South Korea: Chinese address source of attack

SAM KIM - Associated Press - Associated Press

Investigators have traced a coordinated cyberattack that paralyzed tens of thousands of computers at six South Korean banks and media companies to a Chinese Internet Protocol address, authorities in Seoul said Thursday.

IP addresses, which are unique to each computer connected to the Internet, can easily be manipulated by hackers operating anywhere in the world, and the investigation into who was actually behind Wednesday's attack and whether they were in China could take weeks. Suspicion for the simultaneous shutdown is still focused on North Korea, which has threatened Seoul and Washington in recent days over U.N. sanctions imposed for its Feb. 12 nuclear test and is accused of waging similar cyberattacks over the past four years.

The cyberattack did not affect the government or military, and there were no immediate reports that customers' bank records were compromised. But it disabled scores of cash machines across the country, disrupting commerce in this tech-savvy, Internet-dependent country, and renewed questions about South Korea's Internet security and vulnerability to hackers.

If the attack was in fact carried out by North Korea, the purpose would seem to be to send a tacit message — and a warning — to South Korea that Pyongyang is capable of breaching its computer networks.

On Thursday, only one of the six targets, Shinhan Bank, was back online and operating regularly.

South Korean investigators say there is no proof yet that North Korea was behind the attack. However, the outage took place as Pyongyang warned Seoul against holding joint military drills with the U.S. that it considers rehearsals for an invasion.

North Korea also has threatened retaliation for sanctions imposed for the nuclear test, as well as its launch of long-range rocket in December. Pyongyang blames Seoul and Washington for leading the push to punish the North.

The Korean Peninsula has remained in a technical state of war, divided by a heavily militarized border, since the foes signed a truce in 1953. Over the past decade, the two Koreas have engaged in deadly naval skirmishes in waters that both countries claim. And increasingly, their warfare has extended into cyberspace.

Seoul's National Intelligence Services believes Pyongyang was behind six cyberattacks between 2009 and 2012.

Pyongyang, meanwhile, blamed Seoul and Washington for an Internet shutdown that disrupted its network last week.

"If it plays out that this was a state-sponsored attack, that's pretty bald-faced and definitely an escalation in the tensions between the two countries," said James Barnett, former chief of public safety and homeland security for the U.S. Federal Communications Commission.

An ominous question is which other businesses, in South Korea or elsewhere, may also be in the sights of the attacker, said Barnett, who heads the cybersecurity practice at Washington law firm Venable.

"This needs to be a wake-up call," he said. "This can happen anywhere."

Wednesday's attack in South Korea, which disabled some 32,000 computers at broadcasters YTN, MBC and KBS, as well as three banks, appeared to come from "a single organization," regulators said. The initial findings were based on results from an investigation into one target, Nonghyup Bank, and the investigation is continuing into the shutdown at the five other firms.

A malicious code that spread through the Nonghyup server was traced to an IP address in China, said Cho Kyeong-sik, a spokesman for the state-run Korea Communications Commission.

The attack may also have extended to the United States. The website of the U.S.-based Committee for Human Rights in North Korea also was hacked, with reports on satellite imagery of North Korean prison camps and policy recommendations to the U.S. government deleted from the site, according to executive director Greg Scarlatoiu.

However, experts say signs do not point to Chinese hackers since Chinese hacking, either from Beijing's cyber-warfare command or freelance hackers, tends to be aimed at collecting intelligence and intellectual property — not simply at disrupting commerce.

China also is home to a sizable North Korean community, both North Koreans working in the neighboring nation and Chinese citizens of ethnic ancestry who consider North Korea their motherland.

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 that year. The analysis also said North Korea appeared to be linked to a massive computer-based attack in 2009 that brought down U.S. government Internet sites. Pyongyang denied involvement.

Previous hacking attacks on commercial ventures have compromised the personal data of millions of customers. Past malware attacks also disabled access to government websites and destroyed files on personal computers.

Last year, North Korea threatened to attack several South Korean news outlets, including KBC and MBC, for reports critical of Pyongyang's activities.

In recent days, North Korea's Committee for the Peaceful Reunification of Korea — a government agency that often targets South Koreans in its push to draw attention to reunification — warned Seoul's "reptile media" that the North was prepared to conduct a "sophisticated strike" if its negative coverage continued.

"North Korea has almost certainly done similar attacks before," said Timothy Junio, a cybersecurity fellow at Stanford University's Center for International Security and Cooperation. "Part of why this wasn't more consequential is probably because South Korea took the first major incident seriously and deployed a bunch of organizational and technical innovations to reduce response time during future North Korea attacks."

South Korea also created a National Cybersecurity Center and Cyber Command modeled after the U.S. Cyber Command. Junio said South Korea's anti-virus firms also play a large role in stopping hacking attacks.

Immediately after Wednesday's attack, South Korean regulators distributed anti-virus software to government offices, banks, hospitals and other institutions. It could be days before the targeted companies are back online, and weeks before the investigation is complete.

"Hackers attack media companies usually because of a political desire to cause confusion in society," said Lim Jong-in, dean of Korea University's Graduate School of Information Security. "Political attacks on South Korea come from North Koreans."

—

Associated Press writers Youkyung Lee and Hyung-jin Kim in Seoul, Matthew Pennington in Washington, Charles Hutzler in Beijing and Martha Mendoza in San Jose, California, contributed to this report.