North Korean state hackers target retired diplomats and military officials

By Written by Catalin Cimpanu, ContributorContributor Aug. 28, 2019 at 5:53 a.m. PT

Archived: 2026-04-05 15:46:14 UTC

See als

-

In what appears to be the first attack of its kind, a North Korean state-sponsored hacking group has been targeting retired South Korean diplomats, government, and military officials.

Targets of this recent campaign include former ambassadors, military generals, and retired members of South Korea's Foreign Ministry and Unification Ministry.

The attacks occurred between mid-July and mid-August, and targeted officials' Gmail and Naver email accounts, Simon Choi, Founder of IssueMakersLab, told *ZDNet* in an interview this week.

At the technical level, the attacks were basic spear-phishing attempts. North Korean hackers sent emails which redirected victims to fake login pages, where attackers would log victims' account credentials.

Retired officials are an easier target

"Retired people are engaged in government advisory activities, and they maintain ties with incumbent government officials," Choi told *ZDNet*.

The South Korean cyber-security expert suspects hackers are then using access to these accounts to gather information from retired officials or launch attacks against incumbents.

Choi said targeting retired officials is a smart decision, as they tend to be more vulnerable then officials still in office, who benefit from improved cyber-security protections and security alerts about ongoing attacks.

The IssueMakersLab founder couldn't tell if the hackers were successful in compromising any email accounts, but Choi was able to track down their origin.

According to the security researcher, the attacks have been carried out by Kimsuky, a well-known political cyber-espionage group linked to North Korea.

The group, also known as Kimsuki or Velvet Chollima, has been in operation since 2011 and was first detailed in a Kaspersky report back in 2013.

According to a threat group encyclopedia compiled by Thailand's CERT team, the group's historical and primary targets have consisted of various South Korean government, nuclear power plants, and military operations.

In the past two years, the group also expanded some of its operations to include foreign targets, such as academic institutions (by utilizing a Chrome extension), foreign affair ministries, and US think tanks.

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

Security

Editorial standards