2-The Guardian-Chinese hack of US

This article is more than 6 years old

Chinese hack of US national security details revealed days after Russian hack

This article is more than 6 years old

Government sources tell NBC News that Chinese attack targeted personal emails of ‘all top national security’ officials just days after Pentagon hack

A reported spear-phishing attack on the Pentagon’s Joint Staff email system exposed some 4,000 civilian and military employees and is believed to have been sponsored by Russia. Photograph: AFP/Getty Images

A reported spear-phishing attack on the Pentagon’s Joint Staff email system exposed some 4,000 civilian and military employees and is believed to have been sponsored by Russia. Photograph: AFP/Getty Images

Mon 10 Aug 2015 16.06 EDT

First published on Mon 10 Aug 2015 15.33 EDT

The ongoing saga of successful foreign hack attacks on government databases continued Monday with news of another break-in allegedly perpetrated by China .

Just days after the reported spear-phishing attack on the Pentagon’s joint staff email system, which exposed some 4,000 civilian and military employees and is believed to have been sponsored by Russia, anonymous government sources told NBC News that a separate set of Chinese hack attacks targeted the personal emails of “all top national security and trade officials”.

These attacks – among the more than 600 hacks attributed by officials to hackers working for the Chinese government – sought personal email info from top administration officials and began in 2010. NBC’s source said the hacks were still going on but would not name any of the officials targeted.

The US government is dealing with several different investigations into breaches, of security, the largest of which is the hack of the Office of Personnel Management (OPM) – an intrusion that exposed the personal information of some 22 million people.

That investigation has been troubled by intramural squabbling by the agency’s own admission: Patrick McFarland, the office’s inspector general, wrote a strongly worded memo to acting OPM director Beth Cobert accusing the agency’s Office of the Chief Information Officer (OCIO) of hampering its inquiry into the hack, citing multiple instances of uncooperative behavior. Notable among them was the accusation that the “OCIO failed to timely notify the OIG of the first data breach at OPM involving personnel records.”

The US government is trying to put together the best way to safeguard its information but in many cases, better encryption “ would not have helped ”, as Department of Homeland Security assistant secretary for cybersecurity testified before Congress with reference to the OPM hack. In that case, attackers obtained the credentials of an employee at private firm KeyPoint Government Solutions and used them to gain legitimate access to the network.

Lauren Weinstein, technology consultant, said he was skeptical about the anonymous attribution to China for the latest attack. “Just about every email address ever published on a web page is subjected to phishing attacks sooner or later these days,” he said. “If you phish at a few hundred million email addresses, you’ll probably suck up a bunch of them from government officials in the process, whether you specifically targeted them or not. When you keep trying to comb though this kind of data to tease out patterns after the fact, there can be pressure (political and otherwise) to start seeing relationships that aren’t really there, much like staring into a kaleidoscope for too long.”

These newly revealed hacks of private emails took place over the period when then-secretary of state Hillary Clinton was receiving work-related correspondence in her own private accounts, though no victims of the hacks have been named. The timing of the revelations is potentially fortuitous for at least one group of people: proponents of the Cybersecurity Information Sharing Act (Cisa), the controversial bill that will likely come before the Senate again next month.

Internet activists aren't biting: "The US government has proven itself incompetent when it comes to protecting its data," *[Anger]* said Evan Greer of advocacy group Fight for the Future. "Information sharing bills like Cisa would make us even more vulnerable *[Anger]*by dramatically expanding the amount of private data the US government keeps in its databases and the number of government and law enforcement agencies who would house that data."

Topics