The Washington Post

NOT NOW ✖

Get the Checkpoint Newsletter

Free twice-weekly updates delivered just for you.

National Security

Chinese breach data of 4 million federal workers

By Ellen Nakashima June 4 at 11:11 PM

Hackers working for the Chinese state breached the computer system of the Office of Personnel Management in December, U.S. officials said Thursday, and the agency will notify about 4 million current and former federal employees that their personal data may have been compromised.

The hack was the largest breach of federal employee data in recent years. It was the second major intrusion of the same agency by China in less than a year and the second significant foreign breach into U.S. government networks in recent months.Last year, Russia compromised White House and State Department e-mail systems in a campaign of cyberespionage.

[What to do if your information was stolen]

The OPM, using new tools, discovered the breach in April, according to officials at the agency who declined to discuss who was behind the hack.

Other U.S. officials, who spoke on the condition of anonymity, citing the ongoing investigation, identified the hackers as being state-sponsored.

One private security firm, iSight Partners, says it has linked the OPM intrusion to the same cyberespionage group that hacked the health insurance giant Anthem. The FBI suspects that that intrusion, announced in February, was also the work of Chinese hackers, people close to the investigation have said.

The intruders in the OPM case gained access to information that included employees' Social Security numbers, job assignments, performance ratings and training information, agency officials said. OPM officials declined to comment on whether payroll data was exposed other than to say that no direct-deposit information was compromised. They could not say for certain what data was taken, only what the hackers gained access to.

[China calls the accusation 'irresponsible and unscientific']

"Certainly, OPM is a high-value target," Donna Seymour, the agency's chief information officer, said in an interview. "We have a lot of information about people, and that is something that our adversaries want."

The personal information exposed could be useful in crafting "spear-phishing" e-mails, which are designed to fool recipients into opening a link or an attachment so that the hacker can gain access to computer systems. Using the stolen OPM data, for instance, a hacker might send a fake e-mail purporting to be from a colleague at work.

After the earlier breach discovered in March 2014, the OPM undertook "an aggressive effort to update our cybersecurity posture, adding numerous tools and capabilities to our networks," Seymour said. "As a result of adding these tools, we were able to detect this intrusion into our networks."

"Protecting our federal employee data from malicious cyber incidents is of the highest priority at OPM," Director Katherine Archuleta said in a statement.

In the current incident, the hackers targeted an OPM data center housed at the Interior Department. The database did not contain information on background investigations or employees applying for security clearances, officials said.

By contrast, in March 2014, OPM officials discovered that hackers had breached an OPM system that manages sensitive data on federal employees applying for clearances. That often includes financial data, information about family and other sensitive details. That breach, too, was attributed to China, other officials said. OPM officials declined to comment on whether the data affected in this incident was encrypted or had sensitive details masked. They said it appeared that the intruders are no longer in the system.

"There is no current activity," an official said. But Chinese hackers frequently try repeat intrusions.

[The real story of how the Internet became so vulnerable]

Seymour said the agency is working to better protect the data stored in its servers throughout the government, including by using data masking or redaction. "We've purchased tools to be able to implement that capability for all" the data, she said.

Among the steps taken to protect the network, the OPM restricted remote access to the network by system administrators, officials said. When the OPM discovered the breach, it notified the FBI and the Department of

Homeland Security.

A senior DHS official, who spoke on the condition of anonymity because of the ongoing investigation, said the "good news" is that the OPM discovered the breach using the new tools. "These things are going to keep happening, and we're going to see more and more because our detection techniques are improving," the official said.

estigate the incident.
ue to investigate and
hold accountable those who pose a threat in cyberspace," he said.

The intruders used a "zero-day" — a previously unknown cyber-tool — to take advantage of a vulnerability that allowed the intruders to gain access into the system.

[*Why the Internet's massive flaws may never get fixed*]

China is one of the most aggressive nations targeting U.S. and other Western states' networks. In May 2014, the United States announced the indictments of five Chinese military officials for economic cyberespionage — hacking into the computers of major steel and other companies and stealing plans, sensitive negotiating details and other information.

"China is everywhere," said Austin Berglas, head of cyber investigations at K2 Intelligence and a former top cyber official at the FBI's New York field office. "They're looking to gain social and economic and political advantage over the United States in any way they can. The easiest way to do that is through theft of intellectual property and theft of sensitive information."

Rep. Adam B. Schiff (Calif.), ranking Democrat on the House Intelligence Committee, said the past few months have seen a massive series of data breaches affecting millions of Americans.

"This latest intrusion . . . is among the most shocking because Americans may expect that federal computer networks are maintained with state-of-the-art defenses," he said. "The cyberthreat from hackers, criminals, terrorists and state actors is one of the greatest challenges we face on a daily basis, and it's clear that a substantial improvement in our cyber databases and defenses is perilously overdue."

Colleen M. Kelley, president of the nation's second-largest federal worker union, the National Treasury Employees Union, said her organization "is very concerned" about the breach. "Data security, particularly in an era of rising incidence of identity theft, is a critically important matter," she said.

"It is vital to know as soon as possible the extent to which, if any, personal information may have been obtained so that affected employees can be notified promptly and encouraged to take all possible steps to protect themselves from financial or other risks," she said.

Lisa Rein 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.