blackpoint

THREAT PROFILE:

Qilin Ransomware

TABLE OF CONTENTS

Executive Summary

First Identified:
2022

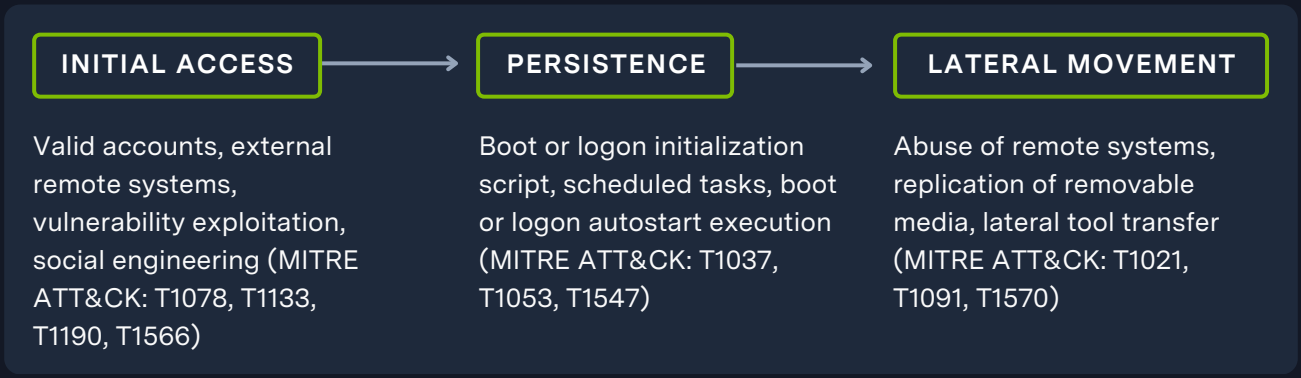
Operation style:
Ransomware-as-a-Service (RaaS); affiliates earn 80% of a payment of ransom demands less than $3 million and 85% of ransom payments over $3 million.

Extortion method:
Double extortion - combining the traditional ransomware extortion method (encryption) with exfiltration of victim's sensitive data; the group threatens to leak the data via a data leak site if the random demand is not paid.

Most frequently targeted industry:
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:
- North America

Known Associations:
- Moonstone Sleet
- Pistachio Tempest
- Scattered Spider
- STAC4365
- WikiLeaksV2



Description

Qilin (AKA Agenda) ransomware was first observed in July 2022 and operates it the double extortion method, where victims' data is stolen and leaked via a data leak site if the ransom demand is not paid. Qilin maintains variants that are written in both Golang and Rust programming languages. The ransomware operation can target both Windows and Linux variants. Qilin operates as a ransomware-as-a-service (RaaS) and affiliates earn 80% of a payment of ransom demands of less than $3 million and 85% of ransom payments over $3 million.

Qilin affiliates have been observed gaining initial access via social engineering attacks – phishing emails with malicious attachments – and valid credentials that have been leaked and/or purchased.

A purported recruiter for the Qilin operation posted on a Russia-language cybercriminal forum advertising the RaaS, offering positions to qualified affiliates, and stating that affiliates are not allowed to target CIS countries. This rule is commonly observed in ransomware operations.

The Qilin affiliates have multiple options in the Qilin panel, indicating the ransomware is customizable for each victim. Affiliates can create and edit blog posts that contain information about attacked companies that have not paid a ransom, create accounts for members of their team by entering their nickname and credentials, and access support for the ransomware. Operators can customize the directories that will be skipped, files that will be skipped, processes that will be killed, mode of encrypting, and list of VMs that will not be killed/shut down.

Qilin affiliates earn 80% of ransom payments less than $3 million and 85% of ransom payments greater than $3 million.

The Linux variant is compiled with GCC 11 in the ELF64 format and is 1.32MB in size. This variant, similar to the Windows variant, provides a number of options for the affiliates to ensure that the right files are encrypted.

Qilin ransomware offers multiple encryption methods, which is also configurable by the affiliate through the panel. Once option uses AES-256 encryption to encrypt the files on the victim's system and uses RSA-2048 to encrypt the generated key. Files are appended with a new random extension. The Linux version uses OpenSSL, and the public key is hardcoded at the address 0x004EB3A8. The statically linked OpenSSL library is used to facilitate the loading of the public key.

In August 2024, security researchers with Sophos reported that the Qilin ransomware group targeted a victim via compromised credentials and the dwell time in the victim environment was 18 days. The operators edited the domain policy to introduce a logon-based Group Policy Object (GPO) containing two items: A PowerShell script, IPScanner.ps1, and a batch script, logon.bat.

The combination of the two scripts resulted in harvesting of credentials saved in Chrome browsers on machines connected to the network. This activity indicates that Qilin is likely changing tactics to include credential harvesting rather than exfiltrating large amounts of victim-specific data.

Description

In October 2024, Halcyon security researchers reported a new and updated version of the Qilin ransomware variant, dubbed “Qilin.B”. Qilin.B is written in the Rust programming language. According to the research, Qilin.B supports AES-256-CTR encryption for systems with Advanced Encryption Standard New Instructions (AES-NI) capabilities. Qilin.B uses RSA-4096 with Optimal Asymmetric Encryption Padding (OAEP) to safeguard encryption keys.

Qilin.B was updated with new defense evasion techniques as well. Qilin.B still terminates services associated with security tools, clears Windows Event Logs, but also deletes itself to reduce indication that the malware was there.

In January 2025, Blackpoint’s APG team identified Qilin using a legitimate signed executable named, upd.exe, which sideloaded a malicious DLL, avupdate.dll. The DLL was responsible for decoding and loading a customized version of the EDR killing tool, EDRSandblast.

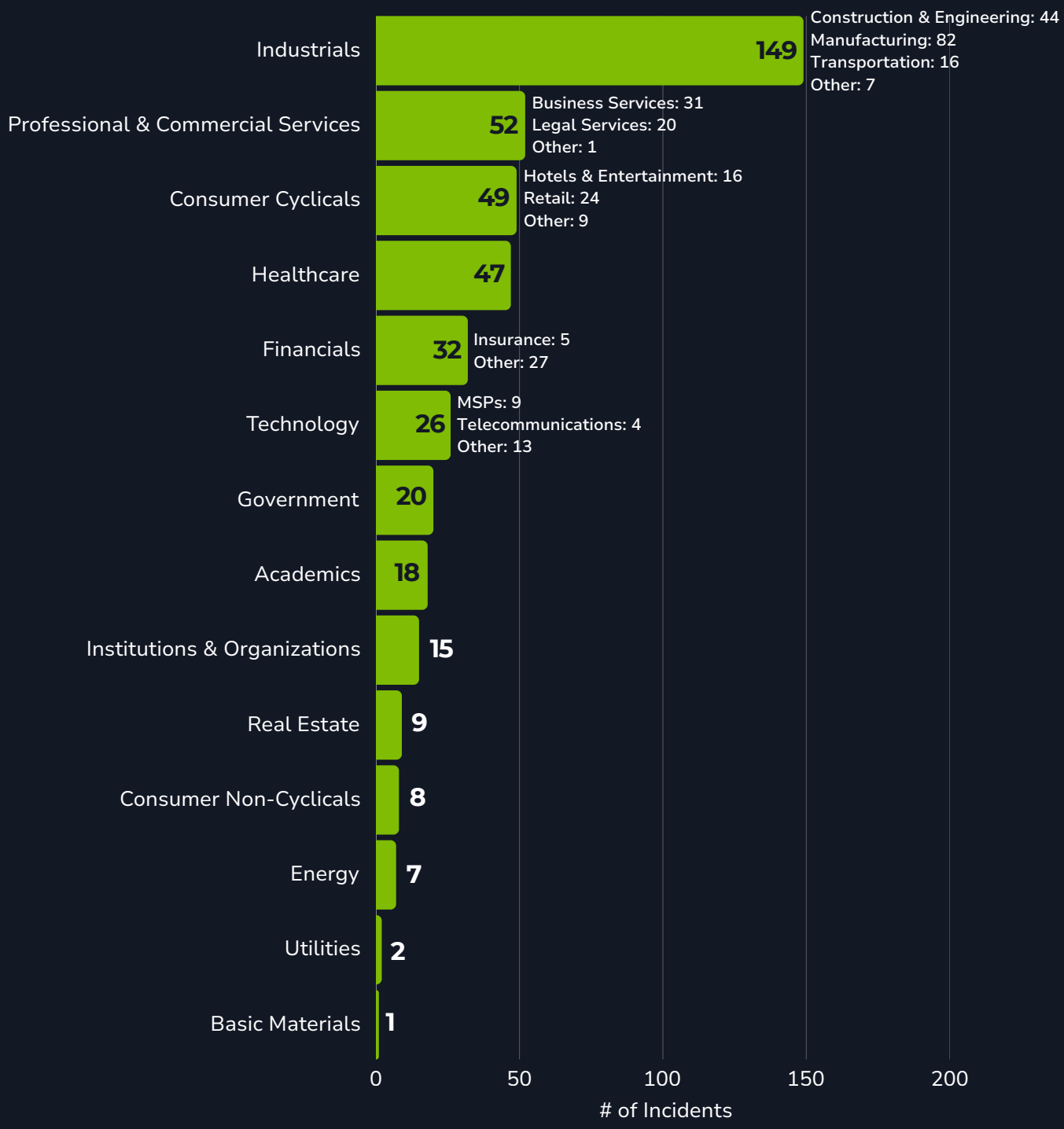
Blackpoint’s APG identified Qilin deploying the EDRSandblast tool via a malicious driver.

In the first half of 2025, as ransomware operations such as Ransomhub, appear to have struggled to stay active; Qilin Ransomware has quickly moved to one of the most active groups in 2025. The shutdown of other groups has likely increased the number of affiliates moving to the Qilin operation, boosting its victim count.

Features the operation maintains - such as spam tools and PR support - and their longer standing operation likely makes Qilin an attractive operation for more sophisticated financially motivated threat groups. It is likely that Qilin activity will continue to be reported over the next 3-6 months.

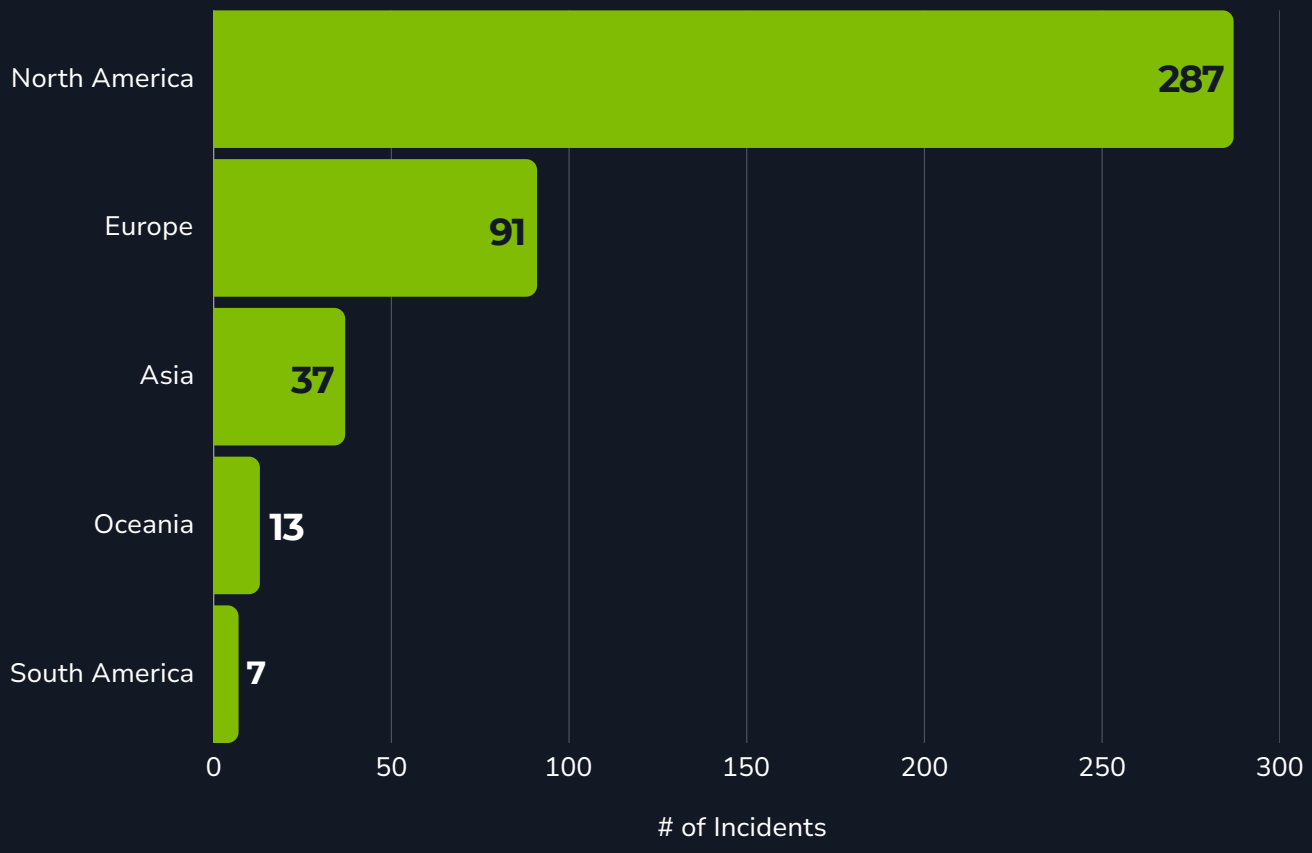
Previous Targets

Previous Industry Targets from 01 July 2024 to 30 Jun 2025

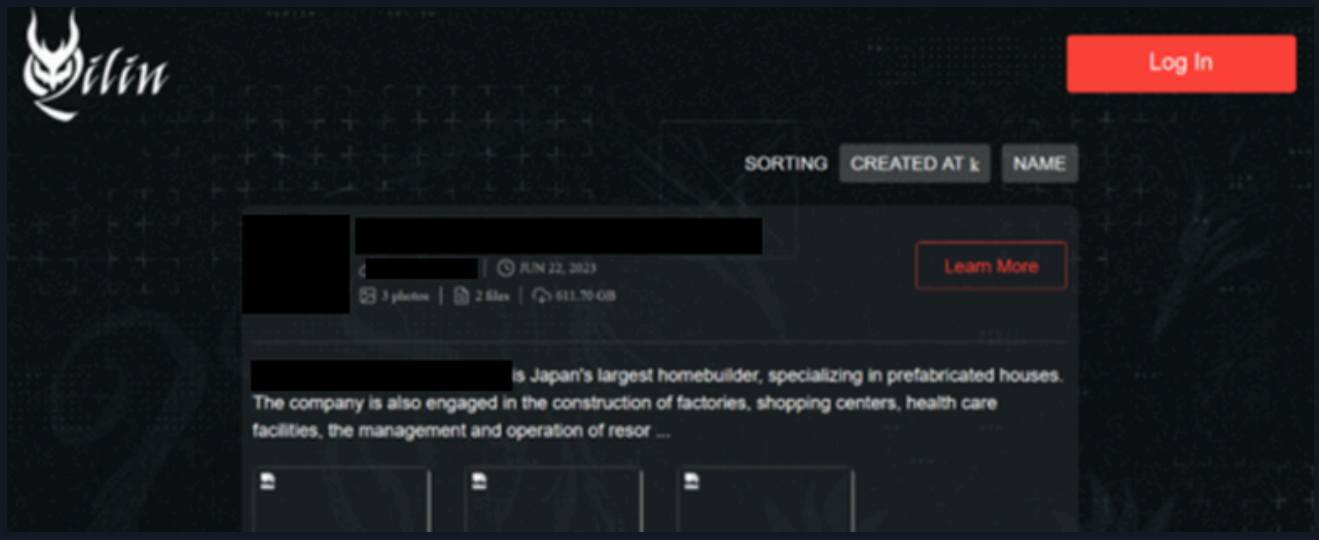


Previous Targets

Previous Victim HQ Regions from 01 July 2024 to 30 Jun 2025



Data Leak Site



hxxp://kbsqoivihgdmwczmxkbovk7ss2dcynitwhhfu5yw725dboqo5kthfaad[.]onion/
hxxp://ozsxj4hwxub7gio347ac7tyqqozvfioty37skqilzo2oqfs4cw2mgtyd[.]onion/
hxxp://ijzn3sicrcy7guixkzjkib4ukbiilwc3xhnmby4mcbccnsd7j2rekvqd[.]onion/

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CVE-2023-27532	Missing Authentication for Critical Function Vulnerability	Veeam Backup & Replication Cloud Connect	7.5
CVE-2024-21762	Out-of-Bound Write Vulnerability	Fortinet FortiOS	9.8
CVE-2024-55591	Authentication Bypass Vulnerability	Fortinet FortiOS	9.8

Associations

Agenda Ransomware

Alias for Qilin Ransomware.

Gold Feather

Alias for Qilin Ransomware.

Phantom Mantis

Alias for Qilin Ransomware.

Water Galura

Alias for Qilin Ransomware.

Moonstone Sleet

Moonstone Sleet is a threat actor that has been attributed to North Korea. In March 2025, Microsoft reported that the group has been observed deploying the Qilin Ransomware variant in a limited number of attacks.

Pistachio Tempest

AKA FIN12, DEV-0237. A ransomware threat group that has been reported to deploy the Qilin Ransomware variant in linked attacks.

Scattered Spider

Security researchers with Microsoft reported that Scattered Spider has shifted to the Ransomhub and Qilin ransomware operations.

STAC4365

An affiliate group of the Qilin Ransomware group that has been reported to rely on an adversary-in-the-middle (AitM) phishing kit to steal credentials.

WikiLeaksV2

Security researchers have connected the Qilin Ransomware operation to the WikiLeaksV2 operation based on the overlap of victims listed and the observation that Qilin has embedded QR codes within their listings that direct users to the WikiLeakV2 leak page indicating a cross-promotion initiative.

Known Tools

AdFind	A free command-line query tool that can be used for gathering information from Active Directory.
Angry IP Scanner	An open-source and cross-platform network scanner that has been used by threat actors to map victim networks and check the status of IP addresses.
AnyDesk	A remote desktop application that provides remote access to computers and other devices.
avupdate.dll	A malicious DLL that Qilin has been observed deploying this DLL to load and execute a file, web.dat (EDRSandblast), and perform various anti-analysis techniques.
bcdedit	A command line tool for managing Configuration Data; it can be used to create new stores, modify existing stores, and add boot menu options.
cmd	A program used to execute commands on a Windows computer.
Cobalt Strike	A commercial, full-featured, remote access tool that is described as "adversary simulation software designed to execute targeted attacks and emulate the post-exploitation actions of advanced threat actors. The tool's interactive post-exploit capabilities cover the full range of ATT&CK tactics, all executed within a single, integrated system.
conhost.exe	A Windows utility that is used to provide the ability to drag and drop files/folders directly into Command Prompt.
EasyUpload.io	A file sharing and transfer service that allows users to upload files, get a shareable link, and share them easily.
EDRSandBlast	A tool written in C that weaponizes a vulnerable signed driver to bypass EDR detections.
esxcli	A tool that allows for remote management of ESXi hosts.
Evilginx	An attack framework used for phishing login credentials along with session cookies, which allows attackers to bypass MFA protection.

Known Tools

FileZilla	A free open-source file transfer protocol software tool that allows users to setup FTP servers or connect to other FTP servers to exchange files.
fsutil	A Windows utility that performs tasks that are related to file allocation table (FAT) and NTFS file systems, such as managing reparse points, managing sparse files, or dismounting a volume.
IPScanner.ps1	A PowerShell script that contained a 19-line script that attempted to harvest credential data stored in the Chrome browser. This script works in tandem with logon.bat.
Logon.bat	A batch script that contained the commands to execute IPScanner.ps1.
main.exe	A simple executable that leveraged several open-sourced networking libraries with the purpose of exposing a remote tunnel into the compromised network.
masscan	An internet-scale port scanner that is similar to nmap.
Microsoft Management Console	A component of Microsoft Windows that provides users an interface for configuring and monitoring the system.
Microsoft Terminal Service Client	A Windows utility that creates connections to Remote Desktop Session Host servers or other remote computers and edits an existing Remote Desktop Connection configuration file.
Mimikatz	An open-source application that allows users to view and save authentication credentials, including Kerberos tickets.
ncat	A general-purpose command line tool for reading, writing, redirecting, and encrypting data across a network.
net	A Windows utility that is used in command-line operations for control of users, groups, services, and network connections. It can gather system and network information, move laterally through SMB/Windows Admin Shares, and interact with services.

Known Tools

NetExec	A network service exploitation tool that helps automate assessing the security of large networks. Threat actors abuse this tool to conduct reconnaissance and lateral movement.
NetXLoader	A highly obfuscated malware loader written in .NET; this malware acts as an initial point of entry for threat actors, allowing them to install additional malicious payloads, including ransomware.
nmap	An open-source utility for network discovery; it runs on all major computer operating systems and includes multiple tools that can be used to transfer data, compare scan results, and generate packets.
nping	An open-source tool for network packet generation, response analysis and response time measurement.
OpenSSL	A commercial grade open-source toolkit for the TLS protocol and is based on a full-strength general purpose cryptographic library.
PC Hunter	A toolkit for Windows with various powerful features for kernel structure viewing and manipulating.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PowerTool	A security tool that scans and analyzes files at kernel level; can help threat actors remove and disable security services/software.
PowerView	A PowerShell tool used to gain network situational awareness of Windows domains.
Proxy Chains	A sequence of two or more proxy servers used to route internet traffic. Qilin has been reported to utilize proxy chains to mask their activities and maintain anonymity during attacks. This technique allows the operator to hide their location and make it more challening for law enforcement and researchers to trace their origins and overall operations.
PsExec	A command-line utility that allows users to execute processes on remote systems; it is part of the Sysinternals suite and is frequently used by system admins for remote management tasks. The tool is also repeatedly abused by threat actors for lateral movement and remote execute.

Known Tools

RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
RSAT	Remote Server Administration Tools. A Windows application that remotely manages the roles and features running Windows Server with snap-ins.
ScreenConnect	AKA ConnectWise. A remote management software used to gain access to a remote computer.
SmokeLoader	AKA Dofoil. A trojan malware that targets Windows operating systems and is used to deploy additional malware variants, including information stealing variants and ransomware.
SoftPerfect	A network scanner that can ping computers, scan ports, discover shared folders and retrieve practically any information about network devices.
svchost.exe	A shared-service process that Windows uses to load DLL files.
SystemBC	AKA Coroxy. A malware written in C that turns infected computers into SOCKS5 proxies.
Task Manager	A task manager, system monitor, and startup manager included with Microsoft Windows systems. It allows a user to view the performance of the system.
Toshiba Power Management Driver	A software component that manages power consumption to optimize battery life and system performance.
Total Network Inventory (TNI)	A desktop-based network inventory management solution that provides users with tools for monitoring and tracking assets.
Total Software Deployment (TSD)	A remote management tool that enables remote deployment on compromised environments.
TPwSav.sys	A driver, originally developed for power-saving features on Toshiba laptops, that has been used by Qilin to bypass EDR protections through a bring-your-own-vulnerable-driver (BYOVD) attack.

Known Tools

upd.exe	The Carbon Black Cloud Sensor AV update tool meant to perform various update functions; however, Qilin has been observed using a sample that contained malicious code.
Veeam Agent Configurator	A tool that provides a command line interface for Veeam Agent for Microsoft Windows.
Veeam Backup & Replication	A backup applications for virtual environments built on VMware vSphere, Nutanix AHV, and Microsoft Hyper-V hypervisors.
vim-cmd	A vSphere CLI tool that is available on every ESXi host and can be used to perform various activities in a VMware environment.
VssAdmin	A Windows service that allows taking manual or automatic backup copies of computer files or volumes.
wbadmin.exe	A command line utility that is used to back up and restore OS, drive volumes, files, folders, and applications from a command line interface.
WinRM	Microsoft's version of the WS-Management protocol, which is a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows interoperation between hardware and operating systems from different vendors.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.
wscript	A shared-service process that Windows uses to load DLL files.
YDArk	A kernel manipulation tool available for download on GitHub. The tool can hide processes at the kernel level - it manipulates the EPROCESS kernel object of the target process by changing its PID to 0 and redirecting forward and backward Active Process Links to the self's EPROCESS address.
Zemana Anti-Rootkit Driver	A driver component used by Zemana anti-malware software to detect and remove rootkits. It is abused by threat actors in bring your own vulnerable driver (BYOVD) techniques to evade detection, elevate privileges, and more.

Observed Behaviors: Windows

Tactic	Commands Observed
Execution	dllhost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} vdsldr.exe -Embedding wscript.exe "C:\Users\$username\Documents\ConnectWiseControl\Files\launch.vbs" -alter {int} -encryption {value} -ips {IP Address} -min-size {value} -no-proc -no-services -password {string} -path {directory} -safe -stat "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'"
Persistence	tsd-setup.tmp /SL5="$402D4,24132872,174080,C:\Users\$username\Documents\ConnectWiseControl\Files\tsd-setup.exe" tsd-setup.tmp $username tsd-setup.tmp /SL5="$A9B0536,24132872,174080,C:\Users\$username\Documents\ConnectWiseControl\Files\tsd-setup.exe" /SPAWNWND=$8430630 /NOTIFYWND=$402D422948 setlang.exe $username setlang.exe "C:\Users\$username\AppData\Roaming\Total Software Deployment\config.ini" TSD language ENGLISH7844 vcredist_x86.exe $username vcredist_x86.exe /q findwnd.exe $username findwnd.exe "TApplication" "Total Software Deployment" tniwinagent.exe $username tniwinagent.exe /service /$IPAddress/login:"current" /driver:2 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<rand6char> = "<path>\qilin.exe" --password <password> --no-vm --no-admin HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\SystemEnableLinkedConnections = 1

Observed Behaviors: Windows

Tactic	Commands Observed
Privilege Escalation	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'-Command ''
Defense Evasion	mmc.exe "C:\Windows\system32\wbadmin.msc" mmc.exe C:\Windows\system32\diskmgmt.msc pbeagent.exe SysLogger.exe 1000 "Monitoring Stopped" wmic service where name='vss' call ChangeStartMode Disabled powershell.exe $logs = Get-WinEvent -ListLog * \| Where-Object {$_.RecordCount} | Select-Object -ExpandProperty LogName ; ForEach ($l in $logs \| Sort \| Get-Unique) {[System.Diagnostics.Eventing.Reader.EventLogSession]::GlobalSession.ClearLog($l)} fsutil.exe behavior set SymlinkEvaluation R2L:1 WMIC.exe service where name='vss' call ChangeStartMode Manual vssadmin.exe delete shadows /all /quiet /C timeout /T 10 & Del
Credential Access	notepad.exe C:\Users\$username\Documents\ConnectWiseControl\Files\mimikatz.log mimikatz.exe $username mimikatz.exe "log" "privilege::debug" "sekurlsa::logonpasswords" "sekurlsa::tickets /export" "exit"
Discovery	powershell.exe -Command "Import-Module ActiveDirectory ; Get-ADComputer -Filter * | Select-Object -ExpandProperty DNSHostName" sc.exe $username sc.exe query hwinfo Command "Import-Module ActiveDirectory ; Get-ADComputer -Filter * | Where-Object { Test-Connection -ComputerName $_.DNSHostName -Count 1 -Quiet } | ForEach-Object { $_.DNSHostName }" Get-DiskImage -ImagePath '' | Select-Object -ExpandProperty Attached
Lateral Movement	%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process %Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -u <USER_NAME> -p <PASSWORD> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process

Observed Behaviors: Windows

Tactic	Commands Observed
Impact	VSSUIRUN.exe D:\ vssadmin.exe delete shadows /for=e: /all wbadmin.exe stop net.exe stop vss net1.exe start vss Fast Skip (N) – step (Y) N: {N} p: {P} Dismount-DiskImage -ImagePath C:\Windows\System32\bcdedit.exe /set safeboot network bcdedit /deletevalue {default} safeboot C:\windows\system32\bcdedit.exe /set safeboot{current} network REG ADD /v LockScreenImagePath /t REG_SZ /d '' /f ; REG ADD /v LockScreenImageUrl / REG_SZ /d ' /v LockScreenImageStatus /t REG_DWORD /d 1 /f

Observed Behaviors: Linux

Tactic	Commands Observed
Execution	-y,--yes --dry-run --no-snap-rm --no-vm-kill -t –timer -d, --debug -h,--help -l,--log-level --no-df --no-ef --no-ff --no-proc-kill -R,--no-rename -p,--path --password -r,--rename esxcfg-advcfg -s 32768 /BufferCache/MaxCapacity esxcfg-advcfg -s 20000 /BufferCache/FlushInterval setrlimit()
Defense Evasion	esxcli vm process list vim-cmd vmsvc/getallvms esxcli vm process kill -t force -w [ID] vim-cmd vmsvc/snapshot.removeall %llu > /dev/null 2>&1
Discovery	storage filesystem list nftw() fdopendir() OpenFileWithPermission ((_int64)”/proc/cpuinfo”, (_int64)”r”); vim-cmd vmsvc/getallvms
Lateral Movement	–spread-vcenter
Impact	vim-cmd vmsvc/snapshot.removeall [ID] > /dev/null 2>&1 for vm_id in `acli vm.list | grep -oP '([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})' | awk '{print $1}'`; do acli vm.update $vm_id ha_priority=0; done

Observed Behaviors: Linux

Tactic	Commands Observed
Impact	for vm_id in `acli vm.list | grep -oP '([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})' | awk '{print $1}'`; do acli vm.force_off $vm_id; done for snap_id in `acli snapshot.list | grep -oP '([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12})' | awk '{print $1}'`; do echo \"yes\" | acli snapshot.delete $snap_id; done

MITRE ATT&CK® Mappings

Initial Access	
T1078: Valid Accounts	
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1204: User Execution	.002: Malicious File
T1569: System Services	.002: Service Execution
T1675: ESXi Administration Command	
Persistence	
T1037: Boot or Logon Initialization Scripts	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Privilege Escalation	
T1055: Process Injection	

MITRE ATT&CK® Mappings

Privilege Escalation	
T1068: Exploitation for Privilege Escalation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	.002: Domain Accounts
T1134: Access Token Manipulation	.002: Create Process with Token
T1548: Abuse Elevation Control Mechanism	
Defense Evasion	
T1014: Rootkit	
T1027: Obfuscated Files or Information	.007: Dynamic API Resolution
T1055: Process Injection	.001: Dynamic-link Library Injection
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1112: Modify Registry	
T1211: Exploitation for Defense Evasion	
T1218: System Binary Proxy Execution	.011: Rundll32
T1480: Execution Guardrails	
T1484: Domain Policy Modification	.001: Group Policy Modification
T1562: Impair Defenses	.001: Disable or Modify System Firewall .002: Disable Windows Event Logging .009: Safe Mode Boot

MITRE ATT&CK® Mappings

Defense Evasion	
T1574: Hijack Execution Flow	.010: Services File Permissions Weakness
T1622: Debugger Evasion	
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1552: Unsecured Credentials	.001: Credentials in Files .006: Group Policy Preferences
Discovery	
T1010: Application Window Discovery	
T1012: Query Registry	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.002: Domain Account
T1120: Peripheral Device Discovery	

MITRE ATT&CK® Mappings

Discovery	
T1614: System Location Discovery	.001: System Language Discovery
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH
T1091: Replication Through Removable Media	
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
Command and Control	
T1001: Data Obfuscation	.001: Junk Data
T1071: Application Layer Protocol	.001: Web Protocols
T1573: Encrypted Channel	.001: Symmetric Cryptography
Exfiltration	
T1011: Exfiltration Over Other Network Medium	.001: Exfiltration Over Bluetooth
T1567: Exfiltration Over Web Service	.002: Exfiltration to Cloud Storage

MITRE ATT&CK® Mappings

Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1529: System Shutdown/Reboot	
T1561: Disk Wipe	.001: Disk Content Wipe
T1657: Financial Theft	

References

- Blackpoint Cyber (2025, January 31) “Qilin Ransomware and the Hidden Dangers of BYOVD.” https://blackpointcyber.com/blog/qilin-ransomware-and-the-hidden-dangers-of-byovd/
- Group-IB (2024, July 17) “Qilin Revisited: Diving into the techniques and procedures of the recent Qilin Ransomware Attacks.” https://www.group-ib.com/blog/qilin-revisited/
- Halcyon Research Team (2024, October 24) “New Qilin.B Ransomware Variant Boasts Enhanced Encryption and Defense Evasion.” https://www.halcyon.ai/blog/new-qilin-b-ransomware-variant-boasts-enhanced-encryption-and-defense-evasion
- HC3 (2024, June 18) “Qilin, aka Agenda Ransomware.” https://www.hhs.gov/sites/default/files/qilin-threat-profile-tlpclear.pdf
- Kirkpatrick, Lee; Jacobs, Paul; et. al. (2024, August 22) Sophos: “Qilin ransomware caught stealing credentials stored in Google Chrome.” https://news.sophos.com/en-us/2024/08/22/qilin-ransomware-caught-stealing-credentials-stored-in-google-chrome/
- Klepuszewski, Piotr (2023, December 05) LinkedIn: “Analyzing the Qilin Ransomware Attack on VMware ESXi Servers.” https://www.linkedin.com/pulse/analyzing-qilin-ransomware-attack-vmware-esxi-servers-klepuszewski-taqjf
- Microsoft Threat Intelligence (@MsftSecIntel) 2025. “Moonstone Sleet has previously exclusively deployed their own custom ransomware in their attacks...” X, March 06, 2025, 2:00PM. https://x.com/MsftSecIntel/status/1897738963340681641
- Montini, Heloise (2023, September 04) SalvageData: “Qilin (Agenda) Ransomware: Complete Guide.” https://www.salvagedata.com/qilin-agenda-ransomware/
- SentinelOne (n.d.) “Agenda (Qilin).” https://www.sentinelone.com/anthology/agenda-qilin/
- Thodex (n.d.) “Agenda (Qilin) Ransomware: Analysis, Detection, and Recovery.” https://www.thodex.com/ransomware/agenda-qilin/
- Tasdelen, Ismail (2025, May 09) “Qilin Ransomware Steals the Show: 72 Data Leaks in April 2025's Cyber Chaos.” https://ismailtasdelen.medium.com/qilin-ransomware-steals-the-show-72-data-leaks-in-april-2025s-cyber-chaos-c0ee32d8e68c
- Tsipershtein, Mark (2025) Cybereason: “Ransomware Gangs Collapse as Qilin Seizes Control.” https://www.cybereason.com/blog/threat-alert-qilin-seizes-control

Adversary Pursuit Group

blackpoint