Union says all federal workers fell victim to hackers

June 11 2015, byKen Dilanian

In this June 5, 2015, file photo, a gate leading to the Homeland Security Department headquarters in northwest Washington. Hackers stole personnel data and Social Security numbers for every federal employee, a government worker union said Thursday, June 11, 2015, charging that the cyberattack on U.S. employee data is far worse than the Obama administration has acknowledged. (AP Photo/Susan Walsh, File)

A major union says the cyber theft of employee information is more damaging than it first appeared, asserting that hackers stole personnel

data and Social Security numbers for 4 million current and former federal workers .

The Obama administration had acknowledged that up to 4 million current and former employees whose information resides in the Office of Personnel Management server are affected by the December cyber breach, but it had been vague about exactly what was taken.

But J. David Cox, president of the American Federation of Government Employees, said in a letter Thursday to OPM director Katherine Archuleta that based on incomplete information OPM provided to the union, "we believe that the Central Personnel Data File was the targeted database, and that the hackers are now in possession of all personnel data for every federal employee, every federal retiree, and up to 1 million former federal employees."

The OPM data file contains the records of non-military, non-intelligence executive branch employees, which cover most federal civilian employees but not members of Congress and their staffs, members of the military or the intelligence agencies.

The union believes the hackers stole military records and veterans' status information, address, birth date, job and pay history, health insurance, life insurance, and pension information; and age, gender and race data, he said.

Also Thursday, Sen. Harry Reid of Nevada, the Democratic Senate leader, said that the hack was carried out by "the Chinese" without specifying whether he meant the Chinese government or individuals. Reid is one of eight lawmakers briefed on the most secret intelligence information. U.S. officials have declined to publicly blame China, which has denied involvement.

The union, which does not have direct access to the investigation, said it is basing its assessment on "sketchy" information provided by OPM. The agency has sought to downplay the damage, saying what was taken "could include" personnel file information such as Social Security numbers and birth dates.

"We believe that Social Security numbers were not encrypted, a cybersecurity failure that is absolutely indefensible and outrageous," Cox said in the letter. The union called the breach "an abysmal failure on the part of the agency to guard data that has been entrusted to it by the federal workforce."

Samuel Schumach, an OPM spokesman, said that "for security reasons, we will not discuss specifics of the information that might have been compromised."

Schumach did, however, address Cox's comment on encryption. "Though data encryption is a valuable protection method, today's adversaries are sophisticated enough that encryption alone does not guarantee protection," he said. "OPM does utilize encryption in some instances and is currently increasing the types of methods utilized to encrypt data."

The central personnel data file contains up to 780 separate pieces of information about an employee.

Cox complained in the letter that "very little substantive information has been shared with us, despite the fact that we represent more than 670,000 federal employees in departments and agencies throughout the executive branch."

The union's release and Reid's comment in the Senate put into sharper focus what is looking like a massive cyber espionage success by China.

Sen. Susan Collins, R-Maine, an Intelligence Committee member, has also said the hack came from China.

Mike Rogers, the former chairman of the House Intelligence Committee, said last week that Chinese intelligence agencies have for some time been seeking to assemble a database of information about Americans. Those personal details can be used for blackmail, or also to shape bogus emails designed to appear legitimate while injecting spyware on the networks of government agencies or businesses Chinese hackers are trying to penetrate.

U.S. intelligence officials say China, like the U.S., spies for national security advantage. Unlike the U.S., they say, China also engages in large-scale theft of corporate secrets for the benefit of state-sponsored enterprises that compete with Western companies. Nearly every major U.S. company has been hacked from China, they say.

The Office of Personnel Management is also a repository for extremely sensitive information assembled through background investigations of employees and contractors who hold security clearances. OPM's Schumach has said that there is "no evidence" that information was taken. But there is growing skepticism among intelligence agency employees and contractors about that claim.

In the Senate on Thursday, Democrats blocked a Republican effort to add a cybersecurity bill to a sweeping defense measure. The vote was 56-40, four votes short of the number necessary.

Democrats had warned of the dangers of cyberspying after the theft of government personnel files, but Democrats voted against moving ahead on the legislation, frustrated with the GOP-led effort to tie the two bills together. President Barack Obama has threatened to veto the defense legislation over budget changes by the GOP.

"The issue of cybersecurity is simply too important to be used as a political chit and tucked away in separate legislation." said Sen. Chris Coons, D-Del.

© 2015 The Associated Press. All rights reserved.

Citation: Union says all federal workers fell victim to hackers (2015, June 11) retrieved 28 April 2024 from https://phys.org/news/2015-06-union-hackers-personnel-federal-employee.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.