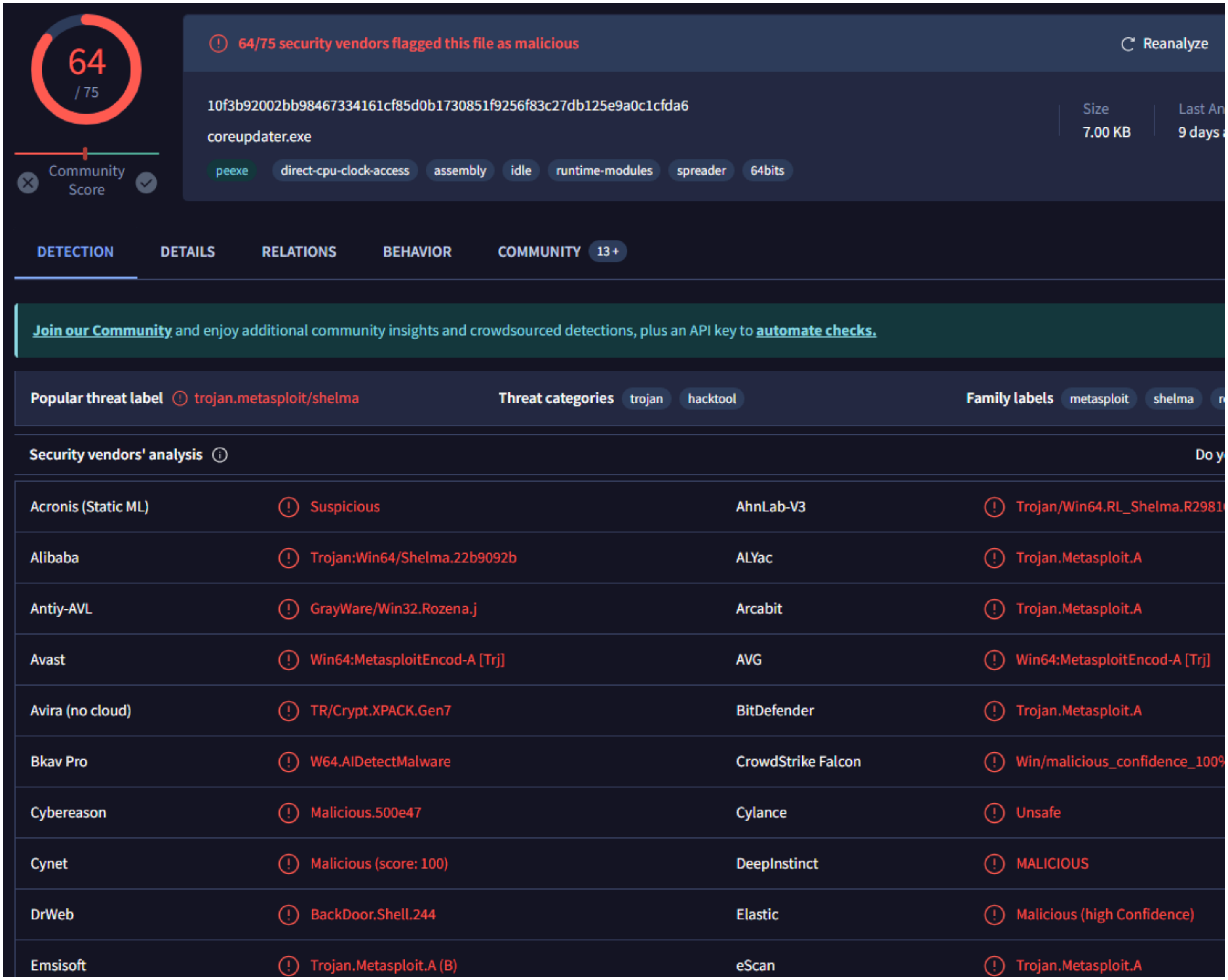
Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

Search for a hash, domain, IP address, URL or gain additional context and threat landscape visibility with OUR THREAT INTELLIGENCE OFFERING.

URL, IP address, domain, or file hash

By submitting data above, you are agreeing to our Terms of Service and Privacy Notice, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; we are not responsible for the contents of your submission. Learn more.

The results are that the file is identified as ***coreupdater.exe***, which matches the name on the system, and it also lets us know that the file is carrying the trojan ***Metasploit***. Metasploit is an example of a Remote Access Software per the Mitre ATT&CK Matrix: "*An adversary may use legitimate desktop support and remote access software to establish an interactive command and control channel to target systems within networks.*" [6]



64/75 security vendors flagged this file as malicious

10f3b92002bb98467334161cf85d0b1730851f9256f83c27db125e9a0c1cfda6

coreupdater.exe

peexe direct-cpu-clock-access assembly idle runtime-modules spreader 64bits

Size 7.00 KB

Last An 9 days

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.metasploit/shelma

Threat categories trojan hacktool

Family labels metasploit shelma r

Security vendors' analysis

Do y

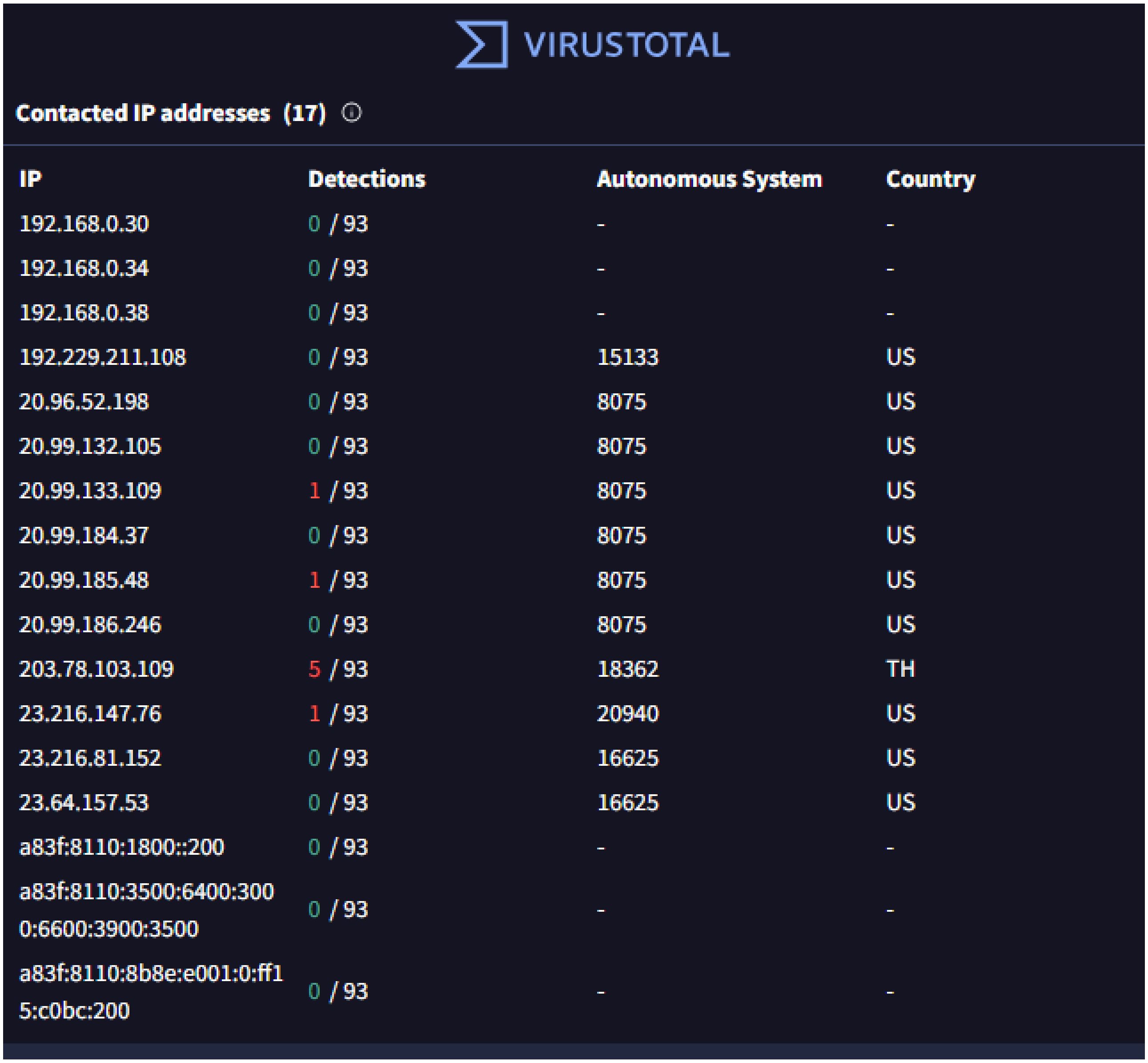
Acronis (Static ML)	Suspicious	AhnLab-V3	Trojan/Win64.RL_Shelma.R2981
Alibaba	Trojan:Win64/Shelma.22b9092b	ALYac	Trojan.Metasploit.A
Antiy-AVL	GrayWare/Win32.Rozena.j	Arcabit	Trojan.Metasploit.A
Avast	Win64:MetasploitEncod-A [Trj]	AVG	Win64:MetasploitEncod-A [Trj]
Avira (no cloud)	TR/Crypt.XPACK.Gen7	BitDefender	Trojan.Metasploit.A
Bkav Pro	W64.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100
Cybereason	Malicious.500e47	Cylance	Unsafe
Cynet	Malicious (score: 100)	DeepInstinct	MALICIOUS
DrWeb	BackDoor.Shell.244	Elastic	Malicious (high Confidence)
Emsisoft	Trojan.Metasploit.A (B)	eScan	Trojan.Metasploit.A

Identify the IP Address that delivered the payload.

Per the GET request shown in the Wireshark traffic analysis, the IP address that delivered ***coreupdater.exe*** to the network is ***194.61.24.102***.

What IP Address is the malware calling to?

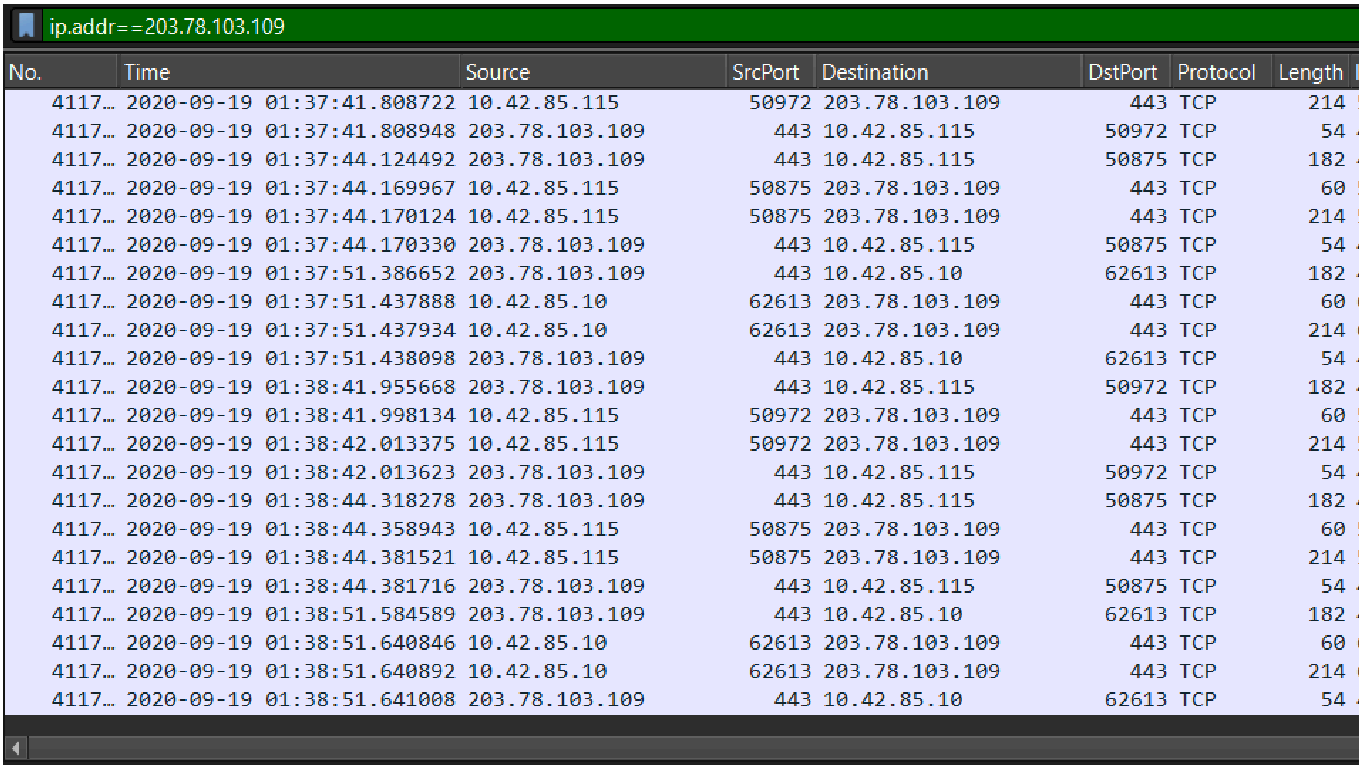
Per the analysis performed on ***coreupdater.exe*** by VirusTotal, as seen on the “Relations” tab of the file analysis, there is a list of IP addresses contacted by the malicious file. We will run the IP addresses one at a time through Wireshark’s filtering capabilities to see what network traffic is related to those IPs using the filter “ip.addr==www.xxx.yyy.zzz” where www.xxx.yyy.zzz is the IP address being searched for.



Contacted IP addresses (17)

IP	Detections	Autonomous System	Country
192.168.0.30	0 / 93	-	-
192.168.0.34	0 / 93	-	-
192.168.0.38	0 / 93	-	-
192.229.211.108	0 / 93	15133	US
20.96.52.198	0 / 93	8075	US
20.99.132.105	0 / 93	8075	US
20.99.133.109	1 / 93	8075	US
20.99.184.37	0 / 93	8075	US
20.99.185.48	1 / 93	8075	US
20.99.186.246	0 / 93	8075	US
203.78.103.109	5 / 93	18362	TH
23.216.147.76	1 / 93	20940	US
23.216.81.152	0 / 93	16625	US
23.64.157.53	0 / 93	16625	US
a83f:8110:1800::200	0 / 93	-	-
a83f:8110:3500:6400:3000:6600:3900:3500	0 / 93	-	-
a83f:8110:8b8e:e001:0:ff15:c0bc:200	0 / 93	-	-

With 6735 traffic entries between 2020-09-18 22:25:18 and 2020-09-19 01:38:51, which is more than the other marked IP addresses, we appear to have found the C&C server for this malware: ***203.78.103.109***



ip.addr==203.78.103.109

No.	Time	Source	SrcPort	Destination	DstPort	Protocol	Length
4117…	2020-09-19 01:37:41.808722	10.42.85.115	50972	203.78.103.109	443	TCP	214
4117…	2020-09-19 01:37:41.808948	203.78.103.109	443	10.42.85.115	50972	TCP	54
4117…	2020-09-19 01:37:44.124492	203.78.103.109	443	10.42.85.115	50875	TCP	182
4117…	2020-09-19 01:37:44.169967	10.42.85.115	50875	203.78.103.109	443	TCP	60
4117…	2020-09-19 01:37:44.170124	10.42.85.115	50875	203.78.103.109	443	TCP	214
4117…	2020-09-19 01:37:44.170330	203.78.103.109	443	10.42.85.115	50875	TCP	54
4117…	2020-09-19 01:37:51.386652	203.78.103.109	443	10.42.85.10	62613	TCP	182
4117…	2020-09-19 01:37:51.437888	10.42.85.10	62613	203.78.103.109	443	TCP	60
4117…	2020-09-19 01:37:51.437934	10.42.85.10	62613	203.78.103.109	443	TCP	214
4117…	2020-09-19 01:37:51.438098	203.78.103.109	443	10.42.85.10	62613	TCP	54
4117…	2020-09-19 01:38:41.955668	203.78.103.109	443	10.42.85.115	50972	TCP	182
4117…	2020-09-19 01:38:41.998134	10.42.85.115	50972	203.78.103.109	443	TCP	60
4117…	2020-09-19 01:38:42.013375	10.42.85.115	50972	203.78.103.109	443	TCP	214
4117…	2020-09-19 01:38:42.013623	203.78.103.109	443	10.42.85.115	50972	TCP	54
4117…	2020-09-19 01:38:44.318278	203.78.103.109	443	10.42.85.115	50875	TCP	182
4117…	2020-09-19 01:38:44.358943	10.42.85.115	50875	203.78.103.109	443	TCP	60
4117…	2020-09-19 01:38:44.381521	10.42.85.115	50875	203.78.103.109	443	TCP	214
4117…	2020-09-19 01:38:44.381716	203.78.103.109	443	10.42.85.115	50875	TCP	54
4117…	2020-09-19 01:38:51.584589	203.78.103.109	443	10.42.85.10	62613	TCP	182
4117…	2020-09-19 01:38:51.640846	10.42.85.10	62613	203.78.103.109	443	TCP	60
4117…	2020-09-19 01:38:51.640892	10.42.85.10	62613	203.78.103.109	443	TCP	214
4117…	2020-09-19 01:38:51.641008	203.78.103.109	443	10.42.85.10	62613	TCP	54

Where is this malware on disk?

Using the Autopsy tool, we were able to trace the file to the following location: *\Windows\System32\coreupdater.exe*

When did it first appear?

Per the Metadata present in the Autopsy tool, the local copy of ***coreupdater.exe*** was created at 2020-09-18 23:40:00 EDT

Did someone move it?

As http downloads on windows systems default to the following location: *%USERPROFILE%\Downloads,* which can also be expressed as *C:\Users\YourUserName\Downloads*,[7] the file's presence in the Windows/System32 folder indicates that the file was moved there after being created on the target system. This is an example of the Defense Evasion technique Masquerading: "*Adversaries may attempt to manipulate features of their artifacts to make them appear legitimate or benign to users and/or security tools. Masquerading occurs when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defenses and observation. This may* *include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate task or service names.*"[8]

What were the capabilities of this malware?

Metasploit was conceived as an open-source penetration testing tool, which incorporates a module-based design. As such, there are many official and community-supported modules available, but they are largely broken down into four types[9]:

- **Auxiliary -** Auxiliary modules do not exploit a target, but can perform data gathering or administrative tasks
- **Exploit -** Exploit modules leverage vulnerabilities in a manner that allows the framework to execute arbitrary code on the target host
- **Payloads -** Arbitrary code that can be executed on a remote target to perform a task, such as creating users, opening shells, etc
- **Post -** Post modules are used after a machine has been compromised. They perform useful tasks such as gathering, collecting, or enumerating data from a session.

Some activities that a baseline installation of ***Metasploit*** can engage in are as follows:

- **Kerberos Login/Brute Force**: Kerberos is an authentication protocol. In response to a client proving their identity, Kerberos generates tickets which can be used to further interact with systems as a proof of identity. Metasploit is capable of automating Kerberos logins with enough frequency to be used as a tool for Brute Force attacks. Per the Mitre ATT&CK Enterprise Matrix, Brute Force are "*Without knowledge of the password for an account or set of accounts, an adversary may systematically guess the password using a repetitive or iterative mechanism.*"[10]
- **Database Suppor**t: ***Metasploit*** can connect directly to a database to perform the following actions:
  - Recording other machines on a network that are found with a nmap scan via the db_nmap command are stored as "Hosts".
    - Hosts can be viewed with the hosts command.
  - Storing credentials successfully extracted by exploits are stored as "creds".
    - Credentials are viewed with the creds command.
  - Keeping track of successful exploitation attempts are recorded as "Vulnerabilities".
    - Successful exploitations can be viewed with the vulns command.
    - The vulns command also tracks unsuccessful exploitation attempts
  - Storing services detected on remote hosts by db_nmap are recorded as "Services"
    - Remote services are viewed with the services command
  - Tracking multiple remote sessions opened by exploit payloads
    - These sessions can be managed and tracked with the sessions command.
  - Storing any difficult to define information returned by successful exploits as "Loot"
    - Viewable with the loot command

    - Keeping track of “Ping back payloads”, a non-interactive payload type that provides users with confirmation of remote execution on a target
    - Pivot through a network with “Routes” comprised of active sessions
        - Viewable with the routes command
    - Building reports comprising all of the above information (Restricted to Pro users)
- **Evading Antivirus**: ***Metasploit*** has robust Antivirus evasion techniques built into it, such as dynamic payload encoding, as well as manual obfuscation method support. This is an example of the Defense Evasion technique Deobfuscate/Decode Files or Information, “*Adversaries may use Obfuscated Files or Information to hide artifacts of an intrusion from analysis.*”[11]
- **Exploit Module Ranking**: Users can define rankings for individual Exploit Modules, which allows searching and sorting of various default and community modules.
- **Hash and Password Cracking:** Metasploit supports hash identification, as well as hash cracking and password cracking using the .jtr filetype, which can be reviewed with *John the Ripper*[12]in order to complete the decoding. Additional plugins allow for the .jtr files to be formatted for *hashcat*[13]decoding. Both of these programs are free to use, making this a useful inclusion.
- **Payload UUID:** Users are able to apply unique user identifiers to payloads, in order to track which user has executed the malware.

Is this malware easily obtained?

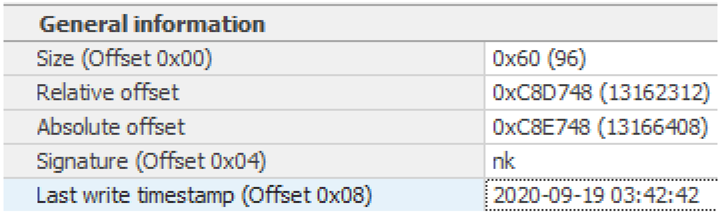
Yes, ***Metasploit*** is an open-source project, with a paid branch; it is easily available on the internet, as it was designed as a penetration testing tool.[14]

Was this malware installed with persistence on any machine?

Using Registry Explorer, we were able to validate that there were registry keys created for the executable ***coreupdater.exe***; reflecting the MITRE ATT&CK matrix Defense Evasion entry for Modify Registry[15].

When?

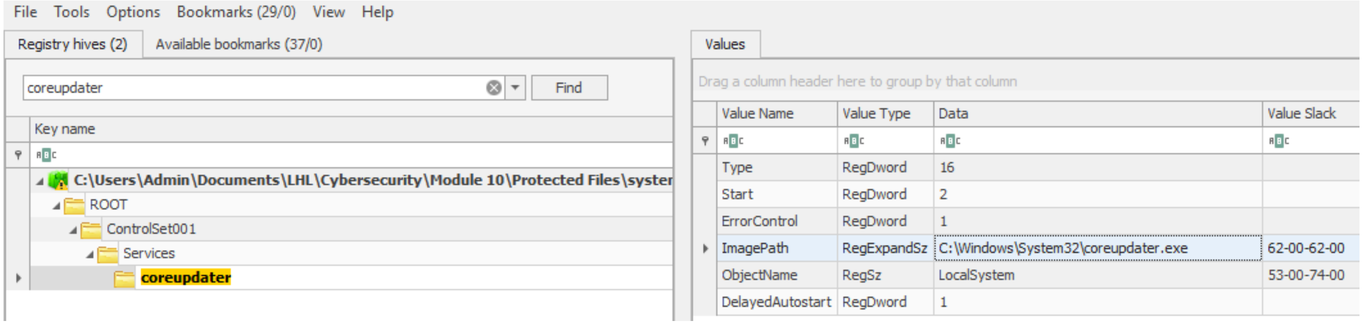
While the Registry Explorer does not allow us to determine the exact time of installation, we can review the Last write timestamp for the entry, which occurred at 2020-09-19 03:42:42, giving us a starting point of activity for the malware.



General information	
Size (Offset 0x00)	0x60 (96)
Relative offset	0xC8D748 (13162312)
Absolute offset	0xC8E748 (13166408)
Signature (Offset 0x04)	nk
Last write timestamp (Offset 0x08)	2020-09-19 03:42:42

Where?

In the system registry, at the following address: *system\ROOT\ControlSet001\Services\coreupdater*


File
Tools
Options
Bookmarks (29/0)
View
Help
Registry hives (2)
Available bookmarks (37/0)
Find
Values
Drag a column header here to group by that column

coreupdater

Key name

- C:\Users\Admin\Documents\LHL\Cybersecurity\Module 10\Protected Files\syster
  - ROOT
    - ControlSet001
      - Services
        - **coreupdater**

Value Name	Value Type	Data	Value Slack
Type	RegDword	16	
Start	RegDword	2	
ErrorControl	RegDword	1	
ImagePath	RegExpandSz	C:\Windows\System32\coreupdater.exe	62-00-62-00
ObjectName	RegSz	LocalSystem	53-00-74-00
DelayedAutostart	RegDword	1	

As well, the malicious file ***coreupdater.exe*** was included in the autorun program csv file for both the Desktop and DC, indicating that it should be run when the machine starts up; this is indicative of the Execution Persistence and Privilege Escalation tactic Scheduled Task/Job[16].

What malicious IP Addresses were involved?

The two main malicious IP Addresses involved in the attack are:

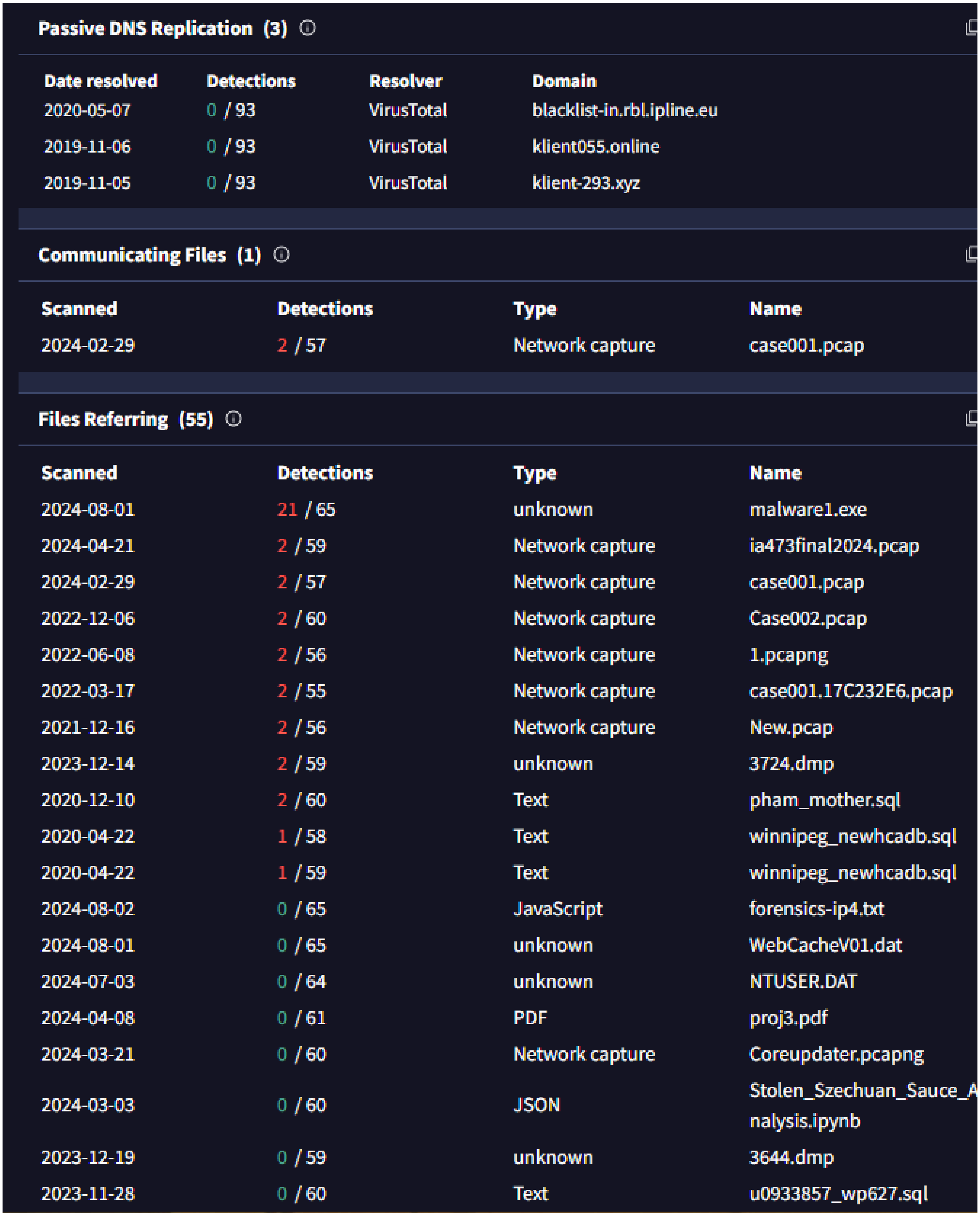
- ***194.61.24.102:*** The scanning and initial malware delivery server, located in the Russian city of Leninsky in the Tul'skaya oblast.
- ***203.78.103.109:*** The Command and Capture (C+C) server, located in the Thai city of Bangkok, in the Krung Thep Maha Nakhon region.

Were any IP Addresses from known adversary infrastructure?

Neither of the IP addresses are from known adversary infrastructure, however, the Proxy Detection Test from ipqualityscore.com indicated that the IP reputation of 194.61.24.102 was rated at high risk, and frequently allows IP tunneling for malicious behavior; this can explain the difference between the locations of the scanning and initial malware delivery and the Command and Capture server.

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

Yes, the IP address 194.61.24.102 is involved in multiple other malware flags from VirusTotal's database, with multiple different associated files.



Passive DNS Replication (3)

Date resolved	Detections	Resolver	Domain
2020-05-07	0 / 93	VirusTotal	blacklist-in.rbl.ipline.eu
2019-11-06	0 / 93	VirusTotal	klient055.online
2019-11-05	0 / 93	VirusTotal	klient-293.xyz

Communicating Files (1)

Scanned	Detections	Type	Name
2024-02-29	2 / 57	Network capture	case001.pcap

Files Referring (55)

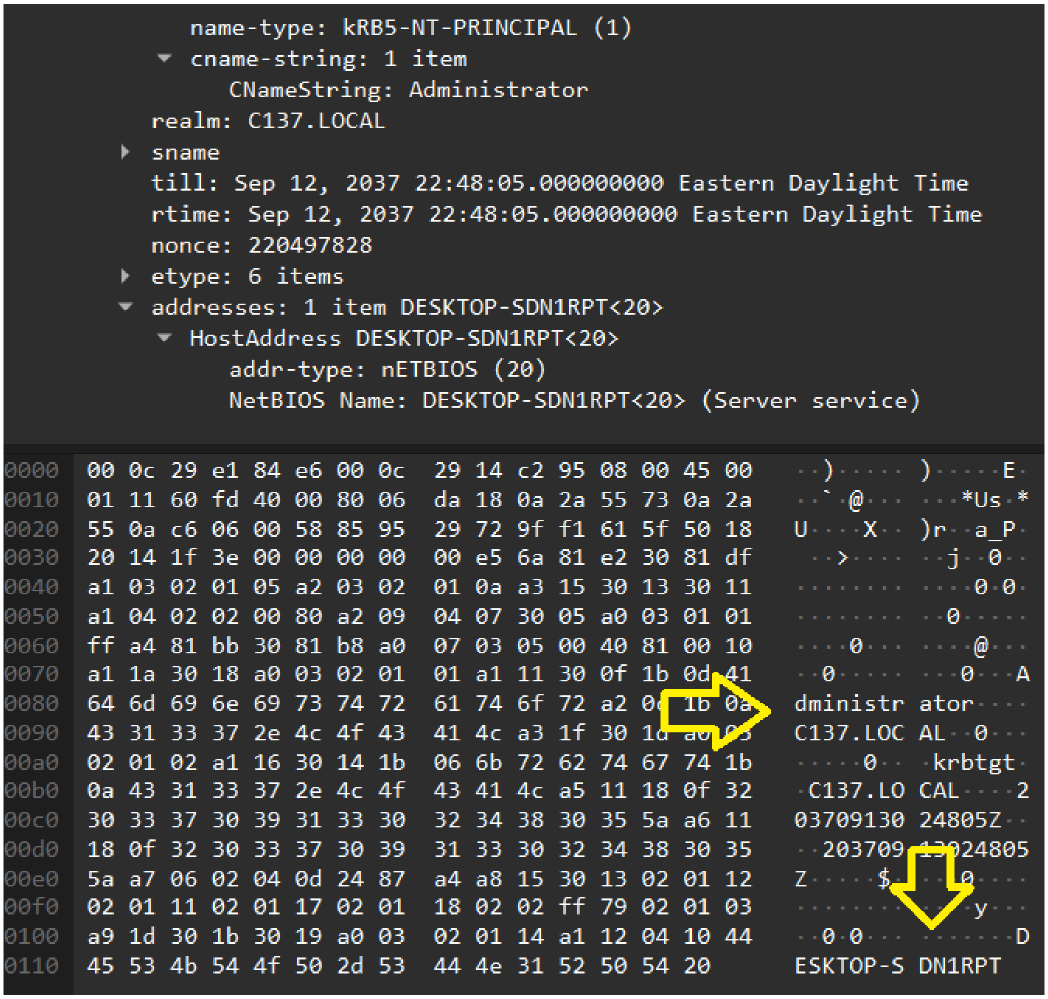
Scanned	Detections	Type	Name
2024-08-01	21 / 65	unknown	malware1.exe
2024-04-21	2 / 59	Network capture	ia473final2024.pcap
2024-02-29	2 / 57	Network capture	case001.pcap
2022-12-06	2 / 60	Network capture	Case002.pcap
2022-06-08	2 / 56	Network capture	1.pcapng
2022-03-17	2 / 55	Network capture	case001.17C232E6.pcap
2021-12-16	2 / 56	Network capture	New.pcap
2023-12-14	2 / 59	unknown	3724.dmp
2020-12-10	2 / 60	Text	pham_mother.sql
2020-04-22	1 / 58	Text	winnipeg_newhcadb.sql
2020-04-22	1 / 59	Text	winnipeg_newhcadb.sql
2024-08-02	0 / 65	JavaScript	forensics-ip4.txt
2024-08-01	0 / 65	unknown	WebCacheV01.dat
2024-07-03	0 / 64	unknown	NTUSER.DAT
2024-04-08	0 / 61	PDF	proj3.pdf
2024-03-21	0 / 60	Network capture	Coreupdater.pcapng
2024-03-03	0 / 60	JSON	Stolen_Szechuan_Sauce_Analysis.ipynb
2023-12-19	0 / 59	unknown	3644.dmp
2023-11-28	0 / 60	Text	u0933857_wp627.sql

Did the attacker access any other systems?

Yes; by analyzing the traffic recording with Wireshark, and using the filer “tcp.stream eq 30468” without quotes. This allows us to find the specific tcp stream (#30468) where the attacker accesses the Desktop C137\DESKTOP-SDN1RPT. This indicates a use of the Lateral Movement tactic sub-technique of Remote Services, “*Adversaries may use Valid Accounts to log into a service that accepts remote connections, such as telnet, SSH, and VNC. The adversary may then perform actions as the logged-on user.*” [17]

How?

By verifying the data in the Kerberos section of Packet 266013, we can conclude that the Administrator account from the Domain Controller (DC) has accessed the Desktop-SDN1RPT



```
          name-type: kRB5-NT-PRINCIPAL (1)
        ▾ cname-string: 1 item
            CNameString: Administrator
      realm: C137.LOCAL
    ▸ sname
      till: Sep 12, 2037 22:48:05.000000000 Eastern Daylight Time
      rtime: Sep 12, 2037 22:48:05.000000000 Eastern Daylight Time
      nonce: 220497828
    ▸ etype: 6 items
    ▾ addresses: 1 item DESKTOP-SDN1RPT<20>
        ▾ HostAddress DESKTOP-SDN1RPT<20>
            addr-type: nETBIOS (20)
            NetBIOS Name: DESKTOP-SDN1RPT<20> (Server service)

0000  00 0c 29 e1 84 e6 00 0c  29 14 c2 95 08 00 45 00   ··)····· )·····E·
0010  01 11 60 fd 40 00 80 06  da 18 0a 2a 55 73 0a 2a   ··`·@··· ···*Us·*
0020  55 0a c6 06 00 58 85 95  29 72 9f f1 61 5f 50 18   U····X·· )r··a_P·
0030  20 14 1f 3e 00 00 00 00  00 e5 6a 81 e2 30 81 df    ··>···· ··j··0··
0040  a1 03 02 01 05 a2 03 02  01 0a a3 15 30 13 30 11   ········ ····0·0·
0050  a1 04 02 02 00 80 a2 09  04 07 30 05 a0 03 01 01   ········ ··0·····
0060  ff a4 81 bb 30 81 b8 a0  07 03 05 00 40 81 00 10   ····0··· ····@···
0070  a1 1a 30 18 a0 03 02 01  01 a1 11 30 0f 1b 0d 41   ··0····· ···0···A
0080  64 6d 69 6e 69 73 74 72  61 74 6f 72 a2 0c 1b 0a   dministr ator····
0090  43 31 33 37 2e 4c 4f 43  41 4c a3 1f 30 1d a0 03   C137.LOC AL··0···
00a0  02 01 02 a1 16 30 14 1b  06 6b 72 62 74 67 74 1b   ·····0·· ·krbtgt·
00b0  0a 43 31 33 37 2e 4c 4f  43 41 4c a5 11 18 0f 32   ·C137.LO CAL····2
00c0  30 33 37 30 39 31 33 30  32 34 38 30 35 5a a6 11   03709130 24805Z··
00d0  18 0f 32 30 33 37 30 39  31 33 30 32 34 38 30 35   ··203709 13024805
00e0  5a a7 06 02 04 0d 24 87  a4 a8 15 30 13 02 01 12   Z·····$· ···0····
00f0  02 01 11 02 01 17 02 01  18 02 02 ff 79 02 01 03   ········ ····y···
0100  a9 1d 30 1b 30 19 a0 03  02 01 14 a1 12 04 10 44   ··0·0··· ·······D
0110  45 53 4b 54 4f 50 2d 53  44 4e 31 52 50 54 20      ESKTOP-S DN1RPT
```

When?

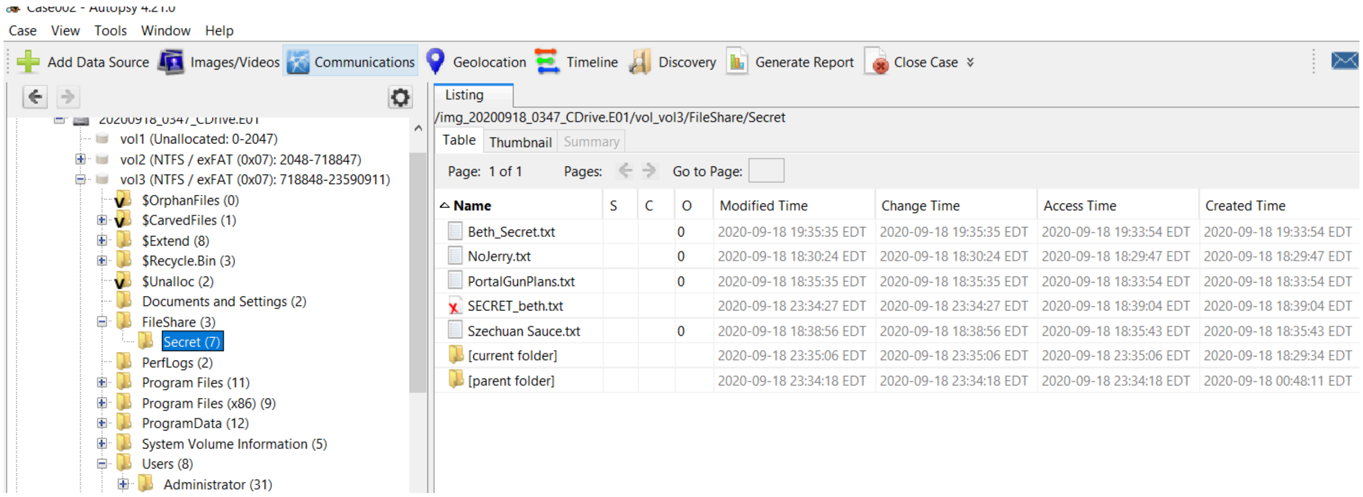
Per the network traffic capture, the access was obtained at 2020-09-18 22:36:24 EDT

Did the attacker steal or access any data?

Yes, the attacker used the Administrator account to access the Secret subfolder of the FileShare folder on the Domain Controller, interacting with the files NoJerry.txt, PortalGunPlans.txt, Szechuan Sauce.txt and SECRET_beth.txt. Furthermore, the file SECRET_beth.txt was deleted, and replaced with the file Beth_Secret.txt.

When?

The file accesses all took place at around 2020-09-18 18:29:47-18:39:04 EDT; Beth_Secret.txt was created at 2020-09-18 19:33:54 EDT, and SECRET_beth.txt was deleted at 2020-09-18 23:34:27 EDT



/img_20200918_0347_CDrive.E01/vol_vol3/FileShare/Secret

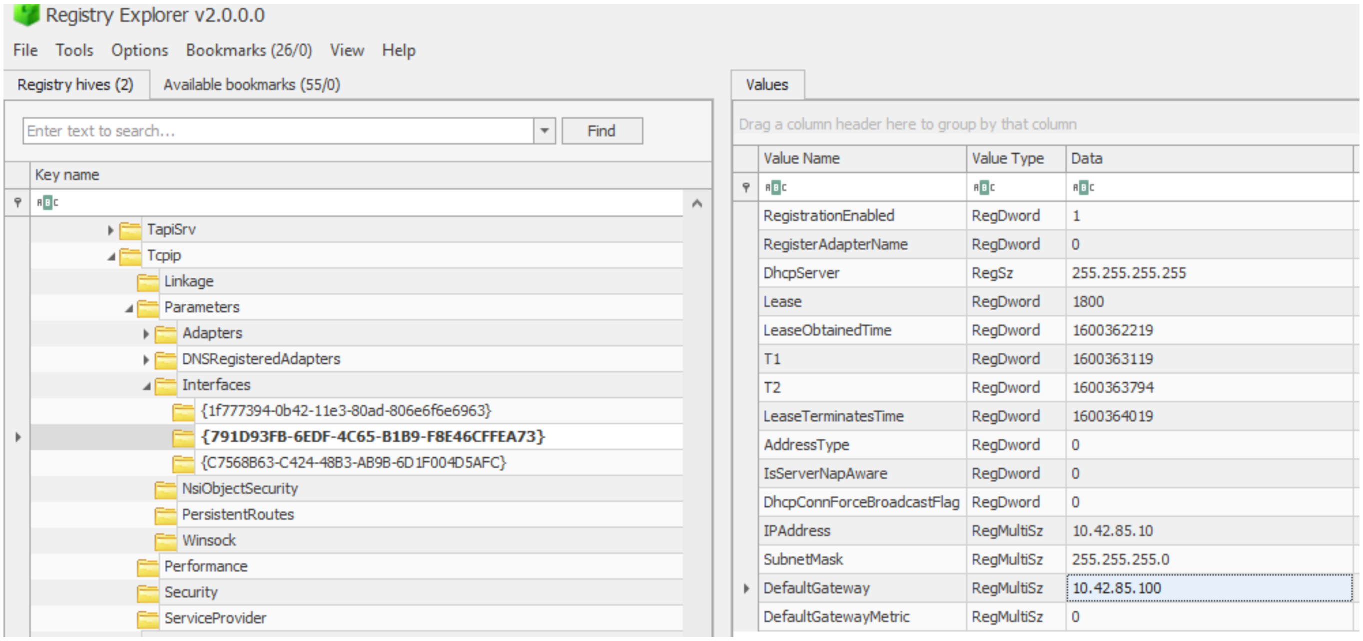
Page: 1 of 1   Pages: Go to Page:

Name	S	C	O	Modified Time	Change Time	Access Time	Created Time
Beth_Secret.txt			0	2020-09-18 19:35:35 EDT	2020-09-18 19:35:35 EDT	2020-09-18 19:33:54 EDT	2020-09-18 19:33:54 EDT
NoJerry.txt			0	2020-09-18 18:30:24 EDT	2020-09-18 18:30:24 EDT	2020-09-18 18:29:47 EDT	2020-09-18 18:29:47 EDT
PortalGunPlans.txt			0	2020-09-18 18:35:35 EDT	2020-09-18 18:35:35 EDT	2020-09-18 18:33:54 EDT	2020-09-18 18:33:54 EDT
SECRET_beth.txt				2020-09-18 23:34:27 EDT	2020-09-18 23:34:27 EDT	2020-09-18 18:39:04 EDT	2020-09-18 18:39:04 EDT
Szechuan Sauce.txt			0	2020-09-18 18:38:56 EDT	2020-09-18 18:38:56 EDT	2020-09-18 18:35:43 EDT	2020-09-18 18:35:43 EDT
[current folder]				2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT	2020-09-18 23:35:06 EDT	2020-09-18 18:29:34 EDT
[parent folder]				2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT	2020-09-18 23:34:18 EDT	2020-09-18 00:48:11 EDT

What was the network layout of the victim network?

By using the Registry Explorer tool, we can review the configuration of the victim's network. Having loaded the System registry indexes for both the Desktop and Domain Controller, IP address information was accessed by navigating to the following path: *System* > *Controlset001* > *Services* > *Tcpip* > *Parameters* > *Interfaces* and reviewing the content within.

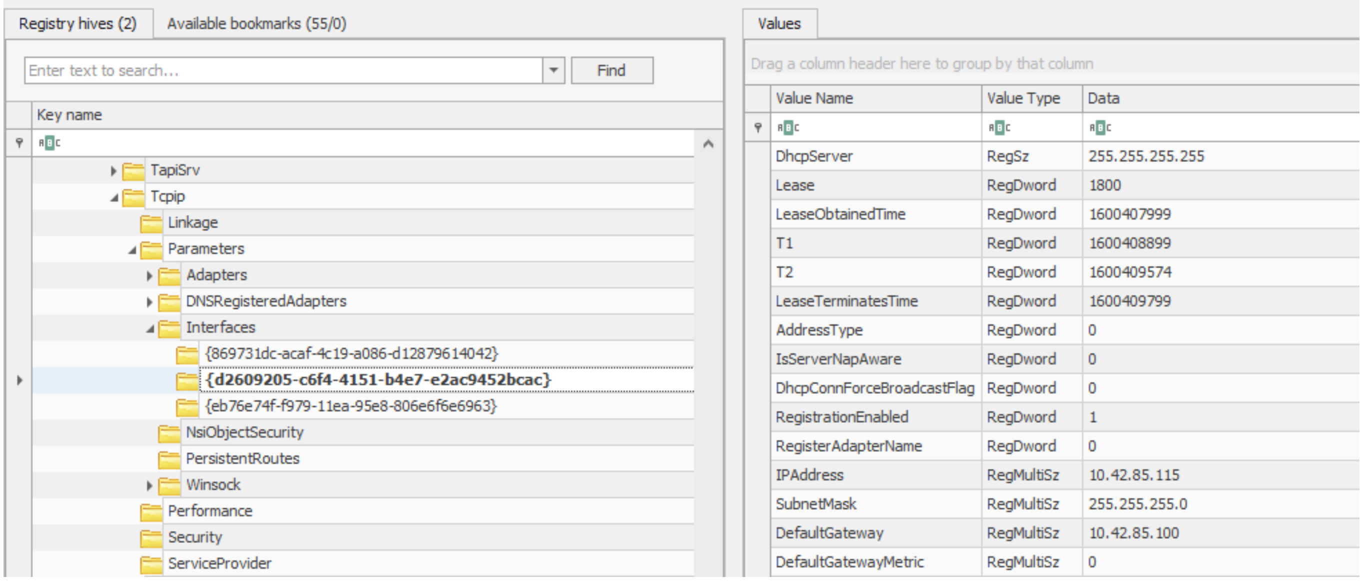
Domain Controller:


Registry Explorer v2.0.0.0
File Tools Options Bookmarks (26/0) View Help
Registry hives (2) Available bookmarks (55/0)
Enter text to search...
Find
Values
Drag a column header here to group by that column

```
Key name
        TapiSrv
        Tcpip
          Linkage
          Parameters
            Adapters
            DNSRegisteredAdapters
            Interfaces
              {1f777394-0b42-11e3-80ad-806e6f6e6963}
              {791D93FB-6EDF-4C65-B1B9-F8E46CFFEA73}
              {C7568B63-C424-48B3-AB9B-6D1F004D5AFC}
            NsiObjectSecurity
            PersistentRoutes
            Winsock
          Performance
          Security
          ServiceProvider
```

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

Desktop:


Registry hives (2) Available bookmarks (55/0)
Enter text to search...
Find
Values
Drag a column header here to group by that column

```
Key name
        TapiSrv
        Tcpip
          Linkage
          Parameters
            Adapters
            DNSRegisteredAdapters
            Interfaces
              {869731dc-acaf-4c19-a086-d12879614042}
              {d2609205-c6f4-4151-b4e7-e2ac9452bcac}
              {eb76e74f-f979-11ea-95e8-806e6f6e6963}
            NsiObjectSecurity
            PersistentRoutes
            Winsock
          Performance
          Security
          ServiceProvider
```

Value Name	Value Type	Data
DhcpServer	RegSz	255.255.255.255
Lease	RegDword	1800
LeaseObtainedTime	RegDword	1600407999
T1	RegDword	1600408899
T2	RegDword	1600409574
LeaseTerminatesTime	RegDword	1600409799
AddressType	RegDword	0
IsServerNapAware	RegDword	0
DhcpConnForceBroadcastFlag	RegDword	0
RegistrationEnabled	RegDword	1
RegisterAdapterName	RegDword	0
IPAddress	RegMultiSz	10.42.85.115
SubnetMask	RegMultiSz	255.255.255.0
DefaultGateway	RegMultiSz	10.42.85.100
DefaultGatewayMetric	RegMultiSz	0

The identical SubnetMask of 255.255.255.0 for both systems indicates that they are on the 10.42.85.0/24 subnet.[18]

What architecture changes should be made immediately?

The ability to use RDP connections on the Domain Controller should be immediately removed for remote connections, either via a firewall access or by securing RDP connections behind a VPN service. This follows the **NIST SP 800-53** Controls **AC-17 REMOTE ACCESS (Sub-control AC-17(02))**[19] and **CM-07 LEAST FUNCTIONALITY** [20].

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

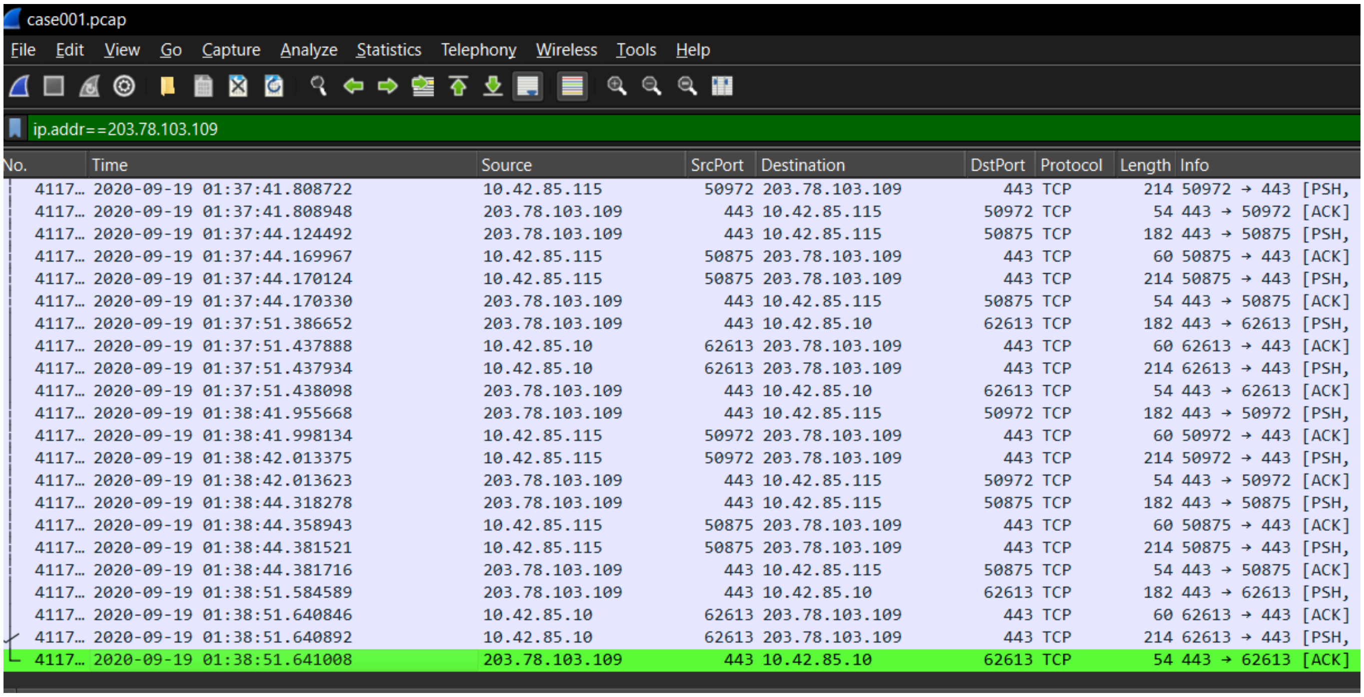
Yes, the attacker used the Administrator account to access the Secret subfolder of the FileShare folder on the Domain Controller, interacting with the file Szechuan Sauce.txt, at 2020-09-18 18:38:56 EDT.

Did the attacker steal or access any other sensitive files? If so, what times?

Yes, the attacker used the Administrator account to access the Secret subfolder of the FileShare folder on the Domain Controller, interacting with the files NoJerry.txt, PortalGunPlans.txt, and SECRET_beth.txt. Furthermore, the file SECRET_beth.txt was deleted, and replaced with the file Beth_Secret.txt. The file accesses all took place at around 2020-09-18 18:29:47-18:39:04 EDT; Beth_Secret.txt was created at 2020-09-18 19:33:54 EDT, and SECRET_beth.txt was deleted at 2020-09-18 23:34:27 EDT

Finally, when was the last known contact with the adversary?

Last known contact with the adversary is at 2020-09-19 01.38.51, when the RDP connection is terminated.



```
ip.addr==203.78.103.109
```

```
No.     Time                         Source           SrcPort Destination      DstPort Protocol Length Info
 4117… 2020-09-19 01:37:41.808722   10.42.85.115      50972 203.78.103.109     443 TCP      214 50972 → 443 [PSH,
 4117… 2020-09-19 01:37:41.808948   203.78.103.109      443 10.42.85.115     50972 TCP       54 443 → 50972 [ACK]
 4117… 2020-09-19 01:37:44.124492   203.78.103.109      443 10.42.85.115     50875 TCP      182 443 → 50875 [PSH,
 4117… 2020-09-19 01:37:44.169967   10.42.85.115      50875 203.78.103.109     443 TCP       60 50875 → 443 [ACK]
 4117… 2020-09-19 01:37:44.170124   10.42.85.115      50875 203.78.103.109     443 TCP      214 50875 → 443 [PSH,
 4117… 2020-09-19 01:37:44.170330   203.78.103.109      443 10.42.85.115     50875 TCP       54 443 → 50875 [ACK]
 4117… 2020-09-19 01:37:51.386652   203.78.103.109      443 10.42.85.10      62613 TCP      182 443 → 62613 [PSH,
 4117… 2020-09-19 01:37:51.437888   10.42.85.10       62613 203.78.103.109     443 TCP       60 62613 → 443 [ACK]
 4117… 2020-09-19 01:37:51.437934   10.42.85.10       62613 203.78.103.109     443 TCP      214 62613 → 443 [PSH,
 4117… 2020-09-19 01:37:51.438098   203.78.103.109      443 10.42.85.10      62613 TCP       54 443 → 62613 [ACK]
 4117… 2020-09-19 01:38:41.955668   203.78.103.109      443 10.42.85.115     50972 TCP      182 443 → 50972 [PSH,
 4117… 2020-09-19 01:38:41.998134   10.42.85.115      50972 203.78.103.109     443 TCP       60 50972 → 443 [ACK]
 4117… 2020-09-19 01:38:42.013375   10.42.85.115      50972 203.78.103.109     443 TCP      214 50972 → 443 [PSH,
 4117… 2020-09-19 01:38:42.013623   203.78.103.109      443 10.42.85.115     50972 TCP       54 443 → 50972 [ACK]
 4117… 2020-09-19 01:38:44.318278   203.78.103.109      443 10.42.85.115     50875 TCP      182 443 → 50875 [PSH,
 4117… 2020-09-19 01:38:44.358943   10.42.85.115      50875 203.78.103.109     443 TCP       60 50875 → 443 [ACK]
 4117… 2020-09-19 01:38:44.381521   10.42.85.115      50875 203.78.103.109     443 TCP      214 50875 → 443 [PSH,
 4117… 2020-09-19 01:38:44.381716   203.78.103.109      443 10.42.85.115     50875 TCP       54 443 → 50875 [ACK]
 4117… 2020-09-19 01:38:51.584589   203.78.103.109      443 10.42.85.10      62613 TCP      182 443 → 62613 [PSH,
 4117… 2020-09-19 01:38:51.640846   10.42.85.10       62613 203.78.103.109     443 TCP       60 62613 → 443 [ACK]
 4117… 2020-09-19 01:38:51.640892   10.42.85.10       62613 203.78.103.109     443 TCP      214 62613 → 443 [PSH,
 4117… 2020-09-19 01:38:51.641008   203.78.103.109      443 10.42.85.10      62613 TCP       54 443 → 62613 [ACK]
```

Works Cited:

[1] MITRE Corporation. (n.d.). Enterprise matrix. Matrix - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/matrices/enterprise/

[2] Internet Assigned Numbers Authority. (n.d.). Internet control message protocol (ICMP) parameters. Internet Assigned Numbers Authority. https://www.iana.org/assignments/icmp-parameters/icmp-parameters.xhtml#icmp-parameters-types

[3] MITRE Corporation. (n.d.). Active scanning. Active Scanning, Technique T1595 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1595/

[4] SpeedGuide. (n.d.). Port 3389 (TCP/UDP). https://www.speedguide.net/port.php?port=3389

[5] MITRE Corporation. (n.d.). Exploit public-facing application. Exploit Public-Facing Application, Technique T1190 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1190/

[6] MITRE Corporation. (n.d.). Remote Access Software. Remote Access Software, Technique T1219 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1219/

[7] TaxDome. (n.d.). How to specify where files are downloaded. TaxDome Client Knowledge Base. https://client-help.taxdome.com/article/28-how-to-specify-where-files-are-downloaded

[8] MITRE Corporation. (n.d.). Masquerading. Masquerading, Technique T1036 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1036/

[9] Modules. Metasploit Documentation Penetration Testing Software, Pen Testing Security. (n.d.). https://docs.metasploit.com/docs/modules.html

[10] MITRE Corporation. (n.d.). Brute Force. Brute Force, Technique T1110 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1110/

[11] MITRE Corporation. (n.d.). Deobfuscate/decode files or information. Deobfuscate/Decode Files or Information, Technique T1140 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1140/

[12] Openwall. (n.d.). John the ripper password cracker. John the Ripper. https://www.openwall.com/john/

[13] hashcat. (n.d.). Hashcat advanced password recovery. hashcat. https://hashcat.net/hashcat/

[14] Metasploit. (n.d.). Penetration testing software, PEN testing security. Metasploit. https://www.metasploit.com/

[15] MITRE Corporation. (n.d.). Modify registry. Modify Registry, Technique T1112 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1112/

[16] MITRE Corporation. (n.d.). Scheduled Task/job. Scheduled Task/Job, Technique T1053 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1053/

[17] MITRE Corporation. (n.d.). Remote Services. Remote Services, Technique T1021 - Enterprise | MITRE ATT&CK®. https://attack.mitre.org/techniques/T1021/

[18] Calculator.net. (n.d.). Home. Calculator.net. https://www.calculator.net/ip-subnet-calculator.html?cclass=any&csubnet=24&cip=10.42.85.10&ctype=ipv4&x=Calculate

[19] Computer Security Division, I. T. L. (n.d.). Access CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=AC-17

[20] Computer Security Division, I. T. L. (n.d.-a). Access CPRT - cybersecurity and privacy reference tool: CSRC. CSRC. https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/SP_800_53_5_1_1/home?element=CM-07

Tools Used:

Wireshark: Free network protocol analysis tool, Wireshark allows for filtering network traffic that it captures.

Autopsy: Autopsy® is an end-to-end open source digital forensics platform. Built by Sleuth Kit Labs, Autopsy is a fast, thorough, and efficient hard drive investigation solution that evolves with the industry’s needs.

Registry Editor: A registry viewer with searching, multi-hive support, plugins, and more. Handles locked files

VirusTotal: A community-driven, free virus analysis tool; supports file uploads, URL submissions, as well as a search feature that scans across IP Addresses, Domains or File Hashes.