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:

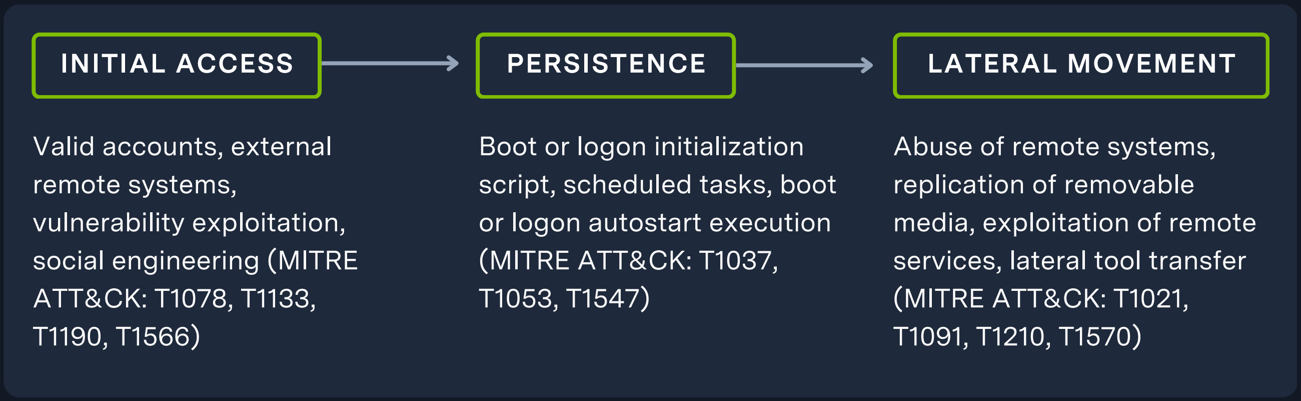
- Industrials (Manufacturing)

Most frequently targeted victim HQ region:

- North America

Known Associations:

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



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

INITIAL ACCESS

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

PERSISTENCE

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

LATERAL MOVEMENT

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

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.

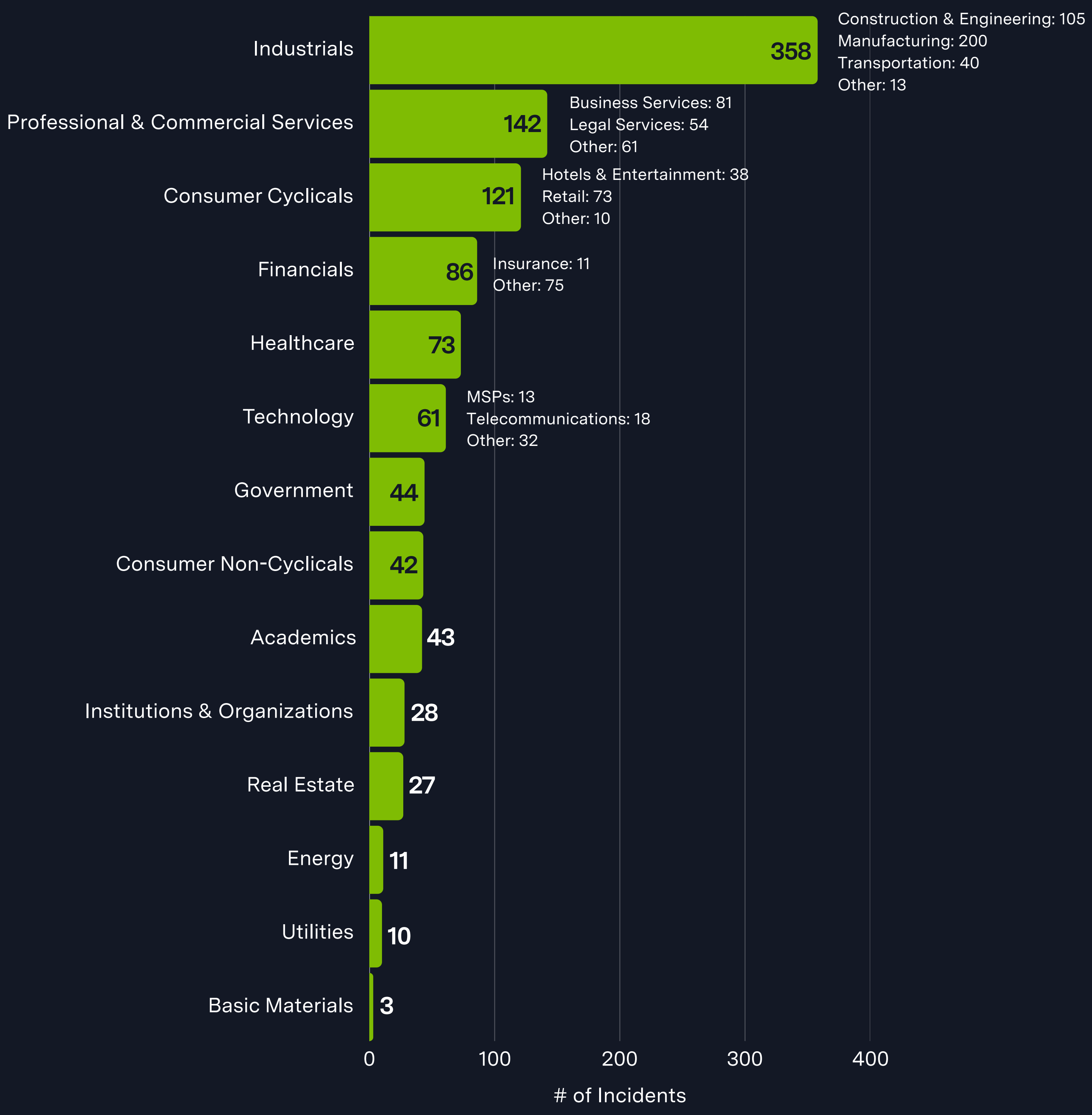
Features the operation maintains - such as spam tools and PR support - and their longer standing operation likely makes Qilin an attractive operation for more sophisticated financially motivated threat groups. It is very likely that Qilin activity will continue to be reported over the next 3-6 months.

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.

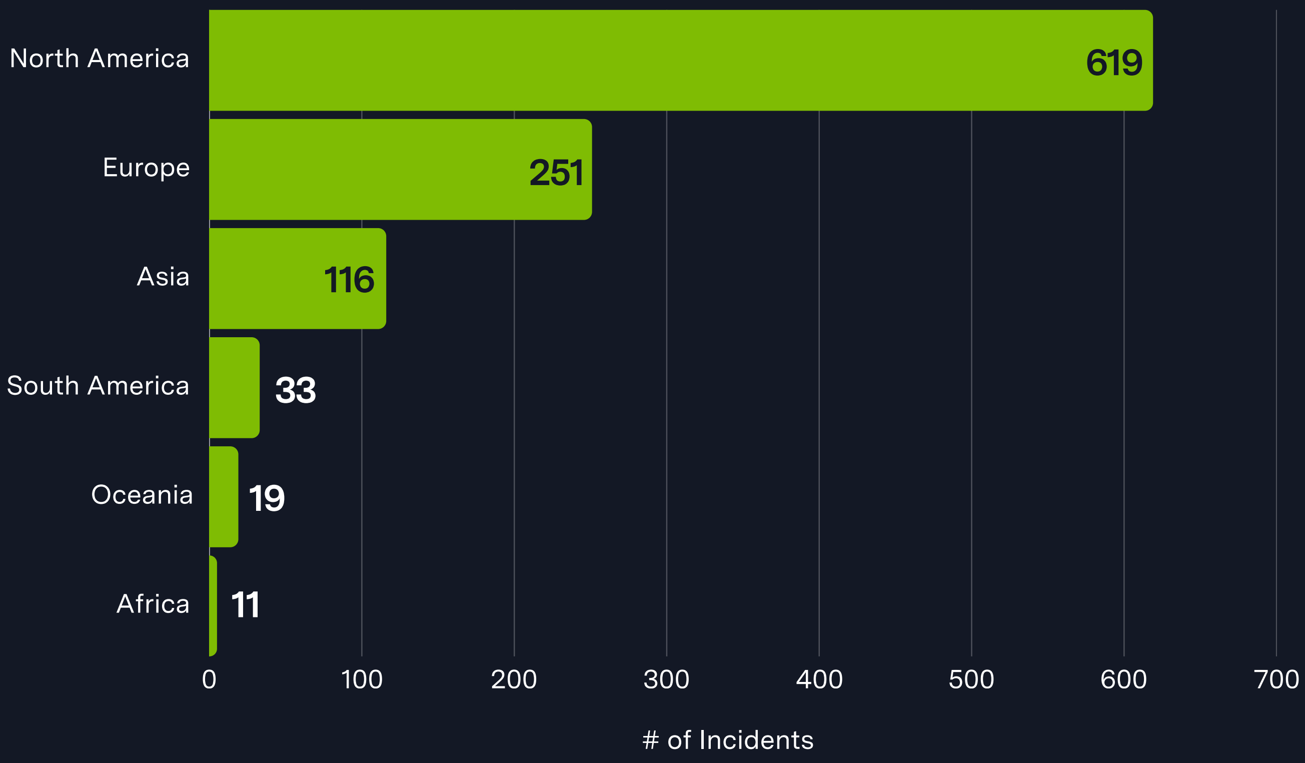
Previous Targets

Previous Industry Targets from 01 Jan 2025 to 31 Dec 2025

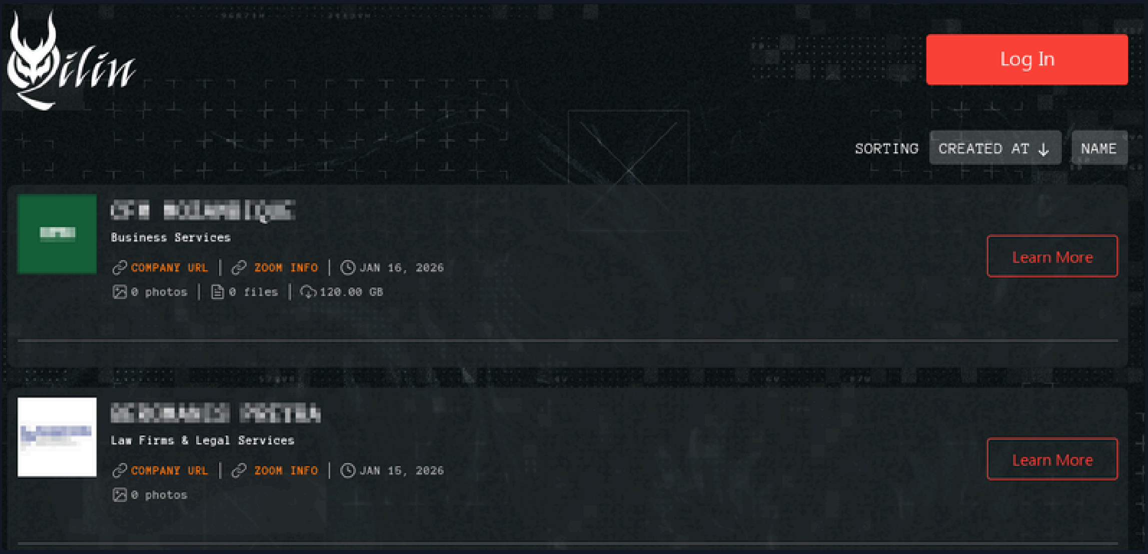


Previous Targets

Previous Victim HQ Regions from 01 Jan 2025 to 31 Dec 2025



Data Leak Site



[redacted]
Business Services
COMPANY URL | ZOOM INFO | JAN 16, 2026
0 photos | 0 files | 120.00 GB

[redacted]
Law Firms & Legal Services
COMPANY URL | ZOOM INFO | JAN 15, 2026
0 photos

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.

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

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.
Atera	An all-in-one solution that combines remote monitoring and management with other tools like helpdesk, patching, and automation. This tool has been abused to gain persistence on compromised environments.
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.
BypassCredGuard.exe	A tool used to bypass Windows Credential Guard and facilitate credential dumping.
cipher.exe	A native Microsoft utility that manages encryption of directories and files on NTFS (New Technology File System) partitions by using the Encrypting File System (EFS).
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.
Cyberduck	An open-source file transfer tool abused to exfiltrate stolen data to cloud storage.
dark-kill	An open-source tool used to disable EDR by loading a malicious driver into the Windows kernel.

Known Tools

Distant Desktop	An RMM tool used to provide remote access to compromised systems.
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.
eskle.sys	A driver that likely belongs to a game-related package and is commonly used by cheat developers to evade anti-cheat systems.
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.
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.
fnarw.sys	A vulnerable driver with little information available; it has been observed in Qilin-attributed activity.
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.
GoToDesk	An RMM tool used to provide remote access to compromised systems.
hlpdrv.sys	A vulnerable driver that has been assessed to be used to gain kernel-level access and potentially terminate traditional endpoint detection and response solutions.
iexplore.exe	A tool used to view sensitive information in files during manual data discovery
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.
Kali	A Linux distribution designed for digital forensics and penetration testing. It was observed being used for network scanning and other reconnaissance activities.[
KILLAV	A tool used to terminate antivirus related services and processes.

Known Tools

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 Paint	A Microsoft utility used to view sensitive information in files during manual data discovery.[
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.
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.
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.
nltest	A Windows command-line utility used to list domain controllers and enumerate domain trusts.

Known Tools

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.
NotePad	A Microsoft utility used to view the contents of stolen logs, credentials, and configuration files.
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 challenging 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.
PuTTY	A free and open-source terminal emulator, serial console and network file transfer application.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
rdpclip.exe	A tool used to facilitate clipboard sharing over RDP sessions during lateral movement.

Known Tools

RSAT	Remote Server Administration Tools. A Windows application that remotely manages the roles and features running Windows Server with snap-ins.
rwdrv.sys	A vulnerable driver that has been assessed to be used to gain kernel-level access and potentially terminate traditional endpoint detection and response solutions.
ScreenConnect	AKA ConnectWise. A remote management software used to gain access to a remote computer.
SharpDecryptPwd	A tool used to extract and persist stored authentication data from multiple client applications, consolidating harvested credentials for exfiltration.
Sliver	An open-source, cross-platform, red team command and control (C2) framework written in Golang.
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.
Splashtop	A remote desktop application that allows users to remotely access their Windows, Mac, and Linux computers from any Windows, Mac, iOS, Android, and Chromebook device.
Stealc	A credential and information stealer first discovered by researchers in January 2023. Researchers assess the malware contains code similarities to prominent stealer families including Vidar, Raccoon, Mars, and RedLine.
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.
TOR	A software suite and network that provides increased anonymity on the Internet. It creates a multi-hop proxy network and utilizes multilayer encryption to protect both the message and routing information.

Known Tools

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.
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.
WinRAR	WinRAR is a data compression, encryption, and archiving tool for Windows. It is frequently abused by threat actors to archive files prior to their exfiltration.

Known Tools

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.
WinSCP	A free and open-source SFTP, FTP, WebDAV, S3, and SCP client for Windows that can be used to exfiltrate files to a remote server.
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	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
Defense Evasion	Command Execution	mmc.exe C:\Windows\System32\wbadmin.msc
		mmc.exe C:\Windows\System32\diskmgmt.msc
		pbeagent.exe SysLogger.exe 1000 "Monitoring Stopped"
		vssadmin.exe delete shadows /all /quiet
		powershell.exe Clear-Windows-Event-Logs (all logs)
		cmd /C net stop vss
		cmd /C net start vss
		cmd /C timeout /T 10 & del <file>
		mshta.exe vbscript:ShellExecute(cmd.exe, runas)
		sc create dark type=kernel binPath=<path>\dark.sys
		sc start dark
		sc delete dark

Observed Behaviors:
Windows

Tactic	Evidence Type	Observed Behavior
Defense Evasion	Configuration Change	wmic service where name='vss' call ChangeStartMode Disabled
		wmic service where name='vss' call ChangeStartMode Manual
		fsutil.exe behavior set SymlinkEvaluation R2L:1
	Output/Artifact	C:\Users\Administrator\<REDACTED>\Downloads\*.exe
		C:\Users\<REDACTED>\Desktop\*.exe
		C:\Users\Administrator\<REDACTED>\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"

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Discovery	Command Execution	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
		%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>

Observed Behaviors: Windows

Tactic	Evidence Type	Observed Behavior
Impact	Command Execution	vssadmin.exe delete shadows /for=<drive> /all
		wbadmin.exe stop
		net.exe stop vss
		net1.exe start vss
		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()
Defense Evasion	Command Execution	esxcli vm process list
		vim-cmd vmsvc/getallvms
		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

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	
Defense Evasion	
T1014: Rootkit	
T1027: Obfuscated Files or Information	.007: Dynamic API Resolution .010: Command Obfuscation .013: Encrypted/Encoded File
T1055: Process Injection	.001: Dynamic-link Library Injection
T1070: Indicator Removal	.001: Clear Windows Event Logs .004: File Deletion
T1112: Modify Registry	

MITRE ATT&CK® Mappings

Defense Evasion	
T1211: Exploitation for Defense Evasion	
T1218: System Binary Proxy Execution	.011: Rundll32
T1222: File and Directory Permissions Modification	.001: Windows File and Directory Permissions Modification
T1480: Execution Guardrails	.002: Mutual Exclusion
T1484: Domain Policy Modification	.001: Group Policy Modification
T1497: Virtualization/Sandbox Evasion	
T1562: Impair Defenses	.001: Disable or Modify System Firewall .002: Disable Windows Event Logging .009: Safe Mode Boot
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
T1555: Credentials from Password Stores	
Discovery	
T1007: System Service Discovery	
T1010: Application Window Discovery	

MITRE ATT&CK® Mappings

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	
Lateral Movement	
T1021: Remote Services	.001: Remote Desktop Protocol .002: SMB/Windows Admin Shares .004: SSH
T1091: Replication Through Removable Media	
T1210: Exploitation of Remote Services	
T1570: Lateral Tool Transfer	

MITRE ATT&CK® Mappings

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
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
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	

MITRE ATT&CK® Mappings

Impact	
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