S. Korea tracks cyber attack to China, North still suspect

March 21 2013, by Lim Chang-Won

Disconnected computer monitors are seen at a visitors center at the Korean Broadcasting System (KBS) headquarters in Seoul on March 20, 2013. Wednesday's concerted cyber attack against South Korean broadcasters and banks originated from an IP address in China, but the identity of the hackers cannot be confirmed, officials said Thursday.

South Korea said Thursday it had sourced a damaging cyber attack on its broadcasters and banks to an IP address in China, fuelling suspicions that

North Korea may have been responsible.

Previous online attacks blamed on North Korea—including one last year on the computer network of the conservative JoongAng newspaper in Seoul—have also been tracked back to Chinese sources.

Internet security analysts in South Korea believe official North Korean hackers learned many of their skills in China and operate from there.

The regulatory Korea Communications Commission (KCC) said Wednesday's attack had used the Chinese IP address to access the targeted computer networks and generate malware that crashed their systems.

"The Chinese IP may trigger various assumptions," said Park Jae-Moon, the KCC director of network policy.

"At this stage, we're still making our best efforts to trace the origin of attacks, keeping all kinds of possibilities open," Park said.

The attack on Wednesday completely shut down the networks of TV broadcasters KBS, MBC and YTN, and halted financial services and crippled operations at three banks—Shinhan, NongHyup and Jeju.

Their networks were mostly back up and running Thursday, although a large number of individual PCs were not operational.

Members of the Korea Internet Security Agency investigate cyber attacks at a briefing room of KISA in Seoul on March 20, 2013. Immediate suspicion for Wednesday's attack that targeted three major TV broadcasters, two banks and an Internet service provider, focused on North Korea.

"For geopolitical reasons, it's convenient for North Korea to use Chinese IP addresses for such attacks," said Choi Yun-Seong, a security expert at the state-run Korea Information Technology Research Institute (KITRI).

"However, domestic and foreign hackers can use them as well, so we cannot say for sure North Korea was behind this," Choi told AFP.

China, North Korea's main patron which has angrily denied being behind a spate of cyber attacks on US interests, also stressed the IP address location was meaningless.

"We have pointed out many times that hacking attacks are a global

problem," foreign ministry spokesman Hong Lei said.

"It is anonymous and trans-national. By using other countries' IP addresses, hackers attack some countries' networks and this is a common practice," he said.

Wednesday's attack came days after North Korea accused South Korea and the United States of being behind a "persistent and intensive" hacking assault that took a number of its official websites offline for nearly two days.

It also coincided with heightened military tensions on the Korean peninsula, following Pyongyang's nuclear test last month.

In testimony last year to the US congressional Armed Services Committee, the commander of US forces in South Korea, General James Thurman, said North Korea was employing "sophisticated computer hackers" trained in cyber attacks.

"Such attacks are ideal for North Korea" because they can be done anonymously, and "have been increasingly employed against a variety of targets including military, governmental, educational and commercial institutions", Thurman said.

North Korea was particularly blamed for cyber attacks in 2009 and 2011 that targeted South Korean financial entities and government agencies.

Those attacks were so-called distributed denial-of-service attacks, which overload a site with data causing it to crash, and are relatively simple to carry out.

Wednesday's coordinated assault was more sophisticated, using malware that can wipe the contents of a computer's hard disk as well as drives

connected to the infected computer.

(c) 2013 AFP