North Korean hackers are targeting Israel's defense sector, Israel Ministry of Defense claims

By Shannon Vavra

Published: 2020-08-12 · Archived: 2026-04-05 13:12:56 UTC

North Korean government-linked hackers have been targeting the Israeli defense sector with fake job offers, Israel's Ministry of Defense said Wednesday.

The actors, which Israel says were part of Lazarus Group, a hacking outfit the U.S. government has linked to North Korea, sent their phony job offers through LinkedIn. The hackers created fake LinkedIn accounts impersonating CEOs and top officials at multinational companies to run their scam, according to the Ministry of Defense. According to ClearSky, an Israeli cybersecurity firm which has been tracking the campaign, the hackers imitated the likes of Boeing, McDonnell Douglas, and BAE. After making contact with targets, the hackers continued conversations with victims over WhatsApp, ClearSky said in a research report issued Thursday.

It's the latest example of North Korean hackers using fake job offers to zero in on targets of its espionage operations. In 2016 and 2017, North Korean hackers sent spearphishing emails posing as job recruiters in an attempt to break into the computer systems of Lockheed Martin, according to the U.S. Department of Justice. Just last month, Lazarus Group hackers appeared to be sending fake job offers through LinkedIn to gather intelligence, according to McAfee research.

Israel's Ministry of Defense said it had blocked the attempts in "real time," adding that "no harm or disruption was made to their networks." The attackers were interested in compromising the employees' computers, infiltrating their networks, and stealing sensitive security information, the Ministry of Defense said.

According to ClearSky, however, the North Korean hackers' campaign has succeeded on a number of occasions, infecting "several dozens" of companies and organizations both in Israel and around the world.

North Korean government-linked hackers have continued to pose as job recruiters or send fake job offers even though it is not apparent if any of their previous efforts have been successful.

The FBI, for instance, has said that in its investigation into the Lockheed Martin incident, the intrusion attempts were unsuccessful. McAfee researchers indicated it was unclear if the North Korean efforts on LinkedIn in recent months had been successful as well.

It was not immediately clear if the operation levied against the Israeli defense sector was identical to the North Korean LinkedIn operation McAfee researchers exposed, dubbed "Operation North Star," but they appeared similar.

McAfee Fellow and Chief Scientist Raj Samani told CyberScoop the tactics, techniques, and procedures (TTPs) of the Israeli targeting "share correlation with Operation North Star identified by McAfee Advanced Threat Research; therefore, there is a possibility that the campaigns are conducted by the same threat actor."

Malware from the McAfee-identified campaign, which was still being used in late July, had been detected in Europe and the U.S.

Last month, the European Union sanctioned a North Korean front company for its involvement in the 2017 WannaCry ransomware attack. The same front company is alleged to have been involved in the conspiracy to target Lockheed Martin with recruitment spearphishing emails, according to the DOJ.
