ZEROFOX INTELLIGENCE

Flash

Threat Collective Touts Red Hat Breach

F-2025-10-02a

Classification: TLP:CLEAR

Criticality: MEDIUM

Intelligence Requirements: Data Breach, Threat Actor

October 2, 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 2, 2025; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Threat Collective Touts Red Hat Breach

| Key Findings

- On October 1, 2025, the threat collective known as "Crimson Collective" claimed via their Telegram channel to have breached Red Hat's private GitHub repositories, allegedly stealing around 570 GB of data from nearly 28,000 internal repositories and approximately 800 Consulting Engagement Reports (CERs).
- Crimson Collective is an extortion threat collective that created their Telegram channel on September 24, 2025, amassing 393 subscribers as of the writing of this report.
- Crimson Collective posted screenshots of an alleged attempt to contact Red Hat regarding the incident, along with a file named *git[.]tar[.]gz* they assert represents only half of the total breached data—which they likely intend to release once the files have been compressed.
- Exposure of internal repositories will very likely reveal proprietary code and security controls across Red Hat's products and services, which would almost certainly enable threat actors to identify further exploitable weaknesses.

Details

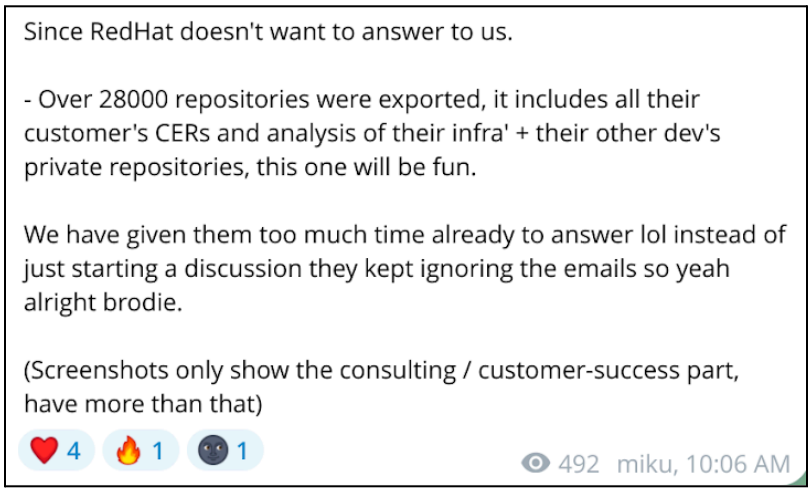
On October 1, 2025, the threat collective known as Crimson Collective claimed via their Telegram channel to have breached Red Hat's private GitHub repositories, allegedly stealing around 570 GB of data from nearly 28,000 internal repositories and approximately 800 CERs. Red Hat subsequently confirmed that a security incident had taken place related to its consulting business but did not confirm the claims made by Crimson Collective.[1] ZeroFox also cannot independently validate the claims made by the collective.

- CERs are formal documents that summarize the activities, findings, recommendations, and outcomes of a consulting project or engagement between a consultant or consulting firm and a client. CERs are likely of interest to threat actors, as they typically contain a host of personally identifiable information (PII) such as full names, email addresses, and phone numbers—all of which are highly sought after data used to conduct various social engineering campaigns.

- Exposure of internal repositories will very likely reveal proprietary code and security controls across Red Hat's products and services, which would almost certainly enable threat actors to identify further exploitable weaknesses.

- Red Hat is a U.S.-based software company that provides open-source software solutions to enterprises. In 2019, Red Hat was acquired by IBM for approximately USD 34 billion—the largest software acquisition at the time.[2]

[1] hXXps://www.bleepingcomputer[.]com/news/security/red-hat-confirms-security-incident-after-hackers-claim-github-breach/
[2] hXXps://www.redhat[.]com/en/about/company

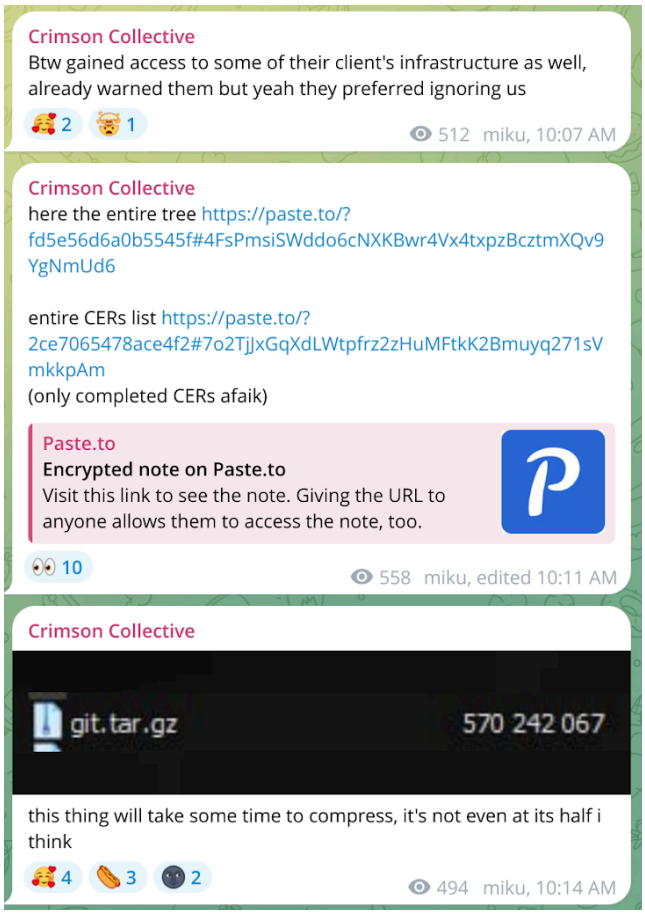


Crimson Collective touts alleged Red Hat data on its Telegram channel

Source: hXXps://t[.]me/thecrimsoncollective

Crimson Collective shared two links allegedly containing Red Hat client CERs and a Git directory listing with names of various companies, likely to validate their claims. Crimson Collective also posted screenshots of an alleged attempt to contact Red Hat regarding the incident, along with a file named *git[.]tar[.]gz* that they assert represents only half of the total breached data—which they likely intend to release once the files have been compressed.

- Crimson Collective is an extortion threat collective that created its Telegram channel on September 24, 2025, amassing 393 subscribers as of the writing of this report.
- On the same day, Crimson Collective also announced that they had defaced Nintendo, which was likely an attempt to promote their brand.



Crimson Collective's Telegram Posts

Source: hXXps://t[.]me/thecrimsoncollective

It is very likely that Crimson Collective will continue to post further alleged data leaks and samples on its Telegram channel to further validate their claims and help establish themselves as a prominent threat collective. Given their high-profile attacks since inception, it is almost certain that Crimson Collective will conduct similar-style attacks in the coming weeks to capitalize on the momentum they have already gained.

- There is a likely chance that Crimson Collective will seek to exploit the data allegedly stolen from Red Hat to further exploit vulnerabilities in its software or in downstream environments where Red Hat's products are already deployed.

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 multifactor 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 (DDW) forums.
- Leverage cyber threat intelligence to inform the detection of relevant cyber threats and associated tactics, techniques, and procedures (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%