Pentagon Official: North Korea Behind Week of Cyber Attacks

Thursday , July 09, 2009

FOX NEWS

North Korea was indeed behind the cyberattacks that targeted dozens of Web sites in the U.S. and South Korea over the past week, a U.S. defense official told Fox News Wednesday afternoon.

The unnamed Pentagon official added that the attack did not penetrate the Department of Defense's computer systems, which are constantly being probed from outside.

Some defense officials complained privately that the Department of Homeland Security was taking the lead on protecting government agencies from cyber attacks, and yet the Pentagon wasn't informed about the attacks until Wednesday — by hearing about it from the media.

Another source told Fox News that the attacks actually began a week ago, not Saturday as previously reported.

• Click here to learn how a brute-force cyber attack works.

• Click here to visit FOXNews.com's Cybersecurity Center.

• Got tech questions? Ask our experts at FoxNews.com's Tech Q&A.

In what's known as a "DDoS," or distributed denial-of-service, attack, a huge number of "zombie computers" gathered together in a "botnet" were directed to all go to U.S. government Web sites at the exact same time, which shuts down less-robust sites because they can't handle all the traffic at once.

"It's just overloading the system," the source said.

In this case, the attacks were able to shut down some Web sites, but they were never able to penetrate the security systems surrounding them. By their very nature, DDoS attacks do not compromise security or steal or damage information — they simply knock Web sites offline and tie up valuable resources and manpower.

"It's not beyond the realm of possibly that a nation such as North Korea would be able to do this," Eugene H. Spafford, director of Purdue University's Center for Education and Research in Information Assurance and Security, told FoxNews.com. "But i suspect it's really a third party, some group or political party sympathetic to North Korea."

Yang Moo-jin, a professor at Seoul's University of North Korean Studies, said he doubts whether the impoverished North has the capability to knock down the Web sites.

But Hong Hyun-ik, an analyst at the Sejong Institute think tank, said the attack could have been done by either North Korea or China, saying he "heard North Korea has been working hard to hack into" South Korean networks.

Mike Fitzpatrick, CEO of NCX Group Inc., a California-based information risk-management firm, thinks that anyone could be responsible, because such a sophisticated botnet wouldn't be wasted on taking down government Web sites, an endeavor with no financial gain.

"They're valuable," he told FoxNews.com. "Someone who goes out of their way to build one of these isn't going to sacrifice it on something like this."

Furthermore, Fitzpatrick think this might just be an attempt to divert our attention from something more sinister.

"It could be a distraction," Fitzpatrick added, "a ploy to suck up resources and personnel from what the real target is."

The powerful attacks were even broader than initially realized, also targeting the White House, the Pentagon and the New York Stock Exchange.

Other targets of the attack included the National Security Agency, Homeland Security Department, State Department, the Nasdaq stock market and The Washington Post, according to an early analysis of the malicious software used in the attacks.

Some government Web sites — such as the Treasury Department, Federal Trade Commission and Secret Service — were still reporting problems days after the attack started.

The South Korean sites included the presidential Blue House, the Defense Ministry, the National Assembly, Shinhan Bank, Korea Exchange Bank and top Internet portal Naver, all of which went down or had access problems beginning late Tuesday.

Earlier Wednesday, South Korea's National Intelligence Service said in a statement that 12,000 computers in South Korea and 8,000 computers overseas had been infected and used for the cyber attack.

The agency said it believed the attack was "thoroughly" prepared and committed by hackers "at the level of a certain organization or state." It said it was cooperating with the American investigators to examine the case.

"It doesn't requre much in the way of resources to do something like this," said Spafford. "Criminal enterprises will rent part of existing botnets to do whatever you want."

But he added that it wouldn't be easy to find out definitively who's behind it.

"You can find out where the computers being used in the attack are, but there's no easy way to trace that back further to see who's controlling the botnet," said Spafford.

South Korea's NIS said it believed the attack was "thoroughly" prepared and committed by hackers "at the level of a certain organization or state." It said it was cooperating with the American investigators to examine the case.

South Korean media reported in May that North Korea was running a cyber warfare unit that tries to hack into U.S. and South Korean military networks to gather confidential information and disrupt service.

An initial investigation in South Korea found that many personal computers were infected with a virus program ordering them to visit major official Web sites in South Korea and the U.S. at the same time, Korean information agency official Shin Hwa-su said.

There have been no immediate reports of similar cyber attack in other Asian countries.

Amy Kudwa, spokeswoman for the Homeland Security Department, said the agency's U.S. Computer Emergency Readiness Team issued a notice to federal departments and other partner organizations about the problems and "advised them of steps to take to help mitigate against such attacks."

The U.S., she said, sees attacks on its networks every day, and measures have been put in place to minimize the impact on federal Web sites.

New York Stock Exchange spokesman Ray Pellecchia could not confirm the attack, saying the company does not comment on security issues.

Others familiar with the U.S. outage said the fact that the government Web sites were still being affected three days after it began signaling an unusually lengthy and sophisticated attack.

Attacks on federal computer networks are common, ranging from nuisance hacking to more serious assaults, sometimes blamed on China. U.S. security officials also worry about cyber attacks from Al Qaeda or other terrorists.

Ben Rushlo, director of Internet technologies at Web site monitoring company Keynote Systems, said problems with the Transportation Department site began Saturday and continued until Monday, while the FTC site was down Sunday and Monday.

According to Rushlo, the Transportation Web site was "100 percent down" for two days, so that no Internet users could get through to it.

"This is very strange. You don't see this," he said. "Having something 100 percent down for a 24-hour-plus period is a pretty significant event."

He added that, "The fact that it lasted for so long and that it was so significant in its ability to bring the site down says something about the site's ability to fend off [an attack] or about the severity of the attack."

Fox News' Jennifer Griffin, Mike Levine, Paul Wagenseil and the Associated Press contributed to this story.