

# Weekly Intelligence Summary

Report Date: 07.07.2025

Intelligence Cut-off Date: 04.07.2025

**Weekly Focus: Qilin emerges as the most active ransomware group globally in June 2025 with sector-wide targeting and enhanced RaaS capabilities.**

**The RaaS group claimed responsibility for 86 incidents, outpacing all other ransomware operators by a margin of over 50 victims in June 2025.**

Qilin is a Ransomware-as-a-Service (RaaS) operation active since at least 2022. The group offers a variety of services to its affiliates, including double extortion, legal guidance, encryption tooling and technical support.

After RansomHub went dark in April 2025, Qilin quickly emerged as a leading RaaS operator. The group is known for deploying the NETXLOADER loader and for its advanced cross-platform capabilities, including customisable Go-based binaries and variants targeting Linux and VMware ESXi environments.

In June, Qilin targeted a broad range of sectors, including telecommunications, blockchain infrastructure, healthcare, transportation and logistics, with a particular focus on US-based organisations. The group also targeted more financial entities than other threat actors, further demonstrating its operational reach.

Notable incidents include the breach of Asefa, a subsidiary of France's Société Mutuelle d'Assurance du Bâtiment et des Travaux Publics (SMABTP) that resulted in the exfiltration of over 200 GB of data. Qilin ransomware was also responsible for the compromise of Western New Mexico University and the subsequent disruption of some operations. It was also observed developing a tactic for credential theft in Chrome.

## Why It Matters...

Qilin has emerged to fill the gap left by the collapse of RansomHub. Previously, RansomHub was considered the successor to Knight ransomware, which itself followed Cyclops ransomware. This sequence reflects the ongoing pattern of continuity within the ransomware-as-a-service (RaaS) ecosystem. While Qilin has gained traction in recent months, it remains uncertain whether the group will demonstrate the same persistence, resilience and operational influence previously associated with RansomHub.

Nonetheless, Qilin's rapid ascent highlights the adaptability of ransomware operations, as the dismantling of one group typically leads to the redistribution of resources and tactics among new or existing threat actor collectives. Qilin is expected to continue targeting a broad range of sectors to reinforce its reputation. It is recommended to adopt a zero-trust approach, ensure critical assets are isolated, and maintain close monitoring for signs of compromise.

## Intelligence Overview

### Nation-State

Ongoing conflict with Israel has likely increased Iranian cyber activity targeting US sectors, including energy, defence, healthcare, and food. Charming Kitten and others exploit unpatched systems and OT assets.

Silver Fox group used fake installers of WPS Office and others to deliver Sainbox RAT and a rootkit via DLL sideloading. Sites and installers were in Chinese, likely targeting native speakers.

### Third-Party

A flaw in Brazilian fintech C&M Software enabled access to reserve accounts at the Central Bank. Over USD 180 million was stolen from six banks and laundered via crypto platforms.

The FBI warns that Scattered Spider is using social engineering and MFA abuse to breach the aviation industry. WestJet and Hawaiian Airlines reported disruptions. The group impersonates IT staff to gain access and deploy ransomware.

### Critical Infrastructure

Weak passwords allowed access to Norway's Risevatnet dam OT system, causing uncontrolled water discharge. The breach went undetected for hours and highlights risks from poor security on internet-exposed infrastructure.

### Hacktivist

After US involvement in the Israel-Iran conflict, defence, finance, and manufacturing. Groups like Mr. Hamza and Mysterious Team Bangladesh claimed responsibility. Attacks appear politically motivated and are likely to continue.