South Korea blames North Korea for cyberattack (Update)

July 16 2013, by Youkyung Lee

A woman walks by a sign at Cyber Terror Response Center of National Police Agency in Seoul, South Korea, Tuesday, July 16, 2013. North Korea is to blame for last month's cyberattacks on the websites of South Korean media companies and the president and prime minister's offices, a South Korean investigation concluded Tuesday. South Korea's ministry of science said it was blaming North Korea based on analysis of codes, Internet addresses and personal computers used to launch the attacks. The attacks occurred June 25, the 63rd anniversary of the beginning of the Korean War. (AP Photo/Ahn Young-joon)

South Korean investigators on Tuesday blamed rival North Korea for a

cyberattack last month on dozens of South Korean media and government websites, including those of the president and prime minister.

The biggest piece of evidence linking Pyongyang to the attacks on June 25, which marked the 63rd anniversary of the beginning of the Korean War, was a North Korean Internet protocol address found in some of the websites and malicious codes, South Korea's Ministry of Science said.

Investigators said North Korea was found responsible after an analysis of Internet addresses, access logs and 82 malicious codes found in the attacked servers, computers and websites.

Last month's attack was the latest of several that South Korea has blamed on North Korea since 2009, including an attack on South Korean broadcasters and banks in March.

Pyongyang has rejected previous accusations and has blamed the United States and South Korea for a cyberattack, also in March, that shut down its websites for two days. There was no immediate comment from North Korea's state media on Tuesday's accusation.

The South Korean government-led team of investigators said the June online assaults, which hit 69 government and private companies' websites and servers, were planned for at least six months. Part of that planning included hacking file-sharing websites in South Korea.

One of the investigators declined to disclose how the attackers hacked the presidential website because other hackers may mimic the attack. But he said the attackers employed a variety of methods to launch the attack and one of them was to make computers automatically send a massive amount of traffic to a targeted website when a user downloaded a malicious code from a file-sharing site. This type of offensive of

shutting down a website by incurring huge traffic is called DDoS attack, or distributed denial of service. Such an attack targeted some government servers in the June attack.

The fact that attackers were preparing cyberattacks months ahead of time raises questions about whether authorities failed to detect early warning signs. Officials could have detected a problem if someone had discovered the file-sharing hacking, but no one did, even while authorities were investigating the March 20 cyberattacks that shut down tens of thousands of computers at South Korean broadcasters and banks.

Chun Kilsoo, director of the government-run Korea Internet Security Center, told reporters in a briefing that the evidence investigators have collected so far points to North Korea. In response to criticism about officials not detecting the June attack preparations, Chun said it was difficult to spot ahead of time because the targets of the March and June attacks were different.

Chun said the attackers tried to steal personal information from the websites targeted in the June 25 cyberattacks. He said investigators could not find out whether that information was stolen during hacking preparations before the attack or during the attack itself.

Local media reported that the personal information of hundreds of thousands of people was stolen from the presidential office's website and the ruling party.

Investigators managed to recover data on the hard drives that the attackers destroyed June 25 and found an Internet protocol address that was used by North Korea.

The attackers in June tried to hide their identities by destroying hard drives and hiding the Internet protocol addresses they used, the ministry

said. The attackers also tried to mislead investigators by using the picture of a global hacking collective called Anonymous, the ministry said.

Hackers can usually disguise IP addresses. But the attackers used the same IP addresses two ways for the June 25 attacks—to send and to receive data—so they could not have been falsified, Chun said.

Investigators also found that the codes used in the June attacks had the same features as the codes used in larger March 20 cyberattacks that shut down tens of thousands of computers at South Korean broadcasters and banks, indicating that the same group of hackers was behind both attacks.

Earlier this month, cybersecurity firms said the hackers behind the March attacks also have been trying to steal South Korean and U.S. military secrets for years with a malicious set of codes they've been sending through the Internet. They did not specifically blame North Korea, but they also didn't dispute South Korea's finding that held North Korea as responsible.

Researchers at Santa Clara, California-based McAfee Labs said the malware was designed to find and upload information referring to U.S. forces in South Korea, joint exercises or even the word "secret."

McAfee said versions of the malware have infected many websites in an ongoing attack that it calls Operation Troy because the code is peppered with references to the ancient city.

South Korea's National Intelligence Service blames North Korea for a denial of service attack in 2009 that crippled dozens of websites, including that of the presidential office. Seoul also believes the North was responsible for cyberattacks on servers of Nonghyup Bank in 2011 and Joongang Ilbo, a national daily newspaper, in 2012.

Experts believe North Korea trains large teams of cyber warriors, and that the South and its allies should be prepared against possible attacks on key infrastructure and military systems. If the inter-Korean conflict were to move into cyberspace, South Korea's deeply wired society would have more to lose than North Korea's, which largely remains offline.

Tuesday's announcement from Seoul comes a day after a meeting in which officials from the rival Koreas failed to find a way to reopen a jointly run factory park. The countries plan another round of talks Wednesday on restarting the Kaesong complex, which had been the last remaining symbol of rapprochement before being shut down in April during a period of unusually high animosity.