UN’s North Korea sanctions experts targeted by ‘sustained’ hack attack – report

23/05/2017

A UN panel of experts investigating possible violations of North Korean sanctions have fallen victim to a “sustained” hack attack launched by unknown perpetrators who were perfectly aware of what the experts were looking for.

In a warning email sent to UN officials and the Security Council’s North Korea sanctions committee – also known as the 1718 committee – the panel chair described the hack attack as part of a *“sustained cyber campaign,”* according to Reuters, which has seen the document.

Read more S. Korea accuses North of hacking railway systems and officials’ phones

The chair of the expert panel said a zip file containing a *“highly personalized message”* had been sent to one of the investigators, *“which shows the hackers have a very detailed insight into the panel’s current investigations structure and working methods.”*

“As a number of 1718 committee members were targeted in a similar fashion in 2016, I am writing to you all to alert you to this heightened risk,” the panel chair wrote in an email sent out on May 8.

The UN sanctions committee secretary sent another email to fifteen Security Council members on May 10 to report that the United Nation’s Office of Information and Communications Technology was *“conducting an analysis of the affected hard drive.”*

“Increased vigilance relating to 1718 Committee-related correspondence is therefore advised until data analysis and related investigations are completed,” the second warning read.

One of the panel members was hacked, according to a spokesman for the Italian Mission to the UN, which currently chairs the 1718 committee.

Details regarding the extent of the breach or who might have been behind the cyberattack are not immediately clear, but suspicion is likely to fall on North Korea.

Earlier this week, cybersecurity experts said that the WannaCry ransomware, which has hit computer networks in 150 countries around the globe, may have been launched by Pyongyang or people trying to frame North Korea. The speculation arose when it was revealed that the virus contains code similar to that in malware attributed to alleged North Korean hackers.

Read more WannaCry ransomware shares code with North Korea-linked malware – researchers

Neel Mehta, a renowned Google security researcher, revealed the resemblance between the code used in what is said to be an early version of WannaCry and that in a hacker tool attributed to the notorious Lazarus Group.

There are widespread rumors suggesting that North Korea maintains a unit of highly trained hackers capable of launching sophisticated attacks on Pyongyang’s adversaries. Citing unverifiable sources among North Korean defectors, Reuters reported that North Korea’s main intelligence agency has a special cyber cell called Unit 180. The secretive detachment is allegedly involved in launching high-profile cyberattacks on financial institutions in order to steal money and other assets.

Pyongyang has never acknowledged conducting such operations, however. On Friday, North Korea’s deputy UN envoy said it was nonsense to link Pyongyang with the WannaCry ransomware attack. *“Relating to the cyberattack, linking to the DPRK, it is ridiculous,”* Kim In Ryong, the deputy envoy, told a news conference, as cited by Reuters.

“Whenever something strange happens, it is the stereotype way of the United States and the hostile forces that kick off noisy anti-DPRK campaign deliberately linking with DPRK,” Kim said.

In April, Russia’s KasperskyLab said it had traced some of the IPs used by the Lazarus Group, which is believed to be behind numerous hacking attacks on banks’ SWIFT servers, back to North Korea, thus establishing *“a direct link”* between the suspected perpetrators and the reclusive state for the first time.

However, KasperskyLab experts fell short of naming North Korea an actual perpetrator, citing lack of evidence.