North Korea has tried to hack 11 officials of the UN Security Council

By Written by Catalin Cimpanu, ContributorContributor Sept. 30, 2020 at 12:50 p.m. PT

Archived: 2026-04-05 13:58:50 UTC

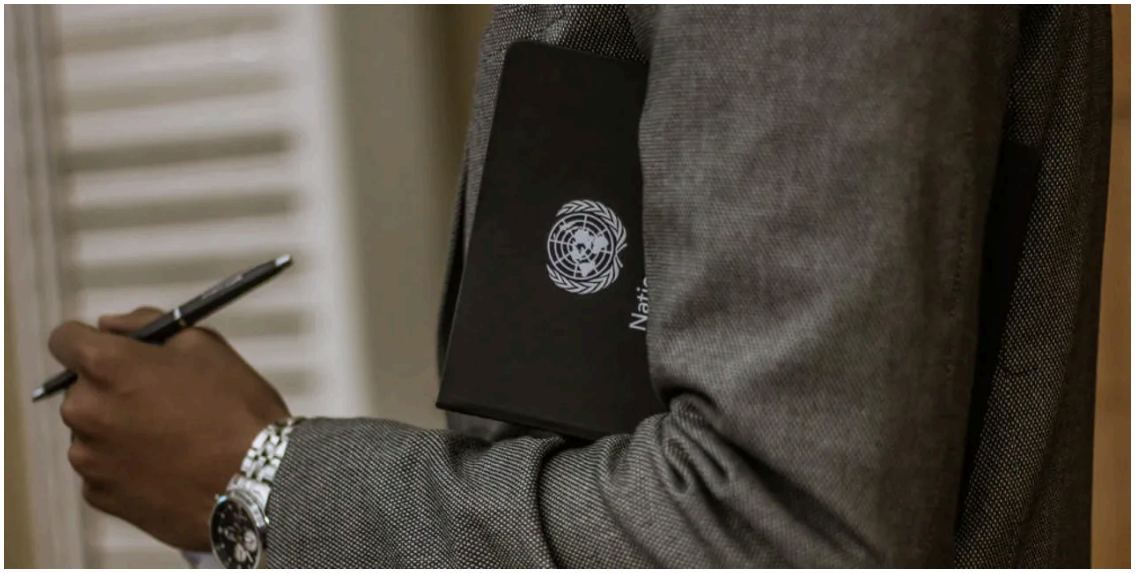

Image: Llyass Seddoug

Special feature

A hacker group previously associated with the North Korean regime has been spotted launching spear-phishing attacks to compromise officials part of the United Nations Security Council.

The attacks, disclosed in a UN report last month, have taken place this year and have targeted at least 28 UN officials, including at least 11 individuals representing six countries of the UN Security Council.

UN officials said they learned of the attacks after being alerted by an unnamed UN member state (country).

The attacks were attributed to a North Korean hacker group known in the cyber-security community by the codename of Kimsuky.

According to the UN report, Kimsuky operations took place across March and April this year and consisted of a series of spear-phishing campaigns aimed at the Gmail accounts of UN officials.

The emails were designed to look like UN security alerts or requests for interviews from reporters, both designed to convince officials to access phishing pages or run malware files on their systems.

The country which reported the Kimsuky attacks to the UN Security Council also said that similar campaigns were also carried out against members of its own government, with some of the attacks taking place via WhatsApp, and not just email.

Furthermore, the same country informed the UN that Kimsuky attacks have extremely persistent with the North Korean hacker group pursuing "certain individuals throughout the 'lifetime' of their [government] career."

Similar Kimsuky attacks detailed in a previous UN report as well

The UN report, which tracks and details North Korea's response to international sanctions, also noted that this campaign has been active for more than a year.

In a similar report published in March, the UN Security Council revealed two other Kimsuky campaigns against its sitting panel officials.

The first was a series of spear-phishing attacks against 38 email addresses associated with Security Council officials — all of whom were members of the Security Council at the time of the attack.

The second were the operations detailed in a report from the National Cybersecurity Agency of France [PDF]. Dating back to August 2019, these were spear-phishing attacks against officials from China, France, Belgium, Peru, and South Africa, all of whom were members of the UN Security Council at the time of the attacks.

Kimsuky has a long history of going after the UN

But these attacks did not stop in April, as stated in the most recent UN report on North Korea, and the Kimsuky group has continued to target the UN, as part of its broader efforts to spy on UN decision-making in regards to North Korean affairs and possible plans on imposing new sanctions.

"We are definitely still observing targeting of the United Nations - something that has been going on for quite some time and has been continuous in the past six months," Sveva Vittoria Scenarelli, a senior analyst in PwC's Threat Intelligence team, told *ZDNet* today.

"From our visibility, we are seeing Kimsuky particularly focused on the OHCHR (the UN's Office of the High Commissioner for Human Rights). For example, we're seeing domains pretending to be OHCHR intranets," Scenarelli added.

The PwC analyst, who is an expert in Kimsuky operations, says most of the group's operations are spear-phishing attacks aimed at obtaining a victim's credentials for various online accounts. Other spear-phishing operations also aim to get the victims infected with malware.

"Sometimes both types of operations are conducted against the same target," Scenarelli said.

Asked about the information put forward by the unnamed country that some Kimsuky operations had targeted select officials throughout the lifetime of their government careers, Scenarelli said this was typical of Kimsuky's past campaigns.

"We have most definitely observed Kimsuky targeting specific individuals — in fact, up to the present moment — even going as far as registering Internet domains containing the individual targets' names, the PwC analyst said.

"It's not as much of an isolated case — rather, we assess that specific individuals are targeted because of their role and the information they have access to. So in this sense, this kind of targeting is highly likely to be driven by specific objectives, be these intelligence collection or something else," Scenarelli added.

"As to whether the targeting continues for the entirety of targets' career, this might depend on the individual target. Though we do not have direct visibility at this level of specificity, we'd assess it is likely that Kimsuky might continue to target that individual so long as they are presumed to have access to information of interest, and so long as Kimsuky's strategic objectives require the threat actor to gain access to certain information.

"If all needed information is acquired, or if these strategic objectives change, then Kimsuky might focus its targeting somewhere else, which is a "pivot" that we've seen the threat actor make before."

Scenarelli is set to hold a talk on Kimsuky operations today at the Virus Bulletin 2020 security conference. This article is unrelated to her presentation.

The world's most famous and dangerous APT (state-developed) malware

Security
