11-21-2008

China Hax!1!

Follow this and additional works at: http://digitalcommons.unl.edu/chinabeatarchive
Part of the Asian History Commons, Asian Studies Commons, Chinese Studies Commons, and the International Relations Commons

http://digitalcommons.unl.edu/chinabeatarchive/267

This Article is brought to you for free and open access by the China Beat Archive at DigitalCommons@University of Nebraska - Lincoln. It has been accepted for inclusion in The China Beat Blog Archive 2008-2012 by an authorized administrator of DigitalCommons@University of Nebraska - Lincoln.
Chinese hackers *may* (we should stress, *may*) have struck again. Just two weeks after *Newsweek* reported (in the juicy campaign expose published in last week’s issue) that last summer both the Obama and McCain campaign computers were infiltrated by hackers who copied documents on policy issues (speculated to be either Chinese or Russian), yesterday Fox News announced that the Pentagon was banning the use of external computing hardware after a worm was found to be spreading through its computing network.

There do not seem to be any online reports linking the new regulation specifically to Chinese hackers, but Fox News anchors this morning reported that sources had said it was likely a Chinese effort to cripple the Pentagon’s computer system between now and the inauguration. No other major news outlets are reporting this story at this time.

In the meantime, here are a few readings on the shady (and apparently, based on the sparse information available online, little understood) world of Chinese hackers—who may or may not be funded by the Chinese government.

*An excerpt from the *Newsweek* piece:*

In midsummer, the Obama campaign’s computers were attacked by a virus. The campaign’s tech experts spotted it and took standard precautions, such as putting in a firewall. At first, the campaign figured it was a routine "phishing" attack, using common methods. Or so it seemed. In fact, the campaign had been the target of sophisticated foreign cyber-espionage.

The next day, the Obama headquarters had two visitors: from the FBI and the Secret Service. "You have a problem way bigger than what you understand," said an FBI agent. "You have been compromised, and a serious amount of files have been loaded off your system." ...

By late afternoon the campaign’s chief technology officer, Michael Slaby, was on the phone with the FBI field agent who was running the investigation out of Los Angeles. Slaby was told that the hackers had been moving documents out of Obama’s system at a rapid rate. Potentially, Obama’s entire computer network had been compromised...

The Obama team was told that its system had been hacked by a "foreign entity." The official would not say which "foreign entity," but indicated that U.S. intelligence believed that both campaigns had been the target of political espionage by some country—or foreign organization—that wanted to look at the evolution of the Obama and McCain camps on policy issues, information that might be useful in any negotiations with a future Obama or McCain administration. There was no suggestion that terrorists were involved; technical experts hired by the Obama campaign speculated that the hackers were Russian or Chinese.

Speculations of Chinese hackers—possibly, some observers have guessed, supported by the Chinese government—have ranged this year from attacks on infrastructure to White House computers. There is little hard evidence available in the public realm to confirm any of these speculations.

*Here’s a back and forth about whether Chinese hackers were responsible for the major power outages in 2003 (the verdict seems to be "no"):*

*From “China’s Cyber Military” by Shane Harris at National Journal (from May 31, 2008):*

Officially, the blackout was attributed to a variety of factors, none of which involved foreign intervention. Investigators blamed “overgrown trees” that came into contact with strained high-voltage lines near facilities in Ohio owned by FirstEnergy Corp. More than 100 power plants were shut down during the cascading failure. A computer virus, then in wide circulation, disrupted the
communications lines that utility companies use to manage the power grid, and this exacerbated the problem. The blackout prompted President Bush to address the nation the day it happened. Power was mostly restored within 24 hours...

Brenner, who works for Director of National Intelligence Mike McConnell, looks for vulnerabilities in the government’s information networks. He pointed to China as a source of attacks against U.S. interests. “Some [attacks], we have high confidence, are coming from government-sponsored sites,” Brenner said. “The Chinese operate both through government agencies, as we do, but they also operate through sponsoring other organizations that are engaging in this kind of international hacking, whether or not under specific direction. It’s a kind of cyber-militia…. It’s coming in volumes that are just staggering.”

At the Wired blog “Threat Level,” Kevin Paulson called shenanigans:

Chinese hackers may have been responsible for the recent power outage in Florida, and the widespread blackout that struck the northeastern U.S. in 2003, according to a new report in the National Journal that shows the intelligence community taking cyberwar hysteria to new and dizzying heights...

It’s official: Cyberterror is the new yellowcake uranium.

Ever since intelligence chief Michael McConnell decided on cyberterrorism as the latest raison d’etre for warrantless NSA surveillance, we’ve seen increasingly brazen falsehoods and unverifiable cyberattack stories coming from him and his subordinates, from McConnell’s bogus claim that cyberattacks cost the U.S. economy $100 billion a year, to one intelligence official’s vague assertion that hackers have caused electrical blackouts in unnamed countries overseas.”

Earlier this month, Financial Times reported that Chinese hackers had breached the White House network:

“We are getting very targeted Chinese attacks so its stretches credulity that these are not directed by government-related organisations,” said the official.

The National Cyber Investigative Joint Task Force, a unit established in 2007 to tackle security, detected the attacks. The official stressed the hackers had accessed only the unclassified computer network, and not the more secure classified network.

“For a short period of time, they successfully breach a wall, and then you rebuild the wall . . . it is not as if they have continued access,” said the official. “It is constant cat and mouse on this stuff.”

The US has increased efforts to tackle cyber security in the past year, especially since Chinese hackers penetrated the Pentagon last year, in an attack that obtained e-mails from the system serving Robert Gates, the defence secretary.

And a Guardian report on a study released yesterday by the US-China economic and security review commission stresses the persistence and growth of cyber-attacks originating in China:

A summary of the study, released in advance, alleges that networks and databases used by the US government and American defence contractors are regularly targeted by Chinese hackers. “China is stealing vast amounts of sensitive information from US computer networks,” says Larry Wortzel, chairman of the commission set up by Congress in 2000 to investigate US-China issues.

The commission, consisting of six Democrats and six Republicans, says in its unanimous report that China’s military modernisation and its “impressive but disturbing” space and computer warfare capabilities “suggest China is intent on expanding its sphere of control even at the expense of its Asian neighbors and the United States.”
Finally, check out this CNN piece from earlier this year, which provides a sneak peek, albeit brief and not terribly informative, into the world of Chinese hackers:

They operate from a bare apartment on a Chinese island. They are intelligent 20-somethings who seem harmless. But they are hard-core hackers who claim to have gained access to the world’s most sensitive sites, including the Pentagon.

In fact, they say they are sometimes paid secretly by the Chinese government — a claim the Beijing government denies...

One hacker says he is a former computer operator in the People’s Liberation Army; another is a marketing graduate; and Xiao Chen says he is a self-taught programmer...

On camera, Xiao Chen denies knowing anyone who has targeted U.S. government Web sites. But off-camera, in conversations over three days, he claims two of his colleagues — not the ones with him in the room — hacked into the Pentagon and downloaded information, although he wouldn’t specify what was gleaned. CNN has no way to confirm if his claim is true.

Tags: cyber attacks, cyber terrorism, hacking, pentagon