S. Korea hacking suspect used China IP addresses: investigators

December 24 2014

The defence ministry's cyber warfare unit has increased its watch level against attacks after the publication last week of a variety of information about the South's nuclear power plant operator on Twitter

A suspect in the hacking attack on South Korean nuclear reactors has used multiple Internet protocol (IP) addresses based in China, investigators said Wednesday.

The defence ministry's cyber warfare unit has increased its watch level against attacks after the publication last week of a variety of information

about the South's [nuclear power](#) plant operator on Twitter.

It included designs and manuals for two reactors, as well as personal information on some 10,000 workers at Korea Hydro and Nuclear Power (KHNP).

The suspected hacker worked from the northeastern Chinese city of Shenyang, according to a joint investigation team of government and prosecution officials quoted by Yonhap news agency.

An IP address, however, is not always a reliable guide to the nationality or geographical location of an Internet user.

The suspect has styled himself president of an anti-nuclear power activist group.

On Tuesday the hacker posted more information on Twitter, including four files of reactor-related information and what seemed to be blueprints of facilities, among other material.

The KHNP said the material released on the Gori and Wolsong nuclear power plants was not classified and would not affect safety.

The investigation team said it has also asked help from the FBI to look into the servers of US-based Twitter, Yonhap reported.

On Sunday the hacker threatened to release more information unless the government shut down three reactors at Gori and Wolsong from December 25.

Officials from the Ministry of Trade, Industry and Energy said the hacker would be unable physically to damage the reactors.

They said that the information released so far appeared to be from the power plants' operating system, which until April 2013 had been connected to the Internet, Yonhap reported.

But KHNP nevertheless launched a two-day drill Monday to test its ability to thwart a cyber attack, after the series of online leaks.

The drill came at a time of heightened concern about cyber crime after a crippling attack against Sony Pictures which both Seoul and Washington have blamed on North Korea.

There has been no indication that the North was behind the release of the nuclear material.

But Justice Minister Hwang Kyo-Ahn said Wednesday in parliament that investigators were looking into a possible cyber attack by North Korea.

"We are investigating whether North Korea is behind it," he said.

South Korea's 23 nuclear reactors supply about 30 percent of the country's electricity.

© 2014 AFP

Citation: S. Korea hacking suspect used China IP addresses: investigators (2014, December 24) retrieved 26 April 2024 from https://phys.org/news/2014-12-korea-hacking-china-ip.html