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:
- Arkana
- Devman
- DragonForce
- Hastalamuerte
- LockBit
- Moonstone Sleet
- Pistachio Tempest
- Scattered Spider
- STAC4365
- WikiLeaksV2

INITIAL ACCESS → **PERSISTENCE** → **LATERAL MOVEMENT**

Valid accounts, external remote systems, vulnerability exploitation, social engineering (MITRE ATT&CK: T1078, T1133, T1190, T1566)

Boot or logon initialization script, scheduled tasks, boot or logon autostart execution (MITRE ATT&CK: T1037, T1053, T1547)

Abuse of remote systems, replication of removable media, exploitation of remote services, lateral tool transfer (MITRE ATT&CK: T1021, T1091, T1210, T1570)

Diamond Model

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.

The Qilin affiliate panel offers extensive customization options, allowing attackers to tailor each ransomware deployment to their specific victim. Affiliates can create and edit blog posts that expose companies refusing to pay, manage team accounts by adding nicknames and credentials, and access dedicated support for the ransomware. Operators can also configure technical parameters such as directories and files to skip, processes to terminate, encryption modes, and virtual machines to exclude from shutdown providing a highly flexible attack framework.

In addition to these technical features, Qilin introduced a "Call Lawyer" button within its panel a unique tactic designed to escalate psychological pressure during negotiations. This feature brings a purported legal advisor into discussions, aiming to intimidate victims by suggesting potential regulatory or legal consequences, to increasing the likelihood of ransom payment.

Modern ransomware variants are increasingly incorporating advanced techniques to strengthen encryption and accelerate performance.

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

Recent developments include the use of Chrome Extension Stealers for credential harvesting, paired with significant encryption enhancements that make decryption nearly impossible without the attacker's key. These improvements leverage AES-256-CTR, a highly secure implementation of the Advanced Encryption Standard using a 256-bit key and Counter mode for robust file protection.

To further harden security, Optimal Asymmetric Encryption Padding (OAEP) is applied, reducing susceptibility to certain cryptographic attacks. Systems with AES-NI capabilities on x86 architectures benefit from accelerated encryption and decryption processes, improving efficiency during large-scale operations. For secure and high-speed streamed communications, many threat actors are also adopting ChaCha20, a modern cipher known for its speed and resilience.

In August 2024, security researchers with Sophos reported that the Qilin group targeted a victim via compromised credentials and the dwell time in the 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 on machines connected to the network. This activity indicates that Qilin is likely changing tactics to include credential harvesting.

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.

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.

In 2025, Qilin was reported to rely on several bullet-proof-hosting (BPH) infrastructures. Rogue BPH services enable threat actors to host content with minimal oversight. These are designed to be resilient to abuse complaints and law enforcement intervention. These factors highlight why BPH services are an attractive option for a major ransomware operation like Qilin.

Qilin has been attributed with launching the WikiLeaksV2 website, where the group publishes information about their activities. This site contains header ads for BEARHOST Servers, one of the largest BPH providers (AKA Underground and Voodoo Servers). Other Services the group has been linked to include:

- Cat Technologies Co. Limited
- Red Bytes LLC
- IPX-FZCO
- Chang Way Technologies Co. Limited

Throughout 2025, Qilin emerged as the most active and disruptive ransomware operations.

Additionally, in Q3 2025 DragonForce Ransomware operation announced a working partnership with both LockBit and Qilin Ransomware. This alliance could aid in restoring LockBit’s reputation among affiliates and increase Qilin’s activity.

This type of cooperative, cartel-style partnership is similar to a partnership between Maze and LockBit in 2020, a time when double extortion was growing.

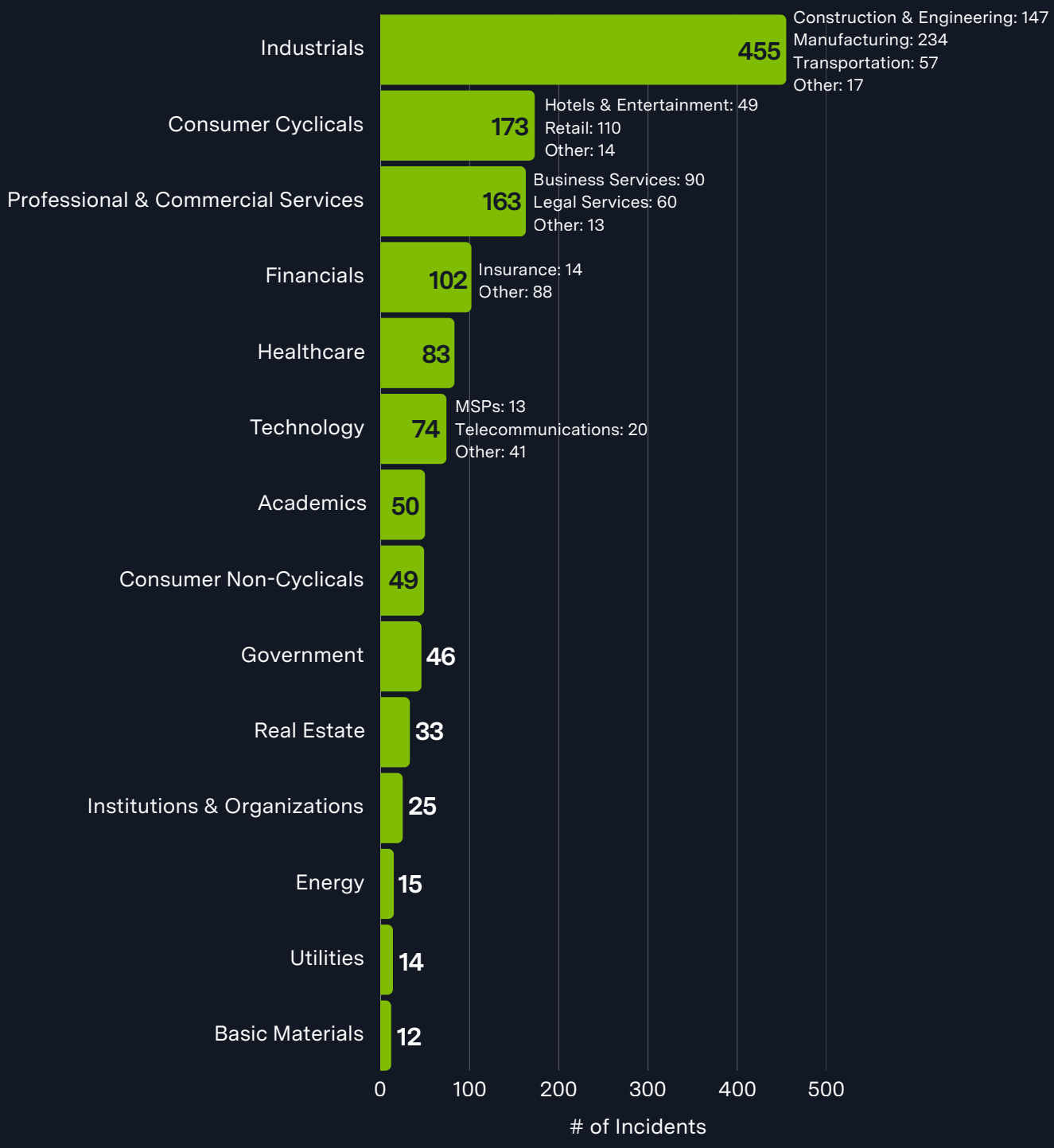
Features the operation maintains - such as spam tools and PR support - and their longer standing operation likely makes Qilin an attractive operation for more sophisticated financially motivated threat groups. It is very likely that Qilin activity will continue to be reported over the next 3-6 months.

In 2025, Qilin ransomware executed several high-profile attacks across different regions, demanding multimillion-dollar ransoms. Key incidents include:

- February 2025 – **Cleveland Municipal Court** (United States) Qilin caused weeks of operational disruption and demanded $4 million. The court refused to pay.
- March 2025 – **Malaysia Airports Holdings Berhad** (Malaysia)Attack disrupted critical airport systems. Qilin demanded $10 million and claimed to have stolen 2 TB of data. Officials confirmed they did not pay.
- June 2025 – **Ciudad Autónoma de Melilla** (Spain) Qilin demanded approximately $2.12 million and alleged theft of 4–5 TB of sensitive data. Authorities declined the ransom.

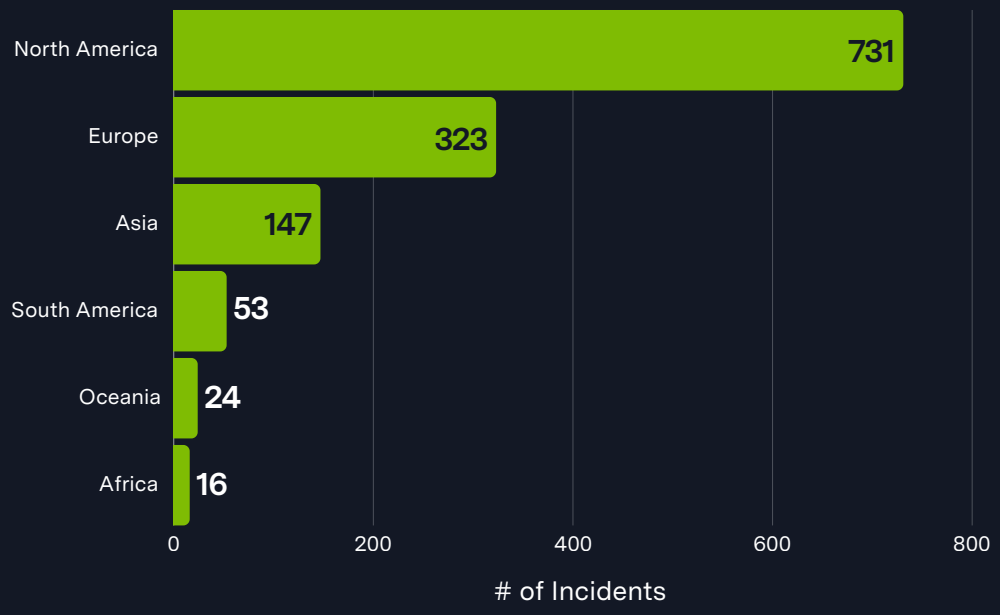
Previous Targets

Previous Industry Targets from 01 Apr 2025 to 31 Mar 2026



Previous Targets

Previous Victim HQ Regions from 01 Apr 2025 to 31 Mar 2026



Data Leak Site

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

Known Exploited Vulnerabilities

Vulnerability	Description	Product Affected	CVSS
CitrixBleed (CVE-2023-4966)	Buffer Overflow Vulnerability	Citrix NetScaler ADC and NetScaler Gateway	7.5
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
CVE-2025-31324	Unrestricted File Upload Vulnerability	SAP NetWeaver	9.8
CVE-2025-49704	Code Injection Vulnerability	Microsoft SharePoint	8.8
CVE-2025-49706	Improper Authentication Vulnerability	Microsoft SharePoint	6.6
CVE-2025-53770	Deserialization of Untrusted Data Vulnerability	Microsoft SharePoint	9.8
CVE-2025-53771	Path Traversal Vulnerability	Microsoft SharePoint	6.5
CVE-2025-5777	Out-of-Bounds Read Vulnerability	Citrix NetScaler ADC and Gateway	9.3

Associations

Agenda Ransomware

Alias for Qilin Ransomware.

Gold Feather

Alias for Qilin Ransomware.

Phantom Mantis

Alias for Qilin Ransomware.

Storm-1934

Microsoft tracks this group as a financially motivated group behind the operation, management, and leadership of the Qilin ransomware operation.

Water Galura

Alias for Qilin Ransomware.

Arkana

When Arkana launched a data extortion site in March 2025, their about section displayed a “Qilin Network” logo, suggesting their was likely a working relationship between the two groups.

Devman

Devman is reportedly a self-identified affiliate of the Qilin operation. Devman operates their own data leak site. One of their victim posts included the phrase “Pwn3d By Qilin & Devman.”

DragonForce Ransomware

DragonForce operators posted on a dark web forum that they were launching a partnership between themselves, LockBit, and Qilin operations.

Hastalamuerte

A known Qilin affiliate who reportedly left the operation after a dispute for unpaid commissions. This affiliate has been attributed with being the founder of “The Gentlemen” Ransomware operation.

LockBit Ransomware

LockBit is purportedly the third arm of an allegiance between DragonForce, LockBit, and Qilin Ransomware operations. The coalition was announced by DragonForce on a dark web forum.

Associations

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

AKA Octo Tempest, 0katapus. 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

Function	Tool	Description
Initial Access	SmokeLoader	Malware loader frequently used to establish initial footholds.
Execution	cmd	Utility used to execute commands on Windows systems.
	main.exe	Generic malicious payload used for ransomware deployment or execution.
	MMC	Microsoft Management Console. Tool used to manage administrative tools.
	PowerShell	Command line shell, scripting language, and automation framework utilized to execute scripts and payloads.
	WMI	Microsoft's framework for managing data and operations used to execute commands and queries remotely.
	wscript	Executes scripts via Windows Script Host.
Persistence	AnyDesk	Remote access tool abused for persistent access.
	Atera	RMM tool abused to maintain persistent access.
	Distant Desktop	RMM tool used for remote access.
	GoToDesk	RMM tool abused for remote access.
	Logon.bat	Batch script executed at user logon to maintain persistence.
	ScreenConnect	AKA ConnectWise. RMM tool that can be used to gain persistent remote access to victim environments.
	Splashtop	Remote desktop software abused for access.
Privilege Escalation	fsutil	Manipulates NTFS/FAT structures.
	PC Hunter	Legitimate toolkit used to disable security software and facilitate encryption..
	PowerTool	Tool used to enable Kernel-level manipulation of security services..

Known Tools

Function	Tool	Description
Stealth	cipher.exe	Overwrites deleted data to prevent recovery.
	conhost.exe	Legitimate Windows host process abused to proxy malicious execution.
	iexplore.exe	Executes content in legacy execution context.
	NetXLoader	Malware loader used to inject or launch malicious payloads in memory.
	scvhost.exe	Hosts services to mask malicious activity.
	upd.exe	Malicious updater-style executable used to disguise payload execution.
	YDArk	Kernel-level process hiding.
Defense Impairment	avupdate.dll	Malicious DLL used to disable or interfere with security tooling.
	bcdedit	Command line tool used to modify boot configuration data for system level changes.
	dark-kill	Disables EDR using a malicious kernel driver.
	EDRSandBlast	Uses vulnerable drivers to bypass EDR.
	eskle.sys	Vulnerable kernel driver abused for privilege escalation or security bypass.
	fnarw.sys	Vulnerable driver leveraged to disable endpoint security controls.
	hlpdrv.sys	Malicious driver to terminate protected processes.
	KILLAV	Disables antivirus-related services.
	rwdrv.sys	Vulnerable driver abused to terminate or bypass security products.
	Toshiba Power Management Driver	Legitimate vulnerable driver abused for kernel-level access.

Known Tools

Function	Tool	Description
Defense Impairment	TPwSav.sys	Toshiba driver abused in BYOVD-style attacks to disable protections.
	Zemana Anti-Rootkit Driver	Legitimate anti-rootkit driver abused for privileged kernel operations.
Credential Access	BypassCredGuard.exe	Bypasses Windows Credential Guard.
	Evilginx	Adversary-in-the-middle phishing framework used to steal credentials and MFA tokens.
	Mimikatz	Hacktool used to extract Windows passwords in plain-text from memory.
	SharpDecryptPwd	Extracts stored authentication data.
	Stealc	Credential and information stealer.
Discovery	AdFind	Active Directory reconnaissance tool used to enumerate users, groups, and domain structure.
	Angry IP Scanner	Maps IP ranges and host availability.
	esxcli	Enumerates and manages ESXi hosts.
	IPScanner.ps1	PowerShell-based network scanner used to identify hosts and services.
	Kali	Penetration testing OS used for recon.
	masscan	Internet-scale port scanner.
	Microsoft Paint	Views image-based artifacts.
	nltest	Windows command-line utility used to enumerate domain controllers and trust relationships.
	nmap	Windows utility used for network discovery and scanning.
	NotePad	Windows utility frequently abused to view logs and collected text artifacts.

Known Tools

Function	Tool	Description
Discovery	nping	Generates and analyzes network packets.
	PowerView	Enumerates Active Directory relationships; used to map network shares, enumerate users/groups, and more.
	RSAT	Remote Server Administration Tools. Enumerates and manages Windows Server roles
	SoftPerfect	Tool that scans networks for connected devices, shared folders, and open ports.
	Task Manager	Enumerates processes and performance.
	TNI	Total Network Inventory. Network inventory and asset discovery tool.
	vim-cmd	VMware ESXi command-line utility used to enumerate and manage virtual machines.
Lateral Movement	Microsoft Terminal Service Client	Native RDP client used for remote access and lateral movement.
	ncat	Network utility used for remote shells, tunneling, and pivoting.
	net	Windows utility abused for discovery, lateral movement, and more.
	NetExec	Network exploitation tool that automates SMB/WinRM lateral movement.
	PsExec	Sysinternals tool used to execute commands remotely on other systems.
	PuTTY	SSH/Telnet client used to access remote systems or pivot through compromised infrastructure.
	RDP	Microsoft protocol used to remotely connect to a Windows computer.
	rdpclip.exe	Legitimate RDP clipboard process abused during remote sessions.
	TSD	Total Software Deployment. Remote deployment platform.

Known Tools

Function	Tool	Description
Lateral Movement	WinRM	Windows utility that executes commands remotely via Windows Remote Management.
Command and Control	Cobalt Strike	Commercial C2 framework abused for post-exploitation.
	ProxyChains	Forces traffic through proxy chains.
	Sliver	Cross-platform adversary emulation framework.
	SystemBC	Turns infected hosts into SOCKS5 proxies.
Exfiltration	Cyberduck	Transfers data to remote/cloud storage.
	EasyUpload.io	Public file-sharing service abused to stage or exfiltrate stolen data.
	FileZilla	File transfer protocol software tool that allows users to set up FTP servers or connect to other FTP servers to exchange files.
	wbadmin.exe	Backs up and exports data.
	WinRAR	Compression utility used to package stolen files for exfiltration.
	WinSCP	Transfers files over SFTP/FTP.
Impact	Veeam Agent Configurator	Backup management utility abused to alter or disable recovery operations.
	Veeam Backup & Replication	Enterprise backup platform targeted for deletion or encryption of backups.
	VssAdmin	Command line tool abused to delete Volume Shadow Copy Service (VSS).
Infrastructure	OpenSSL	Software library for implementing cryptographic functions and securing communications.
	TOR	Open-source software enabling anonymous malicious activities, such as command and control, operating data leak sites, and more.

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	powershell.exe -Command "ServerManagerCmd.exe -i RSAT-AD-PowerShell ..."
		wscript.exe C:\Users\{username}\Documents\ConnectWiseControl\Files\launch.vbs
		dllhost.exe /Processid:{AB8902B4-09CA-4BB6-B78D-A8F59079A8D5} -Embedding
	Output/Artifact	C:\Users\{username}\Documents\ConnectWiseControl\Files\launch.vbs
		C:\Users\{username}\AppData\Roaming\
		C:\Users\{username}\AppData\Roaming\Total Software Deployment\
Persistence	Command Execution	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
	Configuration Change	HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\<rand6char> = "<path>\qilin.exe" --password <password> --no-vm --no-admin
		HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\EnableLinkedConnections = 1
		net user Supportt ***** /add
		net localgroup Administrators Supportt /add

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Persistence	Configuration Change	net user Administrator *****
	Output/Artifact	C:\Users\{username}\AppData\Roaming\Total Software Deployment\
Privilege Escalation	Command Execution	powershell.exe -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"
		C:\Windows\System32\net1 localgroup administrators
	Configuration Change	reg add HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server /v fDenyTSConnections /t REG_DWORD /d 0 /f
	Output/Artifact	C:\ProgramData\Veeam\socks64.dll
Stealth	Command Execution	mmc.exe C:\Windows\System32\wbadmin.msc
		mmc.exe C:\Windows\System32\diskmgmt.msc
		powershell.exe Clear-Windows-Event-Logs (all logs)
		cmd /C timeout /T 10 & del
		mshta.exe vbscript:ShellExecute(cmd.exe, runas)
	Configuration Change	fsutil.exe behavior set SymlinkEvaluation R2L:1
	Output/Artifact	C:\Users\Administrator\\Downloads*.exe
		C:\Users\\Desktop*.exe
Defense Impairment	Command Execution	pbeagent.exe SysLogger.exe 1000 "Monitoring Stopped"
		vssadmin.exe delete shadows /all /quiet
		cmd /C net stop vss & cmd /C net start vss
		sc create dark type=kernel binPath=\dark.sys
		sc start dark & sc delete dark

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Defense Impairment	Configuration Change	wmic service where name='vss' call ChangeStartMode Disabled
		wmic service where name='vss' call ChangeStartMode Manual
	Output/Artifact	C:\Users\Administrator\\Downloads*\dark.sys
Credential Access	Command Execution	mimikatz.exe "privilege::debug" "sekurlsa::logonpasswords"
		mimikatz.exe "sekurlsa::tickets /export"
	Configuration Change	reg add HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest /v UseLogonCredential /d 1
	Output/Artifact	C:\Users\{username}\Documents\ConnectWiseControl\Files\mimikatz.log
	Retrieved Data	SELECT user_name, password FROM VeeamBackup.dbo.Credentials
Discovery	Command Execution	powershell.exe Import-Module ActiveDirectory; Get-ADComputer -Filter *
		`powershell.exe Get-ADComputer
		nltest /domain_trusts
		nltest /dclist:<Domain>
		net group "Domain Admins" /domain
		net user <Username> /domain
		whoami.exe /priv
		tasklist /FI "IMAGENAME eq explorer.exe"
		sc.exe query hwinfo
	Output/Artifact	netscan.exe (network scanning utility staged/executed)
Lateral Movement	Command Execution	%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Lateral Movement	Command Execution	%Temp%\<PSEXEC_NAME>.exe -accepteula \\<HOST_IP> -u <USER_NAME> -p <PASSWORD> -c -f -h -d <LOCKER_PATH> <LOCKER_ARGS> --spread-process
		cmd /C net use
	Configuration Change	net share c=c:\ /grant:everyone,full
		cmd /C fsutil behavior set SymlinkEvaluation R2R:1
		cmd /C fsutil behavior set SymlinkEvaluation R2L:1
	Output / Artifact	C:\Users\<REDACTED>\Desktop\test.exe
		C:\Users\<REDACTED>\Desktop\1.exe
		C:\Users\<REDACTED>\Desktop\2.exe
		C:\Users\<REDACTED>\Desktop\3.exe
Command and Control	Output / Artifact	C:\ProgramData\Veeam\socks64.dll
		C:\ProgramData\USOShared\socks64.dll
		C:\ProgramData\VMware\logs\socks64.dll
		C:\ProgramData\Adobe\socks64.dll
		C:\ProgramData\Veeam\Backup\OracleLogBackup\socks64.dll
Exfiltration	Command Execution	"C:\Program Files\WinRAR\WinRAR.exe" a -ep1 -scul -r0 -iext -imon1 <archive> <target files/directories>
Impact	Command Execution	vssadmin.exe delete shadows /for=<drive> /all
		wbadmin.exe stop
		net.exe stop vss
		net1.exe start vss

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Impact	Command Execution	VSSUIRUN.exe <drive>
		Dismount-DiskImage -ImagePath <image>
		SRManager.exe (Splashtop Remote service interaction)
	Configuration Change	bcdedit.exe /set safeboot network
		bcdedit.exe /deletevalue {default} safeboot
		REG ADD HKCU\Control Panel\Desktop\Wallpaper = <image path>
	Output/Artifact	C:\Users\<REDACTED>\AppData\Local\Programs\WinSCP\WinSCP.exe

Observed Behaviors: Linux

Tactic	Evidence Type	Observed Behavior
Execution	Command Execution	esxcfg-advcfg -s 32768 /BufferCache/MaxCapacity
		esxcfg-advcfg -s 20000 /BufferCache/FlushInterval
		etrlimit()
Stealth	Command Execution	esxcli vm process list
		vim-cmd vmsvc/getallvms
Defense Impairment	Command Execution	esxcli vm process kill -t force -w <VM_ID>
		vim-cmd vmsvc/snapshot.removeall <VM_ID> > /dev/null 2>&1
Discovery	Command Execution	esxcli storage filesystem list
		vim-cmd vmsvc/getallvms
		OpenFileWithPermission("/proc/cpuinfo", "r")
		nftw()
		fdopendir()
Lateral Movement	Command Execution	Use of --spread-vcenter option to propagate via vCenter environments
Impact	Command Execution	vim-cmd vmsvc/snapshot.removeall <VM_ID> > /dev/null 2>&1
	Configuration Change	Disable HA priority across VMs using acli vm.update <VM_ID> ha_priority=0

Kill Chain

Initial Access

- Compromised RDP/VPN
- Exploited Edge Vulnerabilities
- Phishing & Social Engineering

Persistence

- Remote Management Tools
- Scheduled Tasks & Services
- Rogue User Accounts

Stealth

- BYOVD Attacks
- Masquerading/LOLBins
- Obfuscated Scripts

Defense Impairment

- Security Tool Disablement
- EDR Tampering
- Log & Backup Deletion

Lateral Movement

- PsExec & SMB Movement
- Credential Reuse
- Remote Command Execution

Exfiltration

- Data Theft Prior to Encryption
- Archived Data Staging
- Cloud-Based Exfiltration

Impact

- Hybrid encryption model
- Backup Destruction
- Double Extortion Operations

MITRE ATT&CK® Mappings

Reconnaissance	
T1589: Gather Victim Identity Information	.001: Credentials
Resource Development	
T1585: Establish Accounts	.001: Social Media Accounts
Initial Access	
T1078: Valid Accounts	.001: Default Accounts
T1133: External Remote Services	
T1190: Exploit Public-Facing Application	
T1566: Phishing	.001: Spearphishing Attachment .002: Spearphishing Link
Execution	
T1047: Windows Management Instrumentation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	.001: PowerShell .003: Windows Command Shell
T1106: Native API	
T1204: User Execution	.001: Malicious Link .002: Malicious File
T1569: System Services	.002: Service Execution
T1675: ESXi Administration Command	

MITRE ATT&CK® Mappings

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 .004: Winlogon Helper DLL
Privilege Escalation	
T1055: Process Injection	
T1068: Exploitation for Privilege Escalation	
T1078: Valid Accounts	.002: Domain Accounts
T1098: Account Manipulation	.007: Additional Local or Domain Groups
T1134: Access Token Manipulation	.002: Create Process with Token
T1548: Abuse Elevation Control Mechanism	.002: Bypass User Account Control
Stealth	
T1014: Rootkit	
T1027: Obfuscated Files or Information	.007: Dynamic API Resolution .010: Command Obfuscation .013: Encrypted/Encoded File
T1036: Masquerading	.004: Masquerade Task or Service .005: Match Legitimate Resource Name or Location
T1055: Process Injection	.001: Dynamic-link Library Injection
T1070: Indicator Removal	.004: File Deletion
T1211: Exploitation for Defense Evasion	

MITRE ATT&CK® Mappings

Stealth	
T1218: System Binary Proxy Execution	.011: Rundll32
T1480: Execution Guardrails	.002: Mutual Exclusion
T1497: Virtualization/Sandbox Evasion	
T1574: Hijack Execution Flow	.010: Services File Permissions Weakness
T1622: Debugger Evasion	
T1678: Delay Execution	
Defense Impairment	
T1112: Modify Registry	
T1222: File and Directory Permissions Modification	
T1484: Domain Policy Modification	.001: Group Policy Modification
T1685: Disable or Modify Tools	.001: Disable or Modify Windows Event Log .005: Clear Windows Event Logs
T1686: Disable or Modify System Firewall	
T1688: Safe Mode Boot	
Credential Access	
T1003: OS Credential Dumping	.001: LSASS Memory
T1552: Unsecured Credentials	.001: Credentials in Files .006: Group Policy Preferences
T1555: Credentials from Password Stores	

MITRE ATT&CK® Mappings

Discovery	
T1007: System Service Discovery	
T1010: Application Window Discovery	
T1012: Query Registry	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1057: Process Discovery	
T1069: Permission Groups Discovery	.002: Domain Groups
T1082: System Information Discovery	
T1083: File and Directory Discovery	
T1087: Account Discovery	.002: Domain Account
T1120: Peripheral Device Discovery	
T1135: Network Share Discovery	
T1614: System Location Discovery	.001: System Language Discovery
T1654: Log Enumeration	
T1673: Virtual Machine Discovery	
T1680: Local Storage Discovery	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH

MITRE ATT&CK® Mappings

Lateral Movement	
T1091: Replication Through Removable Media	
T1210: Exploitation of Remote Services	
T1570: Lateral Tool Transfer	
Collection	
T1005: Data from Local System	
T1074: Data Staged	.001: Local Data Staging
Command and Control	
T1001: Data Obfuscation	.001: Junk Data
T1071: Application Layer Protocol	.001: Web Protocols .002: File Transfer Protocols
T1105: Ingress Tool Transfer	
T1219: Remote Access Tools	.002: Remote Desktop Software
T1571: Non-Standard Port	
T1573: Encrypted Channel	.001: Symmetric Cryptography
Exfiltration	
T1011: Exfiltration Over Other Network Medium	.001: Exfiltration Over Bluetooth
T1041: Exfiltration Over C2 Channel	
T1048: Exfiltration Over Alternative Protocol	.003: Exfiltration Over Unencrypted Non-C2 Protocol
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	
T1491: Defacement: Publishing Victim Data	.001: Internal Defacement
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/
- Center for Internet Security (2025, September 11) “Qilin Top Ransomware Threat to SLTTs in Q2 2025.” https://www.cisecurity.org/insights/blog/qilin-top-ransomware-threat-to-sltts-in-q2-2025
- 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/
- 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
- Resecurity (2025, October 15) “Qilin Ransomware and the Ghost Bulletproof Hosting Conglomerate.” https://www.resecurity.com/es/blog/article/qilin-ransomware-and-the-ghost-bulletproof-hosting-conglomerate
- Santos, Jacob; Dela Cruz, Junestherry; et. al. (2025, October 23) Trend Micro: “Agenda Ransomware Deploys Linux Variant on Windows Systems Through Remote Management Tools and BYOVD Techniques.” https://www.trendmicro.com/en_us/research/25/j/agenda-ransomware-deploys-linux-variant-on-windows-systems.html
- SentinelOne (n.d.) “Agenda (Qilin).” https://www.sentinelone.com/anthology/agenda-qilin/
- Takeda, Takahiro; Dunk, Jordyn, et. al. (2025, October 26) Cisco: “Uncovering Qilin attack methods exposed through multiple cases.” https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/
- Thodex (n.d.) “Agenda (Qilin) Ransomware: Analysis, Detection, and Recovery.” https://www.thodex.com/ransomware/agenda-qilin/
- Thomas, Will (2025, October 03) SANS: “The Evolution of Qilin RaaS.” https://www.sans.org/blog/evolution-qilin-raas
- 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