blackpoint

THREAT PROFILE:

Qilin Ransomware

Table of Contents

Executive Summary

First Identified:
2022

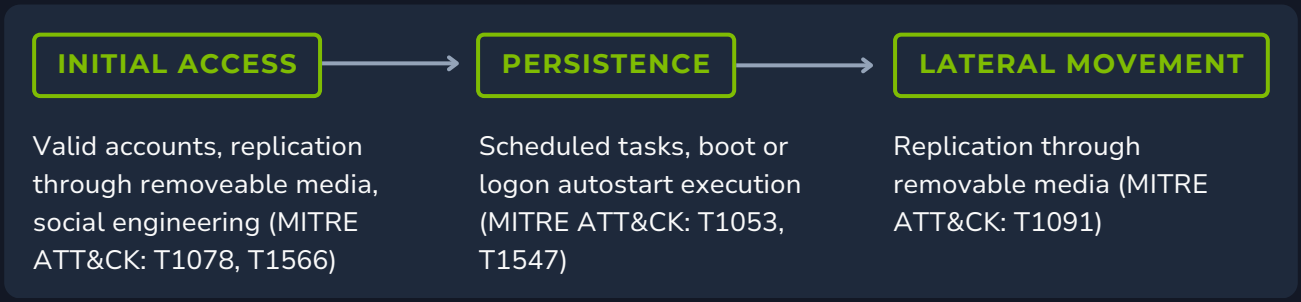
Operation style:
Ransomware-as-a-Service (RaaS), and affiliates earn 80% of a payment of ransom demands of less than $3 million and 85% of ransom payments over $3 million.

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 ransom demand is not paid.

Most frequently targeted industry:
- Healthcare

Most frequently targeted victim HQ region:
- United States, North America

Known Associations:
- Scattered Spider



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, 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 a ransom payment less than $3 million and 85% of ransom payments over $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

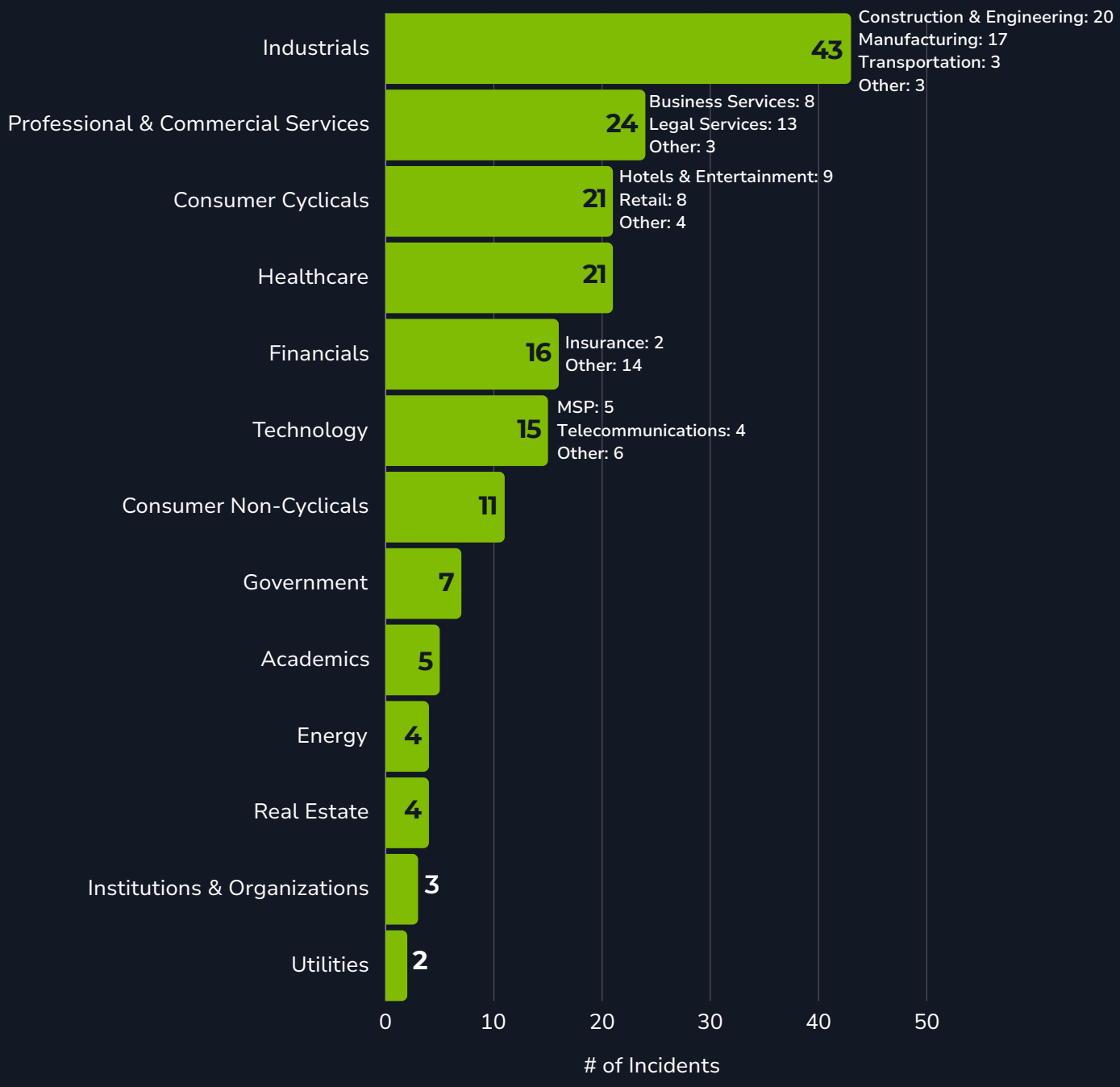
In October 2024, Halcyon security researchers reported a new and updated version of the Qilin ransomware variant, dubbed “Qilin.B”. Qilin.B is written in the Rust programming language. According to the research, Qilin.B supports AES-256-CTR encryption for systems with Advanced Encryption Standard New 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.

Qilin.B is an updated variant of Qilin, using updated encryption and defense evasion techniques.

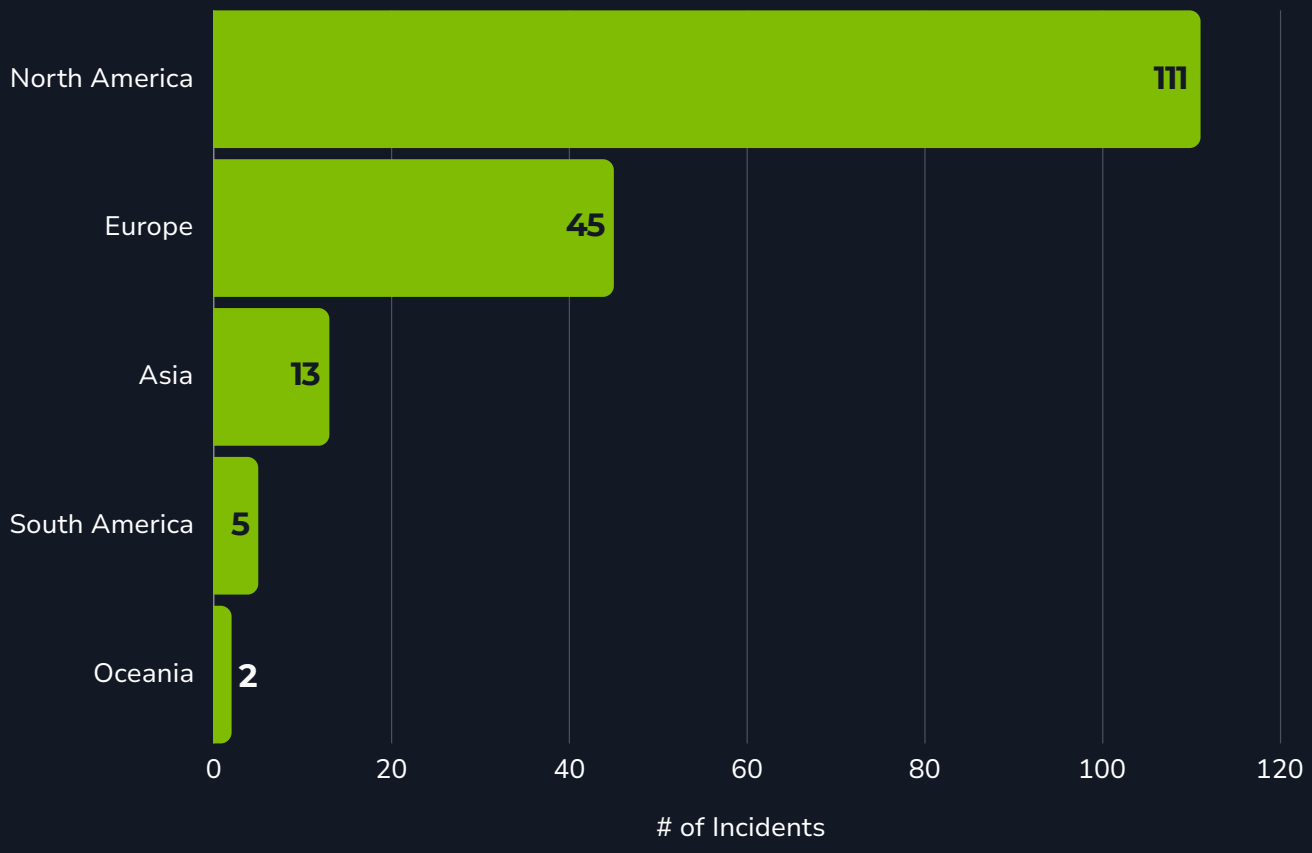
Previous Targets: Qilin

Previous Industry Targets from 01 Jan 2024 to 31 Dec 2024

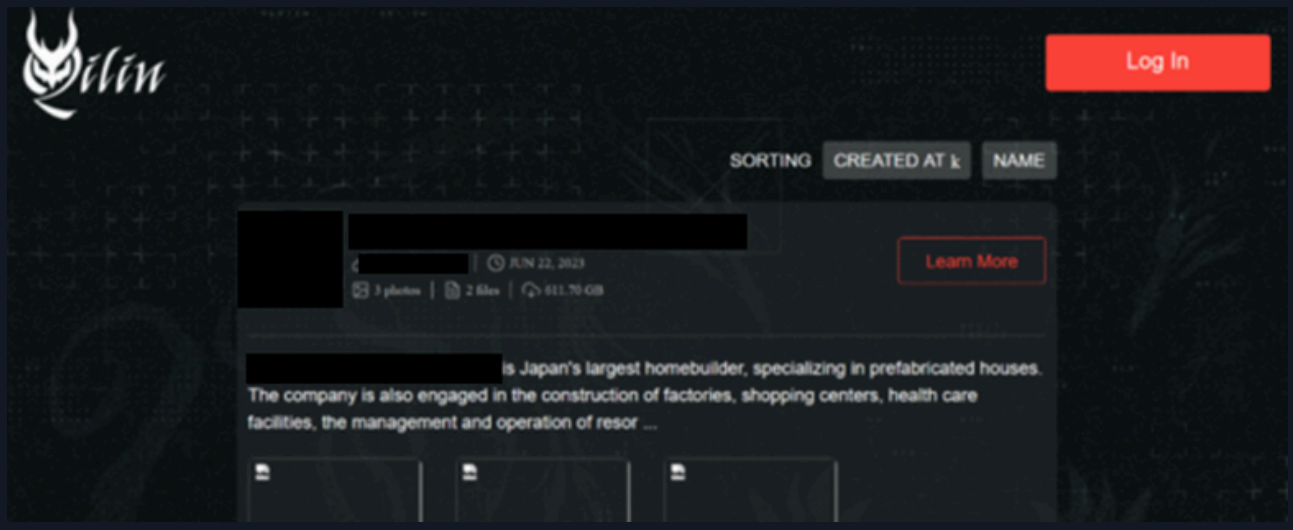


Previous Targets: Qilin

Previous Victim HQ Regions from 01 Jan 2024 to 31 Dec 2024



Data Leak Site: Qilin



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

Known Exploited Vulnerabilities

CVE-2023-27532 (CVSS: 7.5)

Missing Authentication for Critical Function Vulnerability
Product Affected: Veeam Backup & Replication Cloud Connect

Associations: Qilin

Scattered Spider

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

Known Tools: Qilin

Text in **bold** indicates behaviors that have been observed by Blackpoint's SOC.

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.
conhost.exe	A Windows utility that is used to provide the ability to drag and drop files/folders directly into Command Prompt.
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.
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.
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.

Known Tools: Qilin

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.
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.
PowerShell	A task automation and configuration management program that includes a command-line shell and the associated scripting language.
PsExec	A utility tool that allows users to control a computer from a remote location.
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.
svchost.exe	A shared-service process that Windows uses to load DLL files.

Known Tools: Qilin

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.
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.
Veeam Agent Configurator	A Veeam.MBP.AgentConfigurator.exe
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.
WMIC	A utility that provides a command-line interface for Windows Management Instrumentation.
wscript	An automation technology for Microsoft Windows operating systems that provides scripting abilities comparable to batch files, but with a wider range of supported features.

Observed Qilin Behaviors: Windows

Text in green indicates behaviors that have been observed by Blackpoint's SOC.

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
Persistence	explorer.exe tsd-setup.exe tsd-setup.tmp /SL5="$402D4,24132872,174080,C:\Users\$username\Documents\ConnectWiseControl\Files\tsd-setup.exe" tsd-setup.exe /SPAWNWND=$8430630 /NOTIFYWND=$402D4 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 Setup.exe $username Setup.exe /q vcredist_x64.exe $username vcredist_x64.exe /q Setup.exe $username Setup.exe /q findwnd.exe $username findwnd.exe "TApplication" "Total Software Deployment" tsd.exe $username tsd.exe Taskmgr.exe $username Taskmgr.exe /4 tniwinagent.exe $username tniwinagent.exe /service /$IPAddress/login:"current" /driver:2 SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\

Observed Qilin Behaviors: Windows

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
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"
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
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} C:\Windows\System32\bcdedit.exe /set safeboot network bcdedit /deletevalue {default} safeboot C:\windows\system32\bcdedit.exe /set safeboot{current} network

Observed Qilin Behaviors: Linux

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 %llu vim-cmd vmsvc/snapshot.removeall %llu > /dev/null 2>&1
Discovery	storage filesystem list nftw() fdopendir() OpenFileWithPermission ((_int64)"/proc/cpuinfo", (_int64)"r");

MITRE ATT&CK® Mappings: Qilin

Initial Access	
T1078: Valid Accounts	
T1091: Replication Through Removable Media	
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	.001: Malicious Link .002: Malicious File
T1569: System Services	.002: Service Execution
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

MITRE ATT&CK® Mappings: Qilin

Privilege Escalation	
T1055: Process Injection	
T1068: Exploitation for Privilege Escalation	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1078: Valid Accounts	.002: Domain Accounts
T1134: Access Token Manipulation	
T1548: Abuse Elevation Control Mechanism	
Defense Evasion	
T1014: Rootkit	
T1027: Obfuscated Files or Information	
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

MITRE ATT&CK® Mappings: Qilin

Defense 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
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 Discovery	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1082: System Information Discovery	
T1087: Account Discovery	.002: Domain Account
T1614: System Location Discovery	.001: System Language Discovery

MITRE ATT&CK® Mappings: Qilin

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
Exfiltration	
T1011: Exfiltration Over Other Network Medium	.001: Exfiltration Over Bluetooth
Impact	
T1486: Data Encrypted for Impact	
T1489: Service Stop	
T1490: Inhibit System Recovery	
T1529: System Shutdown/Reboot	
T1561: Disk Wipe	.001: Disk Content Wipe

MITRE ATT&CK® Mappings: Qilin

Impact
T1657: Financial Theft

References

- Greig, Jonathan (2023, May 17) The Record: “Researchers infiltrate Qilin ransomware group, finding lucrative affiliate payouts.” https://therecord.media/researchers-infiltrate-qilin-ransomware
- 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
- Kichatov, Nikolay (2023, May 15) Group IB: “You’ve been kept in the dark (web): exposing Qilin’s RaaS program.” https://www.group-ib.com/blog/qilin-ransomware/
- 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
- Montini, Heloise (2023, September 04) SalvageData: “Qilin (Agenda) Ransomware: Complete Guide.” https://www.salvagedata.com/qilin-agenda-ransomware/
- Morales, Nathaniel; Chavez, Ivan Nicole; Ragasa, Nathaniel Gregory; Ladores, Don Ovid; Bonaobra, Jeffrey Francis; Jesus, Monte de (2022, December 22) Trend Micro: “Agenda Ransomware Uses Rust to Target More Vital Industries.” https://www.trendmicro.com/en_th/research/22/l/agenda-ransomware-uses-rust-to-target-more-vital-industries.html
- Quorum Cyber (2023, July) “Threat Intelligence Agenda Ransomware.” https://www.quorumcyber.com/wp-content/uploads/2023/07/Quorum-Cyber-Agenda-Ransomware-Report-TI.pdf
- SecneurX Threat Analysis (2022, December 26) “What is Qilin Ransomware?” https://www.secneurx.com/post/what-is-qilin-ransomware
- Sectrio (2023, July 24) “QILIN Ransomware Report.” https://sectrio.com/qilin-ransomware-report-2023/
- SentinelOne (n.d.) “Agenda (Qilin).” https://www.sentinelone.com/anthology/agenda-qilin/
- ShadowStackRE (2023, December 06) “Qilin Ransomware.” https://www.shadowstackre.com/analysis/qilin
- Thodex (n.d.) “Agenda (Qilin) Ransomware: Analysis, Detection, and Recovery.” https://www.thodex.com/ransomware/agenda-qilin/

Adversary Pursuit Group

blackpoint