North Korean cyber spies deploy new tactic: tricking foreign experts into writing research for them

reuters.com/world/asia-pacific/north-korean-cyber-spies-deploy-new-tactic-tricking-foreign-experts-into-writing-2022-12-12/

By Josh Smith

People visit the the statues of North Korea's founder Kim Il Sung and late leader Kim Jong Il on the 74th anniversary of North Korea's founding, in Pyongyang, North Korea in this photo released by North Korea's Korean Central News Agency (KCNA) September 10, 2022. KCNA via REUTERS

SEOUL, Dec 12 (Reuters) - When Daniel DePetris, a U.S.-based foreign affairs analyst, received an email in October from the director of the 38 North think-tank commissioning an article, it seemed to be business as usual.

It wasn't.

The sender was actually a suspected North Korean spy seeking information, according to those involved and three cybersecurity researchers.

Instead of infecting his computer and stealing sensitive data, as hackers typically do, the sender appeared to be trying to elicit his thoughts on North Korean security issues by pretending to be 38 North director Jenny Town.

"I realized it wasn't legit once I contacted the person with follow up questions and found out there was, in fact, no request that was made, and that this person was also a target," DePetris told Reuters, referring to Town. "So I figured out pretty quickly this was a widespread campaign."

The email is part of a new and previously unreported campaign by a suspected North Korean hacking group, according to the cybersecurity experts, five targeted individuals and emails reviewed by Reuters.

The cybersecurity experts suspect the hackers are targeting people who are influential in foreign governments to better understand where Western policy is headed on North Korea.

The hacking group, which researchers dubbed Thallium or Kimsuky, among other names, has long used “spear-phishing” emails that trick targets into giving up passwords or clicking attachments or links that load malware. Now, however, it also appears to simply ask researchers or other experts to offer opinions or write reports.

According to emails reviewed by Reuters, among the other issues raised were China’s reaction in the event of a new nuclear test; and whether a "quieter" approach to North Korean "aggression" might be warranted.

"The attackers are having a ton of success with this very, very simple method," said James Elliott of the Microsoft Threat Intelligence Center (MSTIC), who added that the new tactic first emerged in January. "The attackers have completely changed the process."

MSTIC said it had identified "multiple" North Korea experts who have provided information to a Thallium attacker account.

A 2020 report by U.S. government cybersecurity agencies said Thallium has been operating since 2012 and "is most likely tasked by the North Korean regime with a global intelligence gathering mission."

Thallium has historically targeted government employees, think tanks, academics, and human rights organisations, according to Microsoft.

"The attackers are getting the information directly from the horse's mouth, if you will, and they don't have to sit there and make interpretations because they're getting it directly from the expert," Elliott said.

NEW TACTICS

North Korean hackers are well-known for attacks netting millions of dollars, targeting Sony Pictures over a film seen as insulting to its leader, and stealing data from pharmaceutical and defence companies, foreign governments, and others.

North Korea's embassy in London did not respond to a request for comment, but it has denied being involved in cyber crime.

In other attacks, Thallium and other hackers have spent weeks or months developing trust with a target before sending malicious software, said Saher Naumaan, principal threat intelligence analyst at BAE Systems Applied Intelligence.

But according to Microsoft, the group now also engages with experts in some cases without ever sending malicious files or links even after the victims respond.

This tactic can be quicker than hacking someone's account and wading through their emails, bypasses traditional technical security programmes that would scan and flag a message with malicious elements, and allows the spies direct access to the experts' thinking, Elliott said.

"For us as defenders, it's really, really hard to stop these emails," he said, adding that in most cases it comes down to the recipient being able to figure it out.

Town said some messages purporting to be from her had used an email address that ended in ".live" rather than her official account, which ends in ".org", but had copied her full signature line.

In one case, she said, she was involved in a surreal email exchange in which the suspected attacker, posing as her, included her in a reply.

DePetris, a fellow with Defense Priorities and a columnist for several newspapers, said the emails he has received were written as if a researcher were asking for a paper submission or comments on a draft.

"They were quite sophisticated, with think tank logos attached to the correspondence to make it look as if the inquiry is legitimate," he said.

About three weeks after receiving the faked email from 38 North, a separate hacker impersonated him, emailing other people to look at a draft, DePetris said.

That email, which DePetris shared with Reuters, offers $300 for reviewing a manuscript about North Korea's nuclear programme and asks for recommendations for other possible reviewers. Elliot said the hackers never paid anyone for their research or responses, and would never intend to.

GATHERING INFORMATION

Impersonation is a common method for spies around the world, but as North Korea's isolation has deepened under sanctions and the pandemic, Western intelligence agencies believe Pyongyang has become particularly reliant on cyber campaigns, one security source in Seoul told Reuters, speaking on condition of anonymity to discuss intelligence matters.

In a March 2022 report, a panel of experts that investigates North Korea's U.N. sanctions evasions listed Thallium's efforts as among activities that "constitute espionage intended to inform and assist" the country's sanctions avoidance.

Town said in some cases, the attackers have commissioned papers, and analysts had provided full reports or manuscript reviews before realising what had happened.

DePetris said the hackers asked him about issues he was already working on, including Japan's response to North Korea's military activities.

Another email, purporting to be a reporter from Japan's Kyodo News, asked a 38 North staffer how they thought the war in Ukraine factored in North Korea's thinking, and posed questions about U.S., Chinese, and Russian policies.

"One can only surmise that the North Koreans are trying to get candid views from think tankers in order to better understand U.S. policy on the North and where it may be going," DePetris said.

Reporting by Josh Smith. Editing by Gerry Doyle

-
-
-
-
-

Our Standards: The Thomson Reuters Trust Principles.