Smarttech
YOUR 24/7 SECURITY PARTNER

THREAT ACTOR SPOTLIGHT

Published 4 September 2026
Threat Intelligence Team

QILIN

Russian-speaking ransomware-as-a-service operation running since 2022 under the original name Agenda. Now the most active ransomware group in the world, with over 2,000 published leak-site victims and no arrests, sanctions, or law enforcement action to date.

Agenda | Water Galura (MITRE) | GOLD FEATHER | Windows | Linux | VMware ESXi

RISK RATING	ACTIVE SINCE	MOTIVATION	PRIMARY VECTOR	RANSOMWARE TIES
Critical	2022	Financial extortion	FortiGate/SAP NetWeaver exploits, phishing	RaaS, 80–85% to affiliates

ATTACK CHAIN

1 Initial Access
Exploits FortiGate and SAP NetWeaver vulnerabilities, or harvests credentials via adversary-in-the-middle phishing.

2 Tool Abuse
Rides legitimate RMM tools such as AnyDesk, ScreenConnect, and TeamViewer, plus Cobalt Strike, to blend into normal traffic.

3 Defense Evasion
Uses BYOVD driver loading and WSL-based execution to slip past standard EDR coverage.

4 Lateral Movement
Moves via PsExec, NetExec, and WinRM across Windows, Linux, and VMware ESXi hosts.

5 Double Extortion
Encrypts and exfiltrates data, then applies a "call a lawyer" negotiation tactic that frames ransom demands around regulatory and litigation risk.

MITRE ATT&CK MAPPING

ID	TECHNIQUE
T1190	Exploit public-facing application (FortiOS, Cisco/Erlang SSH)
T1557	Adversary-in-the-middle credential harvesting
T1562.001	Impair defenses (BYOVD, EDR evasion)
T1021	Lateral movement via PsExec, NetExec, WinRM
T1486	Data encrypted for impact (Windows, Linux, ESXi)
T1567	Exfiltration over web service prior to encryption

SECTOR BY SECTOR Summary

Manufacturing

Consistently the most-hit vertical across every major tracker, where downtime pressure speeds up ransom payment.

Healthcare

A recurring target since the group's earliest attacks, headlined by the 2024 Synnovis breach that disrupted NHS pathology services.

Professional & Business Services

Chosen for the client access these firms hold, extending impact well beyond the firm itself.

Smarttech
YOUR 24/7 SECURITY PARTNER

QILIN

ORIGIN & EVOLUTION

Emerged in 2022 as Agenda before rebranding to Qilin later that year. MITRE tracks the operator group as Water Galura (G1050), with Qilin/Agenda logged as the associated software (S1242). Growth accelerated sharply when RansomHub collapsed in April 2025 and its affiliates migrated en masse to Qilin's platform, cementing it as the most active ransomware operation in the world with no law enforcement action against it to date.

THREAT LANDSCAPE CONTEXT

Sits at the center of a lineage that started as Agenda in 2022. Growth exploded when RansomHub collapsed in April 2025 and its affiliates migrated en masse, making Qilin the market's default landing spot for displaced operators from any collapsed platform.

SIGNATURE TRADECRAFT

Initial access comes through exploited FortiGate and SAP NetWeaver appliances or adversary-in-the-middle phishing. Once inside, it rides legitimate remote tools like AnyDesk and TeamViewer alongside Cobalt Strike, then uses BYOVD loading to blind EDR before moving laterally via PsExec, NetExec, and WinRM. Its most distinctive touch is a "call a lawyer" negotiation feature that reframes ransom demands around regulatory and litigation risk.

ANALYST OUTLOOK

With RansomHub's former affiliates absorbed and no law enforcement pressure applied to date, Qilin shows no signs of slowing. Expect it to keep leading monthly leaderboards through 2026, with healthcare and manufacturing remaining primary targets given the operational pressure those sectors face to pay quickly.

NOTABLE INCIDENTS

Synnovis / NHS

June 2024

Encrypted pathology systems at Synnovis, a key NHS partner, disrupting blood testing and forcing hospitals to cancel operations and declare a critical incident. Demanded roughly $50M, one of the most consequential healthcare ransomware attacks on record.

Doctor.com

June 2024

Breached the healthcare scheduling platform via a VPN vulnerability, claiming around 205GB of data stolen.

US ATF

August 2026

Listed the federal Bureau of Alcohol, Tobacco, Firearms and Explosives on its leak site; the agency confirmed an incident the same day, a rare case of a group publicly claiming a US federal law enforcement agency.