ZEROFOX INTELLIGENCE

Flash

Everest Continues to Tout Prominent Brands in Latest Disclosures

F-2026-02-06a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Dark Web, Threat Actor

February 6, 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 9:00 AM (EST) on February 6, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | Everest Continues to Tout Prominent Brands in Latest Disclosures

| Key Findings

- On February 2, 2026, a ransomware and digital extortion (R&DE) collective known as "Everest" announced an alleged data breach of Iron Mountain on its victim leak site. ZeroFox assesses Everest has very likely overstated the volume and sensitivity of the breach in order to increase pressure on the victim to comply with its extortion demands.

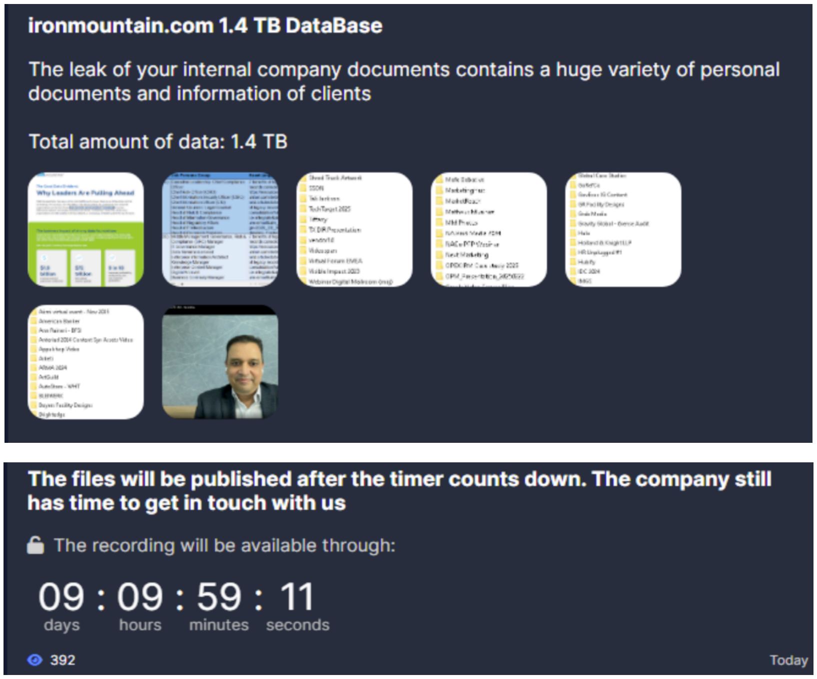
- Everest is a Russian-language collective offering ransomware-as-a-service (RaaS) that has conducted at least 286 separate R&DE incidents since ZeroFox first observed the group in 2021. In light of sensitive reporting, ZeroFox assesses Everest has likely exaggerated the quantity and quality of its alleged victim data—and in some cases fabricated it entirely.

- Everest is the tenth most prominent R&DE collective thus far in 2026 in terms of number of published alleged victims; the group has primarily targeted North America-based entities and organizations in the healthcare sector. However, given Everest's historical tendency to overstate its exfiltrations, ZeroFox assesses it is unlikely their latest claims regarding the Iron Mountain breach are credible.

Details

On February 2, 2026, R&DE collective Everest published an alleged data breach of Iron Mountain, a U.S.-based data storage and recovery services company, on its victim leak site. ZeroFox assesses that Everest has very likely overstated the volume and sensitivity of this alleged breach in an attempt to increase pressure on Iron Mountain to comply with its extortion demands.

- Everest announced the data breach on its victim leak site, claiming to have exfiltrated 1.4 terabytes of internal personal documents and information on the company's clients.
- Despite the collective's claims, Iron Mountain's press release regarding a "cybersecurity issue" stated that only one folder with marketing materials was accessed via compromised login credentials.[1]



ironmountain.com 1.4 TB DataBase

The leak of your internal company documents contains a huge variety of personal documents and information of clients

Total amount of data: 1.4 TB

The files will be published after the timer counts down. The company still has time to get in touch with us

The recording will be available through:

09 : 09 : 59 : 11
days hours minutes seconds

392 Today

Everest's post of Iron Mountain data on its victim leak site

Source: ZeroFox Intelligence

[1] hXXps://www.ironmountain[.]com/about-us/media-center/press-releases/2026/february/iron-mountain-statement-cybersecurity-issue

Everest is a Russian-language collective offering RaaS that has conducted at least 286 separate R&DE incidents since ZeroFox first observed the group in 2021. In light of sensitive reporting, ZeroFox assesses that Everest has historically likely exaggerated the quantity and quality of its alleged victim data—and in some cases fabricated it entirely. The group is known for its hybrid RaaS model incorporating ransomware and initial access broker (IAB) services with insider recruitment programs.[2] According to U.S. Health Sector Cybersecurity Coordination Center (HC3) security researchers, Everest is linked to the "EverBe 2.0" ransomware family and the Russia-based ransomware group known as "BlackByte".[3]

Date	Entitiy	Region	Industry
Feb. 2, 2026	Polycom (Poly-HP Inc.)	U.S.-based	Technology
Feb. 2, 2026	Hsokawa Micron Corporation	Japan-based	Technology
Feb. 2, 2026	Shinwa Co.	Japan-based	Manufacturing
Jan. 20, 2026	McDonald's	U.S.-based, India division	Retail
Dec. 26, 2025	Chrysler	U.S.-based	Manufacturing
Dec. 3, 2025	ASUS	Taiwan-based	Technology

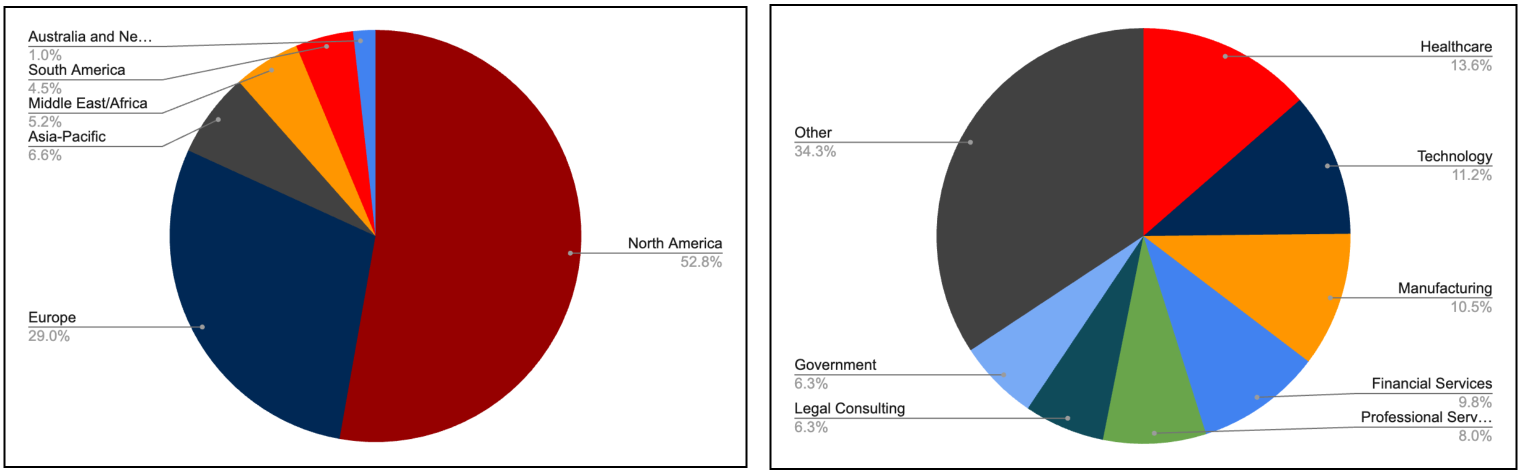
Recent alleged prominent victims Everest added to its leak site

ZeroFox Intelligence

Since February 2021, Everest has disproportionately targeted North-America based organizations, which represent nearly 53 percent of the collective's victims. Everest's targeting is largely consistent with regional trends collective-wide. Notably, Everest's industry-based targeting is predominantly focused on the healthcare sector, followed by technology, manufacturing, and financial services. Everest's attack tempo has increased so far this calendar year, making the collective the tenth most prominent R&DE collective year-to-date (YTD); the group has claimed responsibility for at least 25 separate R&DE incidents so far in 2026.

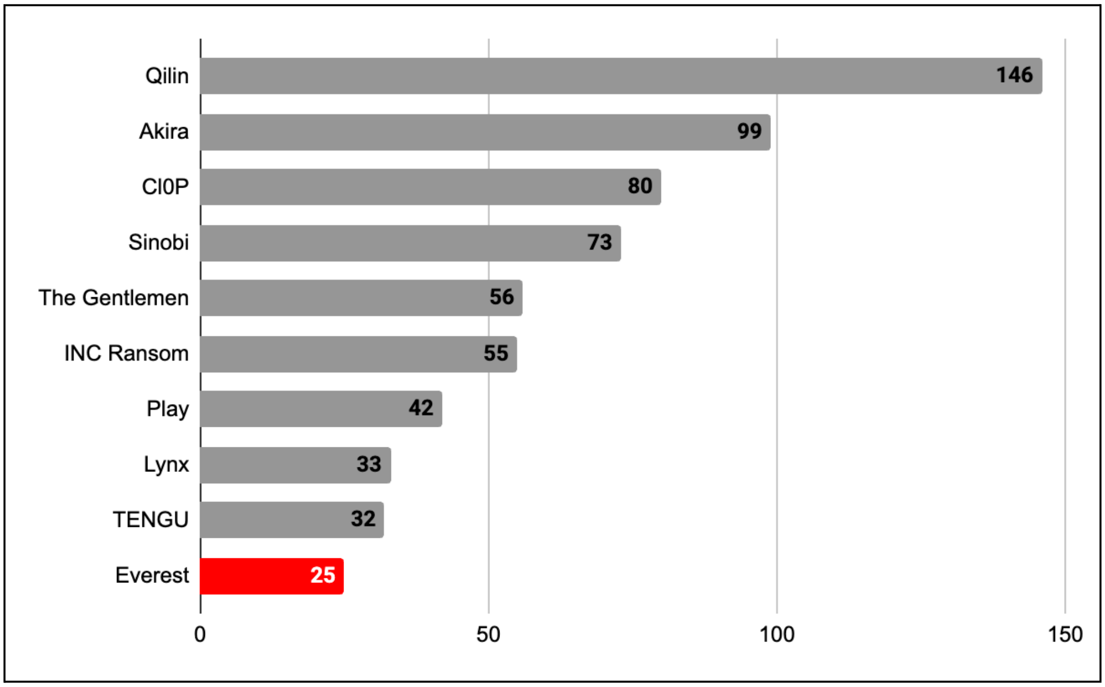
[2] hXXps://www.halcyon[.]ai/threat-group/everest#introduction

[3] hXXps://www.hipaajournal[.]com/wp-content/uploads/2024/08/hhs-hc3-everest-ransomware-group-threat-profile-aug-2024.pdf



Everest's most targeted regions (left) and industries (right) 2021–2026

Source: ZeroFox Intelligence



2026 YTD Top 10 most prominent R&DE collectives

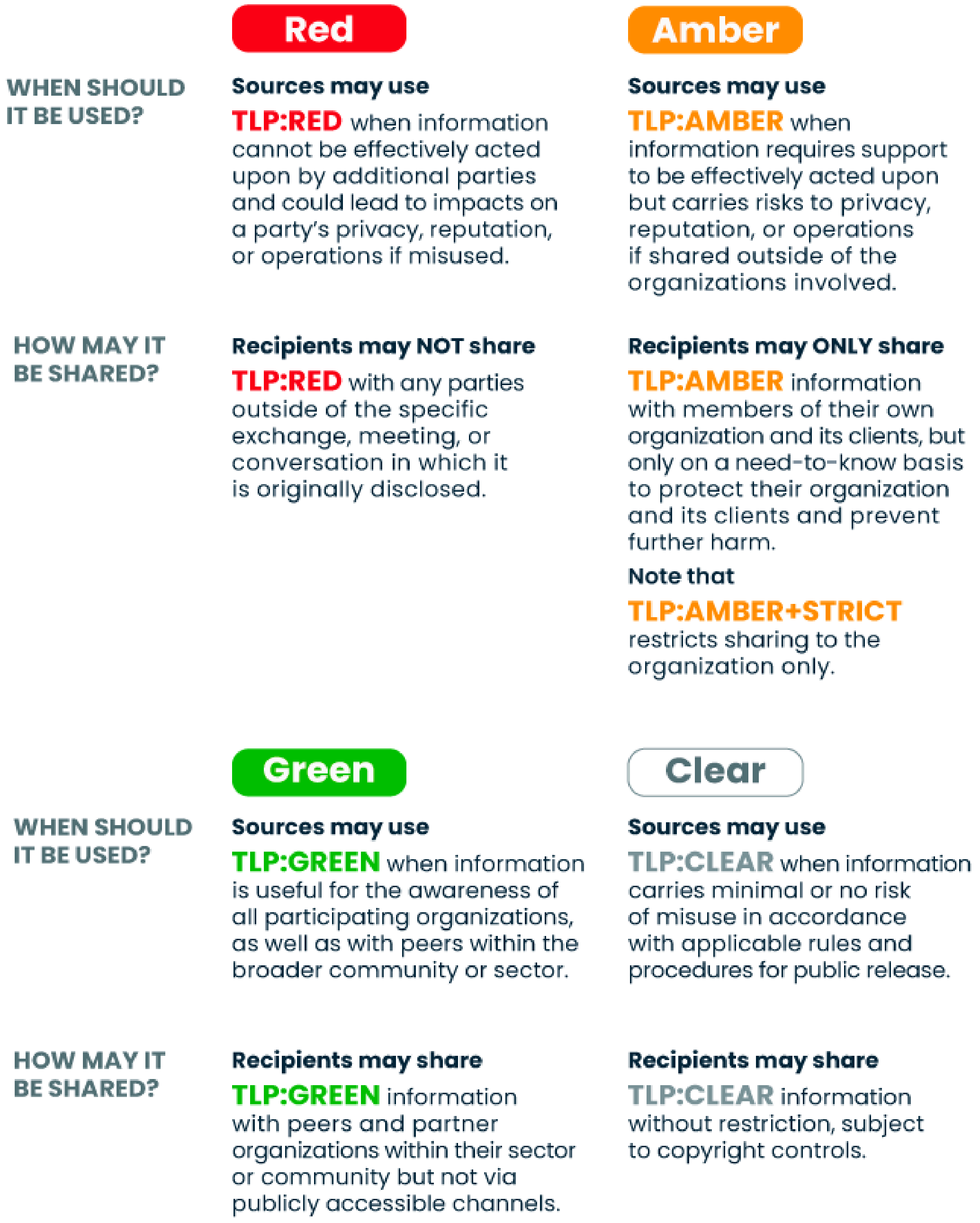
Source: ZeroFox Intelligence

Given Everest's historical tendency to overstate its exfiltrations, ZeroFox assesses it is unlikely their latest claims regarding the Iron Mountain breach are credible and very likely that the collective will continue to exaggerate their claims—especially until their other alleged victims disclose the severity of the incidents. Since a majority of Everest's leak site announcements do not offer distinct indicators of compromise, there is a roughly even chance the collective's attacks are either ransomware-based or merely extortion attempts.

Recommendations

- Develop a comprehensive incident response strategy.
- Deploy a holistic patch management process, and ensure all IT assets are patched with the latest software updates as quickly as possible.
- Adopt a Zero-Trust cybersecurity architecture based upon a principle of least privilege.
- Implement network segmentation to separate resources by sensitivity and/or function.
- Ensure critical, proprietary, or sensitive data is always backed up to secure, off-site, or cloud servers at least once per year—and ideally more frequently.
- Implement secure password policies, phishing-resistant multi-factor authentication (MFA), and unique credentials.
- 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

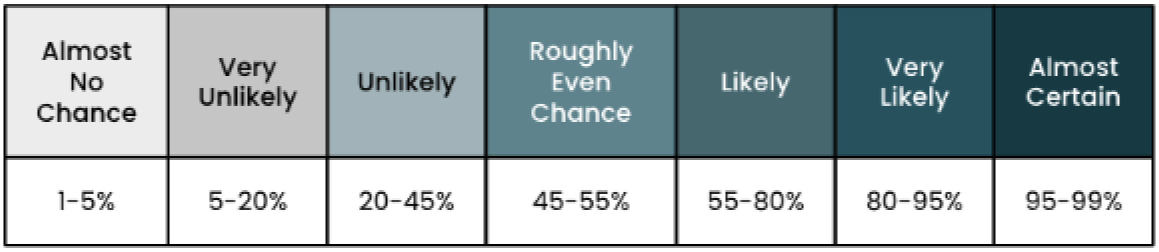


	Red	Amber
WHEN SHOULD IT BE USED?	**Sources may use** **TLP:RED** when information cannot be effectively acted upon by additional parties and could lead to impacts on a party's privacy, reputation, or operations if misused.	**Sources may use** **TLP:AMBER** when information requires support to be effectively 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%