6-The Guardian-OPM

Fri 5 Jun 2015 04.16 EDT

First published on Thu 4 Jun 2015 17.43 EDT

The Obama administration is scrambling to assess the impact of a massive data breach involving the agency that handles security clearances and US government employee records, with suspicion quickly falling on China, which has been accused of carrying out cyber-espionage against the US in the past.

Government officials familiar with the situation told the Associated Press the hack occurred at the Office of Personnel Management (OPM) and the Interior Department, and could potentially affect four million people at every federal agency.

The OPM is the human resources department for the federal government and does checks for security clearances.

A US law enforcement source told the Reuters news agency on Thursday night that a “foreign entity or government” was believed to be behind the attack. Authorities were looking into a possible Chinese connection, the news agency said, quoting a source close to the matter.

Chinese officials issued swift denials, with foreign ministry spokesman Hong Lei branding the accusations irresponsible and unscientific at a news briefing on Friday. “We know that hacker attacks are conducted anonymously, across nations, and that it is hard to track the source,” Hong said. “It’s irresponsible and unscientific to make conjectural, trumped-up allegations without deep investigation.”

“The FBI is conducting an investigation to identify how and why this occurred,” the department of homeland security said in a statement on Thursday. *[Rebuild]* “DHS is continuing to monitor federal networks for any suspicious activity and is working aggressively with the affected

agencies to conduct investigative analysis to assess the extent of this alleged intrusion." *[Rebuild]*

Reports in the New York Times and Washington Post on Thursday, both citing unnamed sources in the federal government, reported Chinese hackers were behind the breach.

Senator Susan Collins, a Maine Republican, said the hackers were believed to be based in China.

Collins, a member of the Senate intelligence committee, said the breach was "yet another indication of a foreign power probing successfully and focusing on what appears to be data that would identify people with security clearances".

The Chinese embassy in Washington responded that jumping to conclusions was "not responsible" and "counterproductive".

Embassy spokesman Zhu Haiquan said China had made great efforts to combat cyberattacks and that tracking such events conducted across borders was difficult.

A Pentagon report in April said hackers associated with the Chinese government repeatedly targeted US military networks seeking intelligence during 2014.

US Representative Adam Schiff, the ranking Democrat on the House select intelligence committee, said: "The last few months have seen a series of massive data breaches that have affected millions of Americans.

He called the latest intrusion "among the most shocking because Americans may expect that federal computer networks are maintained with state-of-the-art defences" *[Disappointment]*.

"It's clear that a substantial improvement in our cyber databases and defences is perilously overdue," Schiff said. *[Disappointment]*

Senate intelligence committee chairman Richard Burr said the government must overhaul its cybersecurity defenses. "Our response to these attacks can no longer simply be notifying people after their personal information has been stolen," he said. "We must start to prevent these breaches in the first place." *[Anger]*

The largest federal employee union, the AFGE, said it would "demand accountability". *[Anger]* The union's president, J David Cox, said it was working with the administration to ensure measures were taken to secure the personal information of affected employees.

In November a former DHS contractor disclosed another cyber-breach that compromised the private files of more than 25,000 DHS workers and thousands of other federal employees.

DHS said its intrusion detection system, known as Einstein, which screens federal internet traffic to identify potential cyber threats, identified the hack of OPM's systems and the Interior Department's data centre, which is shared by other federal agencies.

"DHS is continuing to monitor federal networks for any suspicious activity and is working aggressively with the affected agencies to conduct investigative analysis to assess the extent of this alleged intrusion," the statement said.

Members of Congress were briefed on the breach on Thursday.

The hack follows an attack on the Internal Revenue Service (IRS) that compromised the details of 100,000 taxpayers. On Wednesday the IRS commissioner John Koskinen appeared before a Senate committee and blamed the attack on underfunding and the agency's inability to keep up with increasingly sophisticated threats.

"This incident provides a stark reminder that even security controls that may have been adequate in the past can be overcome by hackers, who are anonymous, persistent and have access to vast amounts of personal data and knowledge," J Russell George, treasury inspector general for tax administration, told the Senate finance committee.

Ken Ammon, chief strategy officer at Xceedium, a government security contractor that specialises in securing privileged access to systems, said: “What we are seeing across the board is a particular weakness in our defence systems.”

Ammon said sophisticated hacking operations funded by nation states were targeting system administrators and gaining access to massive amounts of data. “What you want to be able to do is cut your loses, make sure the attack is isolated to that particular individual and not the terabytes of information stored on the servers.”

In April Barack Obama responded to a growing rash of attacks aimed at US computer networks by launching a sanctions program to target individuals and groups outside the United States that use cyber attacks to threaten US foreign policy, national security or economic stability.

The move followed indictments of five Chinese military officers who were charged with economic espionage. US officials also pointed the finger directly at North Korea for a high-profile attack on Sony over a film spoof depicting the assassination of North Korea’s leader.

China has routinely denied accusations by US investigators that hackers backed by the Chinese government have been behind attacks on US companies and federal agencies.

Obama has moved cybersecurity toward the top of his 2015 agenda after recent breaches and the White House *[Rebuild]*says he raises the issue in meetings with Chinese President Xi Jinping. US military officials have become increasingly vocal about cyber espionage and attacks launched by China, Russia and others.

In unveiling an updated cyber strategy in May, the US defense secretary, Ash Carter, singled out threats from Russia, China, Iran and North Korea and stressed the military’s ability to retaliate with cyber weapons.

The Associated Press and Reuters contributed to this report

Topics