Tracking Cobalt Strike: A Trend Micro Vision One Investigation

trendmicro.com/en_us/research/21/g/tracking_cobalt_strike_a_vision_one_investigation.html

July 5, 2021

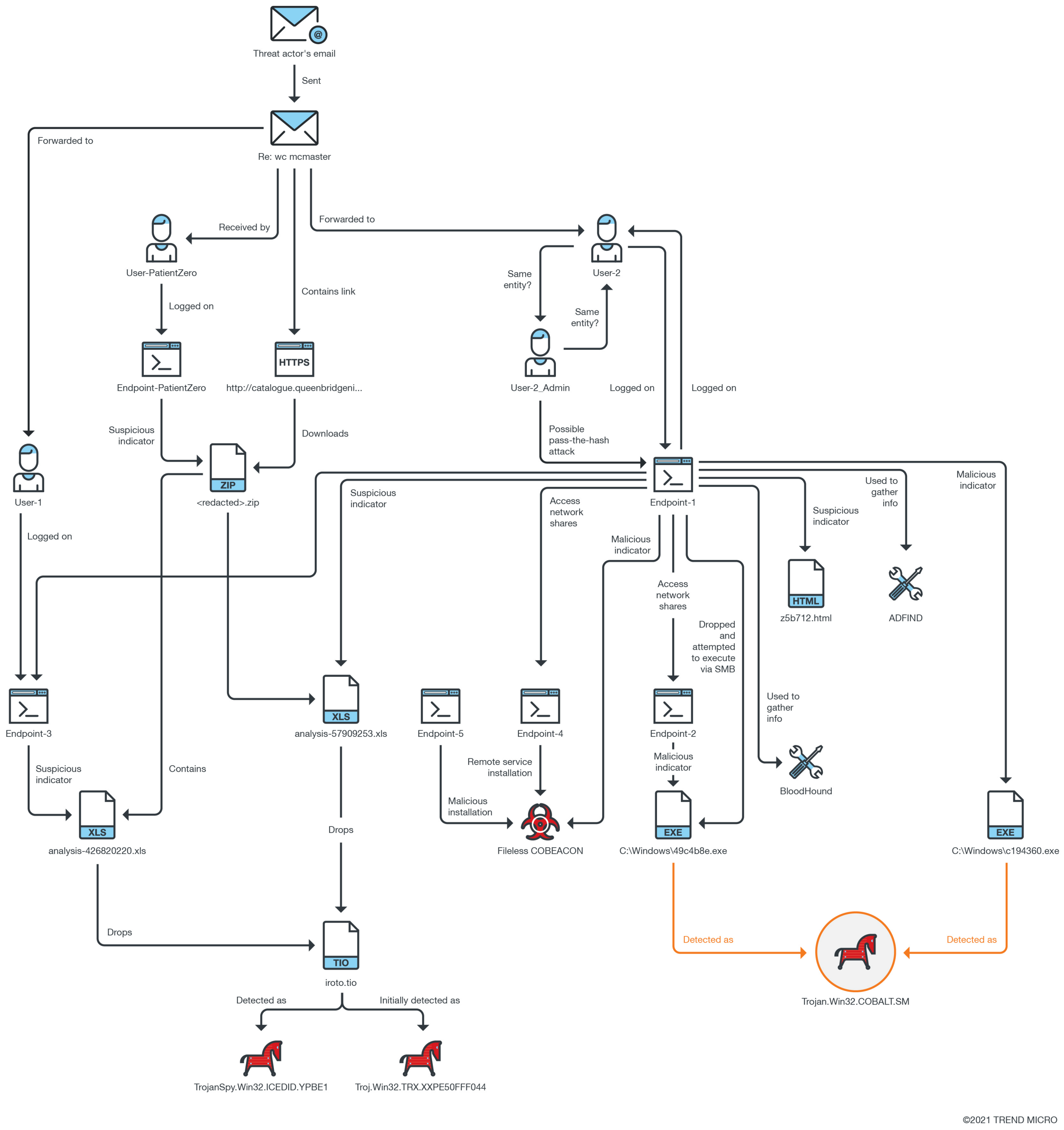


Figure 1. The mapped-out activity of Cobalt Strike in the affected environment

In late May, Trend Micro Managed XDR alerted a customer to a noteworthy Vision One alert on one of their endpoints. What followed was a deeper investigation that involved searching for other similarly infected endpoints and the confirmation of a Cobalt Strike detection.

This blog will cover the tactics and steps we took during this investigation. The alert from one endpoint led to the collection of further evidence and clues that pointed to other infected endpoints, eventually revealing the root of the attack.

Cobalt Strike is a well-known beacon or post-exploitation tool that has been linked to ransomware families like Ryuk, DoppelPaymer, and Povlsomware. The Cobalt Strike variant used here follows its typical characteristics. However, this report focuses on the process of uncovering its tracks in order to fully contain and remove the malware.

An overview of the investigation

We first uncovered several detections related to Cobalt Strike, accompanied by a machine learning detection later verified as IcedID. In such cases, the initial detections usually point to something big: the distribution of ransomware. In fact, we published a report on a similar case wherein we used Cobalt Strike to track a Conti ransomware campaign.

Before we delve into the details we want to detail the process we followed in this investigation. It involved several interconnected steps that occurred simultaneously and repeatedly throughout the process. These steps are mainly:

- Creating an indicators of compromise (IOCs) list and observe for tactics, techniques, and procedures (TTPs) to check in the environment, which will be improved in the next items
- Checking the context of the generated alerts
- Examining the execution profile of the files related to the detection
- Collecting additional logs from the endpoint to correlate events
- Checking detections that occurred around the time range of the alerts

These steps allowed us to retrace the actions taken by the variant from a single endpoint and revealing the full extent and its origins. Figure 1 maps out the Cobalt Strike activity that we tracked; it also indicates where we started, at Endpoint-1.

It is important to note that we already provided the affected customer our initial response very early into the investigation, allowing them to start taking steps to contain the threat as we worked to fully reveal its extent.

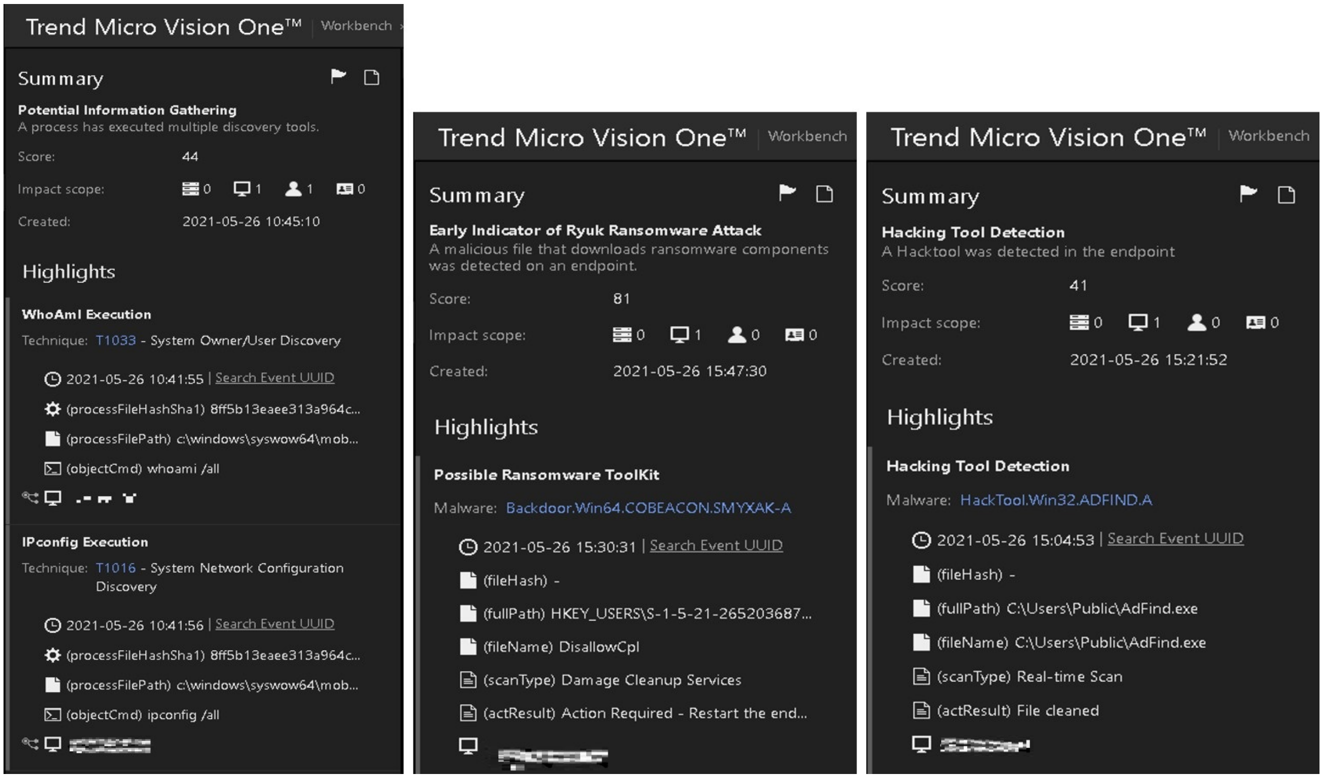
Initial detections, IOCs, and observed TTPs

As we had mentioned earlier, our investigation started when we noticed suspicious activity in one endpoint. For the purpose of this discussion we shall label this endpoint as Endpoint-1, since this is where we encountered the first hints of an attack. We began our investigation from this endpoint to uncover the real entry point.

Endpoint-1

Checking the alerts of Endpoint-1 revealed several important findings that sparked the investigation:

- AdFind.exe was downloaded in the Users\Public directory
- A Cobalt Strike detection occurred, as seen in Figure 1
- Mobsync.exe executed information gathering commands



Trend Micro Vision One™ | Workbench

Summary

Potential Information Gathering

A process has executed multiple discovery tools.

Score: 44

Impact scope: 0 1 1 0

Created: 2021-05-26 10:45:10

Highlights

WhoAmI Execution

Technique: T1033 - System Owner/User Discovery

2021-05-26 10:41:55 | Search Event UUID

(processFileHashSha1) 8ff5b13eaee313a964c...

(processFilePath) c:\windows\syswow64\mob...

(objectCmd) whoami /all

[redacted]

IPconfig Execution

Technique: T1016 - System Network Configuration Discovery

2021-05-26 10:41:56 | Search Event UUID

(processFileHashSha1) 8ff5b13eaee313a964c...

(processFilePath) c:\windows\syswow64\mob...

(objectCmd) ipconfig /all

[redacted]

Trend Micro Vision One™ | Workbench

Summary

Early Indicator of Ryuk Ransomware Attack

A malicious file that downloads ransomware components was detected on an endpoint.

Score: 81

Impact scope: 0 1 0 0

Created: 2021-05-26 15:47:30

Highlights

Possible Ransomware ToolKit

Malware: Backdoor.Win64.COBEACON.SMYXAK-A

2021-05-26 15:30:31 | Search Event UUID

(fileHash) -

(fullPath) HKEY_USERS\S-1-5-21-265203687...

(fileName) DisallowCpl

(scanType) Damage Cleanup Services

(actResult) Action Required - Restart the end...

[redacted]

Trend Micro Vision One™ | Workbench

Summary

Hacking Tool Detection

A Hacktool was detected in the endpoint

Score: 41

Impact scope: 0 1 0 0

Created: 2021-05-26 15:21:52

Highlights

Hacking Tool Detection

Malware: HackTool.Win32.ADFIND.A

2021-05-26 15:04:53 | Search Event UUID

(fileHash) -

(fullPath) C:\Users\Public\AdFind.exe

(fileName) C:\Users\Public\AdFind.exe

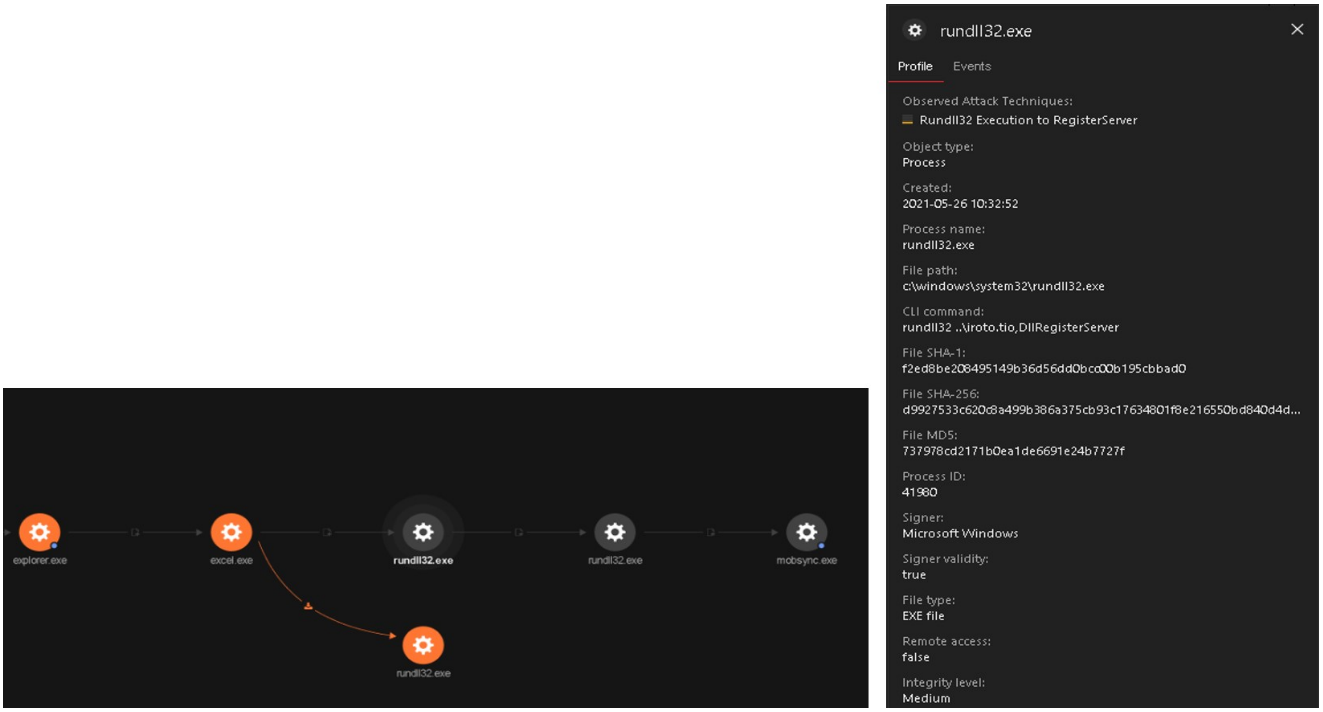
(scanType) Real-time Scan

(actResult) File cleaned

[redacted]

Figure 2. Vision One’s interface showing the early indicators of Cobalt Strike

First let us narrow our focus on the suspicious process, mobsync.exe. Vision One’s Progressive RCA allowed us to pinpoint a possible infection vector that lead to its execution. The process chain for Endpoint-1 started with a user executing a file named excel.exe, which then created a rundll32.exe. The rundll32.exe loaded a file named iroto.tio, leading to the execution of the aforementioned mobsync.exe, which is a legitimate MS tool hijacked via process hollowing.



rundll32.exe

Profile | Events

Observed Attack Techniques:
Rundll32 Execution to RegisterServer

Object type:
Process

Created:
2021-05-26 10:32:52

Process name:
rundll32.exe

File path:
c:\windows\system32\rundll32.exe

CLI command:
rundll32 ..\iroto.tio,DllRegisterServer

File SHA-1:
f2ed8be208495149b36d56dd0bcc00b195cbbad0

File SHA-256:
d9927533c620c8a499b386a375cb93c17634801f8e216550bd840d4d...

File MD5:
737978cd2171b0ea1de6691e24b7727f

Process ID:
41980

Signer:
Microsoft Windows

Signer validity:
true

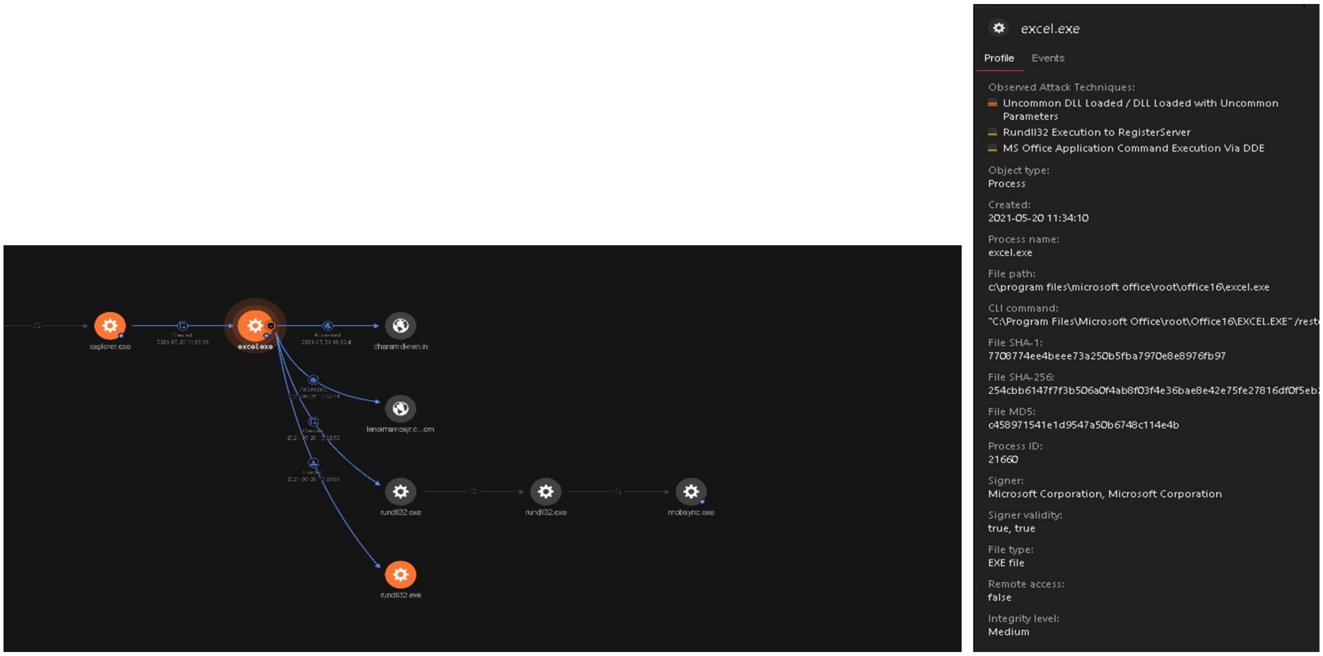
File type:
EXE file

Remote access:
false

Integrity level:
Medium

Figure 3. The file excel.exe shown as the source of the malware as shown in Vision One

Progressive RCA gave us the choice to expand the nodes to find additional indicators that might be useful to the investigation. In this case, we were interested in excel.exe, or the source; and mobsync.exe,which seemed like the final payload at that point.



excel.exe

Profile Events

Observed Attack Techniques:
🟧 Uncommon DLL Loaded / DLL Loaded with Uncommon Parameters
🟨 Rundll32 Execution to RegisterServer
🟨 MS Office Application Command Execution Via DDE

Object type:
Process

Created:
2021-05-20 11:34:10

Process name:
excel.exe

File path:
c:\program files\microsoft office\root\office16\excel.exe

CLI command:
"C:\Program Files\Microsoft Office\root\Office16\EXCEL.EXE" /rest

File SHA-1:
7708774ee4beee73a250b5fba7970e8e8976fb97

File SHA-256:
254cbb6147f7f3b506a0f4ab8f03f4e36bae8e42e75fe27816df0f5eb

File MD5:
c458971541e1d9547a50b6748c114e4b

Process ID:
21660

Signer:
Microsoft Corporation, Microsoft Corporation

Signer validity:
true, true

File type:
EXE file

Remote access:
false

Integrity level:
Medium

Figure 4. The file excel.exe accessing two URLs taken from Vision One

Let us first turn our attention to the excel.exe, which we saw accessing two suspicious URLs dharamdiwan[.]com and lenoirramosjr[.]com before proceeding to drop iroto.tio (not shown in the Figure 3) and loading the dropped file via rundll32.exe.

Vision One's Observed Attack Techniques (OAT) also showed the techniques used via excel.exe and its child processes, one of which is "MS Office Application Command Execution Via DDE." Digging deeper in the Vision One console, we identified analysis-57909253.xlsx as the malicious XLS file that utilized DDE.

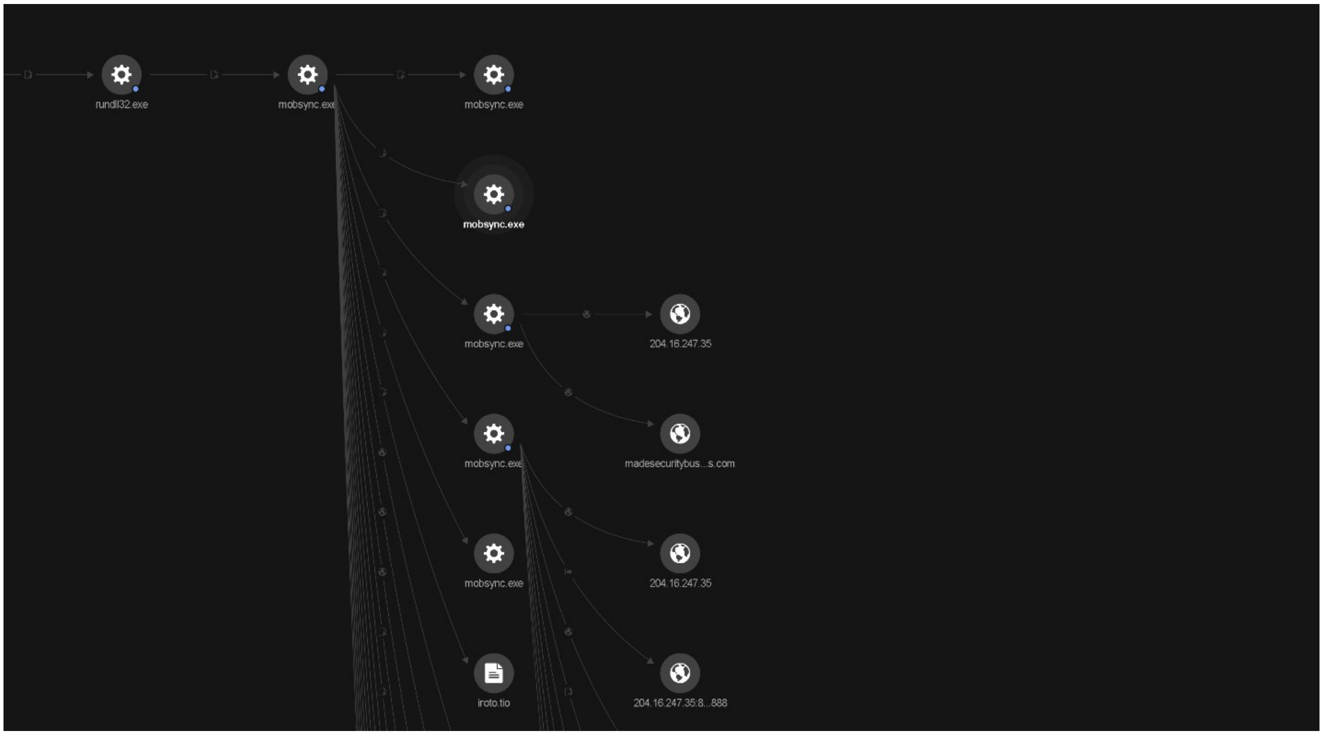


Figure 5. Events related to mobsync.exe

Going back to mobsync.exe revealed several other events, as shown in Figure 5. We summarize the activities done by this injected tool.

It attempts a connection to the following IP addresses:

- 222[.]153[.]124[.]130
- 109[.]106[.]69[.]138
- 75[.]118[.]1[.]141
- 92[.]59[.]35[.]196
- 104[.]98[.]42[.]5
- 204[.]16[.]247[.]35 (madesecuritybusiness[.]com)

It also executed discovery/internal reconnaissance commands and spawned additional mobsync.exe processes, as shown in Table 1.

Date and Time (UTC)	Process
5/26/2021 0:41	whoami /all
5/26/2021 0:41	cmd /c set

5/26/2021 0:41	arp -a
5/26/2021 0:41	ipconfig /all
5/26/2021 0:41	net view /all
5/26/2021 0:42	nslookup -querytype=ALL -timeout=10 _ldap._tcp.dc._msdcs.[WORKGROUP]
5/26/2021 0:42	net share
5/26/2021 0:42	route print
5/26/2021 0:42	netstat -nao
5/26/2021 0:42	net localgroup
5/26/2021 1:50	C:\WINDOWS\SysWOW64\mobsync.exe
5/26/2021 1:50	C:\WINDOWS\system32\ping.exe -t 127.0.0.1
5/26/2021 1:58	C:\WINDOWS\SysWOW64\mobsync.exe
5/26/2021 1:58	esentutl.exe /r V01 /l”C:\Users\[Endpoint-1-User]\AppData\Local\Microsoft\Windows\WebCache” /s”C:\Users\[ENDPOINT-1-USER]\AppData\Local\Microsoft\Windows\WebCache” /d”C:\Users\[ENDPOINT-1-USER]\AppData\Local\Microsoft\Windows\WebCache”

5/26/2021 5:33	C:\WINDOWS\SysWOW64\mobsync.exe
5/26/2021 5:33	C:\WINDOWS\system32\cmd.exe /C ping [ENDPOINT-4]

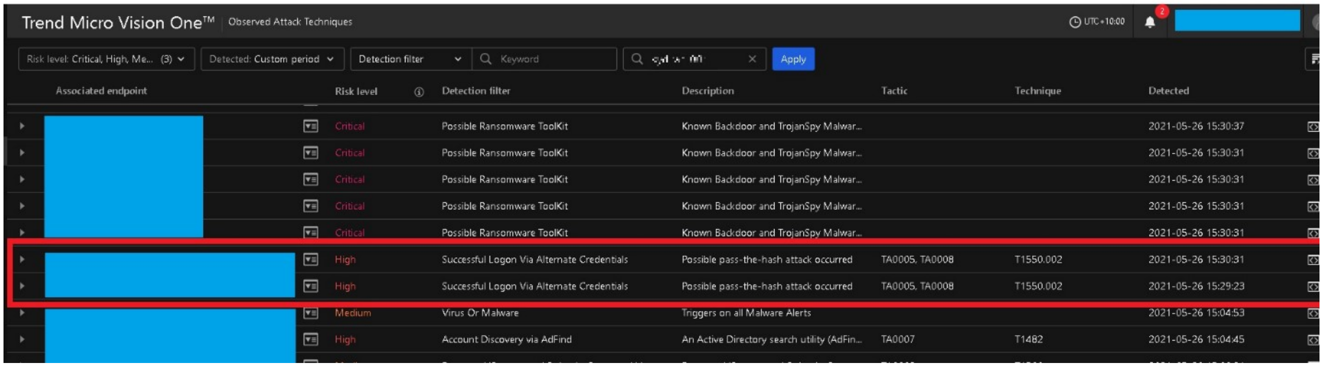
Table 1. A list of the commands executed by mobsync.exe

We also identified Bloodhound and ADfind.exe hacking tools deployed in Endpoint-1. These tools can be used to extract information from the Active Directory.

Date and Time (UTC)	Process
5/26/2021 5:00	C:\WINDOWS\system32\cmd.exe /C del 20210526145501_BloodHound.zip YmNhMTJiMzAtYTgxZi00ZWRmLWE2ZjctZTc3MDFiZGM2ODBj.bin
5/26/2021 5:04	C:\WINDOWS\system32\cmd.exe /C AdFind.exe -f objectcategory=computer -csv name cn OperatingSystem dNSHostName > [REDACTED].csv

Table 2. Bloodhound and ADfind.exe in the logs of Endpoint-1

With Vision One and the Trend Micro Investigation Toolkit (TMIK), we were able to identify potential Pass-the-Hash (PtH) attacks that extracts the password hash from the memory and then simply passes it through for authentication. If there are recent logins of high privilege accounts in the machine, then the password hash of these logins can be extracted by attackers to perform lateral movement to other networked systems. The event logs also showed a related entry for the PtH technique stating, “Found 4624 event logs with seclogo as process for ENDPOINT-1-USER.”



Risk level: Critical, High, Me... (3)
Detected: Custom period
Detection filter
Keyword

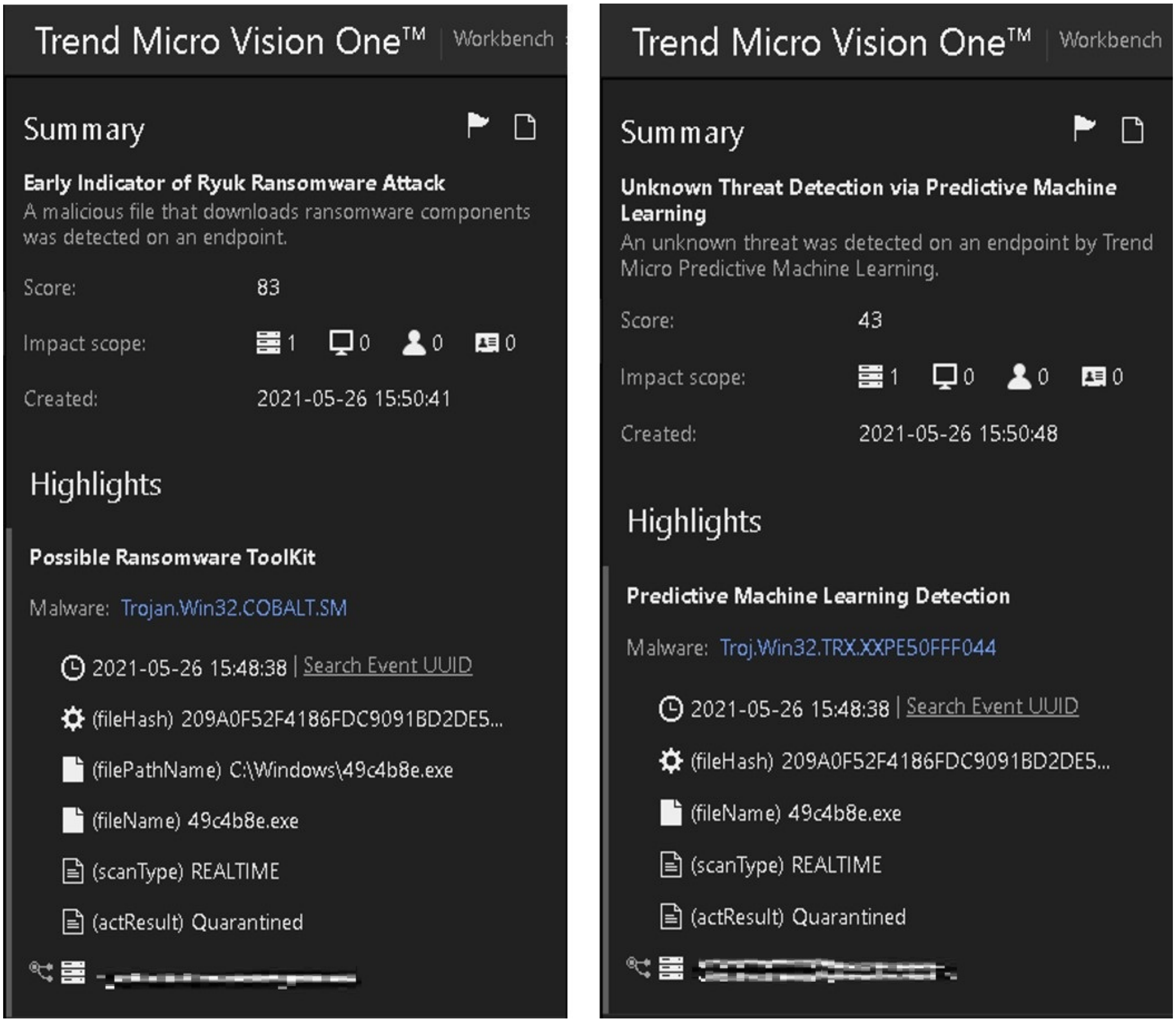
Associated endpoint	Risk level	Detection filter	Description	Tactic	Technique	Detected
[redacted]	Critical	Possible Ransomware ToolKit	Known Backdoor and TrojanSpy Malwar...			2021-05-26 15:30:37
[redacted]	Critical	Possible Ransomware ToolKit	Known Backdoor and TrojanSpy Malwar...			2021-05-26 15:30:31
[redacted]	Critical	Possible Ransomware ToolKit	Known Backdoor and TrojanSpy Malwar...			2021-05-26 15:30:31
[redacted]	Critical	Possible Ransomware ToolKit	Known Backdoor and TrojanSpy Malwar...			2021-05-26 15:30:31
[redacted]	Critical	Possible Ransomware ToolKit	Known Backdoor and TrojanSpy Malwar...			2021-05-26 15:30:31
[redacted]	High	Successful Logon Via Alternate Credentials	Possible pass-the-hash attack occurred	TA0005, TA0008	T1550.002	2021-05-26 15:30:31
[redacted]	High	Successful Logon Via Alternate Credentials	Possible pass-the-hash attack occurred	TA0005, TA0008	T1550.002	2021-05-26 15:29:23
[redacted]	Medium	Virus Or Malware	Triggers on all Malware Alerts			2021-05-26 15:04:53
[redacted]	High	Account Discovery via AdFind	An Active Directory search utility (AdFin...	TA0007	T1482	2021-05-26 15:04:45

Figure 6. Detection of the Pass-the-Hash technique

Aside from Endpoint-1, we also found several other endpoints where we identified Cobalt Strike detections. We specify another two here as they already contain the evidence, such as a list of IOCs and observed TTPs, that we needed to pinpoint “Patient Zero,” or the first machine to be infected by the malware.

Endpoint-2

We will label another endpoint as Endpoint-2. Endpoint-2 is a machine that Vision One also alerted to have shown Cobalt Strike detection.



Trend Micro Vision One™ | Workbench

Summary

Early Indicator of Ryuk Ransomware Attack
A malicious file that downloads ransomware components was detected on an endpoint.

Score: 83

Impact scope: 1 0 0 0

Created: 2021-05-26 15:50:41

Highlights

Possible Ransomware ToolKit

Malware: Trojan.Win32.COBALT.SM

2021-05-26 15:48:38 | Search Event UUID

(fileHash) 209A0F52F4186FDC9091BD2DE5...

(filePathName) C:\Windows\49c4b8e.exe

(fileName) 49c4b8e.exe

(scanType) REALTIME

(actResult) Quarantined

[redacted]

Trend Micro Vision One™ | Workbench

Summary

Unknown Threat Detection via Predictive Machine Learning
An unknown threat was detected on an endpoint by Trend Micro Predictive Machine Learning.

Score: 43

Impact scope: 1 0 0 0

Created: 2021-05-26 15:50:48

Highlights

Predictive Machine Learning Detection

Malware: Troj.Win32.TRX.XXPE50FFF044

2021-05-26 15:48:38 | Search Event UUID

(fileHash) 209A0F52F4186FDC9091BD2DE5...

(fileName) 49c4b8e.exe

(scanType) REALTIME

(actResult) Quarantined

[redacted]

Figure 7. Detection for Cobalt Strike in Endpoint-2

Vision One’s Execution Profile for the file shows ntoskrnl.exe executing 49c4b8e.exe. This sequence of processes in the execution profile implies that the file was transferred via SMB, evidence of lateral movement which was stopped due to the detection.

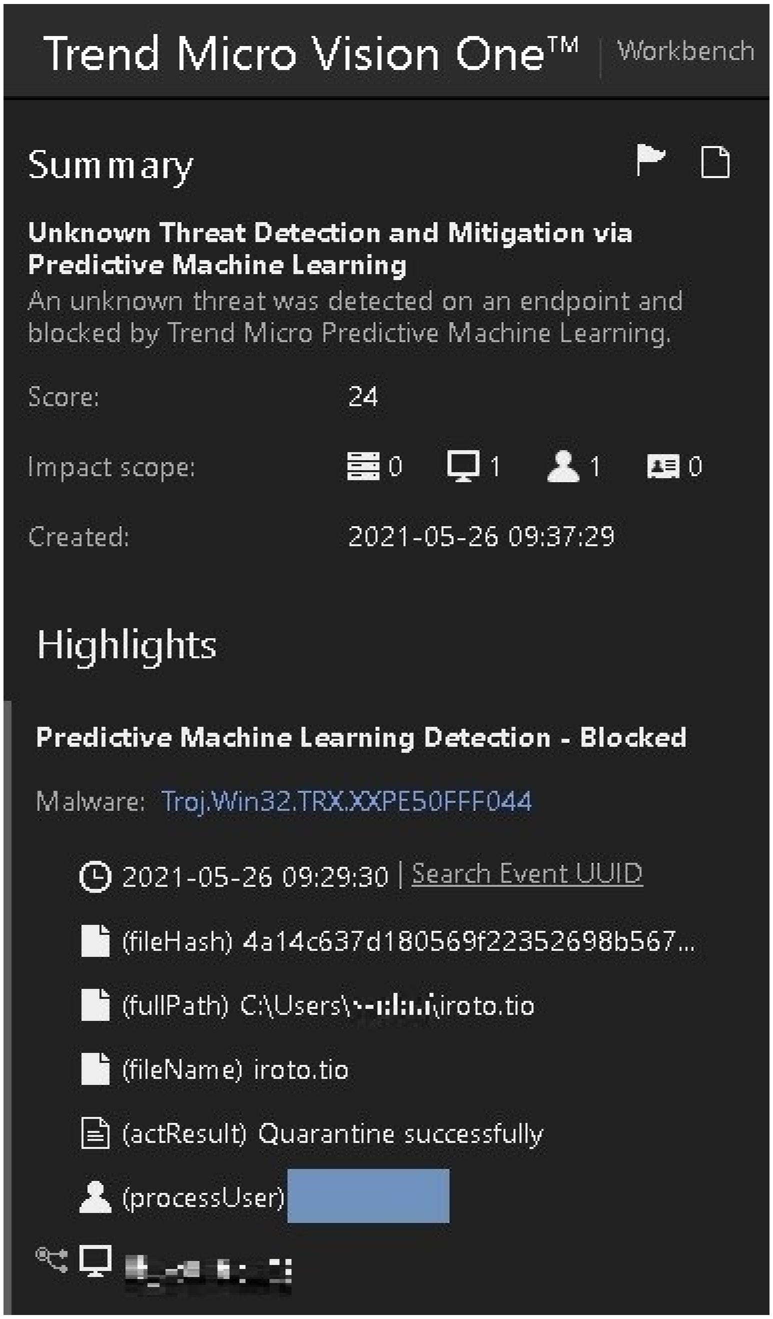
Hunting IOCs and TTPs

With all the findings from Endpoint-1 and Endpoint-2, we were able to observe for TTPs and create an IOC list that we can search across all the machines reporting to Vision One. This search was based on the following indicators:

- Filename and hashes of the detected files
- Suspicious behavior, such as excel.exe spawning rundll32.exe or mobsync.exe spawning cmd.exe
- Possible command and control (C&C) connections
- Compromised accounts used for lateral movement and are transferred files via SMB
- Detections that occurred around the time the alert occurred (commonly used time range is Last 7 days)

Searching the IOCs in the Vision One search app revealed several other machines related to this case, as shown in Figure 1. An example of such a machine is one that we labeled Endpoint-3.

Similar to Endpoint-1, there were malware detections in the machine, where it blocked the execution of excel.exe that spawned rundll32.exe. There was also a machine learning detection related to the file iroto.tio. Finally, inspecting Workbench alerts showed an entry for Cobalt Strike.



Trend Micro Vision One™ | Workbench

Summary

Unknown Threat Detection and Mitigation via Predictive Machine Learning
An unknown threat was detected on an endpoint and blocked by Trend Micro Predictive Machine Learning.

Score: 24

Impact scope: ▤ 0 🖥 1 👤 1 ▣ 0

Created: 2021-05-26 09:37:29

Highlights

Predictive Machine Learning Detection - Blocked

Malware: Troj.Win32.TRX.XXPE50FFF044

2021-05-26 09:29:30 | Search Event UUID

(fileHash) 4a14c637d180569f22352698b567...

(fullPath) C:\Users\[redacted]\iroto.tio

(fileName) iroto.tio

(actResult) Quarantine successfully

(processUser) [redacted]

🖥 [redacted]

Figure 8. Detection of Cobalt Strike in Endpoint-3

Investigating Endpoint-3's execution profile showed that the excel.exe process connected to the same suspicious domains that we mentioned earlier. It also created the file iroto.tio.

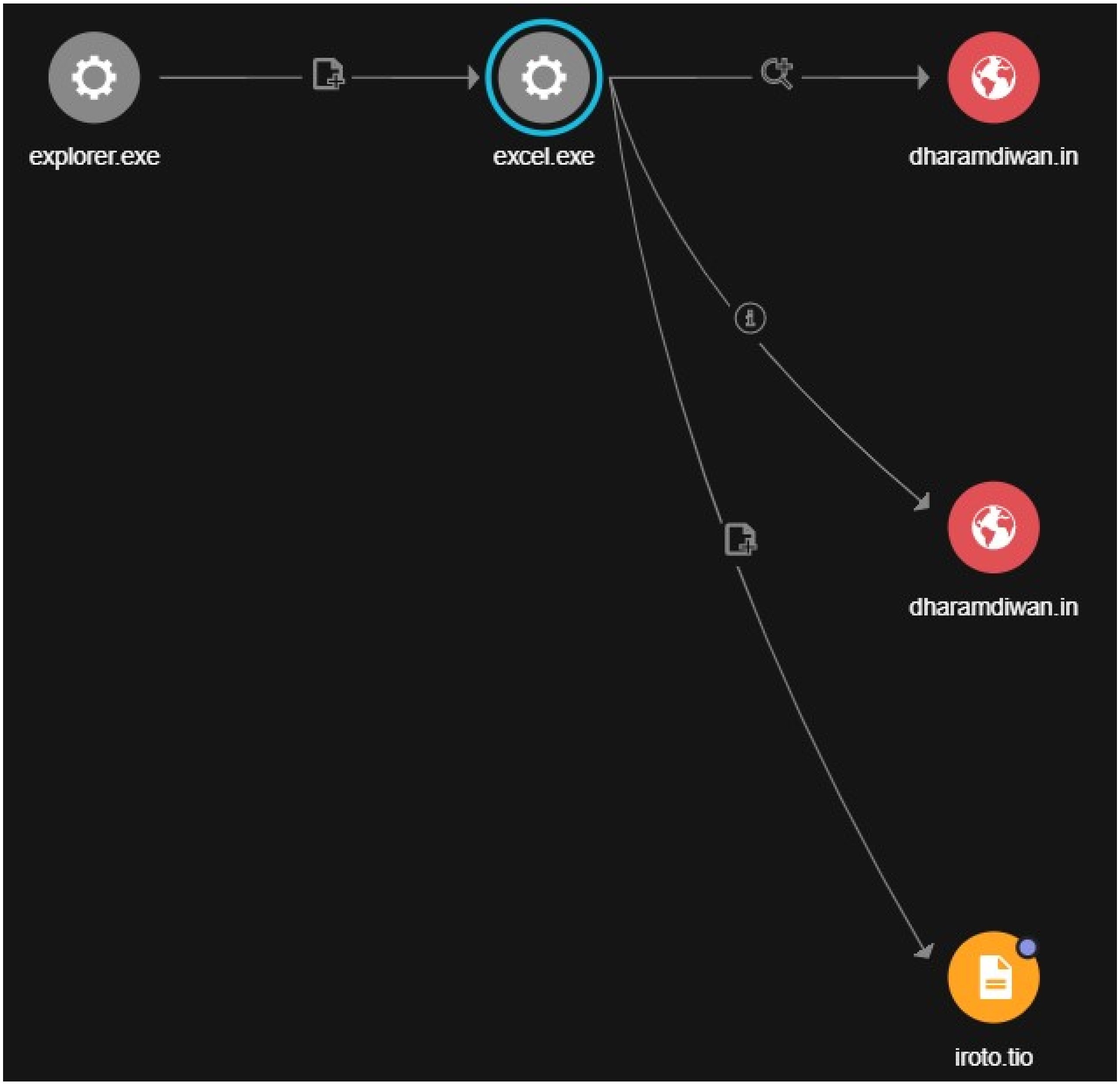
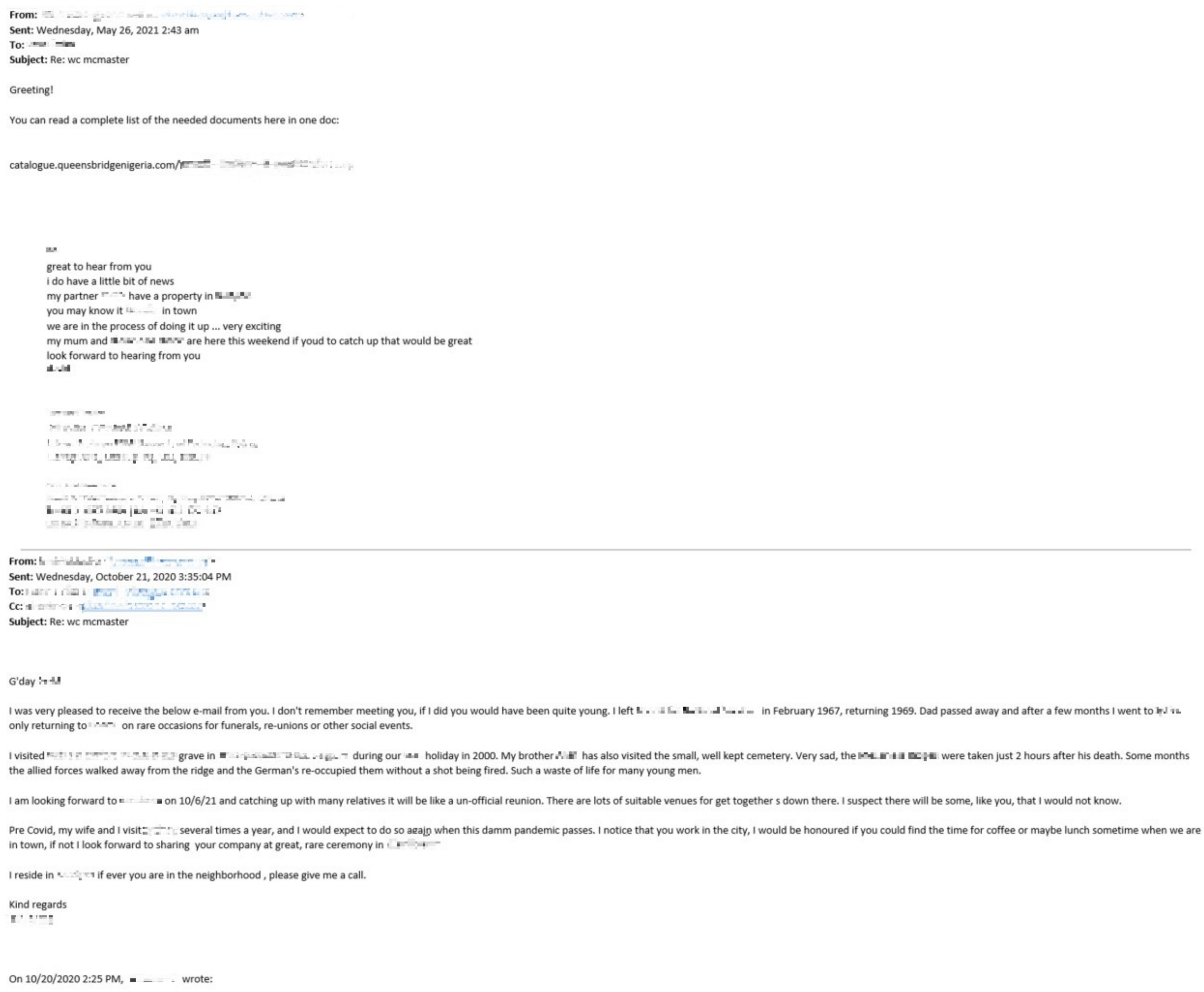


Figure 9. Enpoint-3's execution profile showing excel.exe's activities

With a list of IOCs and TTPs we were able to look for other infected machines or endpoints and were also then capable of narrowing down Patient Zero.

Locating Patient Zero

Since we know for sure that the threat started with an execution of excel.exe and the .xls file it opened, it is logical to assume that the attack started from an email attachment, which was the case here. The Vision One, Managed XDR team was able to eventually track down the entry point of this attack: a socially engineered spear phishing email sent to an internal user.



From: [redacted]
Sent: Wednesday, May 26, 2021 2:43 am
To: [redacted]
Subject: Re: wc mcmaster

Greeting!

You can read a complete list of the needed documents here in one doc:

catalogue.queensbridgenigeria.com/[redacted]

> [redacted]
> great to hear from you
> i do have a little bit of news
> my partner [redacted] have a property in [redacted]
> you may know it [redacted] in town
> we are in the process of doing it up ... very exciting
> my mum and [redacted] are here this weekend if youd to catch up that would be great
> look forward to hearing from you
> [redacted]
>
> [redacted]
>
> [redacted]

From: [redacted]
Sent: Wednesday, October 21, 2020 3:35:04 PM
To: [redacted]
Cc: [redacted]
Subject: Re: wc mcmaster

G'day [redacted]

I was very pleased to receive the below e-mail from you. I don't remember meeting you, if I did you would have been quite young. I left [redacted] in February 1967, returning 1969. Dad passed away and after a few months I went to [redacted] only returning to [redacted] on rare occasions for funerals, re-unions or other social events.

I visited [redacted] grave in [redacted] during our [redacted] holiday in 2000. My brother [redacted] has also visited the small, well kept cemetery. Very sad, the [redacted] were taken just 2 hours after his death. Some months the allied forces walked away from the ridge and the German's re-occupied them without a shot being fired. Such a waste of life for many young men.

I am looking forward to [redacted] on 10/6/21 and catching up with many relatives it will be like a un-official reunion. There are lots of suitable venues for get together s down there. I suspect there will be some, like you, that I would not know.

Pre Covid, my wife and I visit[redacted] several times a year, and I would expect to do so agajn when this damm pandemic passes. I notice that you work in the city, I would be honoured if you could find the time for coffee or maybe lunch sometime when we are in town, if not I look forward to sharing your company at great, rare ceremony in [redacted]

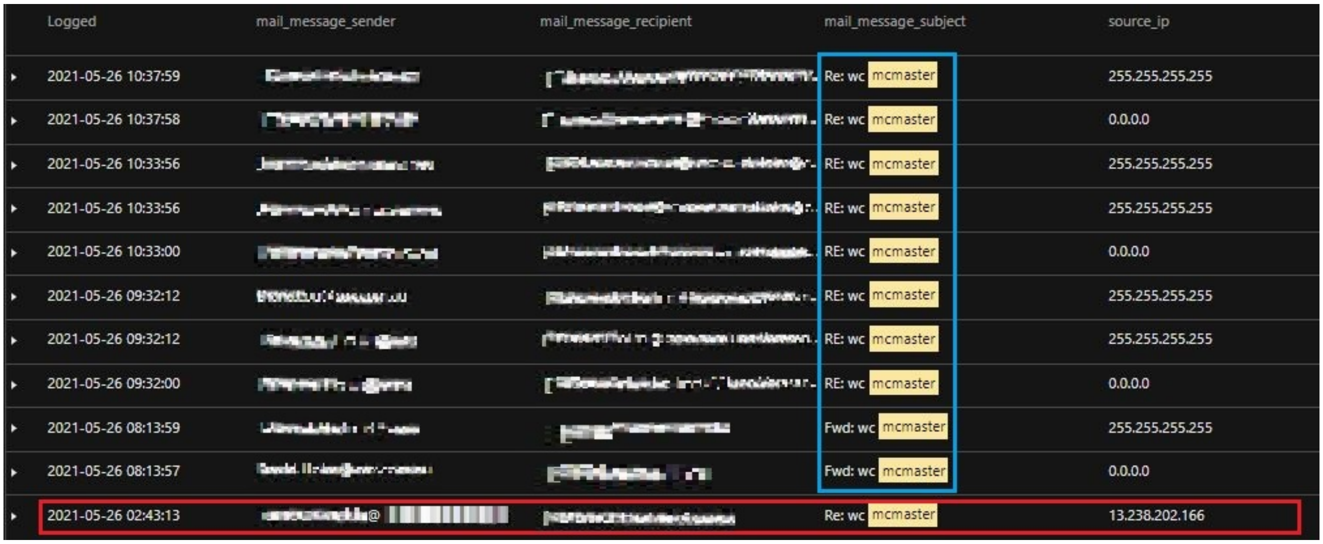
I reside in [redacted] if ever you are in the neighborhood , please give me a call.

Kind regards
[redacted]

On 10/20/2020 2:25 PM, [redacted] wrote:

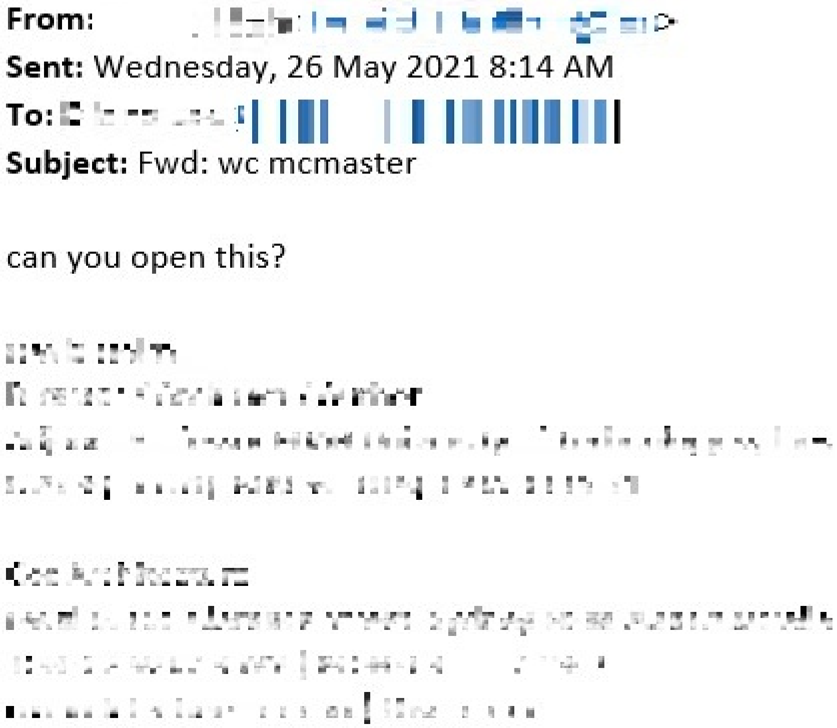
Figure 10. Socially engineered spear phishing email

The threat actor made the email seem as if they were replying to an email the targeted user had sent them, thus making it appear as if they already had an existing conversation thread. They also used a forged sender email address so that the targeted user would think that the email came from a legitimate sender. The email contained a link to download a malicious archive file with the name of the targeted user.



Logged	mail_message_sender	mail_message_recipient	mail_message_subject	source_ip
2021-05-26 10:37:59	[redacted]	[redacted]	Re: wc mcmaster	255.255.255.255
2021-05-26 10:37:58	[redacted]	[redacted]	Re: wc mcmaster	0.0.0.0
2021-05-26 10:33:56	[redacted]	[redacted]	RE: wc mcmaster	255.255.255.255
2021-05-26 10:33:56	[redacted]	[redacted]	RE: wc mcmaster	255.255.255.255
2021-05-26 10:33:00	[redacted]	[redacted]	RE: wc mcmaster	0.0.0.0
2021-05-26 09:32:12	[redacted]	[redacted]	RE: wc mcmaster	255.255.255.255
2021-05-26 09:32:12	[redacted]	[redacted]	RE: wc mcmaster	255.255.255.255
2021-05-26 09:32:00	[redacted]	[redacted]	RE: wc mcmaster	0.0.0.0
2021-05-26 08:13:59	[redacted]	[redacted]	Fwd: wc mcmaster	255.255.255.255
2021-05-26 08:13:57	[redacted]	[redacted]	Fwd: wc mcmaster	0.0.0.0
2021-05-26 02:43:13	[redacted]	[redacted]	Re: wc mcmaster	13.238.202.166

Figure 11. Vision One results showing the malicious email being forwarded to another user or machine



From: [redacted]
Sent: Wednesday, 26 May 2021 8:14 AM
To: [redacted]
Subject: Fwd: wc mcmaster

can you open this?

[redacted]

[redacted]

Figure 12.

The message of the forwarded malicious email

Through Vision One, we were able see that a few minutes after receiving the email, the targeted user forwarded the malicious email to another internal user. These results from Vision One (Figure 11) matched with the email that Managed XDR had acquired (Figure 12), thus proving that the machine was Patient Zero and rounding out our investigation.

Responding to the threat

The overall goal of the investigation was to get a full scope of the Cobalt Strike infection. This involved identifying the IOCs we can use to search for all the machines that were infected, as well as stopping the spread at the root.

All throughout the process we had been reporting to the affected customer, especially after the discovery of each of the affected endpoints. This is to quickly contain the spread of the malware variant. The response to this threat included the following, in no particular order:

- Isolation of affected endpoints as the investigation was being conducted
- Disabling/resetting the passwords of the user accounts that were used for lateral movement
- Collecting related artifacts to the threat and doing further analysis, which were also submitted for detection to improve coverage
- Blocking of domain/IP addresses related to the C&C of the threat
- Further monitoring of the environment to ensure that there's no suspicious activity going on

Many of these steps were done simultaneous to the investigation, so as not to risk possible consequences and prevent the spread of the malware to other machines.

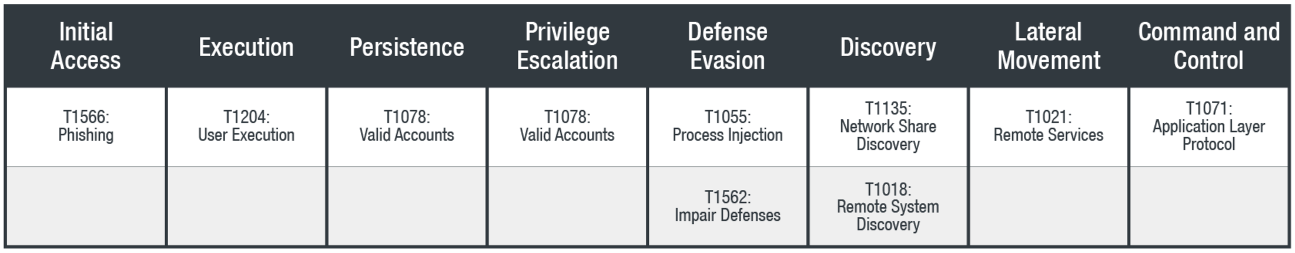
Conclusion and recommendations

The result of the investigation demonstrated the importance of a multi-layered security approach in protecting the environment. This is crucial so that in case one layer of protection fails another is present to keep the environment safe or at least limit the impact of an attack.

Prioritizing detections and combining different techniques can help in catching the threat and initiating a quick response. As this case reflects, preliminary security events should be taken seriously as they usually are the precursor to something bigger, such as breaches and ransomware attacks.

The investigation also highlights the incident response process for handling breaches and malicious activities. It emphasizes how threat response does not end upon the detection of a threat; an investigation is key to understanding a threat and preventing them from occurring again. Using acquired knowledge from previous attacks and boosting user awareness of common threats can improve the overall security posture of any environment.

MITRE mapping



Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Discovery	Lateral Movement	Command and Control
T1566: Phishing	T1204: User Execution	T1078: Valid Accounts	T1078: Valid Accounts	T1055: Process Injection	T1135: Network Share Discovery	T1021: Remote Services	T1071: Application Layer Protocol
				T1562: Impair Defenses	T1018: Remote System Discovery		