abc NEWS

22 Million Affected by OPM Hack, Officials Say

Jul 9, 2015, 3:17 PM ET

By MIKE LEVINE and JACK DATE
Digital Journalist, Law Enforcement & Homeland Security

The U.S. agency burglarized by suspected Chinese hackers has completed its long-awaited damage assessment and more than 22 million people inside and outside government likely had their personal information stolen, officials announced today.

That number is more than five times larger than what the Office of Personnel Management announced a month ago when first acknowledging a major breach had occurred. At the time, OPM only disclosed that the personnel records of 4.2 million current and former federal employees had been compromised.

The extent of the hacking was first reported earlier today by ABC News.

Investigators ultimately determined that 19.7 million applicants for security clearances had their Social Security numbers and other personal information stolen and 1.8 million relatives and other associates also had information taken, according to OPM. That includes 3.6 million of the current and former government employees for a total of 22.1 million.

"If an individual underwent a background investigation through OPM in 2000 or afterwards ... it is highly likely that the individual is impacted by this cyber breach," OPM's statement said today.

Even before today's announcement, there was little doubt that the universe of victims was vastly larger because the hackers had access to far more than personnel records, including files associated with background investigations and information on government workers' families, sources said.

In fact, the hackers allegedly rummaged through various OPM databases for more than a year -- and lawmakers and U.S. officials alike have described the breach as a significant threat to national security.

"It is a huge deal," FBI Director James Comey told a Senate panel on Wednesday.

Since reports surfaced saying more than just personnel records were stolen, the Obama administration has publicly maintained the theft of background-investigation files was a "separate incident" still under investigation. Some U.S. officials and lawmakers believe that distinction -- encompassing the same cyber-campaign -- kept the full scope of the OPM breach hidden for weeks.

"I'm sure you will probably obfuscate, [but] when will the American people know ... the extent of this penetration?" Sen. John McCain, R-Arizona, asked OPM Director Katherine Archuleta at a hearing on Capitol Hill two weeks ago.

Despite mounting public pressure and push-back from top FBI officials during closed-door briefings, senior OPM officials continued to say they couldn’t offer even an estimate until they determined exactly how many people were affected by the "separate but related incident." As part of a "time-consuming analysis," investigators had to ensure they weren't double-counting people whose personal information may have been stored in more than one system breached, Archuleta said two weeks ago.

"Throughout this investigation, OPM has been committed to providing information in a timely, transparent and accurate manner," OPM said in a statement today.

U.S. intelligence and law enforcement officials are particularly concerned over the theft of forms known as SF-86s that current and prospective federal workers, including certain military personnel and even contractors, submit for security clearances. The forms require applicants to provide personal information not only about themselves but also relatives, friends, “associates” and foreign contacts spanning several years. The forms also ask applicants about past drug use, financial history, mental health history and personal relationships.

Such information could be exploited to pressure or trick employees and U.S. officials into further compromising their agencies, or they could provide ways for hackers to target people outside government, sources have told ABC News.

An OPM system known as "e-QIP" that allows applicants to submit SF-86s and other materials online remains suspended in the wake of the breach.

The attack on OPM began in late 2013, when hackers infiltrated the systems of a government contractor, KeyPoint Government Solutions, and stole the "credentials" of an employee, according to two days of testimony on Capitol Hill.

Sources suspect that was the start of an unprecedented cyber-campaign out of China to collect information on federal workers inside the United States and others around the world.

A major breach of OPM systems wasn't detected until April, after OPM began implementing new cyber-security measures. That led investigators to realize the files associated with background investigations had been taken.

OPM is now offering what it calls "a comprehensive suite of monitoring and protection services" to those impacted.

Editor’s Note: The story has been updated. A previous version stated that the total number of people affected was more than 25 million.

http://abcnews.go.com/US/exclusive-25-million-affected-opm-hack-sources/story?id=32332731