SKorean police: Hackers extracted data in attacks

July 14 2009, By JAE-SOON CHANG , Associated Press Writer

Employees of AhnLab Inc. work at Security Operation Center in Seoul, South Korea, Friday, July 10, 2009. South Korea's spy agency told lawmakers that the cyber attacks that caused a wave of Web site outages in the U.S. and South Korea were carried out by using 86 IP addresses in 16 countries, amid suspicions North Korea is behind the effort. (AP Photo/Lee Jin-man)

(AP) -- Hackers extracted lists of files from computers that they contaminated with the virus that triggered cyberattacks last week in the United States and South Korea, police in Seoul said Tuesday.

The attacks, in which floods of computers tried to connect to a single Web site at the same time to overwhelm the server, caused outages on prominent government-run sites in both countries.

The finding means that hackers not only used affected computers for

Web attacks, but also attempted to steal information from them. That adds to concern that contaminated computers were ordered to damage their own hard disks or files after the Web assaults.

Still, the new finding does not mean information was stolen from attacked Web sites, such as those of the White House and South Korea's presidential Blue House, police said. It also does not address suspicions about North Korea's involvement, they said.

Police reached those conclusions after studying a malicious computer code in an analysis of about two dozen computers - a sample of the tens of thousands of computers that were infected with the virus that triggered the attacks, said An Chan-soo, a senior police officer investigating the cyberattacks. The officer said that only lists of files were extracted, not files themselves.

"It's like hackers taking a look inside the computers," An said. "We're trying to figure out why they did this."

Extracted file lists were sent to 416 computers in 59 countries, 15 of them in South Korea. Police have found some file lists in 12 receiver computers and are trying to determine whether hackers broke into those systems and stole the lists, An said.

Investigators have yet to identify the hackers or determine for sure where they operated from. Dozens of high-profile U.S. and South Korean Web sites were targeted.

There have been no new Web attacks since the last wave launched Thursday evening.

South Korea's spy agency, the National Intelligence Service, lowered the country's cyberattack alert Monday as affected Web sites returned to

normal.

North Korea is suspected of involvement. The spy agency told lawmakers last week that a North Korean military research institute had been ordered to destroy the South's communications networks, local media reported.

The agency said in a statement Saturday that it has "various evidence" of North Korean involvement, but cautioned it has yet to reach a final conclusion.