Computer Networks in South Korea Are Paralyzed in Cyberattacks

nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

Choe Sang-Hun March 20, 2013

Continue reading the main story

SEOUL, South Korea — Computer networks running three major South Korean banks and the country's two largest broadcasters were paralyzed Wednesday in attacks that some experts suspected originated in North Korea, which has consistently threatened to cripple its far richer neighbor.

The attacks, which left many South Koreans unable to withdraw money from A.T.M.'s and news broadcasting crews staring at blank computer screens, came as the North's official Korean Central News Agency quoted the country's leader, Kim Jong-un, as threatening to destroy government installations in the South, along with American bases in the Pacific.

Though American officials dismissed those threats, they also noted that the broadcasters hit by the virus had been cited by the North before as potential targets.

The Korea Communications Commission said Thursday that the disruption originated at an Internet provider address in China but that it was still not known who was responsible.

Many analysts in Seoul suspect that North Korean hackers honed their skills in China and were operating there. At a hacking conference here last year, Michael Sutton, the head of threat research at Zscaler, a security company, said a handful of hackers from China “were clearly very skilled, knowledgeable and were in touch with their counterparts and familiar with the scene in North Korea.”

But there has never been any evidence to back up some analysts’ speculation that they were collaborating with their Chinese counterparts. “I’ve never seen any real evidence that points to any exchanges between China and North Korea, ” said Adam Segal, a senior fellow who specializes in China and cyberconflict at the Council on Foreign Relations,

Wednesday’s attacks, which occurred as American and South Korean military forces were conducting major exercises, were not as sophisticated as some from China that have struck United States computers, and certainly less sophisticated than the American and Israeli cyberattack on Iran’s nuclear facilities. But it was far more complex than a “denial of service” attack that simply overwhelms a computer system with a flood of data.

The malware is called “DarkSeoul” in the computer world and was first identified about a year ago. It is intended to evade some of South Korea’s most popular antivirus products and to render computers unusable. In Wednesday’s strikes, the attackers made no effort to disguise the malware, leading some to question whether it came from a state sponsor — which tend to be more stealthy — or whether officials or hackers in North Korea were sending a specific, clear message: that they can reach into Seoul’s economic heart without blowing up South Korean warships or shelling South Korean islands.

North Korea was accused of using both those techniques in attacks over the past three years.

The cyberattacks Wednesday come just days after North Korea blamed South Korea and the United States for attacks on some of its Web sites. The North’s official Korean Central News Agency said last week that North Korea “will never remain a passive onlooker to the enemies’ cyberattacks that have reached a very grave phase as part of their moves to stifle it.”

The South Korean government cautioned that it was still too early to point the finger for Wednesday’s problems at the North, which has been threatening “pre-emptive nuclear attacks” and other, unspecified actions against its southern neighbor for conducting the military exercises with the United States this month and for supporting new American-led United Nations sanctions against the North.

“We cannot rule out the possibility of North Korean involvement, but we don’t want to jump to a conclusion,” said Kim Min-seok, a spokesman for the Defense Ministry.

The military raised its alert against cyberattacks, he added, and the Korea Communications Commission asked government agencies and businesses to triple the number of monitors for possible hacking attacks. South Korea's new president, Park Geun-hye, instructed a civilian-government task force to investigate the disruptions.

Image
The computers of South Korea's cable channel YTN were frozen during the attacks on Wednesday.Credit...YTN/Agence France-Presse — Getty Images
It could take months to determine the true source of the attacks, and sometimes investigators never come to a firm conclusion. In 2009, a similar campaign of coordinated cyberattacks over the Fourth of July holiday hit 27 American and South Korean Web sites, including South Korea's presidential palace, called the Blue House; its Defense Ministry; and Web sites belonging to the United States Treasury Department, the Secret Service and the Federal Trade Commission.

But those were all "distributed denial of service" attacks in which attackers flood the sites with traffic until they fall offline. While many suspected North Korea, a clear link to the country was never established.

South Korea's two leading television stations, the publicly financed Korean Broadcasting System and MBC, maintained normal broadcasts but said their computers were frozen. The cable channel YTN reported a similar problem. The KBS Web site was shut down.

Shinhan Bank, the country's fourth-largest lender, reported that its Internet banking servers had been temporarily blocked. Technicians restored operations, the government's Financial Services Commission said in a statement.

Two other banks, NongHyup and Jeju, reported that operations at some of their branches had been paralyzed after computers were infected with viruses and their files erased, the commission said. After two hours, the banks' operations returned to normal, they said. A fourth bank, Woori, reported a hacking attack, but said it had suffered no damage.

The Web site of the Washington-based Committee for Human Rights in North Korea was hacked by an entity calling itself "Hitman 007-Kingdom of Morocco," which stole the committee's publications and other documents, said its executive director, Greg Scarlatoiu.

He said he did not know whether the attack was linked to the disruptions in South Korea, but noted that it came a day before the United Nations Human Rights Council was to vote on the resolution calling for the establishment of an independent investigation of North Korean human rights abuses, including its running of prison gulags. The committee has been an active supporter of such an inquiry.

"This type of mishap is not to be unexpected, given the nature of our work," Mr. Scarlatoiu said.

In testimony to Congress last year, Gen. James D. Thurman, the American commander in South Korea, described what he called North Korea's "growing cyberwarfare capability."

"North Korea employs sophisticated computer hackers trained to launch cyberinfiltration and cyberattacks" against South Korea and the United States, General Thurman said. "Such attacks are ideal for North Korea," he added, "providing the regime a means to attack" South Korean and American businesses "without attribution."

But security researchers and foreign policy experts say that North Korea faces significant hurdles. "They simply don't have access to the same technology due to sanctions," said Mr. Sutton, of Zscaler. "And a large portion of their population does not have ready access to the Internet, so they don't have that natural pool of talent to recruit from."

Lee Seong-won, an official at the communications commission, told reporters on Wednesday that the malicious code, once activated, disrupted the booting of computers. "It will take time for us to find out the identity and motive of those who were behind this attack," he said.

The government investigators were also checking whether the images of skulls that reportedly popped up on some computer screens had anything to do with the virus attack.

In recent years, North Korea has vowed to attack South Korean television stations and newspapers for carrying articles critical of its government, even citing the map coordinates of their headquarters.