Los Angeles Times

http://www.latimes.com/news/nationworld/nation/la-na-cyber-security9-2009jul09,0,2952825.story
From the Los Angeles Times

Attack on government computers draws speculation and shrugs

Some suspect North Korea launched the cyber attack whose targets included the White House and the NYSE. Others scoff at the idea. South Korea was also hit.

By Julian E. Barnes and Josh Meyer

July 9, 2009

Reporting from Washington — Despite a broad and persistent cyber attack whose targets included the White House, the New York Stock Exchange and the Washington Post, government websites were operating normally on Wednesday, officials said.

The attack began July 4 and caused little damage, but it touched off a debate among experts over whether it represented a mild nuisance or the opening salvo of a potential electronic war.

Federal officials and experts said it would be impossible to determine who was behind the attack, at least for now. But intelligence officials in South Korea, where websites also were attacked, reportedly have fingered North Korea.

One senior congressional official briefed on the attacks said U.S. computer security officials also considered North Korea a suspect.

The computers contacting the U.S. websites appeared to be based in either North or South Korea, said the official, who discussed the classified briefings on condition of anonymity.

At its height, the attack involved 50,000 private computers infected with a virus that caused them to continuously contact websites in an effort to overwhelm them. The "denial of service" attack, as it is known, appeared to wind down by Wednesday.

Some experts downplayed any North Korean link. It is difficult to determine the origin of computer attacks, they said, because attackers can mask their location and identity. And denial-of-service attacks are fairly rudimentary -- more the hallmark of hackers than hostile and resourceful foreign governments, they said.

Amit Yoran, the former computer security czar for the Bush administration, expressed skepticism that North Korea was involved. He said the attacks appeared to rely on slight variants of 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," he said.

The attack temporarily disabled several federal government websites, including those operated by the Treasury Department, the Transportation Department and the Federal Trade Commission.

It also appeared to target the White House, State Department and Defense Department websites.

Because of stronger defenses, Pentagon websites were not affected, and attempts to crash the White House website failed.

The attacks also targeted private websites, such as those of the NYSE and Washington Post.

One U.S. official with knowledge of the attacks downplayed their seriousness and said they 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 spoke on condition of anonymity because of the sensitive information involved, said the website outages were intermittent and differed among agencies. The official said websites were slowed or shut down but not compromised.

The Homeland Security Department, which is responsible for protecting most government computers, said an emergency-response team had advised federal agencies about mitigating such attacks.

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

John Wheeler, a former Air Force official who worked on computer issues, speculated that North Korea might have shifted its weaponry from missiles to electronics. He said the attackers could have deposited malicious software on the websites that could be activated later.

"If you are in someone's cyberspace, 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 battlefield with mines."

Other security experts played down the incident.

"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.

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

"What this turned up is some poorly run government websites," Harper said. "What we are talking about in these so-called cyber attacks is some inconvenience.

"Someone in the tech department has to figure out what is going on and put them back together."

julian.barnes@latimes.com

josh.meyer@latimes.com

If you want other stories on this topic, search the Archives at latimes.com/archives.

Home Delivery | Advertise | Archives | Contact | Site Map | Help