

## Experts suspect North behind SKorea computer crash

HYUNG-JIN KIM - Associated Press - Associated Press



Computer networks at major South Korean banks and top TV broadcasters crashed simultaneously Wednesday, paralyzing bank machines across the country and prompting speculation of a cyberattack by North Korea.

Screens went blank at 2 p.m. (0500 GMT), the state-run Korea Information Security Agency said, and more than six hours later some systems were still down.

Police and South Korean officials couldn't immediately determine responsibility, but some experts suspected a cyberattack orchestrated by Pyongyang. The rivals have exchanged threats amid joint U.S.-South Korean military drills and in the wake of U.N. sanctions meant to punish North Korea over its nuclear test last month.

The latest network paralysis took place just days after North Korea accused South Korea and the U.S. of staging a cyberattack that shut down its websites for two days last week. Loxley Pacific, the Thailand-based Internet service provider, confirmed the North Korean outage but did not say what caused it.

The South Korean shutdown did not affect government agencies or potential targets such as power plants or transportation systems, and there were no immediate reports that bank customers' records were compromised, but the disruption froze part of the country's commerce.

Some customers were unable to use the debit or credit cards that many rely on more than cash. At one Starbucks in downtown Seoul, customers were asked to pay for their coffee in cash, and lines formed outside disabled bank machines.

Shinhan Bank, a major South Korean lender, reported a two-hour system shutdown

## Experts suspect North behind SKorea computer crash

Published on Electronic Component News (<http://www.ecnmag.com>)

---

Wednesday, including online banking and automated teller machines. It said networks later came back online and that banking was back to normal. Shinhan said no customer records or accounts were compromised.

Another big bank, Nonghyup, said its system eventually came back online. Officials didn't answer a call seeking details on the safety of customer records. Jeju Bank said some of its branches also reported network shutdowns.

Broadcasters KBS and MBC said their computers went down at 2 p.m., but officials said the shutdown did not affect daily TV broadcasts. Computers were still down more than five hours after the shutdown began, the news outlets said.

The YTN cable news channel also said the company's internal computer network was paralyzed. Footage showed workers staring at blank computer screens.

KBS employees said they watched helplessly as files stored on their computers began disappearing.

Last year, North Korea threatened to attack several news companies, including KBC and MBC.

"It's got to be a hacking attack," Lim Jong-in, dean of Korea University's Graduate School of Information Security. "Such simultaneous shutdowns cannot be caused by technical glitches."

The Korea Information Security Agency had reported that an image of skulls and a hacking claim had popped up on some of the computers that shut down, but later said those who reported the skulls did not work for the five companies whose computers suffered massive outages. KISA was investigating the skull images as well.

An official from the Korea Communications Commission, South Korea's telecom regulator, said in a televised news briefing that investigators speculate that malicious code was spread from company servers that send automatic updates of security software and virus patches.

LG Uplus Corp., which provides network services for the companies that suffered outages, saw no signs of a cyberattack on its networks, company spokesman Lee Jung-hwan said.

The South Korean military raised its cyberattack readiness level but saw no signs of cyberattacks on its networks, the Defense Ministry said.

No government computers were affected, officials said. President Park Geun-hye called for quick efforts to get systems back online, according to her spokeswoman, Kim Haing.

The shutdown raised worries about the overall vulnerability to attacks in South Korea, a world leader in broadband speed and mobile Internet access. Previous

## Experts suspect North behind SKorea computer crash

Published on Electronic Component News (<http://www.ecnmag.com>)

---

hacking attacks at private companies compromised millions of people's personal data. Past malware attacks also disabled access to government agency websites and destroyed files in personal computers.

Seoul believes North Korea runs an Internet warfare unit aimed at hacking U.S. and South Korean government and military networks to gather information and disrupt service.

Seoul blames North Korean hackers for several cyberattacks in recent years. Pyongyang has either denied or ignored those charges. Hackers operating from IP addresses in China have also been blamed.

In 2011, computer security software maker McAfee Inc. said North Korea or its sympathizers likely were responsible for a cyberattack against South Korean government and banking websites earlier that year. The analysis also said North Korea appeared to be linked to a 2009 massive computer-based attack that brought down U.S. government Internet sites. Pyongyang denied involvement.

The shutdown comes amid rising rhetoric and threats of attack from Pyongyang over the U.N. sanctions. Washington also expanded sanctions against North Korea this month in a bid to cripple the government's ability to develop its nuclear program.

North Korea has threatened revenge for the sanctions and for ongoing U.S.-South Korean military drills, which the allies describe as routine but which Pyongyang says are rehearsals for invasion.

Last week, North Korea's Committee for the Peaceful Reunification of Korea warned South Korea's "reptile media" that the North was prepared to conduct a "sophisticated strike" on Seoul.

North Korea also has claimed cyberattacks by the U.S. and South Korea. The North's official Korean Central News Agency accused the countries of expanding an aggressive stance against Pyongyang into cyberspace with "intensive and persistent virus attacks."

South Korea denied the allegation and the U.S. military declined to comment.

Lim said he believes hackers in China were likely culprits in the outage in Pyongyang, but that North Korea was probably responsible for Wednesday's attack.

"Hackers attack media companies usually because of a political desire to cause confusion in society," he said. "Political attacks on South Korea come from North Koreans."

Orchestrating the mass shutdown of the networks of major companies would have taken at least one to six months of planning and coordination, said Kwon Seok-chul, chief executive officer of Seoul-based cyber security firm Cuvepia Inc.

## **Experts suspect North behind SKorea computer crash**

Published on Electronic Component News (<http://www.ecnmag.com>)

---

Kwon, who analyzed personal computers at one of the three broadcasters shut down Wednesday, said he hasn't yet seen signs that the malware was distributed by North Korea.

"But hackers left indications in computer files that mean this could be the first of many attacks," he said.

Lim said tracking the source of the outage would take months.

—

Associated Press writers Sam Kim and Foster Klug contributed to this report.

**Source URL (retrieved on 12/27/2014 - 4:21pm):**

<http://www.ecnmag.com/news/2013/03/experts-suspect-north-behind-skorea-computer-crash>