After hacking, government workers warned of potential fraud

5 June 2015, byTed Bridis, Ken Dilanian And Eric Tucker

The Homeland Security Department headquarters in northwest Washington, Friday, June 5, 2015. China-based hackers are suspected once again of breaking into U.S. government computer networks, and the entire federal workforce could be at risk this time. The Department of Homeland Security said in a statement that data from the Office of Personnel Management—the human resources department for the federal government—and the Interior Department had been compromised. (AP Photo/Susan Walsh)

An immense hack of millions of government personnel files is being treated as the work of foreign spies who could use the information to fake their way into more-secure computers and plunder U.S. secrets.

Federal employees were told in a video Friday to change all their passwords, put fraud alerts on their credit reports and watch for attempts by foreign intelligence services to exploit them. That message came from Dan Payne, a senior counterintelligence official for the Director of National Intelligence.

"Some of you may think that you are not of interest because you don't have access to classified information," he said. "You are mistaken."

Federal officials said Friday the cyberattack appeared to have originated in China, but they didn't point fingers directly at the Chinese government. The Chinese said any such accusation would be "irresponsible and unscientific."

"We know that the attack occurred from somewhere in China, but we don't know whether it was an individual or a group or a nation-state attack," said Rep. Jim Langevin, a Democrat and leading voice in Congress on cybersecurity. He added, though that it had "all the hallmarks of a nation-state attack."

White House spokesman Josh Earnest said he could not divulge much while the case was under investigation. Still, he noted that investigators "are aware of the threat that is emanating from China."

One U.S. official said the breach of data involving more than 4 million past and present federal workers was being investigated as a national security matter. That suggests authorities believe a nation was behind it rather than a more loosely organized gang of cybercriminals. The official was not authorized to discuss an ongoing investigation and spoke only on condition of anonymity.

The breach was an embarrassing showing for the U.S. government's vaunted computer-defense system for civilian agencies—dubbed "Einstein"—which is costing $376 million this year alone. It's supposed to detect unusual Internet traffic that might reflect hacking attempts or stolen data being transmitted outside the government.

A wide range of information is prized by spies—classified military secrets but also economic strategy and internal foreign policy debates.

This latest breach occurred in December but wasn't discovered until April, officials say. It was made public Thursday.

"The scale of it is just staggering," said Rep. Adam Schiff, top Democrat on the House Intelligence Committee. There's no telling how many more attacks could be spawned by the information stolen in this case, he said.

White House press secretary Josh Earnest speaks about the Chinese hack of the computer system of the Office of Personnel Management, Friday, June 5, 2015, during the daily press briefing at the White House in Washington. (AP Photo/Evan Vucci)

Although most Americans think of identity thieves stealing from credit card or bank accounts, the information about civilian federal workers has other value for spies.

"They're able to identify people who are in positions with access to significant national security information and can use personal data to target those individuals," said Payne, the counterintelligence official.

He said details from personnel files could be used to craft personalized phony messages to trick workers. Federal employees who think they're opening an email from co-workers or family members might infect their computers with a program that would steal more information or install spy software.

Spies also could use details about an employee's interests or background to befriend them and try to manipulate them into revealing secrets.

Kevin Mitnick, a former hacker who now runs Mitnick Security Consulting of Las Vegas, called confidential details about federal employees "a gold mine."

"What's the weakest link in security?" Mitnick said. "The human. Now you know all about your target."

The hackers may have made off with even more information about workers who undergo security clearance background checks. That information includes the names of family, neighbors, even old bosses and teachers, as well as reports on vices, arrests and foreign contacts.

However, OPM spokesman Samuel Schumach said there was no evidence to suggest that security clearance information collected by OPM was compromised. It's stored separately from routine personnel files, he said.

"The kind of data that may have been compromised in this incident could include name, Social Security Number, date and place of birth, job assignments, training files, performance ratings and current and former addresses," Schumach said in an email.

The breach occurred at a network maintained by the Department of Interior, which also houses the personnel agency's files. Schumach said agencies share computer systems partly to save money—and it's also supposed to strengthen security.

Security experts said the hackers may have gone after the personnel agency because it's an easier target than the Pentagon or National Security Agency.

Private cybersecurity researchers said they believe the personnel agency was targeted by the same hackers who got into the Anthem and Primera health insurance groups last year.

John Hultquist, head of cyberespionage intelligence at iSight, said the Dallas-based security firm had found evidence linking the insurance and government attacks, but declined to say whom they suspect. "We think they are creating a database

they can leverage for follow-on espionage," Hultquist said.

A spokesman for the Director of National Intelligence declined to discuss whether there was evidence against China or whether intelligence agency employees were among those whose information was compromised.

U.S. investigators have improved their ability to attribute cyberattacks in recent years, officials said, and Chinese attacks often have identifiable signatures.

The Homeland Security Department noted that the Einstein defenses were just one part of the government's cybersecurity, and said it was used to confirm the breach. But that's like a smoke alarm sounding after the house burned down.

Einstein also helped understand how the break-in happened and protect against a repeat of a similar attempt.

"It didn't fare so well," said James Lewis, a leading cybersecurity expert at the Center for Strategic and International Studies, a Washington think-tank. "It's only a victory if you defeat the opponent, and we didn't."

APA citation: After hacking, government workers warned of potential fraud (2015, June 5) retrieved 28 November 2022 from https://phys.org/news/2015-06-giant-hack-pursuit-bigger-secrets.html