DPRK Using Unpatched Zimbra Devices to Spy on Researchers

By Dark Reading Staff

Published: 2023-02-07 · Archived: 2026-04-05 22:43:50 UTC

1 Min Read

Source: Panther Media via Alamy Stock Photo

A recent round of compromises that exploited unpatched Zimbra devices was an effort sponsored by the North Korean government and intended to steal intelligence from a collection of public and private medical and energy sector researchers.

Analysts with W Labs explained in a new report that due to an overlap in techniques — and thanks to a misstep by one of the threat actors — they were able to attribute "with high confidence" the recent round of cyber incidents against unpatched Zimbra devices as the work of Lazarus Group, a well-known threat group sponsored by the North Korean government. Lazarus operated this campaign and other similar intelligence-gathering efforts through the end of 2022.

The researchers named the campaign "No Pineapple" after an error message generated by the malware during their investigation. The threat actors quietly exfiltrated about 100GB of data, without waging any disruptive cyber operations or destroying information.

"The campaign targeted public and private sector research organizations, the medical research, and energy sector as well as their supply chain," the W Labs report added. "The motivation of the campaign is assessed to be most likely for intelligence benefit."

About the Author

Dark Reading

Dark Reading is a leading cybersecurity media site.
