

3 February 2025 • 22:39

Qilin 22:56

Your company's network is attacked and the entire system is encrypted.
We have downloaded all the company's confidential data.

VICTIM 14:38

ok, what do we need to do?

Qilin 15:22

We will provide the list of files we took. You can send 3 encrypted files
and we will decrypt them as proof. After payment you will receive everything.

VICTIM 22:41

ok, I need to get with our team when they're back on Monday to see
what we're able to get and send to you

Qilin 14:10

As a sign of goodwill we are ready to give a 10% discount.
Stop at \$63,000. You can pay — we have reviewed your financials.

Qilin 12:58

We see that you are not interested in the security of your patients
and choose to play the silent way. Tomorrow we publish a press release.

26 February 2025 — Victim data published on dark web. Deal never closed.

QILIN BE KILLING IT



Inside the Rise of 2026's Most Lethal Ransomware Operation

RootCon 2026

Salimah Liyakkathali

Hi, I am Salimah

\$ whoami

Salimah Liyakkathali

\$ experience

- Global Cyber Readiness and Response – Intel & DFIR, Accenture
- Global Intelligence Operational Analyst at MxDR, Accenture
- Previously in Academia focused on ICS/OT Security

\$ skills

- Threat Intelligence
- Incident Response
- Readiness
- Detection Engineering
- ICS/OT Security

\$ hobbies

- Climbing
- Mountaineering
- Diving



CONTENTS

What we cover in 45 minutes

- 01 Who Is Qilin**
Origins, rebrand, operators
- 02 The Rise**
Jul 2022 to today
- 03 By The Numbers**
Victims, sectors, geography
- 04 Full-Service Extortion**
More than a ransomware crew
- 05 Attack Chain**
Initial access to impact
- 06 Signature TTPs**
WSL trick · Veeam credential harvesting
- 07 Backup Targeting Compared**
How other groups stack up
- 08 Campaigns & Case Files**
Korean Leaks · NHS Synnovis · timeline walkthrough
- 09 Dark Web Intel**
Who they really are
- 10 What Makes Qilin Different**
Vs. LockBit, RansomHub, Akira
- 11 What Actually Stops Them**
Field-tested defenses

WHO IS QILIN?

Born as	"Agenda" ransomware — July 2022, RAMP + XSS forums
Rebranded	September 2022 → Qilin. Full Rust rewrite. New brand.
Name origin	麒麟 Qílín — Chinese mythological creature (power, justice). Russian crew. Chinese branding. Deliberate misdirection.
Operator	Handle: "Haise" (RAMP since May 29 2022), "TRAMP" (DutyFree forum)
Origin	Russia-based. Excludes CIS + BRICS targets (classic opsec). Broke own rule March 2025: attacked Ukraine Ministry of Foreign Affairs.
Platform	Windows · Linux · VMware ESXi
Affiliate cut	80% (ransoms ≤\$3M) → 85% (ransoms >\$3M)



*Russian crime group.
Chinese mythology branding.
DPRK state-actor affiliate.*

THE RISE

Jul 2022

'Haise' posts Agenda on RAMP. Clunky Go binary. Crowded market. Struggles to gain traction.

Sep 2022

Rebrand to Qilin. Full Rust rewrite. Cross-platform. ESXi targeting. New affiliate panel.

2023

Steady growth. FIN12 (DEV-0237) joins as affiliate - experienced hospital hunters from Conti/Ryuk.

Feb 2024

Operation Cronos takes down LockBit. Thousands of skilled affiliates suddenly homeless.

Mar 2024

ALPHV/BlackCat exit scams. More displaced affiliates. Qilin aggressively recruits on RAMP + XSS.

Jul 2024

Scattered Spider (Octo Tempest) joins Qilin. Social engineering + ransomware in one operation.

Apr 2025

RansomHub collapses. Qilin absorbs the fallout. 280% jump in attack claims in 6 weeks.

Jun 2025

#1 globally. 100 victims in a single month. 24% of all US state/local govt ransomware.

2026

500+ victims in first half. Cartel with LockBit5 + DragonForce. No signs of slowing.

BY THE NUMBERS

1,500+

Total victims
since launch

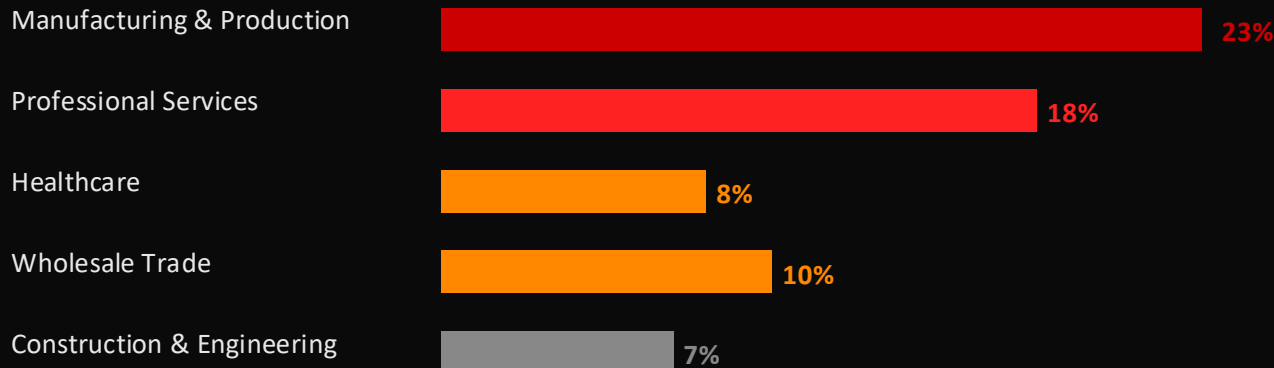
500+

Victims in
2026 alone

40+/mo

Average monthly
victim posts

TOP TARGETED SECTORS



TOP TARGETED COUNTRIES

1. **US** US
2. **FR** France
3. **CA** Canada
4. **GB** UK
5. **DE** Germany

**Which of these features does
Qilin have that NO other major
ransomware group has?**

A Double extortion
(encrypt + leak)

B In-house legal team +
"Call Lawyer" button

C Rust-based payload

D ESXi targeting

**Which of these features does
Qilin have that NO other major
ransomware group has?**

A Double extortion
(encrypt + leak)

B In-house legal team +
"Call Lawyer" button

C Rust-based payload

D ESXi targeting

FORGET 'RANSOMWARE GROUP'.

full-service extortion startup?



CORE PRODUCT

Rust ransomware — Win / Linux / ESXi
Configurable: normal, step-skip, fast, percent modes



DATA STORAGE

1 PB affiliate storage included
No external cloud needed. Exfil direct to panel.



LEGAL DEPT

'Call Lawyer' button in negotiation panel
Frames ransom as cheaper than GDPR/HIPAA fines.



PR TEAM

In-house journalists write shame posts
Assist with psychological pressure during negotiations



DDoS SERVICE

April 2025: DDoS added to affiliate panel
Triple extortion: encrypt + leak + knock offline



TALENT ACQUISITION

RAMP, XSS, DutyFree, T1erOne, Rehub
80–85% rev share. English speakers accepted (\$5K deposit)

ATTACK CHAIN



INITIAL ACCESS

Phishing / ClickFix / VPN brute-force / dark-web creds / CVE exploitation (FortiGate, SAP NetWeaver CVE-2025-31324 CVSS 10)



DISCOVERY

AD enumeration · GPO abuse to enable RDP · NTLM brute-force · ZoomInfo API for target revenue research



PERSISTENCE

Cobalt Strike beacons · backdoor admin accounts · scheduled tasks · AnyDesk / ScreenConnect / Splashtop



CREDENTIAL ACCESS

Chrome credential dump across network · Veeam backup DB harvest · Pass-the-hash via Restricted Admin mode



DEFENSE EVASION

WSL + ELF encryptor (bypasses Windows EDR) · BYOVD driver kill (eskle.sys / TPwSav.sys) · AMSI disable via PS



EXFILTRATION

WinSCP · Cyberduck · In-panel 1 PB storage — double extortion leverage before encryption



ENCRYPTION

Single EXE: encrypts, kills VSS, kills processes, spreads via PsExec, hits ESXi via PowerCLI — no second binary needed

THE WSL TRICK

Linux kills Windows EDR

Attackers install or enable WSL on the compromised Windows host

Deploy a Linux ELF binary (ransomware) inside the WSL environment

Most Windows EDR tools only inspect PE binaries — not Linux ELF

Combine with BYOVD: load vulnerable driver to kill any AV that notices

Use WinSCP + Splashtop to transfer and execute the binary remotely

AMSI disabled via obfuscated PowerShell with numeric character encoding

 **Windows Host**
EDR active — watching PE

 **WSL Subsystem**
EDR blind here

 **ELF Ransomware**
executes here

*"This attack challenges
traditional Windows-focused
security controls."
— Trend Micro Research*

DESTROY RECOVERY FIRST

Veeam as a credential warehouse

Qilin operators recognized that backup systems store credentials for every system they back up

1

Identify Veeam Servers

Scan for Veeam backup infra. Known to hold creds for every production system it manages.

3

Domain + Server Creds

Pulls credentials for DCs, remote hosts, critical servers. Now you own everything.

2

PowerShell Harvest

Base64-encoded scripts decode & extract credentials from Veeam databases in memory.

4

Then Deploy Ransomware

Victim has no working backups. No restore path. Maximum extortion leverage.

BACKUP TARGETING: HOW GROUPS COMPARE

From crude VSS deletion → to credential warehouse harvesting

LEVEL 1	Technique / What They Do	Ryuk 2019–21	Conti 2020–22	LockBit 2022–24	BlackCat 2021–24	Akira 2023–	QILIN 2022–
VSS Deletion	Delete Volume Shadow Copies (vssadmin / wmic)	✓	✓	✓	✓	✓	✓ Built-in (same as everyone)
LEVEL 2	Kill backup software processes before encrypt	✗	✓	✓	✓	✓	✓ Hardcoded process kill list
Process / File Kill	Delete / corrupt backup catalog / files	✓	~	~	✓	✓	~ Secondary — not primary goal
LEVEL 3	Actively hunt NAS + network backup shares	✓	✓	~	✓	✓	~ Targets shares but not primary
Backup Infra Hunt	Target ESXi to kill virtual backup hosts	✗	~	✓	✓	✓	✓ ESXi variant; PowerCLI used
LEVEL 4	Extract credentials FROM Veeam config database	✗	✗	✗	✗	✗	★ UNIQUE — systematic, custom tooling
Cred Harvest	Use backup creds for lateral movement	✗	✗	✗	✗	✗	★ UNIQUE — backup = recon pivot
	Harvest WEEKS BEFORE encryption (timing discipline)	✗	✗	✗	✗	~	★ UNIQUE — documented 6+ day gap

✓ Documented

~ Partial/some affiliates

✗ Not documented

★ Qilin unique / primary



CRITICAL INCIDENT: NHS SYNNOVIS — June 2024

London, UK. Synnovis provides pathology services for major NHS hospital trusts. Qilin demanded \$50M. NHS refused. Consequences followed.



5 major NHS trusts + GP practices disrupted — Critical Incidents declared



10,000+ outpatient appointments + 1,700 operations cancelled or delayed



~600 patient safety incidents linked to the attack



2 cases of severe harm — long-term or permanent damage



1 patient death confirmed linked to the attack — King's College Hospital NHS Trust



\$50M ransom demanded. Rejected. 400GB patient data published. £32.7M cost to Synnovis.

This is a patient safety story.

>> WHO ARE THEY? DARK WEB INTEL

Handle

"Haise" on RAMP (joined May 29 2022). "TRAMP" on DutyFree. Multiple liaisons on XSS.

Forums

RAMP seized Jan 2026. Immediately migrated to T1erOne + Rehub. DDoSed XSS when LE took it over.

Branding

WikiLeaksV2 cleamnet site — self-describe as 'political activists'. Broke CIS rule: attacked Ukraine MFA Mar 2025.

Recruitment

English speakers: \$5,000 deposit, refunded after first payout. Unusual — most Russian RaaS reject English-speakers.

Codebase

Code similarities to Black Basta, BlackMatter, REvil — shared dev resources in the Russian underground ecosystem.

INSIDER DRAMA



\$48K AFFILIATE SCAM

'hastalamuerte' filed RAMP arbitration: Haise vanished mid-negotiation with \$48K BTC. Haise won. Power asymmetry in RaaS.



PANEL CREDENTIALS LEAKED

'Nova' posted Qilin affiliate panel credentials + screenshots to humiliate operators. Internal structure exposed to researchers.



DEVMAN — CELEBRITY AFFILIATE

Posted luxury watches + cars on social. Co-branded: 'Pwn3d by Qilin & Devman'. Later tried to steal Qilin's source code.



SCATTERED SPIDER JOINS

Jul 2024: Octo Tempest become Qilin affiliates. Best social engineers + best RaaS platform. Vishing IT helpdesks.

WHAT MAKES QILIN DIFFERENT

Vs. LockBit · RansomHub · Akira · BlackCat

Feature	Qilin	LockBit	RansomHub	Akira
Affiliate revenue split	80–85%	~70%	~90%	~80%
Cross-platform Win/Lin/ESXi	✓ All 3	✓ All 3	✓ All 3	✓ Win/Lin
"Call Lawyer" legal intimidation	✓ UNIQUE	✗	✗	✗
In-panel DDoS (triple extortion)	✓ Apr 2025	✗	✗	✗
In-house journalists / PR team	✓ UNIQUE	✗	✗	✗
PB-scale data storage for affiliates	✓ 1 PB+	✗	✗	✗
Cleartnet + Tor leak sites	✓ Both	Tor only	Tor only	Tor only
Nation-state affiliate (DPRK)	✓ DPRK	✗	Suspected	✗
Cartel / coalition partner	✓ Sep 2025	✓ Sep 2025	Defunct	✗
LOLBIN-only encryptor variant	✓ Observed	Partial	✗	Partial
WikiLeaks-style cleartnet shame site	✓ WikiLeaksV2	✗	✗	✗

★ ONLY Qilin combines legal intimidation + in-house PR + PB storage + DDoS + DPRK affiliate in one platform.

NOTABLE CAMPAIGNS

KR KOREAN LEAKS

September 2025

25 South Korean financial firms hit in one month

Almost all in asset management sector

All compromised via a single compromised MSP

Classic supply chain pivot — one entry, 25 victims

Potential Moonstone Sleet (DPRK) involvement

KP MOONSTONE SLEET

2025 — Microsoft Threat Intelligence

North Korea-linked state actor (APT)

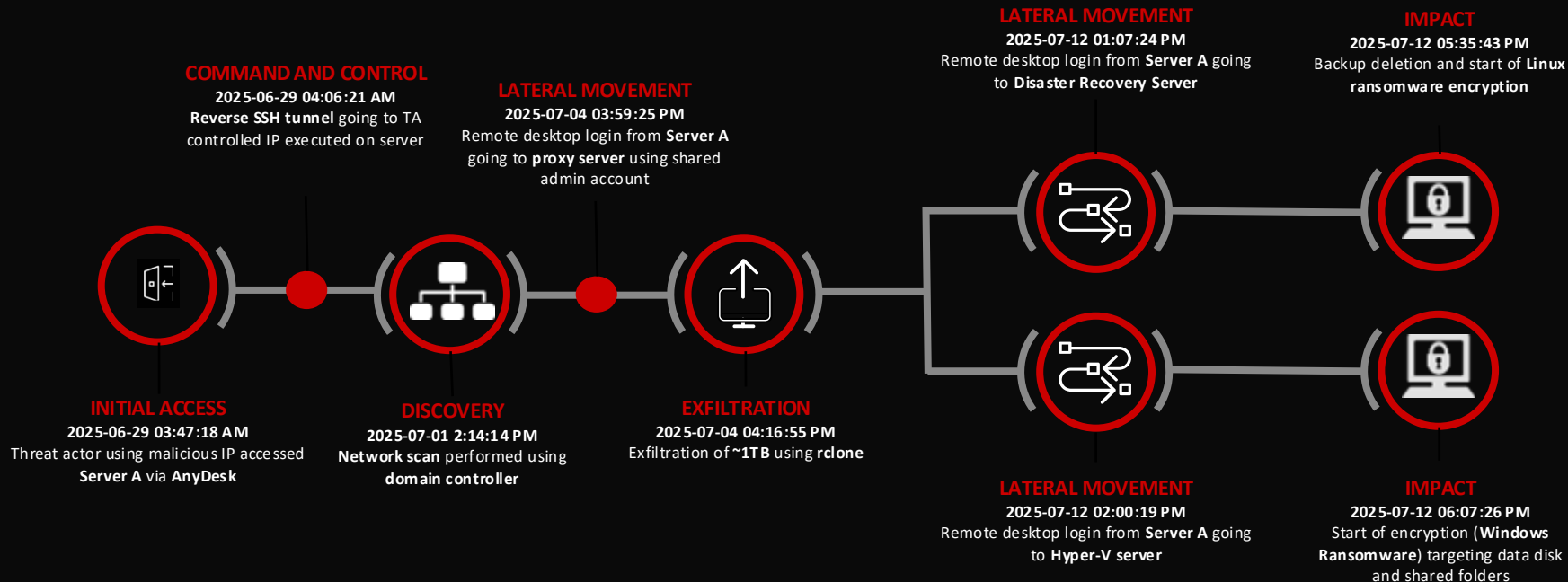
First documented nation-state use of a RaaS operator's own ransomware

Revenue for DPRK weapons programs via cybercrime

Using criminal tooling = plausible deniability on attribution

Crime or espionage?

Attack Timeline



MITRE ATT&CK MAPPING

Initial Access

T1078

Valid Accounts (dark-web creds, VPN)

Defense Evasion

T1562.001

BYOVD — kill security tools

Initial Access

T1566

Phishing / ClickFix fake CAPTCHA

Credential Access

T1003

OS Credential Dumping (Veeam DB)

Execution

T1059.001

PowerShell (base64, AMSI bypass)

Lateral Movement

T1021.001

Remote Desktop Protocol

Persistence

T1053

Scheduled Tasks / Startup Items

Exfiltration

T1048

Exfil over Alt Protocol (WinSCP)

Privilege Esc

T1484.001

Group Policy Mod (enable RDP)

Impact

T1486

Data Encrypted for Impact

Defense Evasion

T1055

WSL ELF execution (bypasses EDR)

WHAT ACTUALLY STOPS THEM



MFA on Everything

VPN, RDP, admin accounts. Most Qilin initial access uses stolen creds against MFA-less services.



Dark Web Cred Monitoring

They check for your leaked creds before you do. Monitor your domains on breach marketplaces.



WSL / Linux Binary Visibility

Ensure EDR covers ELF execution in WSL. Most orgs have zero visibility here right now.



Backup Segmentation + Immutability

Air-gap or immutable backups. Qilin pillages Veeam first — backup creds must be inaccessible from prod.



PowerShell Logging + AMSI

Log all PS execution. Alert on AMSI disable attempts and base64 scripts over 100 chars.



Monitor GPO Changes

Qilin enables RDP via AD GPO. Unexpected GPO modification = high-priority alert.

Remember NHS Synnovis Attack?

*'We see that you are not interested
in the security of your patients.'*



That victim never paid.

Their patient data is on the dark web.

-
- ▶ 500+ victims in 2026 and counting
 - ▶ WSL/EDR bypass is a real gap in most org defenses
 - ▶ They destroy backups first — test your recovery
 - ▶ MFA + cred monitoring stops most initial access
-