12 November 2025

EMERGING THREATS

Qilin Ransomware Group

Qilin Ransomware Group is a rapidly evolving ransomware-as-a-service (RaaS) operation that first became widely visible in mid-2022 and has since escalated its attacks in both volume and sophistication. According to recent intelligence, Qilin offers affiliates highly customizable ransomware payloads (written in Go and Rust) and supports both Windows and Linux/ESXi targets. They have also matured its business model to include double-extortion tactics, where victims not only face encrypted networks and systems, but also the threat of public data leaks via a dedicated leak site, increasing pressure to pay. Over the last several months, Qilin has increased its affiliate recruitment efforts (especially following disruption of competing RaaS operations), aggressively targeting high-impact sectors such as healthcare, manufacturing, legal and financial services. It is also worthy to note the reach of the threat group's geographical footprint, which includes victims in the United States, United Kingdom, Canada, Germany, France, Japan and Australia (among others globally). These developments reflect a shift from opportunistic encryption attacks toward large-scale, customized, high-value extortion operations that permit malicious actors to gain unauthorized access, steal sensitive data, encrypt critical systems, disrupt operations, and exploit victims for maximum ransom leverage.

THREAT SUMMARY

Qilin Ransomware Group is a rapidly evolving ransomware-as-a-service (RaaS) operation that first became widely visible in mid-2022 and has since escalated its attacks in both volume and sophistication. According to recent intelligence, Qilin offers affiliates highly customizable ransomware payloads (written in Go and Rust) and supports both Windows and Linux/ESXi targets. They have also matured its business model to include double-extortion tactics, where victims not only face encrypted networks and systems, but also the threat of public data leaks via a dedicated leak site, increasing pressure to pay. Over the last several months, Qilin has increased its affiliate recruitment efforts (especially following disruption of competing RaaS operations), aggressively targeting high-impact sectors such as healthcare, manufacturing, legal and financial services. It is also worthy to note the reach of the threat group's geographical footprint, which includes victims in the United States, United Kingdom, Canada, Germany, France, Japan and Australia (among others globally). These developments reflect a shift from opportunistic encryption attacks toward large-scale, customized, high-value extortion operations that permit malicious actors to gain unauthorized access, steal sensitive data, encrypt critical systems, disrupt operations, and exploit victims for maximum ransom leverage.

The impact of Qilin's campaigns has been significant, with organizations reporting major operational downtime, data loss, reputational damage, regulatory exposure, and large ransom demands often reaching tens to hundreds of millions of dollars. In Q2 2025 it became the most reported ransomware against U.S. SLTT (State, Local, Tribal, Territorial) government entities, accounting for nearly a quarter of all incidents reported to MS-ISAC. During the second half of 2025 the group has reportedly added more than 40 victims per month to its leak site. Qilin's increasing prevalence and broad industry targeting mark it as a serious threat to business continuity, data confidentiality and regulatory compliance.

TITAN References:

- Service Profile: Qilin ransomware-as-a-service
- Info Report: 21 Oct 2025

SYNOPSIS

Qilin ransomware operates as a highly modular and customizable threat distributed through a Ransomware-as-a-Service model, enabling affiliates to tailor payloads to specific victims and environments. Initial access is typically achieved through phishing campaigns, exploitation of exposed services such as RDP or VPN gateways, and abuse of known software vulnerabilities. After gaining initial foothold, researchers have observed attackers conducting reconnaissance (for example using nltest, net user and tasklist) and leveraging tools like PsExec for lateral spread across Windows environments. They harvest credentials (running reg add HKLM\\SYSTEM\u2026WDigest to enable plaintext memory retention) and may deploy remote-access or backdoor frameworks such as Cobalt Strike or SystemBC before encryption. In multiple cases the ransomware run-encryption workflow was observed with dual executables: encryptor_1.exe which spreads via PsExec and encryptor_2.exe which encrypts network shares from a single host.

The Qilin encryptor itself is written in Golang and Rust, supports both Windows and Linux/ESXi targets, and offers configurable modes such as skip-step, percent or speed, and custom file extensions. The advanced variant Qilin.B employs AES-256-CTR (for systems with AES-NI) or ChaCha20, and protects encryption keys with RSA-4096/OAEP. Post-encryption activities include deletion of shadow copies, clearing event logs, terminating specified services or processes, unlocking WSL environments to run Linux-based encryptors on Windows, and exfiltration via tools like Cyberduck. Files are appended with a company-ID extension, ransom notes named README-RECOVER-[company_id].txt appear, and victim's details are published on a dedicated leak site to pressure payment.

QILIN RANSOMWARE GROUP COLLECTION

https://hunter.cyborgsecurity.io/research/search?state=(compatible:!f,filters:(),library:!(cyborg_collections),page:0,size:10,sort:last_updated_desc,term:!('e86e6e9a-bc80-4a68-a17c-20ac5cfe747a'),touched:!t)

RELATED HUNT PACKAGES

ENABLING RDP CONNECTIONS THROUGH REGISTRY MODIFICATION

https://hunter.cyborgsecurity.io/research/hunt-package/c44db69a-314e-46cc-b14a-7e5bd6a6e551

SINGLE-CHARACTER NAMED FILES USED FOR EXECUTION

https://hunter.cyborgsecurity.io/research/hunt-package/f20c5f61-c68a-446d-95c4-e227d3ac1078

AUTORUN OR ASEP REGISTRY KEY MODIFICATION

https://hunter.cyborgsecurity.io/research/hunt-package/8289e2ad-bc74-4ae3-bfaa-cdeb4335135c

DRIVER FILE CREATED IN TEMP DIRECTORY - POTENTIAL MALWARE INSTALLATION

https://hunter.cyborgsecurity.io/research/hunt-package/120bf3d2-ab6b-4254-b313-4b543e91c177

COMMON SUSPICIOUS POWERSHELL EXECUTION ARGUMENT TECHNIQUES - BYPASS AND UNRESTRICTED POLICIES

https://hunter.cyborgsecurity.io/research/hunt-package/9762067d-ac45-450e-b1f0-bea9d2e219d7

MSI FILE INSTALLATION FROM SUSPICIOUS LOCATION

https://hunter.cyborgsecurity.io/research/hunt-package/61b3d776-20c3-4804-9543-0c806c00d868

VMWARE SERVICES AND FUNCTIONS DISABLED ON ESXI - POTENTIAL RANSOMWARE

https://hunter.cyborgsecurity.io/research/hunt-package/05136231-4c4c-469e-b193-61b0f15e8bea

MIMIKATZ NON-INTERACTIVE EXECUTION

https://hunter.cyborgsecurity.io/research/hunt-package/9d76a729-5c52-46e4-980c-221fe6f089a0

SCREENCONNECT RELAY MODE ENGAGEMENT - POSSIBLE REMOTE ADMINISTRATION TOOL USAGE

https://hunter.cyborgsecurity.io/research/hunt-package/f5d9bda0-a982-485e-94f7-701352850fad

REMOTE SERVICES - SMB SHARE MOUNTS/ADMIN SHARES/SCANNING

https://hunter.cyborgsecurity.io/research/hunt-package/29b036ae-4879-4509-a0ac-65d46ea76cf1

RUN REGISTRY KEY AUTORUN CREATED FROM PUBLIC USERS DIRECTORY

https://hunter.cyborgsecurity.io/research/hunt-package/f40b2b7c-6a29-4827-8382-bda4cdff7eb4

SUSPICIOUS EXECUTABLE OR SCRIPTS LAUNCHED IN COMMON CONFIGURATION OR SYSTEM RELATED FOLDERS

https://hunter.cyborgsecurity.io/research/hunt-package/F2DD3A46-1C5D-42D3-B3FA-5BEC58D75E0B

SCHEDULED TASK CREATED

https://hunter.cyborgsecurity.io/research/hunt-package/aaa77f56-4a4c-4fdd-a6e3-156e1996d310

WINRAR ARCHIVE CREATED

https://hunter.cyborgsecurity.io/research/hunt-package/259d569c-a60f-46e5-bc89-284489617d62

USER ADDED TO DEFAULT PRIVILEGED WINDOWS SECURITY GROUPS

https://hunter.cyborgsecurity.io/research/hunt-package/b6365ad5-0ccd-4426-97bc-b9484eb9579f

RDP RESTRICTED ADMIN MODE ENABLED - REGISTRY KEY DETECTION

https://hunter.cyborgsecurity.io/research/hunt-package/4cbffa4d-cbb5-45f2-86e4-591a065fc10e

EXCESSIVE WINDOWS DISCOVERY COMMANDLINE ARGUMENTS - POTENTIAL MALWARE INSTALLATION

https://hunter.cyborgsecurity.io/research/hunt-package/8bb5819f-06a4-4e5d-9099-e43115601999

SHADOW COPIES DELETION USING OPERATING SYSTEMS UTILITIES

https://hunter.cyborgsecurity.io/research/hunt-package/2e3e9910-70c1-4822-804a-ee9919b0c419

WDIGEST DOWNGRADE ATTACK - REGISTRY KEY MODIFICATION

https://hunter.cyborgsecurity.io/research/hunt-package/61eece5f-432b-45ad-ab6a-ff1e5e783396

SUSPICIOUS CHILD PROCESS - NOTEPAD.EXE

https://hunter.cyborgsecurity.io/research/hunt-package/377e204f-5fee-4bf0-8eb4-8e05d271b922

WINDOWS DEFENDER TAMPERING - POSSIBLE MALWARE ACTIVITY

https://hunter.cyborgsecurity.io/research/hunt-package/aa6e2535-e1e3-4f0f-80e4-68cc47fc2684

MITRE CONTEXT

- **Exploits Vulnerabilities:**
  - CVE-2023-4966
  - CVE-2025-31324
- **MITRE Tactic Names:**
  - Credential Access
  - Defense Evasion
  - Initial Access
  - Impact
  - Lateral Movement
  - Executio,
  - Collection
  - Persistence
  - Discovery
  - Privilege Escalation
  - Command and Control
- **MITRE Technique Names:**
  - Domain Account
  - Registry Run Keys / Startup Folder
  - Remote Access Software
  - Scheduled Task/Job
  - PowerShell
  - Portable Executable Injection
  - Local Data Staging
  - Malicious File
  - SMB/Windows Admin Shares
  - Service Stop
  - Remote System Discovery
  - Archive via Utility
  - Remote Desktop Protocol
  - Inhibit System Recovery
  - Ingress Tool Transfer
  - Modify Registry
  - Spearphishing Attachment
  - OS Credential Dumping

    - Pass the Hash
    - Command and Scripting Interpreter
    - LSASS Memory
    - Local Accounts
    - Disable or Modify Tools
    - Mshta
- **MITRE Technique IDs:**
    - T1560.001
    - T1219
    - T1059
    - T1489
    - T1218.005
    - T1059.001
    - T1053
    - T1074.001
    - T1003.001
    - T1562.001
    - T1547.006
    - T1490
    - T1018
    - T1550.002
    - T1003
    - T1547.001
    - T1055.002
    - T1566.001
    - T1021.001
    - T1021.002
    - T1105
    - T1136.002
    - T1112
    - T1078.003
    - T1204.002
- **Threat Names:**
    - Qilin Ransomware

REFERENCES

1. https://blog.talosintelligence.com/uncovering-qilin-attack-methods-exposed-through-multiple-cases/
2. https://www.trendmicro.com/en_us/research/25/j/agenda-ransomware-deploys-linux-variant-on-windows-systems.html
3. https://blog.qualys.com/vulnerabilities-threat-research/2025/06/18/qilin-ransomware-explained-threats-risks-defenses
4. https://www.checkpoint.com/cyber-hub/threat-prevention/ransomware/qilin-ransomware/