The Washington Post

Chinese cyberspies have hacked Middle East experts at major U.S. think tanks

By: Andrea Peterson
July 7, 2014

Middle East experts at major U.S. think tanks were hacked by Chinese cyberspies in recent weeks as events in Iraq began to escalate, according to a cybersecurity firm that works with the institutions.

The group behind the breaches, called "DEEP PANDA" by security researchers, appears to be affiliated with the Chinese government, says Dmitri Alperovitch, chief technology officer of the firm CrowdStrike. The company, which works with a number of think tanks on a pro bono basis, declined to name which ones have been breached.

Alperovitch said the firm noticed a "radical" shift in DEEP PANDA's focus on June 18, the same day witnesses reported that Sunni extremists seized Iraq's largest oil refinery. The Chinese group has typically focused on senior individuals at think tanks who follow Asia, said Alperovitch. But last month, it suddenly began targeting people with ties to Iraq and Middle East issues.

This latest breach follows a pattern identified by experts of Chinese cyberspies targeting major Washington institutions, including think tanks and law firms. It's rarely clear why Chinese cyberspies hack specific American targets, but experts say there are a few clues to why the DEEP PANDA group may have been interested in Middle East experts at think tanks.

China's need for natural resources has skyrocketed along with its economic profile, and the country has increasingly turned to the Middle East to fuel its energy needs. China surpassed the U.S. as the world's largest net importer of petroleum and other liquid fuels last September, according to the US Energy Information Administration. In Iraq, China is a major oil investor.

"It wouldn't be surprising if the Chinese government is highly interested in getting a better sense of the possibility of deeper U.S. military involvement that could help protect the Chinese oil infrastructure in Iraq," wrote Alperovitch in a company blog post.

Experts say that breaking into organizations like think tanks can give adversaries access to sensitive communications about international strategy – and potentially allow them to use compromised e-mail accounts to get at other targets: A phishing message coming from a trusted

acquaintance at a prominent think tank that asks a user to download an attachment is more likely to succeed than a seemingly random e-mail.

"If you can go after these indirect targets that have some of the information or you can see who they are communicating with you build up a lot of intelligence," explains Benjamin Johnson a former National Security Agency employee who now works at cybersecurity firm Bit9.

The troubling implication of this is that pretty much everyone is a target, he says. "If you have a relationship with anyone who has something valuable in terms of information, you yourself are a target because it might be easier for them to go after you than the target directly," Johnson explains.

"It's similar to when companies are trying to do a merger, and an adversary might go after their law firm or accounting firm where a lot of information might be stored," he added.

Experts say Chinese interest in U.S. think tanks is part of a larger information gathering strategy aimed at understanding how Washington works. Chinese officials often assume that think tanks and news outlets are being influenced by the U.S. government as their Chinese counterparts are by Beijing, these experts say.

"The Chinese think that American think tanks are like Chinese think tanks," says James Lewis at the Center for Strategic and International Studies, which has been hacked before. In the midst of the most recent campaign, CSIS staff received an e-mail warning them of phishing attacks, he said.

"The downside is that they're going to read this stuff and be confused -- then quite possibly come to the wrong conclusions," Lewis explains.

Alperovitch says the digital signatures of the group behind the attack, called "DEEP PANDA" by security researchers, indicate it is affiliated with the Chinese government. "We have attribution details leading us to believe it is operating out of mainland China and traditionally goes after things of interest to Chinese state-owned enterprises and foreign relations information relevant to the Chinese government."

But despite the rise in attacks on think tanks, Richard Bejtlich, Chief Security Strategist at FireEye and a nonresident senior fellow at the Brookings Institution, says he hasn't seen a lot of major changes in how think tanks respond to security breaches -- partially because of the very significant price tag associated with a professional cybersecurity force.

"You don't tend to see an significant IT department or a large security department," said Bejtlich. "It takes a very high investment to resist a state sponsored group trying to get into your systems." And it's harder to get researchers at think tanks to adhere to stricter security measures at a think tank, he says, because the environment can be more like a university than some place with stricter security needs like a financial institution.

“A lot of think tanks don’t realize how how lucrative they are because they publish everything they work on,” Alperovitch explains, "but fellows working for them often have close connections with government officials."

Even after increased awareness of the issue among organizations following widely publicized breaches in recent years, many non-profit think tanks do not have the resources to fend off cyberattacks, according to experts.

DEEP PANDA's cyberattacks are notable for their extreme stealth, according to Alperovitch. "The group leverages existing tools on the system and very rarely brings in malicious tools that might be noticed by administrators of that network." Instead, the hackers set up scripts that use existing Windows tools to operate malicious programs that run only in memory -- making them almost impossible to detect using traditional forensic methods.

"These are well-funded, motivated teams that are doing whatever they can to get all this information," he warns.

The Washington Post contacted a number of think tanks in Washington regarding the breaches; most declined to comment directly on whether they had been hacked.

“The Council’s IT architecture is a priority and we continue to do all we can to reduce our vulnerability," a Council on Foreign Relations spokesperson told the Post in a statement. "We will not comment on reports of specific incidents.”

"Brookings takes security extremely seriously, and we constantly monitor the evolving technology landscape to ensure our systems are as secure as possible," said Brookings Chief Information Officer Helen Mohrmann in a statement.

A Cato employee who asked to remain anonymous because he was not authorized to speak on the record acknowledged the organization was probably being targeted, but had not yet identified any breaches. "We have been beefing up security because we are aware of the interest in think tanks and are always mindful of the possibility," he said.

In May, the U.S. government indicted five Chinese military employees on charges related to commercial cyberspying -- accusing them of stealing trade secrets and strategic business intelligence from leading steel, nuclear plant and solar power firms.

The Chinese government denied the allegations, calling them based on "fabricated facts" and has consistently disputed that it is engaging in the type of cyber-espionage campaigns that security researchers have identified.

Whether going after private enterprises, non-profits, or government targets, Chinese hacker groups generally cast wide collection nets, according to Johnson. "Sometimes it's hard to say exactly what they're after because it seems like everything of value is on the table," he says. "You name it, they're going after it."