ZEROFOX INTELLIGENCE

Flash

North Korean Threat Actor Revealed as Medusa Affiliate

F-2026-02-27a

Classification: TLP:CLEAR

Criticality: LOW

Intelligence Requirements: Malware, Threat Actor, Geopolitics

February 27, 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 7:00 AM (EST) on February 26, 2026; per cyber hygiene best practices, caution is advised when clicking on any third-party links.

| Flash | North Korean Threat Actor Revealed as Medusa Affiliate

| Key Findings

- On February 24, 2026, North Korean threat actor "Lazarus Group" reportedly widely deployed Medusa ransomware in a series of attempted attacks against healthcare organizations. These attacks indicate that state-sponsored threat actors are almost certainly using cybercrime infrastructure to generate revenue for the North Korean government.
- By combining with Medusa, Lazarus Group has likely gained access to an established ransomware infrastructure with which to conduct financially motivated attacks. However, Medusa is an independent threat actor, and not all Medusa ransomware-as-as-service (RaaS) attacks should be attributed to Lazarus Group.
- Lazarus Group's deployment of Medusa RaaS likely indicates the collective is seeking to improve the operational security of its financially motivated attacks by concealing its activities behind the established brand of the Medusa RaaS operation.
- Given the group's history of conducting state-sponsored attacks that advance North Korean government objectives, it is very likely their financially motivated

operations are intended to generate revenue for the communist regime in Pyongyang.

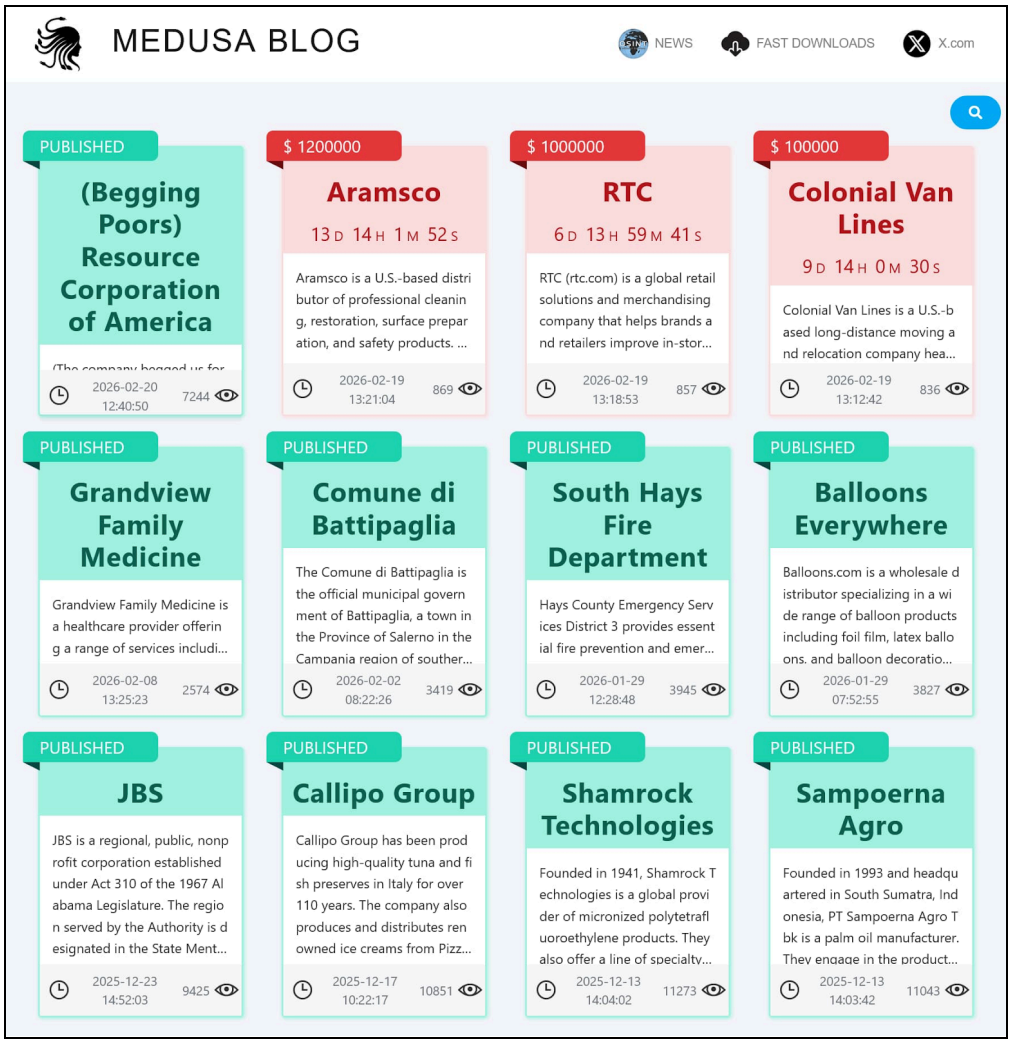
Details

On February 24, 2026, North Korean threat actor Lazarus Group reportedly widely deployed Medusa ransomware in a series of attempted attacks against healthcare organizations in the United States—and likely successfully attacked healthcare entities in the Middle East. These attacks indicate that state-sponsored threat actors are almost certainly using cybercrime infrastructure to generate revenue for the North Korean government.

- Lazarus Group is a North Korean state-sponsored threat actor that has conducted several high-profile attacks that were very likely both financially lucrative and in support of advancing Pyongyang's foreign policy objectives. Most notably, Lazarus Group was likely responsible for the 2014 Sony Pictures breach and the 2017 WannaCry ransomware campaign.
- In the past, Lazarus Group has used other RaaS platforms for its financially motivated attacks, including Holy Ghost, PLAY, Maui, and Qilin.[1]

By combining with Medusa, Lazarus Group has likely gained access to an established ransomware infrastructure with which to conduct financially motivated attacks. However, Medusa is an independent threat actor, and not all Medusa RaaS attacks should be attributed to Lazarus Group.

[1] hXXps://www.bleepingcomputer[.]com/news/security/north-korean-lazarus-group-linked-to-medusa-ransomware-attacks/

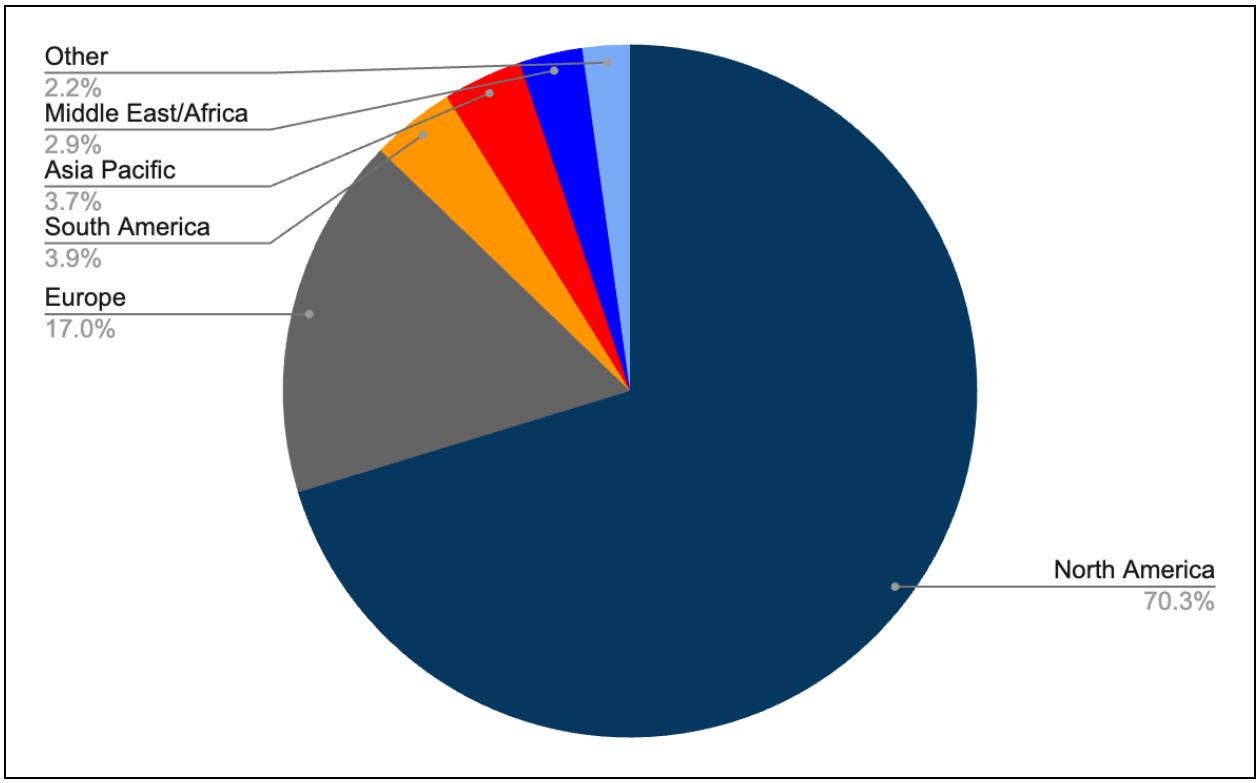


Medusa's blog listing of alleged victims

Source: ZeroFox Intelligence

The latest Lazarus Group attacks utilized a multi-stage attack process, during which several tools were launched in order to gain access to a network, avoid detection, and extract data. After all data has been extracted, Medusa is then deployed to lock down access to the data until a ransom is agreed upon and paid.

North Korea often seeks alternative funding sources to overcome budget shortfalls stemming from international sanctions against it. In the past, the communist regime in Pyongyang has generated funds through a variety of illicit, black market activities—to include financially motivated cyberattacks. Lazurus is almost certainly using the Medusa RaaS to generate revenue for the North Korean government.



Medusa attacks by region since January 2021

Source: ZeroFox Intelligence

Medusa is an RaaS platform that first emerged in January 2021; as of this writing, Medusa has been used in at least 371 attacks across all sectors. At least 70 percent of Medusa attacks have targeted organizations in North America, which is consistent with ransomware targeting trends globally.

Lazarus Group's deployment of Medusa almost certainly indicates the collective is seeking to improve the operational security of its financially motivated attacks by concealing its activities behind the established brand of the Medusa RaaS operation. Given the group's history of conducting state-sponsored attacks that advance North Korean government objectives, it is very likely Lazarus Group's financially motivated operations are intended to generate revenue for the communist regime in Pyongyang.

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%