ZEROFOX INTELLIGENCE

Flash

Rumored New Coalition of Ransomware Groups Yet to Materialize

F-2025-10-10a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Deep and Dark Web, Ransomware, Threat Actor

October 10, 2025

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 7:00 AM (EDT) on October 10, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Rumored New Coalition of Ransomware Groups Yet to Materialize

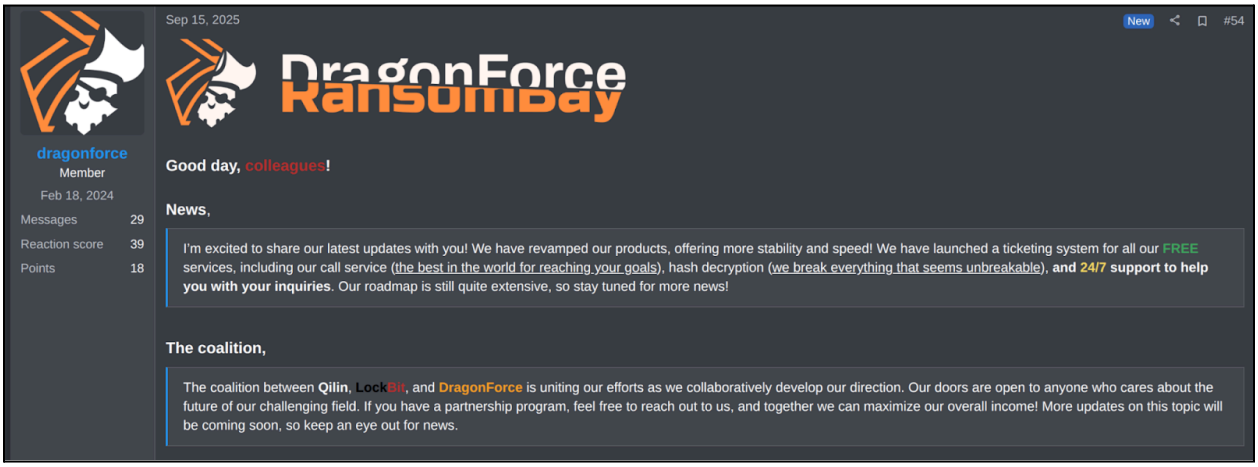
| Key Findings

- On September 15, 2025, an account associated with the ransomware and digital extortion (R&DE) collective DragonForce posted on the dark web forum Russian Anonymous Marketplace (RAMP), announcing a coalition with Qilin and LockBit, two other prominent ransomware-as-a-service (RaaS) collectives.
- In the post, DragonForce explained that the coalition is about uniting efforts as they collaboratively develop their direction—likely meaning that the collectives will assist each other in enhancing their products and services to better serve their affiliates and maximize profits, while also evading law enforcement (LE).
- Notably, ZeroFox has not observed either Qilin or LockBit publicly confirming or denying the alleged coalition. However, both Qilin and LockBit are known to post only rarely on RAMP.
- It is unlikely that DragonForce's announcement of a coalition with LockBit and Qilin represents a formalized amalgamation of the three collectives.

Details

On September 15, 2025, an account associated with the R&DE collective DragonForce posted on the dark web forum RAMP, announcing a coalition with Qilin and LockBit, two other prominent RaaS collectives. Additionally, the group announced new updates to its current service offerings, including a ticketing system and a 24/7 support to help users with their enquiries.

- DragonForce began operations in December 2023 and has conducted an average of 10 attacks per month, disproportionately impacting North America, which accounts for approximately 59 percent of all incidents. Meanwhile, manufacturing and professional services were the industries most targeted, with each accounting for approximately 17 percent of all incidents.



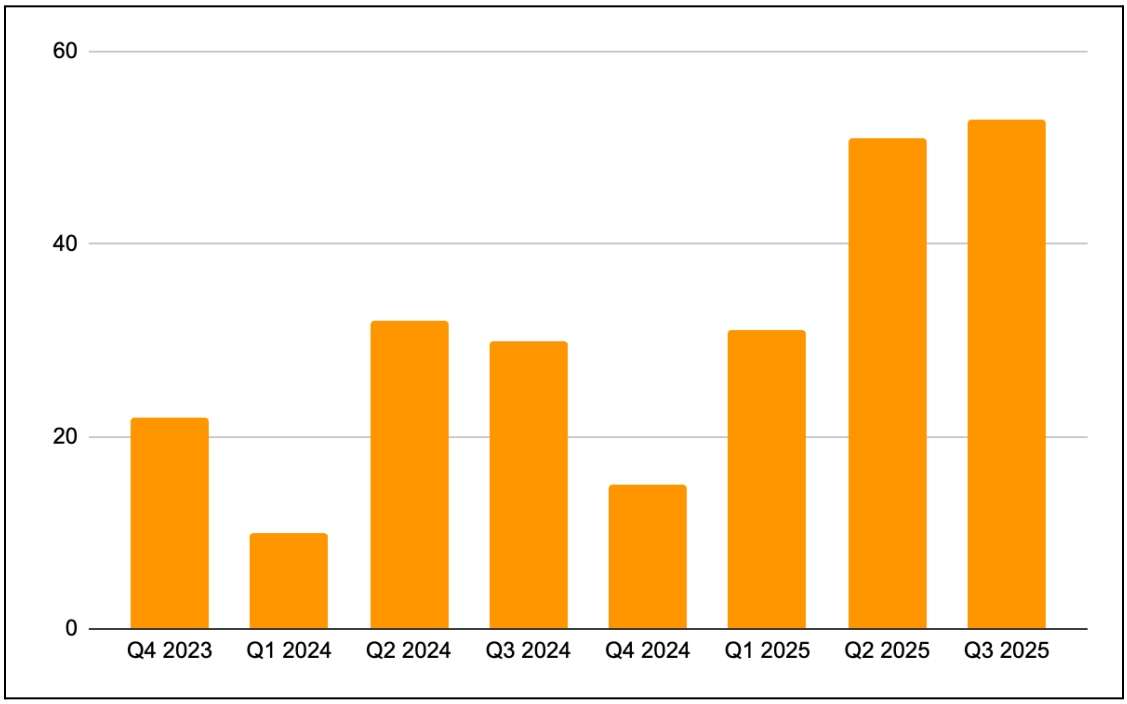
DragonForce's RAMP post

Source: ZeroFox Intelligence

- In the post, DragonForce explained that the coalition is about uniting efforts as they collaboratively develop their direction—likely meaning that the collectives will assist each other in enhancing their products and services to better serve their affiliates and maximize profits, while also evading LE. DragonForce also stated that it was open to working with any actors in the RaaS field and welcomed interested parties to contact the group.

ZeroFox notes that neither Qilin nor LockBit have publicly confirmed or denied the alleged coalition. However, both Qilin and LockBit are known to post only rarely on RAMP.

- Around April 4, 2025, following the apparent cessation of RansomHub, a DragonForce account posted on RAMP, claiming that RansomHub "will be up soon" and that the collective had decided to move to DragonForce's infrastructure. This statement was also posted to the DragonForce[.]onion victim leak page.
- In a separate post, DragonForce urged RansomHub to consider its offer, without providing any further detail. ZeroFox has not observed any evidence to suggest that RansomHub has, in fact, moved to DragonForce's infrastructure.

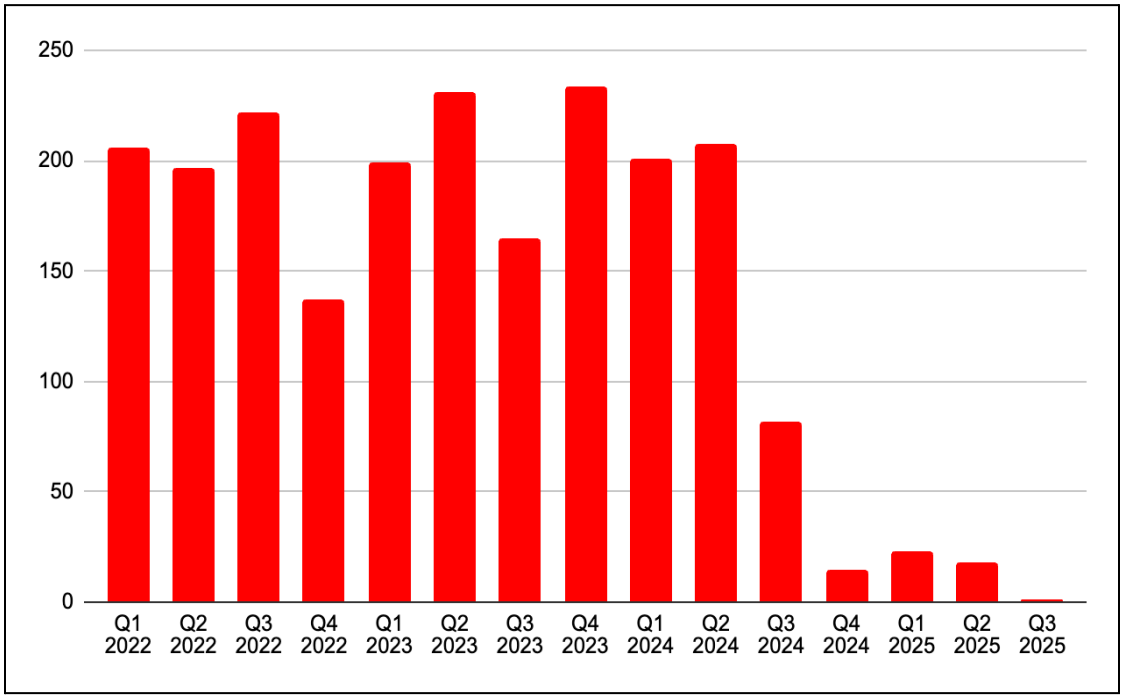


DragonForce's R&DE incidents by quarter

Source: ZeroFox Intelligence

LockBit is a RaaS collective that has almost certainly struggled to garner the reputation necessary to attract and retain affiliates since a disruption by LE entities in February 2024. Prior to this, LockBit was among the most prominent ransomware collectives, having conducted more attacks during 2022 and 2023 than any other outfit. LockBit has continued to conduct attacks throughout 2024 and 2025, though at a much lower tempo. So far in 2025, the collective has accounted for approximately 1 percent of global ransomware attacks—which roughly equates to 42 separate incidents.

- In mid-September 2025, LockBit released its latest ransomware strain “LockBit 5.0”, which coincides with the alleged coalition announcement by DragonForce.
- LockBit is almost certainly seeking to regain credibility and market share in the ransomware space after its significant decrease in output starting in Q3 2024.



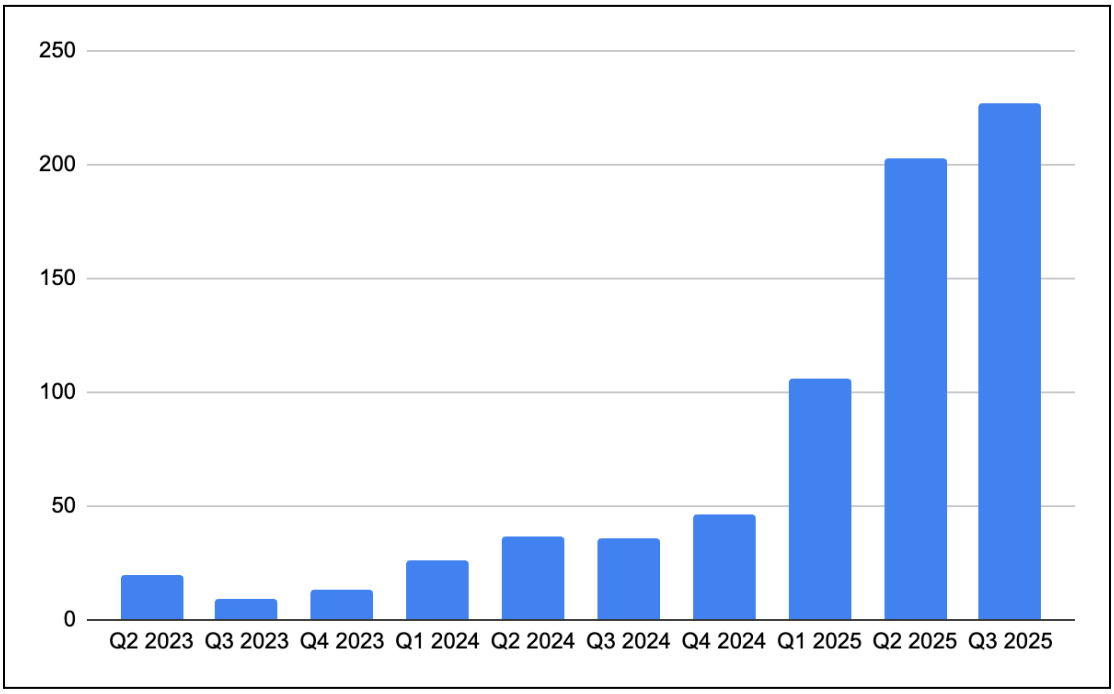
LockBit’s R&DE incidents by quarter

Source: ZeroFox Intelligence

Qilin is a Russian-language RaaS collective first observed by ZeroFox in July 2022. The collective has continuously increased ransomware attacks over the past two years. In 2023, the collective conducted at least 42 separate attacks (1.04 percent of all attacks); in 2024, the collective sharply increased the number of attacks to at least 145 separate incidents (nearly 3 percent of all attacks). So far in October, Qilin has exponentially increased its attack tempo, with at least 561 separate incidents in all of 2025 (a nearly 287 percent increase from 2024); the number of attacks will almost certainly exceed 600 by the end of the year.

- Notably, Qilin was the fifth most prominent R&DE collective in Q1 2025, with approximately 106 incidents; the group demonstrated nearly twice as many

incidents and became the first most prominent collective in Q2 2025, which continued into Q3 2025.



Qilin's R&DE incidents by quarter

Source: ZeroFox Intelligence

It is unlikely that DragonForce's announcement of a coalition with LockBit and Qilin represents a formalized amalgamation of the three collectives. It is likely that DragonForce, Qilin, and LockBit are in contact with each other and will assist one another in their campaigns and future projects. However, this more likely represents a friendly professional relationship rather than the unification of their resources and objectives. Lastly, it is likely that DragonForce is using this announcement as a means to promote its own brand by association with other prominent collectives, similar to what it likely did with RansomHub earlier in the year.

| 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%