US wonders: Why stolen data on federal workers not for sale?

June 18 2015, byTed Bridis

In this June 16, 2015, photo, Office of Personnel Management (OPM) Director Katherine Archuleta testifies on Capitol Hill in Washington, before the before the House Oversight and Government Reform Committee hearing on the OPM data breach. The Obama administration is increasingly confident that China's government, not criminal hackers, was responsible for the extraordinary theft of personal information about as many as 14 million current and former federal employees and others, The Associated Press has learned. (AP Photo/Cliff Owen)

The Obama administration is increasingly confident that China's

government, not criminal hackers, was responsible for the extraordinary theft of personal information about as many as 14 million current and former federal employees and others, The Associated Press has learned. One sign: None of the data has been credibly offered for sale on underground markets popular among professional identity thieves.

Investigators inside U.S. intelligence and law enforcement agencies, using secret "beacons" employed across the Internet, have been monitoring data transmissions across overseas networks for the file properties associated with the American personnel records, and scouring communications among targeted foreign hackers for credible references to the theft, two people directly involved in the investigation said. They spoke on condition of anonymity because parts of the case and techniques being used are classified.

The investigation is being coordinated at the little-known National Cyber Investigative Joint Task Force, which is led by the FBI and includes 19 intelligence agencies and law enforcement, including the National Security Agency, CIA, Homeland Security Department, Secret Service and U.S. Cyber Command.

Investigators also have watched underground markets where identity thieves peddle information and found no trace of the data stolen from the U.S. Office of Personnel Management, they said. In the chessboard world of espionage, they also acknowledged that by revealing what they said was indirect evidence that spying was actually the motive, it might encourage Beijing's government to sell at least some of the data surreptitiously to implicate identity thieves in what would be a counter-counterintelligence false-flag operation.

China has openly denied involvement in the break-in, and the U.S. has publicly provided no direct evidence proving China was responsible.

The administration acknowledged earlier this month that hackers stole the personnel files and background investigations of current and former civilian, intelligence and military employees, contractors and even job applicants. Initially, the U.S. said the stolen data included Social Security numbers, birth dates, job actions and other private information for 4.2 million workers.

Days later, it acknowledged that the cyber spies obtained detailed background information on millions of military, intelligence and other personnel who have been investigated for security clearances. That information included details about drug use, criminal convictions, mental health issues and the names and addresses of relatives and any foreigners with whom they had contact.

White House spokesman Josh Earnest on Wednesday said President Barack Obama continues to have confidence in OPM's director, Katherine Archuleta.

Rep. Jason Chaffetz, R-Utah, head of the House Oversight and Government Reform Committee, and Rep. Jim Langevin, D-R.I., who is considered a leader in Congress on cybersecurity issues, urged her to resign. "I am deeply concerned by her refusal to acknowledge her culpability in the breach," Langevin said. "Ms. Archuleta should tender her resignation immediately."

A day earlier, Archuleta acknowledged to Congress "a high degree of confidence" that hackers stole information from background investigations for current, former and prospective federal employees_after her agency had downplayed that possibility. She said OPM had not encrypted the sensitive information because "an adversary possessing proper credentials can often decrypt data." She also said that some of OPM's systems were too old to support encryption.

But Richard "Dickie" George, who spent 41 years at the National Security Agency before retiring in 2011 as its top cyber security leader, called that "a false assertion," saying in an interview that the data could and should have been encrypted.

"That line is a giant red herring she threw out there to hide the blame," said George, a mathematician and cryptographer.

Data has been encrypted as far back as 1975, he said. Moreover, the security clearance data that was stolen "isn't being frequently accessed, so not an availability issue - just encrypt it and store it. Doesn't take a supercomputer to do that."

He added, "You could have decent access control that would limit access to that data base and the ability to decrypt it to a small group of people. They just don't know what they're doing."

Archuleta did not acknowledge in Tuesday's congressional hearing that China was believed to be responsible. She declined to estimate how many employees in the security clearance hack, telling lawmakers she would only discuss such subjects in a classified setting.

The two people who spoke to AP, and a third congressional aide familiar with the case who also spoke on condition of anonymity after classified briefings, said that as many as 14 million current and former employees were affected in both breaches.

"What's your best estimate? Is the 14 million number wrong or accurate?" Chaffetz asked Archuleta at the congressional hearing.

She answered: "We do not have an estimate because where this is an ongoing investigation."

The new disclosures bode poorly for U.S. efforts to quietly and quickly locate the stolen data—especially the detailed personal histories of millions of people with security clearances—on foreign computer servers and hack them to delete, encrypt or corrupt the material to render it useless. The administration has assessed that multiple backup copies have already been made with at least some stored on computers physically disconnected from any networks, the two people involved in the investigation told the AP.