Google says North Korea-backed hackers sought cyber research

January 27 2021, by Kim Tong-Hyung

In this April 24, 2018, file photo, a North Korean flag flutters in the wind atop a 160-meter tower in North Korea's village Gijungdong as seen from the Taesungdong freedom village inside the demilitarized zone in Paju, South Korea. (AP Photo/Lee Jin-man, File)

Google says it believes hackers backed by the North Korean government have been posing as computer security bloggers and using fake accounts on social media while attempting to steal information from researchers in the field.

Google didn't specify how successful the hackers were or what kind of information could have been compromised. Experts say the attacks reflect North Korean efforts to improve its cyber skills and be able to breach widely used computer products, such as Google's Chrome internet browser and Microsoft's Windows 10 operating system.

While the country has denied involvement, North Korea has been linked to major cyberattacks, including a 2013 campaign that paralyzed the servers of South Korean financial institutions, the 2014 hacking of Sony Pictures, and the WannaCry malware attack of 2017.

The U.N. Security Council in 2019 estimated North Korea earned as much as $2 billion over several years through illicit cyber operations targeting cryptocurrency exchanges and other financial transactions, generating income that is harder to trace and offsets capital lost to U.S.-led economic sanctions over its nuclear weapons program.

Adam Weidemann, a researcher from Google's Threat Analysis Group, said in the online report published late Monday that hackers supposedly backed by North Korea created a fake research blog and multiple Twitter profiles to build credibility and interact with the security researchers they targeted.

After connecting with researchers, the hackers would ask them if they wanted to collaborate on cyber-vulnerability research and share a tool that contained a code designed to install malicious software on the targets' computers, which would then allow the hackers to take control of the device and steal information from it.

Several targeted researchers were compromised after following a Twitter link to a blog set up by the hackers, Weidemann said.

"At the time of these visits, the victim systems were running fully patched and up-to-date Windows 10 and Chrome browser versions," Weidemann wrote. "At this time we're unable to confirm the mechanism of compromise, but we welcome any information others might have."

Google published a list of social media accounts and websites it said were controlled by the hackers, including 10 Twitter profiles and five LinkedIn profiles.

Simon Choi, a senior analyst at NSHC, a South Korean computer security firm, said cyberattacks linked to North Korea over the past few years have demonstrated an improving ability in identifying and exploiting vulnerabilities in computer security systems. Before 2016, the North Koreans had mainly relied on methods used by Chinese or Russian hackers, he said.

"It's notable that the computer security experts on Twitter who said they were approached by the hackers had been engaged in vulnerability research for Chrome and Windows 10," Choi said.

"It's that not easy to successfully penetrate these systems that are built with the latest security technologies. For the North Koreans, it makes more sense to steal the vulnerabilities already discovered by the researchers because developing their own ways to exploit these systems is harder."

In 2018, U.S. federal prosecutors charged a computer programmer working for the North Korean government for his alleged involvement in the cyberattacks that hacked Sony Pictures and unleashed the WannaCry ransomware virus. Park Jin Hyok, who is believed to be in North Korea,

conspired to conduct attacks that also stole $81 million from Bangladesh's central bank, according to the charges.

The 2014 Sony hack led to the release of tens of thousands of confidential Sony emails and business files. The WannaCry cyberattack in 2017 scrambled data on hundreds of thousands of computers at government agencies, banks and other businesses across the globe and crippled parts of the British health care system.