Experts disagree on seriousness of attacks on government Web sites

July 9 2009, By Julian E. Barnes and Josh Meyer

Government Web sites were operating normally on Wednesday, officials said, after a broad attack on public and private computer systems that targeted sites operated by the White House, the New York Stock Exchange and The Washington Post, among others.

The attack caused little damage, but touched off a debate among experts over whether it represented a mild nuisance or the opening salvo of a potential electronic war.

At least for now, federal officials and experts said it would be impossible to determine who was behind the attack. However, South Korean intelligence officials reportedly have fingered North Korea. One senior congressional official briefed on the attacks said U.S. officials consider North Korea a suspect, although other top experts played down that likelihood.

Amit Yoran, the former computer security czar for the Bush administration, was skeptical of North Korean involvement, and said the attacks appeared to rely on only slight variants on known methods and techniques.

"They're loud and clumsy and not really what we would expect out of a sophisticated adversary," said Yoran, now chairman of a computer security firm. "There are a million conspiracy theories we can come up with, but what we need to do is the forensic analysis and then come up with conclusions."

The computer attack, which began on July 4, temporarily disabled some federal government Web sites, including those operated by the Treasury Department, Transportation Department and Federal Trade Commission.

The attack also appeared to target the White House, State Department and Defense Department Web sites. Because of stronger defenses, Pentagon Web sites were not affected and attempts to crash the White House Web site failed. The attacks also targeted private Web sites, such as those of the stock exchange and The Washington Post.

The "denial of service" attack, as it is known, appeared to wind down by Wednesday. At its height, it used an estimated 50,000 private computers that were infected with a virus that used them in attempts to overwhelm the U.S. Web sites by constantly requesting access to them.

Fueling a suspected North Korean link, the infected computers contacting the U.S. Web sites appeared to be based in either North or South Korea, said the congressional official, discussing the classified briefings on condition of anonymity.

But in computer attacks, it is difficult for officials to determine the exact origin, since attackers can mask their location and identity, experts said. At that, denial of service attacks are fairly rudimentary -- more the hallmark of hackers than hostile and resourceful foreign governments.

One U.S. official with knowledge of the attacks downplayed the seriousness of the incident and said the recent attacks were similar to countless other "probes" of government computer systems.

"This is not unlike other attacks. It is just more noticeable due to the nature of the sites that were attacked," the official said. "Because of the measures we have in place, we were able to mitigate these very quickly."

The official, who also spoke on condition of anonymity because of the sensitive information involved, said the Web site outages were intermittent, and differed among the various departments. The official said that Web sites were slowed or shut down but not compromised.

The Department of Homeland Security, which is responsible for protecting most government computers, said an emergency response team had advised federal departments about steps to take to help mitigate such attacks.

"We see attacks on federal networks every single day, and measures in place have minimized the impact to federal Web sites," said Amy Kudwa, a department spokeswoman.

John Wheeler, a former Air Force official who worked on computer issues, speculated that North Korea may have shifted its hostile intents from missiles to electronic attacks. He said the attackers could have left behind malicious software that can be activated later to aid in other computer attacks.

"If you are in someone's cyber space you will leave behind aids for when you come back," Wheeler said. "It is basic to war fighting that you prepare the battlefield and part of that is salting the battle field with mines."

But other security experts played down the attacks.

"This is as bad as a cyber attack gets and it was mostly not noticeable to ordinary Americans," said Jim Harper, director of information policy studies for the Cato Institute.

Harper said the attack could not be equated to a military strike.

"What this turned up is some poorly run government Web sites. What we are talking about in these so-called cyber attacks is some inconvenience," he said. "Someone in the tech department has to figure out what is going on and put them back together."

___