

Diverse group of Chinese hackers wrote code in attacks on Google, U.S. companies

21/02/2010 06:12 by admin

By Ellen Nakashima

Washington Post Staff Writer

Saturday, February 20, 2010; A09

Some of the computer codes used in the recent attacks on the networks of Google and dozens of other major U.S. companies were developed by a diverse group of Chinese hackers, including security professionals, consultants and temporary contractors, according to an industry source.

The series of attacks, disclosed Jan. 12 by Google, were routed in part through servers at technical schools in China, a commonly used tactic that allows hackers to obfuscate their identity, said the source, who is familiar with the investigation into the security breaches.

The source said that some of the contractors involved in the attack were based at Chinese and U.S. tech companies in China. He and another industry source said other servers in China were also used.

The two schools whose servers were used are Shanghai Jiaotong University, a prestigious institution in China akin to Caltech, and Lanxiang Vocational School, both of which have links to the top ranks of information security specialists in China, said one of the sources. Neither source was authorized to speak on the record. The connection to the schools was first reported Thursday night on the New York Times Web site.

It is not clear who ordered or coordinated the attacks. The Chinese government has denied involvement.

The developers of the code, who took advantage of a vulnerability in systems using Internet Explorer 6, include students who "hack for prestige," said one source, whose firm is among several investigating the attacks. He said investigators have narrowed the list of hackers to about six individuals but declined to divulge their names.

The code developers did not execute the attack or "nose around" in the networks of Google or other companies, he said. "They're out in the open with it, passing the code back and forth to one another on open source hacker forums," in some cases with their "hacker handles" attached, he said.

None of the handful of code developers involved in the Internet Explorer part of the attack -- there could be other code developers involved -- is a graduate of the two Chinese schools, though they have links to them through people they are working with, the source said.

Ties to government

Jiatong University has a long history of cooperation with Chinese information security companies. It receives funding from the Chinese Ministry of Science and Technology, under a national program known as 863, to train information security experts and advance China's leadership in the field. Professors include government public security officials.

Lanxiang Vocational helped create what has become known as China's "Great Firewall," which filters Internet information in the country. According to the school's Web site, it established a military department in 2006 to train "high quality technology officers." Many of those students have gone on to form "the important technology backbone" of the People's Liberation Army, the site said.

Computer servers at universities and businesses have been used before by hackers in China to route attacks, often without the institutions' knowledge, said James C. Mulvenon, a China cyber expert and a director at the Center for

Rallying For Democracy

<http://www.rallyingfordemocracy.org>

Intelligence Research and Analysis in Washington. He said several think tank networks were penetrated last spring in attacks in which hackers used servers housed at Lanxiang Vocational. Although he did not know whether those hackers were part of the same wave of attacks that hit Google, he said, "it would be a remarkable coincidence . . . to be attacked by the same obscure vocational school in Jinan in China."

The decentralized nature of the attack helps explain why it's so difficult to determine who ordered it and why.

Despite China's denial, the government there is believed to have used a series of proxies in the past to carry out different aspects of cyberattacks. Russia has used similar tactics, experts say.

"You will not necessarily find a card-carrying Chinese government or military person doing the activity," Mulvenon said. "They're much more comfortable casting a wider net in terms of people to help them, in sharp contrast to our system. We don't just let random strangers do this stuff."

Rob Lee, a director at the Northern Virginia cyber forensics company Mandiant, said hackers in China routinely direct their attacks through a series of constantly changing Internet protocol addresses. They do that "to maintain a foothold on targets' networks but also to try to bury where they're coming from," he said.