ZEROFOX INTELLIGENCE

Flash

Qilin's Latest Spree of Alleged Victims

F-2026-06-08a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Ransomware, Threat Actor

June 8, 2026

Scope Note

ZeroFox Intelligence is derived from a variety of sources, including—but not limited to—curated open-source accesses, vetted social media, proprietary data sources, and direct access to threat actors and groups through covert communication channels. Information relied upon to complete any report cannot always be independently verified. As such, ZeroFox applies rigorous analytic standards and tradecraft in accordance with best practices and includes caveat language and source citations to clearly identify the veracity of our Intelligence reporting and substantiate our assessments and recommendations. All sources used in this particular Intelligence product were identified prior to 11:00 AM (EDT) on June 8, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Qilin's Latest Spree of Alleged Victims

| Key Findings

- Between June 2–5, 2026, ransomware and digital extortion (R&DE) threat actor Qilin claimed 15 new victims across nine countries in 72 hours; its targets spanned the healthcare, hospitality, manufacturing, consumer services, and critical infrastructure sectors.
- Qilin (also known as Agenda) is a sophisticated Russian-language R&DE threat collective that primarily offers ransomware-as-a-service (RaaS) to affiliates and targets high-value critical infrastructure with a double extortion model.
- On June 4, 2026, Qilin posted sensitive data samples allegedly from Avcon Jet—an Austrian-based and major European aviation company offering business jet management and chartered flights internationally—on its dark web leak site.
- ZeroFox assesses that Qilin will very likely conclude Q2 2026 as the most active ransomware collective globally. This would signify both dominance in the first half of 2026 and an unbroken 12-month period as the leading ransomware threat actor, beginning in Q2 2025.

Details

Between June 2–5, 2026, Qilin claimed 15 new victims across nine countries; its targets spanned the healthcare, hospitality, manufacturing, consumer services, and critical infrastructure sectors. The collective added the following organizations to its victim leak site: Avcon Jet, Central Florida Cosmetic & Family Dentistry, Clínica Maitenes, Don Don Group, Eat Salas, InterSPA-Gruppe, Jay's Catering, JNP ENG, MarketJoy, MESIA - Sines, Nova Medical Products, Ontario Home Builders, Pro-MEC Engineering Services, Swim-Mor Pools and Spa, and Trican Well Service.

- The collective's early June attacks all occurred within a 72-hour timeframe but were spread across regions, demonstrating a model in which distributed affiliate networks execute individually sourced intrusions rather than conducting a single coordinated campaign.
- At the time of writing, none of the alleged victims have made statements confirming or denying Qilin's claims. However, Qilin is widely considered to be a credible threat collective, and the victim list on its leak site is almost certainly accurate.

On June 4, 2026, Qilin posted sensitive data samples allegedly from Avcon Jet on its dark web leak site. The exposed data allegedly includes Avcon Jet's employee passports and resumes, aircraft maintenance work orders, export airworthiness certificates, training records, and cyber incident response plan.

- Employees whose passports and other sensitive information were exposed are very likely to be targets for social engineering attacks by an array of actors.
- In addition, if the sample data includes Avcon Jet's legitimate cyber incident response plan, threat actors are very likely to leverage it in subsequent attacks against the company, as it likely contains information to facilitate bypassing or exploiting Avcon Jet's defenses. It will also likely provide actors insight into the company's future response strategies.

Qilin's Avcon Jet post on its dark web leak site
Source: ZeroFox Intelligence
[Analyst Note: The images were redacted due to privacy concerns.]

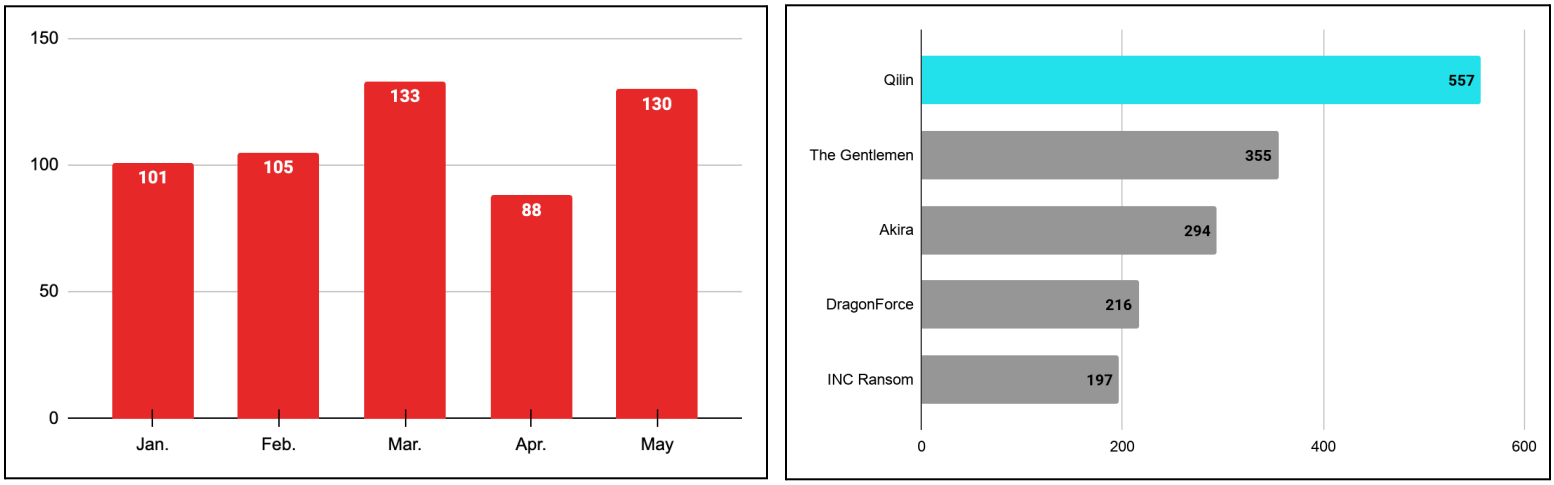
Due to the combination of U.S. Food and Drug Administration (FDA) regulatory submissions and HIPAA-protected patient information, Nova Medical Products is likely among the most vulnerable victims in this latest round of attacks. Qilin likely views healthcare entities as high-priority targets due to the immense legal and regulatory consequences such organizations are very likely to face following a breach. MESIA - Sines is also likely a high-value target, given its proximity to the Port of Sines in Portugal and its role as a strategic European energy hub.

Date	Victim	Country	Sector
June 2	Avcon Jet	Austria	Aviation
June 2	Clínica Maitenes	Chile	Healthcare
June 2	Nova Medical Products	United States	Healthcare
June 3	Eat Salad	Brazil	Food & Agriculture
June 3	JNP ENG	South Korea	Manufacturing
June 3	MarketJoy	United States	Consumer Services
June 3	MESIA - Sines	Spain	Energy
June 4	Don Don Group	Slovenia	Manufacturing
June 4	Trican Well Service	Canada	Energy
June 5	Central Florida Cosmetic & Family Dentistry	United States	Healthcare
June 5	Jay's Catering	United States	Hospitality
June 5	Pro-MEC Engineering Services	United States	Manufacturing
June 5	InterSPA-Gruppe	Germany	Professional Services
June 5	Ontario Home Builders	Canada	Construction
June 5	Swim-Mor Pools and Spa	United States	Construction

Qilin's alleged victims between June 2–5, 2026
Source: ZeroFox Intelligence

Qilin is a sophisticated Russian-language R&DE threat collective that primarily offers RaaS to its affiliates network and targets high-value critical infrastructure with its double extortion model.

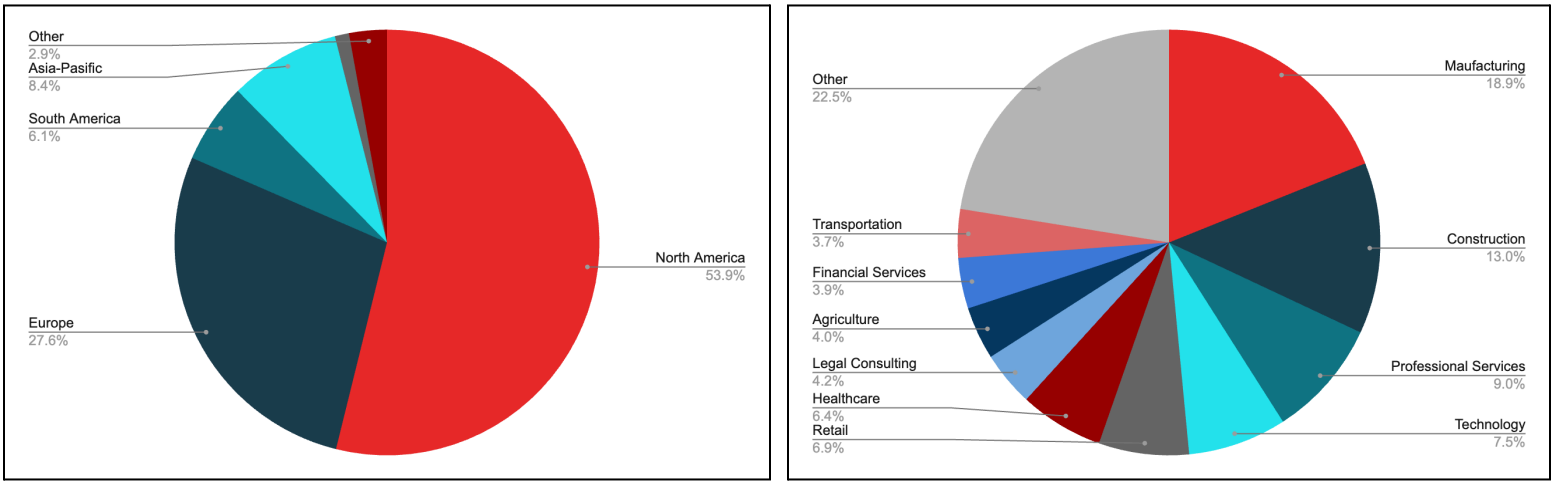
- Qilin has remained the first most active R&DE collective since Q2 2025, signifying nearly an entire year of outpacing any other collective. Since its launch in 2022, ZeroFox has observed the collective conduct at least 1,761 separate R&DE attacks.
- Between January and May 2026, Qilin was responsible for at least 557 separate incidents; notably, the collective claimed 56.9 percent more victims than the next most active collective.



Qilin R&DE incidents per month (left) and the top five most active collectives (right) January - May 2026

Source: ZeroFox Intelligence

So far in 2026, Qilin has continued to disproportionately target organizations in the North America region, which represents 53.9 percent of the collective's victims. Manufacturing, construction, professional services, technology, and retail were the top five most targeted sectors by the collective, together comprising 55.3 percent of Qilin's victims.



Qilin's most targeted regions (left) and industries (right) January–May 2026

Source: ZeroFox Intelligence

ZeroFox assesses that Qilin will very likely conclude Q2 2026 as the most active ransomware collective globally, signalling both its dominance in the first half of 2026 and an unbroken 12-month period as the leading ransomware threat actor, beginning in Q2 2025. The collective is very likely to continue or exceed its current operational tempo, outpacing other collectives by a substantial margin, and will likely remain consistent with its established tactics, techniques, and procedures (TTPs), targeting geographically dispersed, multi-sector entities with double-extortion operations.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- Configure email servers to block emails with malicious indicators, and deploy authentication protocols to prevent spoofed emails.
- Proactively monitor for compromised accounts and credentials being brokered in deep and dark web (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated TTPs.

Appendix A: Traffic Light Protocol for Information Dissemination

	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** TLP:RED when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** TLP:AMBER when information requires support to be effectively acted upon but carries risks to privacy, reputation, or operations if shared outside of the organizations involved.
HOW MAY IT BE SHARED?	**Recipients may NOT share** TLP:RED with any parties outside of the specific exchange, meeting, or conversation in which it is originally disclosed.	**Recipients may ONLY share** TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm. **Note that** TLP:AMBER+STRICT restricts sharing to the organization only.

	Green	Clear
WHEN SHOULD IT BE USED?	**Sources may use** TLP:GREEN when information is useful for the awareness of all participating organizations, as well as with peers within the broader community or sector.	**Sources may use** TLP:CLEAR when information carries minimal or no risk of misuse in accordance with applicable rules and procedures for public release.
HOW MAY IT BE SHARED?	**Recipients may share** TLP:GREEN information with peers and partner organizations within their sector or community but not via publicly accessible channels.	**Recipients may share** TLP:CLEAR information without restriction, subject to copyright controls.

Appendix B: ZeroFox Intelligence Probability Scale

All ZeroFox intelligence products leverage probabilistic assessment language in analytic judgments. Qualitative statements used in these judgments refer to associated probability ranges, which state the likelihood of occurrence of an event or development. Ranges are used to avoid a false impression of accuracy. This scale is a standard that aligns with how readers should interpret such terms.

Almost No Chance	Very Unlikely	Unlikely	Roughly Even Chance	Likely	Very Likely	Almost Certain
1-5%	5-20%	20-45%	45-55%	55-80%	80-95%	95-99%