



| Flash |

RansomHub Extortion Attacks on Sharp Upward Trajectory

F-2024-08-21a

Classification: TLP:CLEAR

Criticality: High

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

August 21, 2024

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 9:00 AM (EDT) on August 21, 2024**; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | RansomHub Extortion Activity on Sharp Upward Trajectory

› Key Findings

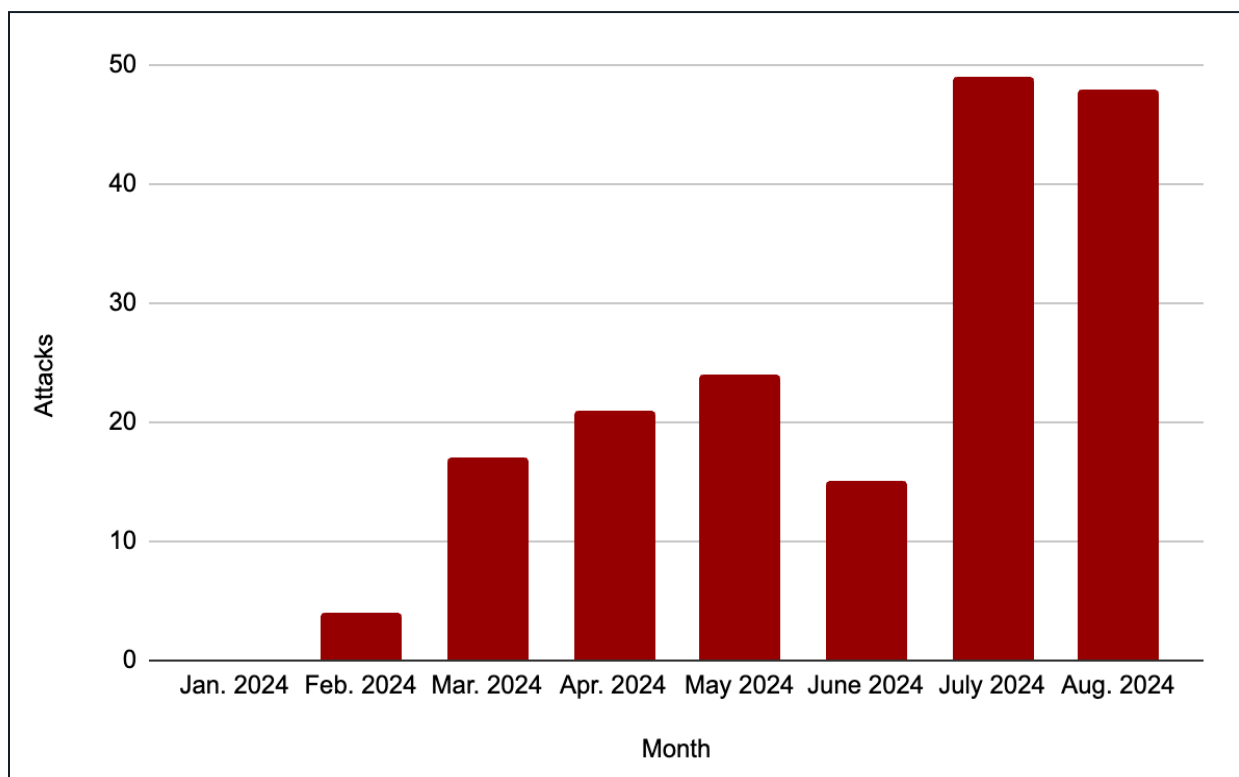
- The ransomware-as-a-service (RaaS) operation “RansomHub” has almost certainly significantly increased its operational tempo in recent weeks, having conducted more attacks so far in Q3 2024 than in Q1 and Q2 2024 combined.
- RansomHub’s activity as a proportion of all ransomware activity observed by ZeroFox is also on a sharp upward trajectory, with the group accounting for approximately 2 percent of all attacks in Q1, 5.1 percent in Q2, and 14.2 percent so far in Q3.
- There is a likely chance that RansomHub will remain the most prominent ransomware collective for the coming months and continue to attract affiliates.
- The collective will almost certainly continue to target a highly diverse array of sectors, and the proportion of attacks targeting organizations located in North America will very likely increase.

| Details

The RansomHub RaaS operation has almost certainly significantly increased its operational tempo in recent weeks, having conducted more attacks so far in Q3 2024

than in Q1 and Q2 2024 combined, and August 2024 is set to be the group's most active month by a substantial margin.

- RansomHub was first observed in approximately February 2024 and exhibited a higher tempo of attacks during those initial weeks than is usually observed from new ransomware operations.
- Due to reported overlaps in the payloads leveraged, RansomHub has been widely speculated to have links to the now-defunct ransomware group "Knight," which was active primarily between September 2023 and February 2024.



RansomHub attacks by month

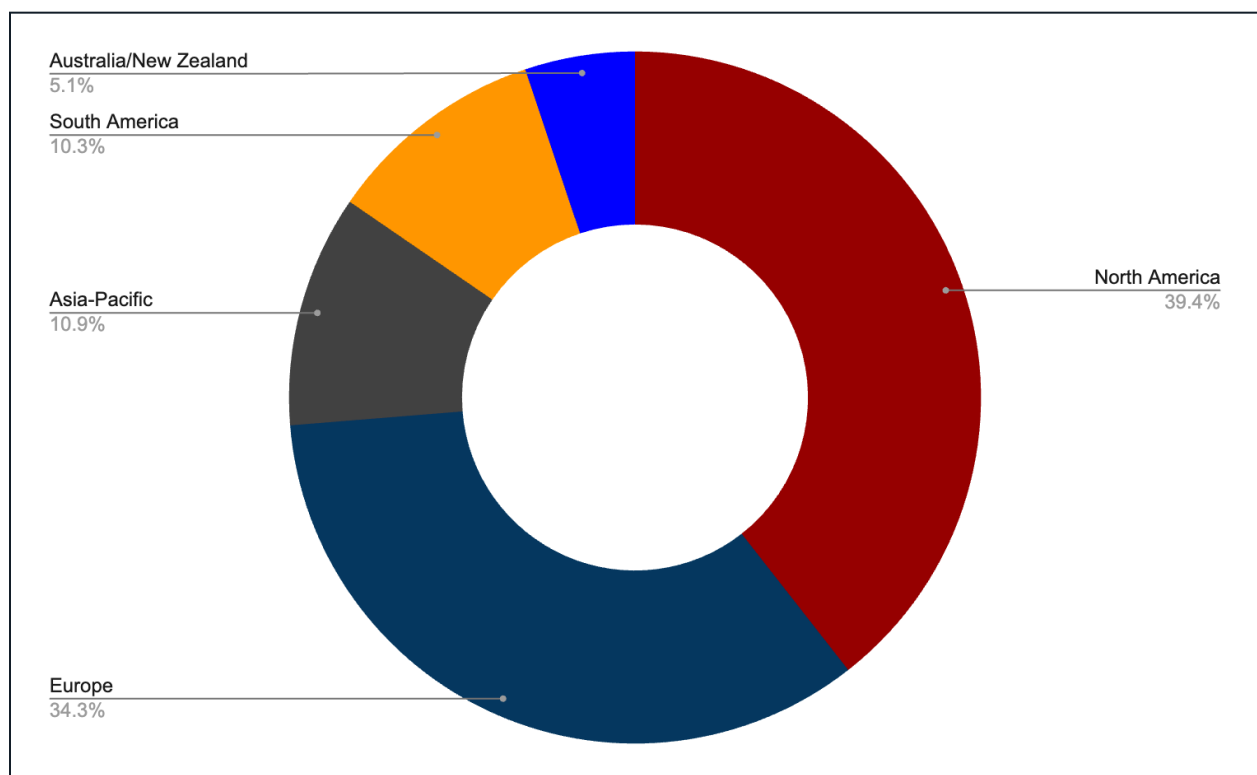
Source: ZeroFox Intelligence

RansomHub activity has been steadily increasing each month since February 2024, with at least 48 attacks observed so far in August. Its activity as a proportion of all ransomware activity observed by ZeroFox is also on a sharp upward trajectory, with the group accounting for approximately 2 percent of all attacks in Q1, 5.1 percent in Q2, and 14.2 percent so far in Q3—higher than any other ransomware collective.

- This upward trajectory is in spite of a slight overall reduction of attacks observed by ZeroFox across the ransomware landscape since May 2024.

During 2024, RansomHub's targeting of some regions across the globe has consistently been disproportionately higher than that observed across the broader ransomware threat landscape, particularly in the collective's initial months.

- Approximately 11 percent of RansomHub attacks have targeted organizations in the Asia-Pacific region, compared to 6 percent across the threat landscape.
- Approximately 10 percent of RansomHub attacks have targeted organizations in South America, compared to 4 percent across the threat landscape.
- Approximately 34 percent of RansomHub attacks have targeted organizations in Europe, compared to 25 percent across the threat landscape.



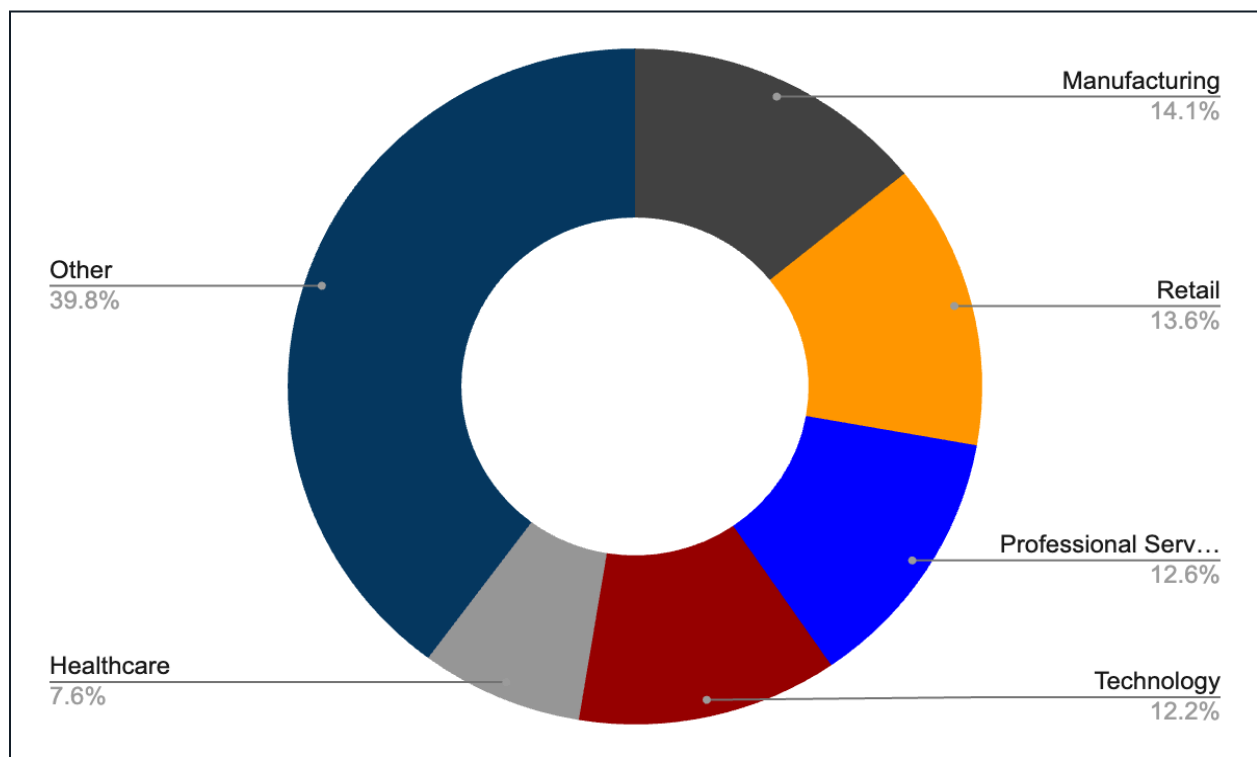
RansomHub attacks by region

Source: ZeroFox Intelligence

North America organizations have been disproportionately under-targeted by RansomHub, comprising approximately 39 percent of the collective's activity compared

to 57 percent across the threat landscape. This trend is very likely shifting, however, as North American organizations have been making up an increasing proportion of RansomHub attacks since the collective was first observed in February 2024, reaching approximately 45 percent so far in Q3 2024. This shift is very likely reflective of the collective obtaining affiliates that are experienced in seeking and exploiting targets deemed highly lucrative, many of which are in the United States.

RansomHub targets organizations from a diverse array of sectors. However, throughout 2024, the vast majority of sectors observed by ZeroFox have been under-targeted in comparison to the broader threat landscape. This is very likely due primarily to the dispersion of resources across a vast array of sectors, suggesting that the collective operates a diverse host of affiliates that seek lucrative targets relatively indiscriminately. In Q3 2024, slight increases have been observed in RansomHub's targeting of the healthcare and technology sectors. While this has reached disproportionate levels, attacks targeting these sectors are also increasing across the broader threat landscape.



RansomHub attacks by industry

Source: ZeroFox Intelligence

RansomHub's success, continued growth, and highly-competitive 90 percent affiliate payout rate are almost certainly continuing to attract highly competent affiliates from other ransomware collectives and driving the development of new tactics, techniques, and procedures (TTPs).

- In April 2024, Change Healthcare was added to RansomHub's victim leak site—despite the prominent breach having been claimed by the now-defunct, prominent ransomware collective "ALPHV."
- In recent weeks, the threat collective "Scattered Spider" has reportedly been observed leveraging RansomHub ransomware, suggesting affiliation between the groups.¹
- RansomHub was reportedly recently observed leveraging a new malicious tool in its attacks designed to terminate endpoint detection and response processes before they can respond to the intrusion.²

Contact

You can contact the main system administrator on the contacts below, waiting for an answer can take some time from 1 minute to several days depending on the workload.

With questions about decryption to write only in a chat on the site, if the person who encrypted your network does not answer you more than two days or you have any other problems, you can contact me.

Please don't say just hello in chat. If you feel it's a bit brusque to simply say "Hi" and ask the question, you can still preface your message with as many pleasantries as you see fit. It may seem trivial, but asking your question before getting that initial salutatory reply also allows for asynchronous communication. If the other party is away, and you leave before they come back, they can still answer your question, instead of just staring at a "Hello" and wondering what they missed. When done right - everyone's happy! 🌸

Join our alliance advantage?

We only share 10%, and the alliance can take 90% of the payment.

With your wallet address for receipt, we do not limit the payment method. Pay you at first, then pay 10% to us.

RansomHub affiliate notice

Source: ZeroFox Intelligence

There is a likely chance that RansomHub will remain the most prominent ransomware collective for the coming months and continue to attract affiliates. The collective will almost certainly continue to target a highly diverse array of sectors, and the proportion of attacks targeting organizations located in North America will very likely increase.

¹ [hXXps://www.darkreading\[.\]com/endpoint-security/ransomhub-rolls-out-brand-new-edr-killing-byovd-binary](https://www.darkreading.com/endpoint-security/ransomhub-rolls-out-brand-new-edr-killing-byovd-binary)

² [hXXps://news.sophos\[.\]com/en-us/2024/08/14/edr-kill-shifter/](https://news.sophos.com/en-us/2024/08/14/edr-kill-shifter/)

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 deep and dark web forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated 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%