Written by **Steven Yates** on July 8, 2009

Cyber Attacks Originating With N. Korea?

A number of South Korean websites experienced similar problems. Eyes are turning to North Korea as the prime suspect.

In the United States, websites of the Treasury Department, the Secret Service, the Federal Trade Commission, and the Transportation Department were all down for varying lengths of time in what is called a "denial of service" attack, with problems continuing into the work week. The *Washington Post* website was also affected, as were some banking sites.

In South Korea, 11 organizations' websites, including that of the presidential Blue House and Defense Ministry, had gone down or experienced access problems by the end of the day Tuesday, according to information released by the Korea Information Security Agency run by the South Korean government.

According to the government's computer experts, the length of time the sites were down testifies to the degree of sophistication of the attacks. According to Ben Rushio of Keynote Systems, problems at the Transportation Department site began Saturday and continued until Monday, while the Federal Trade Commission site was down Sunday and Monday. Even on Tuesday, said Rushio, users were unable to access the FTC site 70 percent of the time. Keynote Systems, based in San Mateo, California, is a company that monitors and publishes data on website outages. It monitors some 40 government sites.

It is common knowledge among the web-savvy that a website can only handle so much traffic. If a site gets overloaded, it can't be accessed and effectively shuts down. During periods of severely inclement weather such as major hurricanes, weather sites are often overloaded with traffic. Denial of service attacks overload sites with Internet traffic deliberately, using viruses or hacking programs to deluge a targeted site. An attack is made more sophisticated if hackers can infect thousands of computers with malware programs and tie them together into "botnets."

The *Washington Post* was told by an anonymous government official, "It certainly seems to be a well-organized attack. There are a lot of computers involved. What we don't know is who is orchestrating it."

American and South Korean security agencies are cooperating to investigate the cyber attacks and try to trace them.

As of this morning, eyes are turning to North Korea, although mainland China has not been ruled out. Although one authority at Seoul University, Yang Moo-jin, doubted whether impoverished North Korea, still under the heel of the communist Pyongyang government, has the capability of forcing all these websites offline, others say that the North Koreans are capable of it, and that "North Korea has been

working hard to hack into" South Korean networks. They may have had help by pro-North Korean forces based in South Korea. Early this morning South Korea's National Intelligence Service stated that some 12,000 computers in South Korea alone were affected, with 8,000 computers overseas adding to the cyber attacks. Many personal computers were infected with a virus taking them simultaneously to both South Korean and U.S. government websites.

The South Korean news agency Yonhap stated that investigators were able to determine that at least some of the attacks on South Korean computers originated overseas. Yonhap cited a South Korean official who on condition of anonymity stated that the cyber attack used a method common to Chinese hackers.

No other Asian countries experienced any cyber attacks.

A curious line of text deep in the malware was found to contain the phrase "get/china/dns." Be this as it may, investigators still do not know who orchestrated these cyber attacks. Tracing such attacks to their source is difficult since hackers are very good at covering their tracks. Government officials state that their computers face daily attempts at unauthorized access or other potentially harmful incidents. The number of breaches of government computers has increased significantly over the past couple of years. According to Homeland Security, there were 5,499 such breaches in 2008, as opposed to 3,928 in 2007 and 2,172 in 2006.