The Washington Post

National Security

Chinese government has arrested hackers it says breached OPM database

By Ellen Nakashima December 2 at 1:52 PM

The Chinese government recently arrested a handful of hackers it says were connected to the breach of Office of Personnel Management's database this year, a mammoth break-in that exposed the records of more than 22 million current and former federal employees.

The arrests took place shortly before a state visit in September by President Xi Jinping, and U.S. officials say they appear to have been carried out in an effort to lessen tensions with Washington.

The identities of the suspects — and whether they have any connection to the Chinese government — remain unclear.

Hacks of government and corporate data emanating from China have been a constant source of tension between the United States and China. This week, Attorney General Loretta Lynch and Homeland Security Secretary Jeh Johnson will be meeting with senior Chinese officials to try to establish guidelines for working together on law enforcement requests to investigate cyberattacks. The OPM hack — which came in two waves — was also on the agenda.

If the individuals detained were indeed the hackers, the arrests would mark the first measure of accountability for what has been characterized as one of the most devastating breaches of U.S. government data in history.

But officials said it has been difficult to confirm whether the people rounded up were connected to the OPM breach.

"We don't know that if the arrests the Chinese purported to have made are the guilty parties," said one U.S. official who — like others interviewed — spoke on condition of anonymity because of the subject's sensitivity. "There is a history [in China] of people being arrested for things they didn't do or other 'crimes against the state.' "

Since the intrusions were first disclosed in June, U.S. government officials have said they suspected the Chinese government's involvement, in particular the civilian Ministry of State Security.

Some officials say the hackers may have been MSS contractors who possibly acted on their own but knew the agency would be interested in the data.

Chinese officials have characterized the arrests as a criminal matter, rather than state-sponsored, and told their American counterparts that the individuals will be prosecuted, said U.S. officials, who spoke on the condition of anonymity.

Beijing has repeatedly insisted that the government played no role in the intrusions, which compromised sensitive personal, financial and biometric data of the employees, as well as data on their family members.

The Washington Post previously reported the arrests were linked to thefts of data from U.S. companies to be sold or passed to Chinese state-run firms. Rather, they were linked to the OPM breach.

In the weeks before the summit with Xi, Chinese officials learned from media reports that the Obama administration was preparing a package of economic sanctions against Chinese firms that benefited from the hacking of U.S. companies.

Xi's special envoy, Meng Jianzhu, a member of the political bureau of the Communist Party Central Committee, soon arrived in Washington to meet with U.S. officials who said he appeared distressed by the possibility of sanctions. The officials said Meng seemed to think the Americans were primarily concerned about the OPM hack, rather than cyberattacks of U.S. firms. He asserted that the Chinese government had not directed the breach and pledged to round up the hackers behind the OPM attack.

U.S. officials have characterized the OPM breaches as traditional espionage — spying to help a foreign government, in this case, build databases on U.S. government employees and officials. Experts say that such information can help foreign governments recruit spies or blackmail employees for information. Or it might help them craft more effective "spearphish" emails purporting to be from colleagues or family members that contain malicious software that when activated can compromise a computer.

If China caught the real perpetrators, "it would be the most important arrest that we've perhaps seen in cybercrime," said Jason Healey, senior research scholar at Columbia University School of International Public Affairs.

The news comes on the heels of other breakthroughs. At the summit, Xi made a historic pledge that China would not conduct economic espionage in cyberspace. Up to that point, the Chinese government had never acknowledged conducting such espionage, which is focused on targeting companies rather than governments.

Then, two weeks ago, Xi repeated that commitment to 19 heads of state at the Group of 20 conference in Antalya, Turkey. At the G20, all the leaders pledged for the first time their states would not engage in cyber-industrial espionage.

"The last two months have been nothing but shocks," Healey said. "Who would have thought that we would have gone from no norm on commercial espionage and no movement on the OPM hack to a new G20 norm and today's news of criminal arrests on OPM? This is a string of incredible diplomatic successes."Officials and analysts say that a combination of factors have led to China's change in behavior. The threat of economic sanctions was key. And so were last year's indictments of five People's Liberation Army officers on charges of cyber-economic spying.

Following the indictments, the PLA ratcheted down its hacking of U.S. companies, although MSS activity continued or picked up, officials and analysts said. The Chinese were smarting from the indictments, officials said, and brought them up in every meeting.

"I think that China has realized that this is an issue that really matters to the United States, and that if they're going to continue to manage the relationship with us in a positive way, they had to figure out some way to address our concerns," a U.S. official said.

When asked Wednesday whether the Chinese government had in fact arrested suspects connected to the OPM breach, White House press secretary Josh Earnest declined to comment on the issue, but said that Obama met with Xi in Paris and raised the issue of cybersecurity.

"This continues to be a top priority of President Obama in terms our relationship with China," Earnest said.

David Nakamura contributed to this report.

Ellen Nakashima is a national security reporter for The Washington Post. She focuses on issues relating to intelligence, technology and civil liberties.

Congress to lift funding ban on gun violence research

Preliminary reports from the San Bernardino police chief: 14 dead and 17 wounded.

Mysterious ‘ghost ships’ keep washing up in Japan with bodies on board

Like something out of a nightmare, the boats show up barnacle encrusted and carrying only the skeletons of their former crew. Experts believe the victims are North Koreans who got stranded somehow at sea.

Your Three.
Video curated for you.

It's in the details: Five ways to enhance your kitchen makeover

In search of the Delmarva fox squirrel

0:00

Why seasonal allergies make you miserable

1:21

Show Me More