

US experts close in on Google hackers

22/02/2010 08:41 by admin

Financial Times

US experts close in on Google hackers
By Joseph Menn in San Francisco

Published: February 21 2010 23:33 | Last updated: February 21 2010 23:33

US analysts believe they have identified the Chinese author of the critical programming code used in the alleged state-sponsored hacking attacks on Google and other western companies, making it far harder for the Chinese government to deny involvement.

Their discovery came after another team of investigators tracked the launch of the spyware to computers inside two educational institutions in China, one of them with close ties to the military.

A freelance security consultant in his 30s wrote the part of the program that used a previously unknown security hole in the Internet Explorer web browser to break into computers and insert the spyware, a researcher working for the US government told the Financial Times. Chinese officials had special access to the work of the author, who posted pieces of the program to a hacking forum and described it as something he was "working on".

The developments will add to the furore over the hacking campaign, revealed last month when Google said its systems had been compromised. It threatened to pull out of China, and secretary of state Hillary Clinton asked the Chinese foreign minister for a probe.

The disclosure of the cyberspying campaign has brought attention to technology security matters and the policies of the Chinese, who western experts say have been using software vulnerabilities to steal commercial and military know-how.

The Obama administration has pledged to make cyber-security a priority.

"We're realising there are other aspects of this problem beyond the technological and that there are other agencies that need to get involved," said Mischel Kwon, a former US cybersecurity official now working for RSA Security.

Beyond the immediate forensic inquiry, the work of US researchers sheds light on how cyber-operations are conducted in China.

The man who wrote code to take advantage of the browser flaw is not a full-time government worker, did not launch the attack, and in fact would prefer not be used in such offensive efforts, according to the US team that discovered his role.

"If he wants to do the research he's good at, he has to toe the line now and again," the US analyst said. "He would rather not have uniformed guys looking over his shoulder, but there is no way anyone of his skill level can get away from that kind of thing. The state has privileged access to these researchers' work."

A separate team of US contractors has traced the launch of the spyware to computers at Shanghai Jiaotong University and Lanxiang Vocational School, according to two people familiar with that inquiry.

Jiaotong University has one of the best security departments in the country, US analysts said, with former government

Rallying For Democracy

<http://www.rallyingfordemocracy.org>

cyber commanders in residence.

The state-run Xinhua news agency said officials at both schools denied involvement.

In theory, outsiders could have compromised both schools's machines before using them to collect data from the Western companies.

But US analysts said at least Jiaotong University's networks are closely monitored, making them an odd choice for an independent attacker seeking to avoid detection. In addition, "Our investigation shows the hosts that did the attacks were not compromised that we could tell", said an analyst involved in that probe.

Additional reporting by Patti Waldmeir in Shanghai