THE WALL STREET JOURNAL.

http://www.wsj.com/articles/u-s-suspects-hackers-in-china-behind-government-data-breach-sources-say-1433451888

U.S.

U.S. Suspects Hackers in China Breached About 4 Million People's Records, Officials Say

Described as one of the largest thefts of government data ever seen

By **DEVLIN BARRETT**, **DANNY YADRON** and **DAMIAN PALETTA**
Updated June 5, 2015 6:33 a.m. ET

U.S. officials suspect that hackers in China stole the personal records of as many as four million people in one of the most far-reaching breaches of government computers.

The Federal Bureau of Investigation is probing the breach, detected in April at the Office of Personnel Management. The agency essentially functions as the federal government's human resources department, managing background checks, pension payments and job training across dozens of federal agencies.

Investigators suspect that hackers based in China are responsible for the attack, though the probe is continuing, according to people familiar with the matter. On Thursday, several U.S. officials described the breach as among the largest known thefts of government data in history.

It isn't clear exactly what was stolen in the hack attack, but officials said the information can be used to facilitate identity theft or fraud. The Department of

READ MORE ON CAPITAL JOURNAL »

- What Does Breach Mean for Cyber Bill? (http://www.wsj.com/articles/what-does-breach-mean-for-cyber-bill-1433458572?mod=capitaljournalrelatedbox)

Homeland Security said it "concluded at the beginning of May" that the records had been taken.

At a Chinese Foreign Ministry briefing on Friday, ministry spokesman Hong Lei said, "Cyberattacks are anonymous, cross-border and hard to trace. If you keep using the words "maybe" or "perhaps" without making a thorough study, this is irresponsible and unscientific." He said China opposes all forms of cyberattacks. "We hope the U.S. side will shed its suspicions."

In response to previous allegations of Chinese hacking and cyber-espionage, Beijing has said that China is also a target of hacking attacks from overseas.

China and the U.S. have sparred over cybersecurity, with the U.S. accusing Chinese government military officers of sustained hacking of U.S. firms for economic advantage. Chinese authorities have denied those accusations.

Investigators believe the attack is separate from a hacking incident detected last year at the Office of Personnel Management. That attack was far smaller, although officials didn't disclose at the time how many employees were affected. In another apparently unrelated computer attack, Russian hackers are suspected in a large, long-running breach of State Department computers.

In February, The Wall Street Journal reported that the State Department had been unable to evict suspected Russian hackers from its unclassified email system despite months of effort and help from spies and private companies.

The breach disclosed Thursday is the latest sign of the U.S. government's struggles to protect its own data, even though the Obama administration has spent much of the past year pushing companies to do a better job protecting their computer networks and sharing crucial intelligence on cyber weapons.

Last week, the Internal Revenue Service said identity thieves illegally obtained prior-year tax-return data for more than 100,000 households from an agency website. The criminals used personal data obtained elsewhere to gain access to the tax-return data, the IRS said. The return data can help in filing false refund claims.

The FBI said the agency is working with other parts of the government to investigate a breach of data held by the Office of Personnel Management. *PHOTO: JAMES LAWLER DUGGAN/REUTERS*

The IRS is working on an agreement with tax-preparation firms on ways to strengthen security of the tax system.

The data breach at the Office of Personnel Management is smaller as measured by the number of people affected than some so-called mega breaches in the private sector.

Health insurer Anthem Inc. said earlier this year that hackers gained access to personal information on as many as 80 million customers. Home Depot Inc. said last year that 56 million cards might have been compromised in a five-month attack on its payment terminals.

The Office of Personnel Management hasn't said how many of the four million people affected by its latest breach are current or former employees or government contractors.

The agency has estimated that there are about 4.2 million federal employees, including 1.5 million who serve as uniformed military personnel.

"We take very seriously our responsibility to secure the information stored in our systems, and in coordination with our agency partners, our experienced team is constantly identifying opportunities to further protect the data with which we are entrusted," said Katherine Archuleta, director of the Office of Personnel Management.

The Department of Homeland Security said it detected the huge breach partly through the use of a system known as Einstein. The agency described Einstein as "an intrusion detection and prevention system that screens federal Internet traffic to identify

potential cyber threats."

Einstein located the breach on the Department of the Interior's data center, which is used by multiple U.S. agencies.

The Office of Personnel Management previously told more than 48,000 people that their personal data might have been taken in a hack at KeyPoint Government Solutions, which does background checks for security clearances.

Rep. Adam Schiff of California, the ranking Democrat on the House Permanent Select Committee on Intelligence, said the breach disclosed Thursday is "among the most shocking because Americans may expect that federal computer networks are maintained with state of the art defenses."

An FBI spokesman said the agency "will continue to investigate and hold accountable those who pose a threat in cyberspace."

Office of Personnel Management officials said they were taking a number of steps to beef up their network security and help affected employees.

The agency is restricting the number of federal employees who can access government networks remotely and deploying new anti-malware software.

The Office of Personnel Management also will also send notifications to the roughly four million people whose personally identifiable information might have been compromised.

The agency cautioned that the number of affected individuals could grow and said it would offer credit-report data, credit monitoring and identity-theft insurance to affected employees.

It also urged employees to be vigilant and look for any suspicious activity in their bank accounts or financial statements that could indicate possible identity theft.

Federal officials and private investigators at FireEye Inc., a Silicon Valley security company that investigated several health-care breaches, have said they are confident that China's state-backed hacking units are behind the theft of large data files on millions of Americans. Investigators have linked the thefts to China through circumstantial evidence such as the type of hacking tools and Internet Protocol addresses tied to intruders.

But the stolen information apparently hasn't shown up on the digital black market, where criminals buy and sell credit- card and Social Security numbers.

Researchers from another security company, iSight Partners Inc., are investigating possible links between the Office of Personnel Management incident and some of the recent health care breaches, including Anthem Inc. and Premera Blue Cross, said John Hultquist, an iSight senior manager. Mr. Hultquist said he sees some similarities in the registration records for the phony Web addresses used to trick employees at the three organizations to let hackers inside the systems.

Write to Devlin Barrett at devlin.barrett@wsj.com, Danny Yadron at danny.yadron@wsj.com and Damian Paletta at damian.paletta@wsj.com