Experts work to untangle US, Korea cyber attack

By LOLITA C. BALDOR and JORDAN ROBERTSON – 13 hours ago

WASHINGTON (AP) — U.S. authorities trying to unravel the widespread cyber attacks against government Web sites in the United States and South Korea this week are facing a lengthy, complex investigation that may never identify a culprit, at least not one they would be willing to reveal.

Cyber experts familiar with the probe are divided over the extent of North Korean involvement, split between those who believe hackers may have simply used zombie computers in the region and those who think the communist nation has moved to the digital battlefield.

Active involvement by North Korea would signal a new advancement by the nuclear-ambitioned nation.

If Pyongyang is behind the attacks, "it probably establishes a new pattern of behavior," said Rod Beckstrom, former head of the U.S. cybersecurity center. "If this is them, they are now in the club. And they're probably only going to get better."

Effects of the outage lingered Thursday, as State Department spokesman Ian Kelly said that cyber attacks on the department's computers continued, though not at the high volume seen in the first wave of the assault. A new wave of computer attacks also battered government sites in South Korea but did not knock them offline.

"We are taking measures to deal with this and any potential new attacks," Kelly said.

Investigators in both the U.S. and South Korea face a steep task in trying to trace the attack to its source. The assault involved more than 100,000 zombie computers linked together in a network known as a "botnet." Most of those computers were in South Korea, but others were in Japan, China, the U.S. and possibly other countries, experts said.

Analysts and former government officials on Thursday said the effort to find the culprit in the wave of Web attacks would be a multi-pronged federal investigation that includes agents lurking in nefarious cyber chat rooms seeking tips on the attackers, and analysts poring over the computer code looking for digital fingerprints. And they say there's just a 10 percent chance they'll be successful.

Beckstrom, now head of the Internet's key oversight agency, the Marina del Rey, Calif.-based Internet Corporation for Assigned Names and Numbers, said Thursday the attacks lacked sophistication and was just a "basic hack job" a smart teenager could have launched. But others suggest it displayed characteristics of a higher level, more coordinated effort.

"Just from looking at footprint, it was Bigfoot, not Bambi," said Charles Dodd, founder and chief technology officer for Nicor Cyber Security.

The assault began July 4 and targeted dozens of government and private sites in the U.S., including some federal agencies that were shut down for days as the attack continued into Tuesday.

Treasury Department and Federal Trade Commission Web sites were knocked out by the blizzard of digital requests, while others such as the Pentagon and the White House were able to fend it off with little disruption.

Jack Thomas Tomarchio, head of Nicor Cyber Security and a former deputy undersecretary at the Homeland Security Department, said a North Korean link, if true, would be troubling because "they play by their own set of rules, so it is more difficult to calibrate how they're going to respond."

He added that the attacks overall show that the federal government is still very vulnerable in terms of its cyber security and that agencies have miles to go to plug the holes.

"This is not Pearl Harbor. I'm not trying to alarm the country," he said. "But we do have a serious intrusion problem."

Investigators — including staff at the Homeland Security Department and the National Security Agency and a number of government contractors — are following three paths, according to Alan Paller, director of research at SANS Institute, a computer-security organization in Bethesda, Md.

Copies of the malicious code, he said, have been shipped out to a dozens of analysts and cyber security companies, who are now analyzing it, looking for errors or other hints that would point them to the author. Investigators, including many who speak foreign languages, are roaming the Internet chat rooms, hoping to find someone bragging about the attack or providing clues as to its origin. And still others are following the electronic trail, tracing the attack back to the initially infected computers.

The attack, Paller said, was a wake-up call, that showed that — without a big effort hackers were able to bring some federal agencies' Web presence to its knees.

What some analysts have been able to tell so far is that the program used in the attacks has elements of a fast-spreading e-mail worm from 2004 called "MyDoom." But, experts said it has enough new elements that some antivirus software didn't immediately recognize it as a threat.

The infection spread fast. Joe Stewart, director of malware research for the counterthreat unit of SecureWorks Inc., who has been analyzing the code, says it appears to have been written

Associated Press

Map