North Korean hackers spoof venture capital firms in Japan, Vietnam and US

By Jonathan Greig

Published: 2023-06-06 · Archived: 2026-04-06 00:19:04 UTC

Hackers based in North Korea are spoofing financial institutions and venture capital firms in the U.S., Vietnam and Japan, according to new research.

Recorded Future's Insikt Group linked the campaign to APT38, a state-sponsored group in North Korea notorious for several high-profile attacks on cryptocurrency firms and other organizations.

"We discovered 74 domains resolving to 5 IP addresses, as well as 6 malicious files, in the most recent cluster of activity from September 2022 to March 2023," the researchers said. "Previous Insikt Group reporting on overlapping activity attributed to TAG-71 highlighted the group's spoofing of domains belonging to financial firms in Japan, Taiwan, and the United States, as well as popular cloud services used by a large number of enterprises."

The Record is an editorially independent unit of Recorded Future.

The report noted that North Korean hacking groups have a long history of launching financially-motivated attacks and intrusion campaigns on cryptocurrency exchanges, commercial banks and e-commerce systems.

These campaigns are meant to bolster "the North Korean government's continued efforts to generate funds for the regime, which remains under significant international sanctions."

Insikt Group researcher Mitch Haszard said what stood out most from the recent campaign was the spoofing of venture capital firms. He noted that APT38 has previously targeted international financial transactions cooperative SWIFT and cryptocurrency exchanges.

"Both kind of have a clear, 'we are here to steal money' purpose, but the spoofing of venture capital firms is something new and slightly different," he said.

Dating back to March 2022, the researchers said they detected 18 malicious servers being used by North Korean hackers that allowed them to deliver malware and "heavily spoofed popular cloud services, cryptocurrency exchanges, and private investment firms to trick potential victims into opening malicious content or providing their login credentials."

By targeting investment banking and venture capital firms, the group is aiming to "expose sensitive or confidential information of these entities or their customers, which may result in legal or regulatory action, jeopardize pending business negotiations or agreements, or expose information damaging to a company's strategic investment portfolio."

In a campaign that ran from January 2023 to March 2023, Insikt Group found three more IP addresses associated with the group.

These addresses hosted 21 domains themed around common terms associated with document software like “doc-share” and “autoprotect” while several others purport to be financial institutions within Japan, Vietnam, and the United States.

Several of the IP addresses were also tied to another financially-motivated hacking group identified by researchers with security firm Kaspersky.

Due to the crippling financial sanctions faced by North Korea, the country’s hackers will likely continue to launch financially-motivated attacks, the researchers surmised.

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
