blackpoint

THREAT PROFILE:

Qilin Ransomware

Table of Contents

Executive Summary

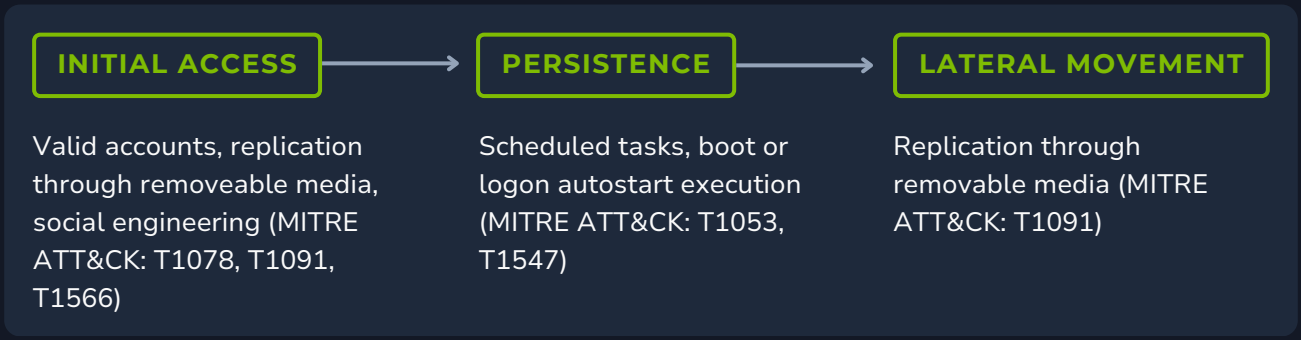
First Identified:
2022

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:
- Industrials (Construction & Engineering & Manufacturing)

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



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.

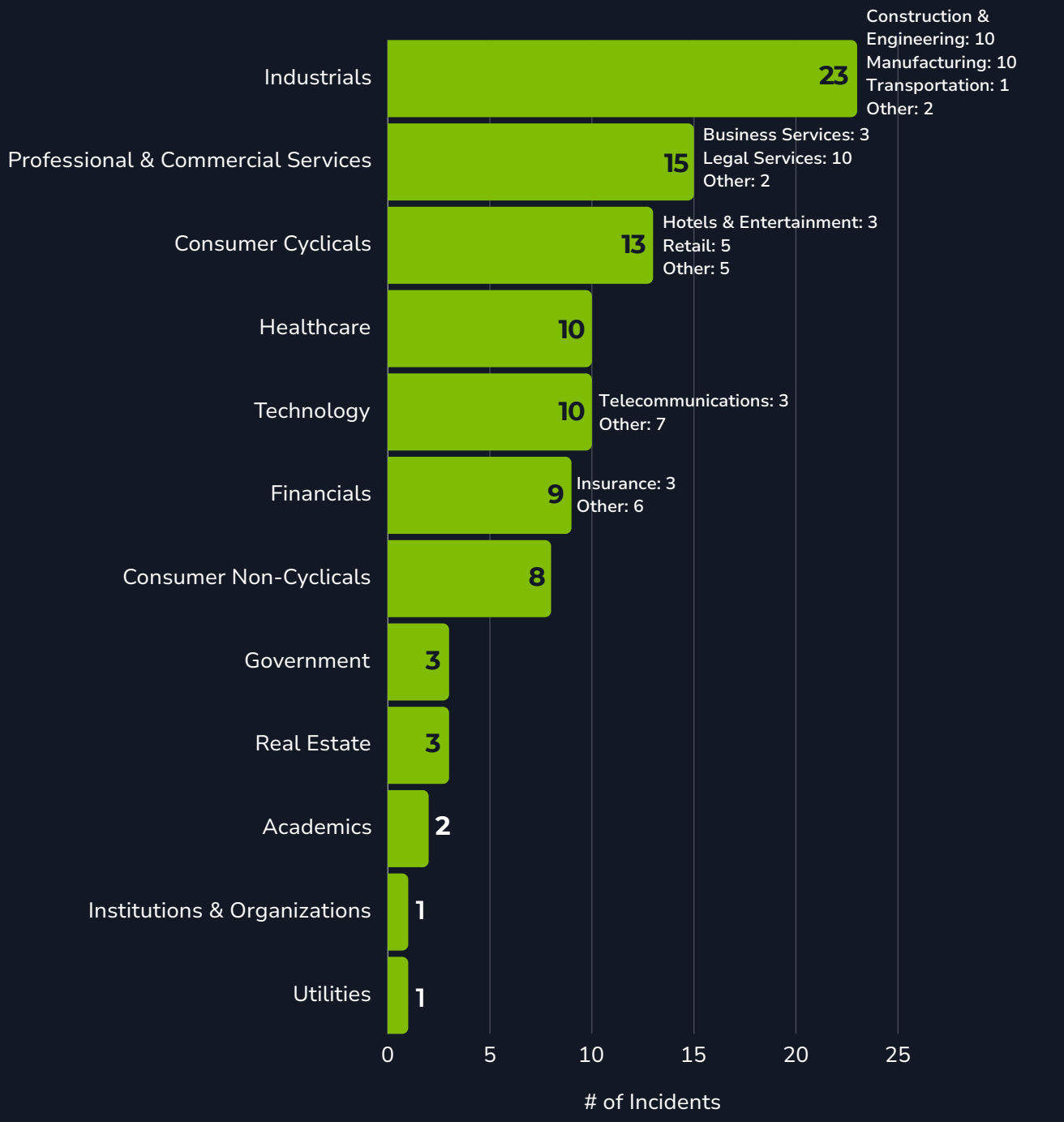
Qilin ransomware offers multiple encryption methods, which is also configurable by the affiliate through the panel. Once option uses AES-256 encryption to encrypt the files on the victim's system and uses RSA-2048 to encrypt the generated key. Files are appended with a new random extension. The Linux 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.

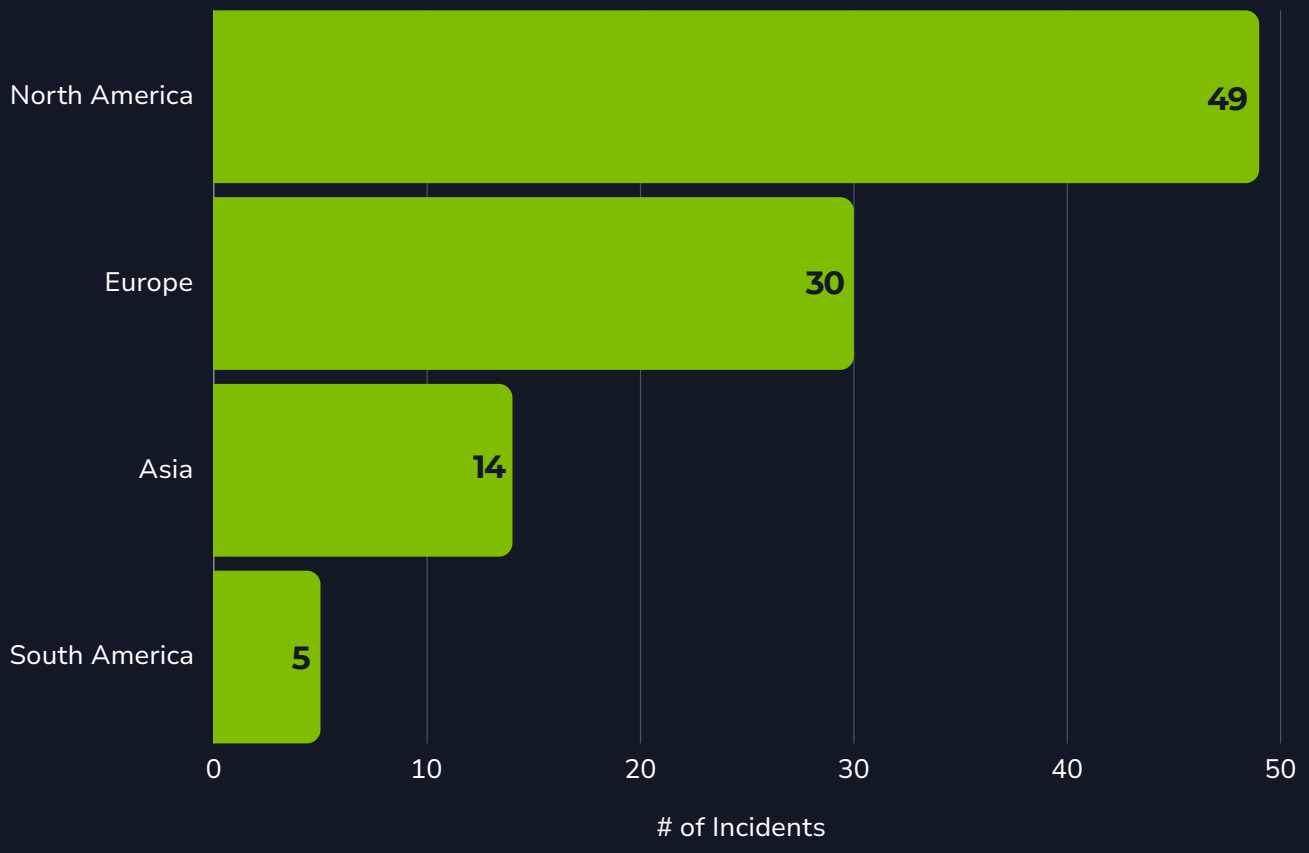
Previous Targets: Qilin

Previous Industry Targets from 01 Jul 2023 to 30 Jun 2024

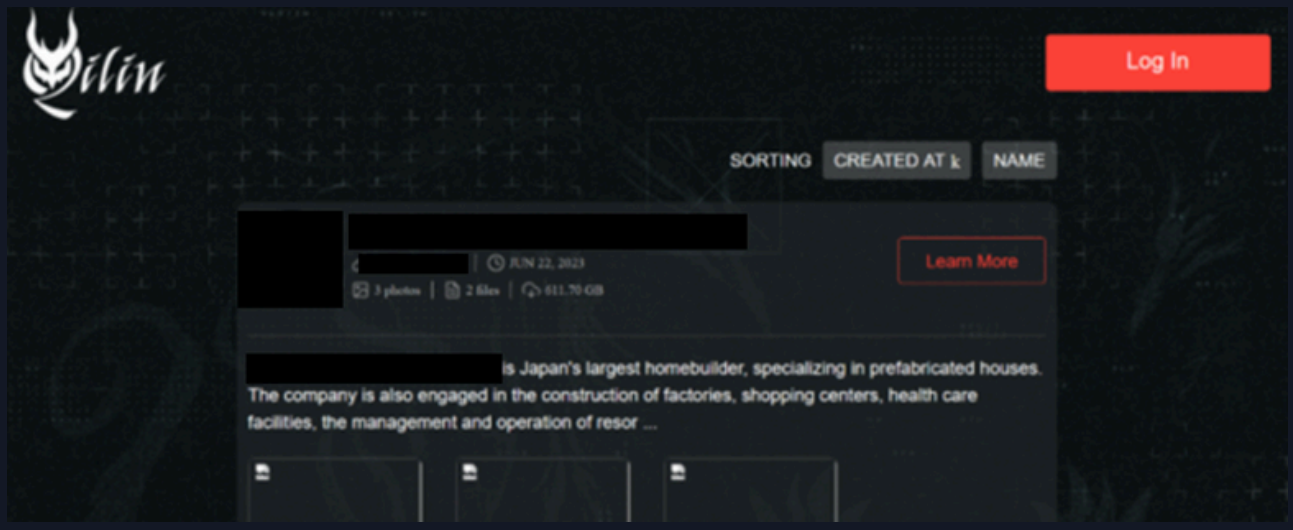


Previous Targets: Qilin

Previous Victim HQ Regions from 01 Jul 2023 to 30 Jun 2024



Data Leak Site: Qilin



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

Known Tools: Qilin

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.
esxcli	A tool that allows for remote management of ESXi hosts.
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.
ncat	A general-purpose command line tool for reading, writing, redirecting, and encrypting data across a network.
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.
RDP	A protocol that provides a user with a graphical interface to connect to another computer over a network connection.
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.

Observed Qilin Behaviors: Windows

Execution	-alter {int} -encryption {value} -ips {IP Address} -min-size {value} -no-proc -no-services -password {string} -path {directory} -safe -stat
Persistence	SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\
Defense Evasion	vssadmin.exe delete shadows /all /quiet
Impact	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 --no-snap-rm --no-vm-kill -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	
T1566: Phishing	.002: Spearphishing Link
Execution	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1059: Command and Scripting Interpreter	
T1204: User Execution	.001: Malicious Link
Persistence	
T1053: Scheduled Task/Job	.005: Scheduled Task
T1547: Boot or Logon Autostart Execution	.001: Registry Run Keys / Startup Folder
Privilege Escalation	
T1055: Process Injection	
Defense Evasion	
T1112: Modify Registry	
T1484: Domain Policy Modification	.001: Group Policy Modification

MITRE ATT&CK® Mappings: Qilin

Defense Evasion	
T1562: Impair Defenses	.002: Disable Windows Event Logging .009: Safe Mode Boot
Credential Access	
T1552: Unsecured Credentials	.001: Credentials in Files .006: Group Policy Preferences
Discovery	
T1012: Query Discovery	
T1018: Remote System Discovery	
T1046: Network Service Discovery	
T1082: System Information Discovery	
T1614: System Location Discovery	.001: System Language Discovery
Lateral Movement	
T1091: Replication Through Removable Media	
Collection	
T1005: Data from Local System	
Impact	
T1486: Data Encrypted for Impact	

MITRE ATT&CK® Mappings: Qilin

Impact
T1489: Service Stop
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
- 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/
- Trust-IT (2023, December 13) “Qilin Ransomware: A Growing Threat in Cybersecurity.” https://www.trust-it.gr/qilin-ransomware-a-growing-threat-in-cybersecurity/
- Ward, B. (2023, October 23) Medium: “Member Report: Qilin Ransomware Group Attacks Member OEM’s Supplier.” https://medium.com/@shigeyuki.form/member-report-qilin-ransomware-group-attacks-member-oems-supplier-63887f5afeef

Adversary Pursuit Group

blackpoint