ZEROFOX INTELLIGENCE

Flash

Qilin Claims Record Number of Monthly Attacks for 2026

F-2026-09-09b

Classification: TLP:CLEAR

Criticality: Moderate

Intelligence Requirements: Ransomware, Threat Actor, Dark Web

September 9, 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 10:00 AM (EDT) on September 9, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Qilin Claims Record Number of Monthly Attacks for 2026

| Key Findings

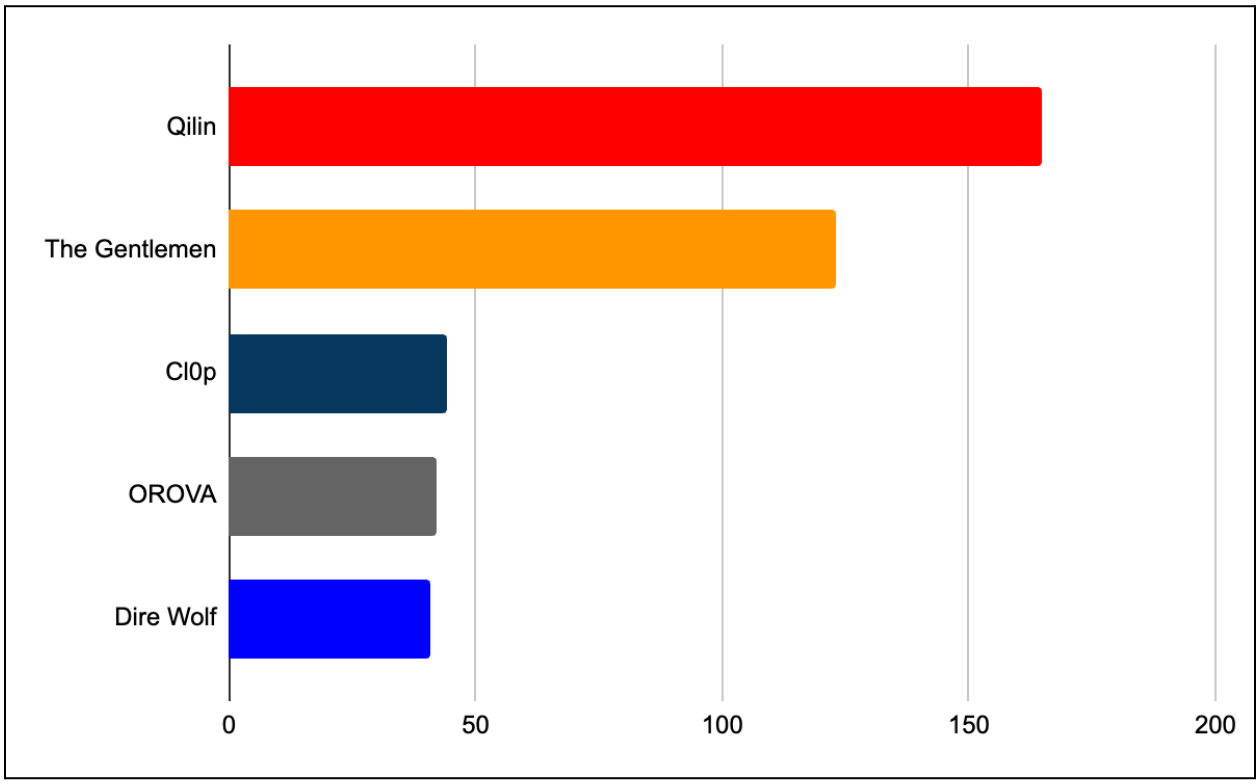
- ZeroFox observed that Qilin was the most prominent ransomware and digital extortion (R&DE) collective in August 2026, accounting for at least 165 incidents—a record number of incidents for one collective so far this year.
- Qilin has remained the most active R&DE collective globally, signaling both its dominance thus far into 2026 and an unbroken 17-month period as the leading ransomware threat actor since Q2 2025.
- Qilin accounted for a nearly 29 percent share of the top 10 most active collectives, which together were responsible for at least 6,453 incidents since April 2025 (Q2 2025). The next most active collective, Akira, had a share of approximately 14 percent, underpinning Qilin's continuous prominence.
- 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)

and continue to target geographically dispersed, multi-sector entities with double-extortion operations.

Details

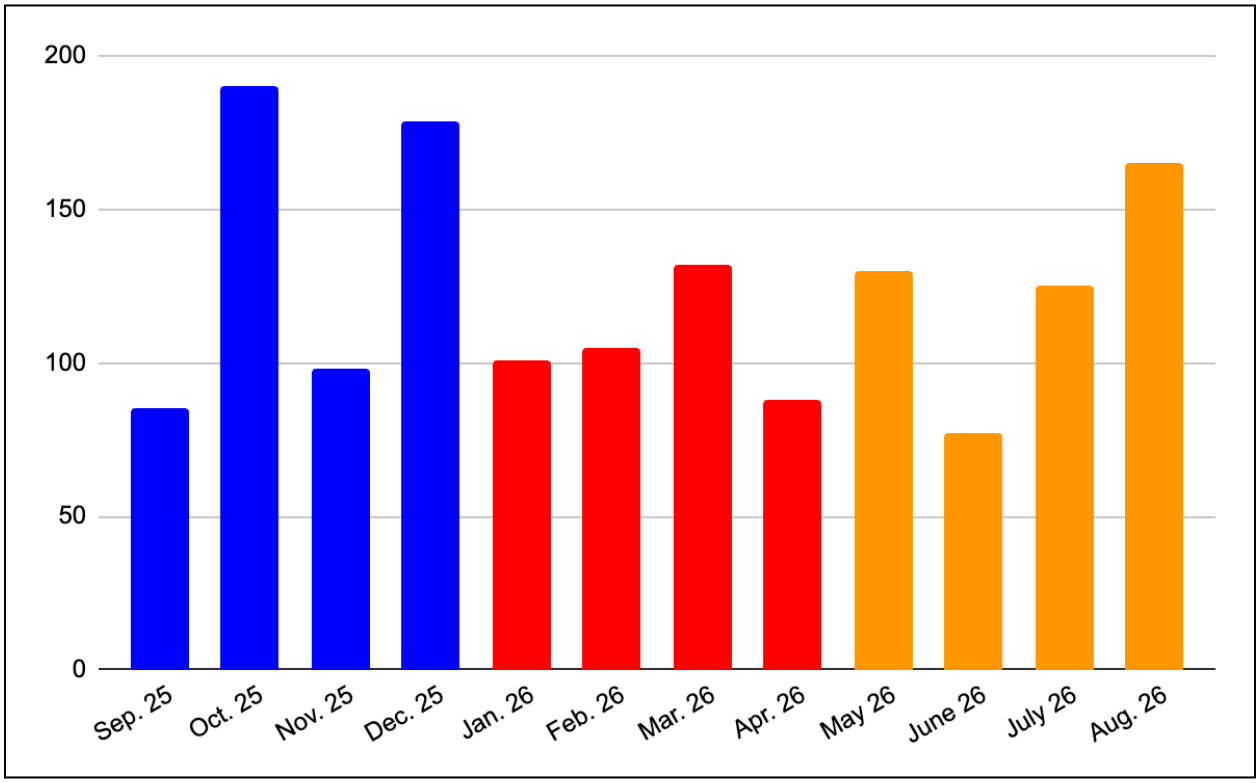
ZeroFox observed that Qilin was the most prominent R&DE collective in August 2026, accounting for at least 165 incidents—a record number of incidents for one collective so far this year.

- This count was surpassed only in October 2025 (190 incidents) and December 2025 (179 incidents), both claimed by Qilin.
- Between September 1, 2025, and August 31, 2026, Qilin claimed at least 1,480 incidents; the second highest number of attacks was 767 by The Gentlemen, demonstrating that Qilin has been the most prominent collective over this 12-month period by a substantial margin.



Top five most prominent R&DE collectives in August 2026
Source: ZeroFox Intelligence

Qilin is a financially motivated R&DE collective operating a ransomware-as-a-service (RaaS) model. The group first emerged in July 2022 under the name "Agenda" before rebranding to its current identity. Qilin operates a dedicated dark web data leak site (DLS) that is regularly updated with the names and associated details of alleged targeted entities. Descriptions on the site provide background information on the targets and potential motives for selection; the content and level of detail vary across posts.



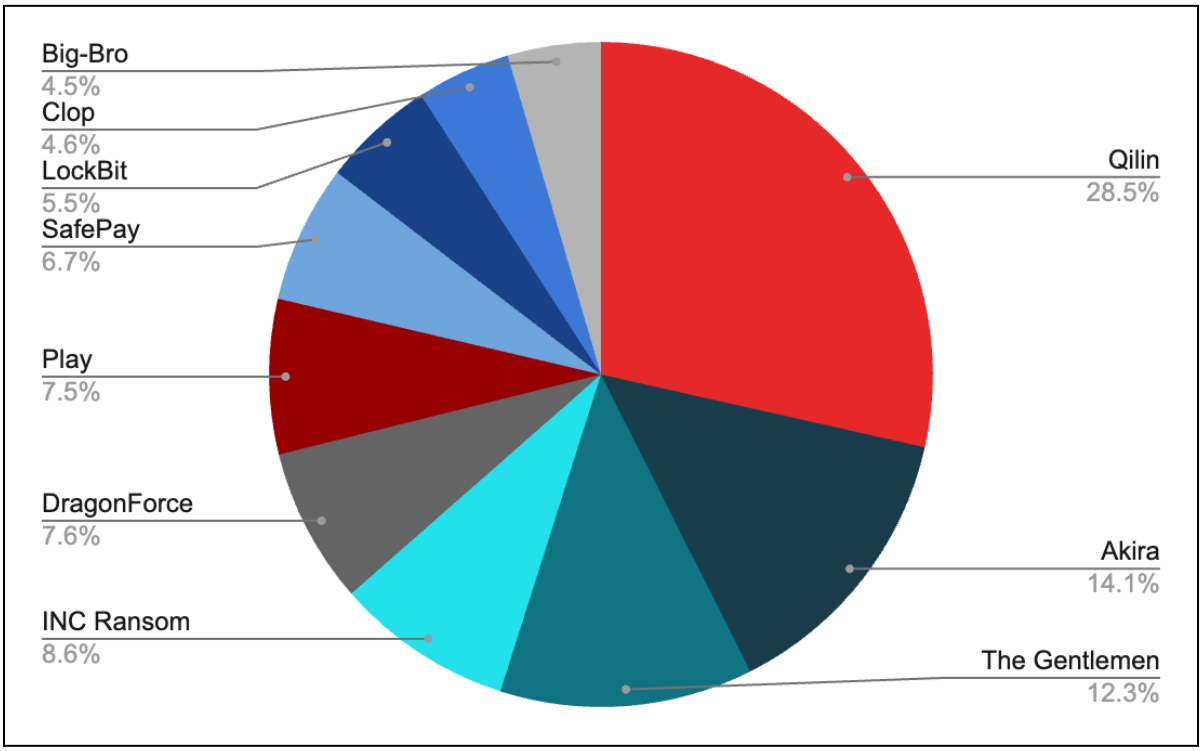
Qilin R&DE incidents by month
Source: ZeroFox Intelligence

Qilin has remained the most active R&DE collective globally, signaling both its dominance thus far into 2026 and an unbroken 17-month period as the leading ransomware threat actor since Q2 2025. Since Q2 2025, Qilin has conducted at least 1,835 separate R&DE attacks, significantly outpacing any other collective by nearly double; in the same time period, the next most leading actor, Akira, has conducted at least 905 attacks.

- Qilin accounted for a nearly 29 percent share of the top 10 most active collectives, which together were responsible for at least 6,453 incidents since April 2025 (Q2

2025). The next most active collective, Akira, has a share of approximately 14 percent, underpinning Qilin's continuous prominence.

- Qilin disproportionately targets organizations in the North American region. Manufacturing, construction, professional services, retail, and healthcare are the collective's top five most targeted sectors.



Top 10 most active R&DE collectives since April 2025 (Q2 2025)
Source: ZeroFox Intelligence

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 TTPs and continue to target geographically dispersed, multi-sector entities with double-extortion operations. Qilin is likely to remain the most active collective, surpassing its own precedents each month.

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%