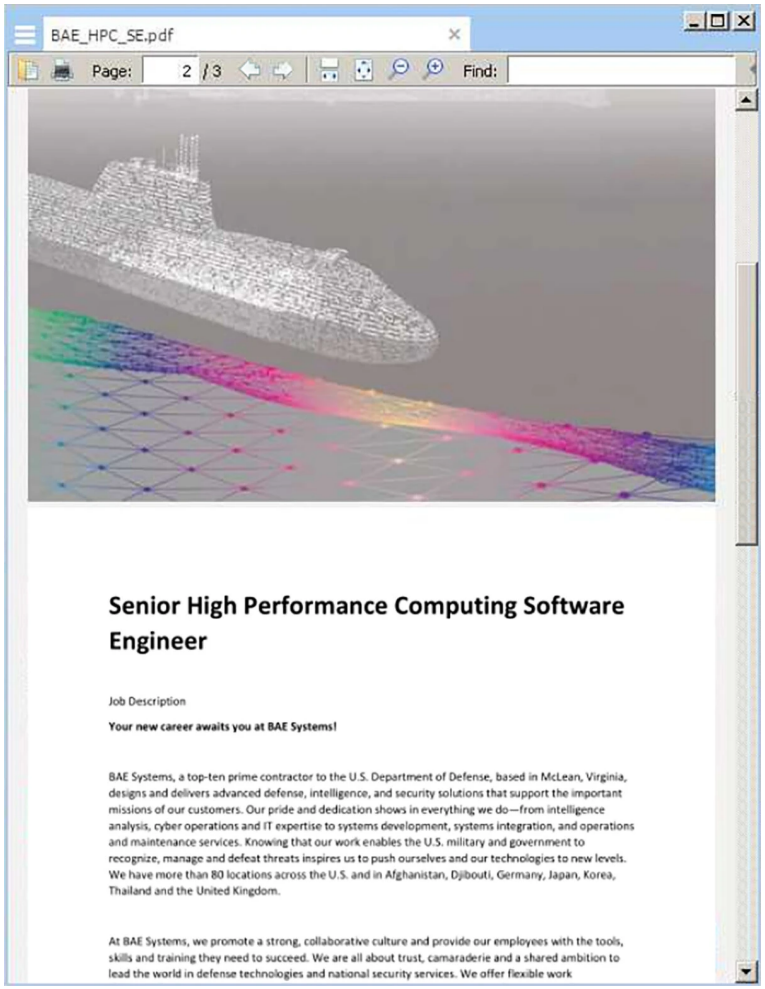
The New York Times

North Korean Hacking Group Attacks Israeli Defense Industry

Israel says the attack was thwarted, but a cybersecurity firm says it was successful. Some officials fear that classified data stolen by North Korea could be shared with Iran.



An image distributed by the cybersecurity company ClearSky shows a fake recruiting announcement that was part of an elaborate hacking campaign.


By Ronen Bergman and Nicole Perlroth

Published Aug. 12, 2020 Updated Aug. 14, 2020

TEL AVIV — Israel claimed Wednesday that it had thwarted a

cyberattack by a North Korea-linked hacking group on its classified defense industry.

The Defense Ministry said the attack was deflected “in real time” and that there was no “harm or disruption” to its computer systems.

However, security researchers at ClearSky, the international cybersecurity firm that first exposed the attack, said the North Korean hackers penetrated the computer systems and were likely to have stolen a large amount of classified data. Israeli officials fear the data could be shared with North Korea’s ally, Iran.

The episode adds Israel to the list of countries and companies that have been targeted by North Korea’s hacking unit, known to private security analysts as the Lazarus Group. American and Israeli officials have said the Lazarus Group, also known as Hidden Cobra, is backed by Pyongyang.

U.S. federal prosecutors unmasked North Korean members of the Lazarus Group in a 2018 criminal complaint, which said the group was working on behalf of Lab 110, a North Korean military intelligence unit.

The complaint accused the group of playing a role in North Korea’s devastating 2017 ransomware attack, known as “WannaCry,” which paralyzed 300,000 computers across 150 countries; the 2016 cyber-theft of $81 million from Bangladesh Bank; and the crippling 2014 cyberattack at Sony Pictures Entertainment that resulted in the leak of executive emails and destroyed more than two-thirds of

the studio's computer servers.

Though the group's track record is mixed, North Korea's growing army of more than 6,000 hackers has grown only more sophisticated and emboldened with time, according to American and British officials tracking the group.

In a report last April, officials at the State Department, the Department of Homeland Security, the Treasury Department and the F.B.I. accused North Korea of increasingly using digital means to evade sanctions and generate income for its nuclear weapons program. The report also accused North Korea of shopping out its hackers to other cybercriminals and countries in what is known as "hacking for hire."

The Justice Department charged a North Korean citizen, Park Jin Hyok, with criminal conspiracy to conduct multiple cyberattacks as a member of the Lazarus Group. Reed Saxon/Associated Press

An Israeli security official said there was concern that the stolen data would be used not only by North Korea, but by Iran.

Israel has been fighting an escalating cyberconflict with Iran in recent months. Israel said it foiled a cyberattack on its water infrastructure in April that officials said was aimed at raising chlorine to dangerous levels as Israelis were quarantined at home with the coronavirus.

Israel, which blamed Iran, retaliated two weeks later with a cyberattack on an Iranian port that knocked its computers offline

and created miles-long shipping traffic around Iran's Shahid Rajaee port facility in early May.

The North Korean attack on Israeli's defense industry began with a LinkedIn message last June, ClearSky researchers said. North Korean hackers posing as a Boeing headhunter sent a message to a senior engineer at an Israeli government-owned company that manufactures weapons for the Israeli military and intelligence.

The hackers created a fake LinkedIn profile for the headhunter, Dana Lopp. There is indeed a real Ms. Lopp, a senior personnel recruiter at Boeing. She did not respond to a message on Wednesday.

Ms. Lopp was one of several headhunters from prominent defense and aerospace companies — including Boeing, McDonnell Douglas and BAE Systems — whom North Korea's hackers mimicked on LinkedIn.

After establishing contact with their Israeli targets, the hackers asked for an email address or phone number to connect via WhatsApp or, to increase credibility, suggested switching to a live call. Some of those who received the calls, and whom ClearSky approached later, said the other side spoke English without an accent and sounded credible.

That level of sophistication had not been demonstrated by Lazarus before, the researchers said. Israeli officials speculated Wednesday that North Korea may have outsourced some of their operation to native English speakers abroad.

At some point, the hackers asked to send their targets a list of job requirements. That file contained invisible spyware that infiltrated the employee's personal computer and attempted to crawl into classified Israeli networks.

ClearSky said the attacks, which started early this year, "succeeded, in our assessment, to infect several dozen companies and organizations in Israel" and around the globe.

The hacking campaign was a notable step up from a previous attempt by North Korea to hack the Israeli defense industry last year. In 2019, ClearSky reported a somewhat clumsy effort by Lazarus to break into an Israeli defense corporation's computers by sending emails in broken Hebrew that were likely written with electronic translation. The emails immediately aroused suspicion and the attack was stopped.

North Korea's hackers appear to have learned their lesson and in mid-2019 began using LinkedIn and WhatsApp to establish contact with a number of military industries in the West, attacking aerospace and defense companies in Europe and the Middle East. In August, a United Nations report said that North Korean hackers used similar methods to track officials of the organization and of member states.

Boaz Dolev, the chief executive and owner of ClearSky, said that in the wake of these reports the company began seeing attempts to attack Israeli defense companies. It quickly found Lazarus's fake

LinkedIn profiles and messages to employees of Israeli defense companies.

ClearSky researchers discovered that, in at least two cases, North Korea's hackers had installed hacking tools on Israeli networks. The tool, known as a remote access trojan, has been used by North Korean hackers in previous cyberattacks on Turkish banks and other victims, stealing passwords and other data.

The successful installation was a red flag, researchers said, that North Korea made it further into the Israeli networks than officials let on.

"North Korea's Lazarus is once again proving high capability and originality in its social engineering and hacking methods," Mr. Dolev said.