



| Flash |

Speculation Unfolds Surrounding RansomHub Cessation

F-2025-04-09a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Ransomware, Threat Actor, Dark Web

April 9, 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 08:30 AM (EDT) on April 9, 2025**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Speculation Unfolds Surrounding RansomHub Cessation

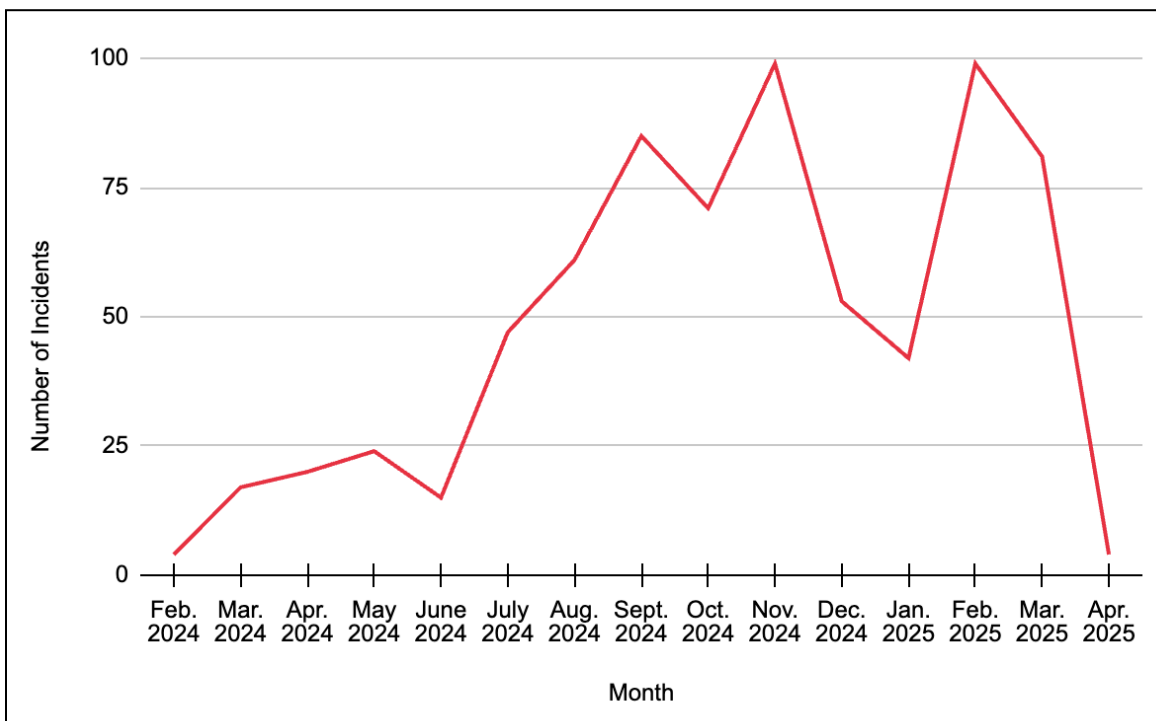
| Key Findings

- Ransomware and digital extortion (R&DE) collective RansomHub's dark web victim leak site has been offline since April 1, 2025, and no new victims have been observed.
- Around April 4, an account associated with the DragonForce R&DE collective posted on the Russian-speaking deep and dark web (DDW) forum RAMP, claiming that RansomHub "will be up soon" and that RansomHub had decided to move to DragonForce's infrastructure.
- As of the writing of this report, RansomHub is very likely non-operational, posing a significantly reduced threat to global organizations across industries. There is a likely chance that RansomHub will remain non-operational during the coming weeks.
- Should RansomHub's operations recommence, the collective will very likely suffer from significant reputational damage, regardless of whether original RansomHub or DragonForce infrastructure is leveraged.

Details

RansomHub's victim leak site has been offline since April 1, 2025, and no new victims have been observed. The ransomware-as-a-service (RaaS) group had been conducting an average of approximately 20 attacks per week throughout Q1 2025, with February 2025 seeing more incidents than any other month.

- RansomHub was first observed by ZeroFox in approximately February 2024 and quickly established a notable attack tempo, which increased throughout the year. By the end of 2024, RansomHub was responsible for approximately 10 percent of all global R&DE incidents.
- The collective's initial efficacy has been attributed to a number of factors, such as a highly competitive affiliate payout rate of 85–90 percent and the attracting of affiliates from other recently defunct R&DE collectives.

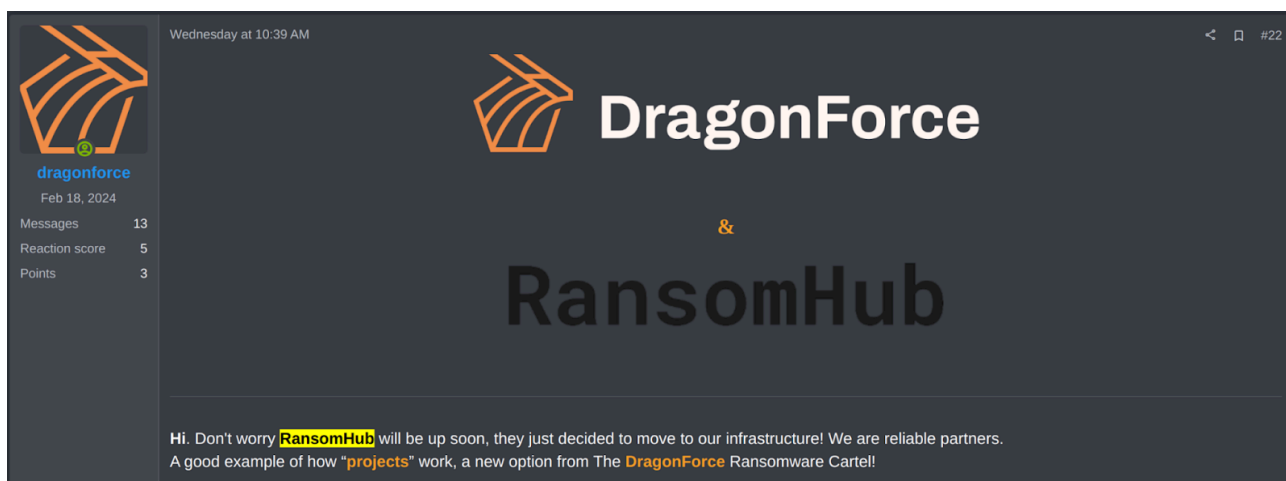


RansomHub attacks by month

Source: ZeroFox Intelligence

In the past week, ZeroFox has observed significant chatter taking place in DDW forums related to connections between RansomHub and another prominent R&DE collective, DragonForce. Around April 4, a DragonForce account posted in the Russian-speaking DDW forum 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 their offer”, without providing any detail.

- ZeroFox first observed DragonForce in approximately December 2023. Since then, the collective has conducted an average of nine attacks per month, which have disproportionately impacted the North American region and the manufacturing industry.

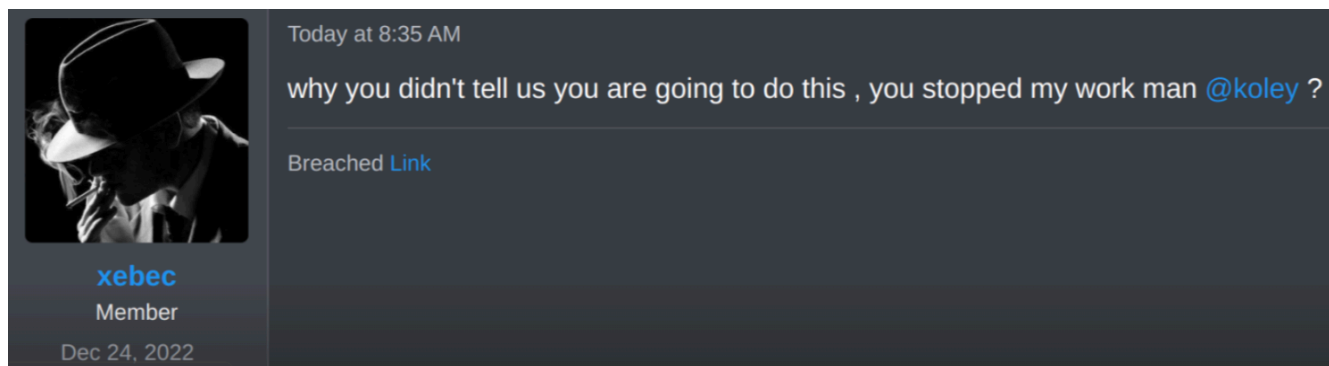


RAMP post by DragonForce

Source: ZeroFox Intelligence

In response to DragonForce’s posts, several threat actors expressed confusion surrounding RansomHub’s current and future operational capacity, speculating about the situation. Others levied dissatisfaction toward DragonForce, suggesting that the collective had defaced RansomHub’s digital infrastructure. Parallels were drawn with DragonForce’s alleged targeting of the Mamona (previously BlackLock) collective earlier in 2025.

- Unusual activity has also been observed from the actor “Koley”, who is widely recognized within DDW forums as the face of the RansomHub collective. Despite historically posting regularly in the RAMP forum, Koley has been inactive since April 1, 2025.



RAMP post alluding to lack of communication from RansomHub

Source: ZeroFox Intelligence

Some actors have warned that RansomHub affiliates will soon be subjected to exit scam-type activity, drawing parallels between the collective’s silence and that observed from ALPHV prior to their cessation of operations and the prominent April 2024 breach of Change Healthcare. Others suggested that RansomHub has been disrupted by Western law enforcement (LE) entities or has received information suggesting that LE scrutiny is imminent.

A post by the actor “Rjun” speculated that RansomHub had been targeted by Russian LE entities following the collective’s targeting of victims based within the Commonwealth of Independent States (CIS).

- The targeting of CIS countries, which include Russia and Belarus, is both forbidden by many RaaS collectives and against the norms which underpin much of the Russian-speaking DDW threat landscape. ZeroFox observed similar speculation within a Russian media article.¹

As of the writing of this report, RansomHub is very likely non-operational, posing a significantly reduced threat to global organizations across industries. It is currently

¹ [hxxps://mayday\[.\]rocks/ransomhub-hakerskaya-opg/](https://hxxps://mayday[.]rocks/ransomhub-hakerskaya-opg/)

unclear whether RansomHub has initiated a collaboration with DragonForce, the extent to which resources would be shared, and what this would mean for the future threat posed by both DragonForce and RansomHub. ZeroFox has observed no evidence that control of RansomHub infrastructure has been transferred or that RansomHub affiliates are associating with DragonForce.

There is a likely chance that RansomHub will remain non-operational during the coming weeks. Should operations recommence, the collective will very likely suffer from significant reputational damage, regardless of whether original RansomHub or DragonForce infrastructure is leveraged. Reaching pre-disruption levels of credibility has often proven difficult for even the most prominent RaaS outfits in recent years; such disruptions often mark the beginning of a collective's decline.

| Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are updated with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity posture based upon a principle of least privilege, and implement network segmentation to separate resources by sensitivity and/or function.
- Implement phishing-resistant multi factor authentication (MFA), secure and complex password policies, and ensure the use of unique and non-repeated credentials.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud-based servers at least once per year—and ideally more frequently.
- 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 DDW forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (TTPs).
- Utilize ZeroFox Intelligence and our proprietary platform to understand potential exposure in stealer logs.

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%