US data breach is intelligence coup for China

June 13 2015, by Rob Lever

The Theodore Roosevelt Federal Building that houses the Office of Personnel Management headquarters, pictured in Washington, DC, on June 5, 2015

The hacking of millions of US government employees is likely part of an effort by Chinese intelligence for long-term profiling—and possibly more nefarious things.

Security analysts say considerable evidence points to China, and that the

cyber-intrusion shows the long and patient efforts in Beijing to collect and compile data which may be useful in the future.

"It's normal for big intelligence agencies to create large biographic databases on their opponents," said James Lewis, a senior fellow at the Center for Strategic and International Studies, a Washington think tank.

Lewis said that while data on individuals may not seem significant on the surface, analysis of huge amounts of information can provide a strategic advantage.

"They get the same kinds of big data insights that companies use for targeted advertising," he told AFP.

Reports last week indicated some four million current or former government employees were hit, but a union letter said many more—every federal employee, every federal retiree, and up to one million former federal employees—could also have had personal data compromised.

These types of cyberattacks are troublesome because they involve stealth access that allows intruders to remain on computer networks for long periods of time, analysts say.

"It's the difference between a 'smash-and-grab' and a long-term persistent" operation, said Ryan Kazanciyan, chief security architect at Tanium, a California-based security firm.

"If you think about what you can do from the perspective of espionage instead of fraud, that data is incredibly valuable," Kazanciyan told AFP.

"If you want to target someone, this data can be used to conduct spearphishing, it can be used for blackmail."

Potentially, Kazanciyan said the database can be used to help determine the identities and locations of US undercover agents.

Spy recruiting tool

John Dickson, a former air force intelligence officer who is now a partner with the security firm Denim Group, said the database contains a trove of important information for a foreign intelligence service, including background checks from people with security clearances.

"This is valuable for an intelligence agency if they want to recruit someone" to spy, he said.

The entrance to the Theodore Roosevelt Federal Building that houses the Office of Personnel Management headquarters, pictured in Washington, DC, on June 5, 2015

"It has to be a nation-state. Nobody else would be interested in this information."

An analysis of the incident by the Virginia-based security firm ThreatConnect backs the theory that China was behind the breach.

"The primary motivation we see is for espionage," ThreatConnect's Rich Barger said.

"This isn't a criminal act in which they would sell the information or steal identities. This helps understand the inner workings of the US government."

John Schindler, a former National Security Agency officer who is now a consultant, said the data is "the Holy Grail" from an intelligence perspective.

The hack "is unprecedented in its scope, offers our adversaries the opportunity to penetrate our government and use that information to deceive it at a strategic level," he said in a blog post.

Health hack connection?

The attack targeting the US Office of Personnel Management could be connected to other data breaches even though they may not seem similar on the surface, say analysts.

In recent months, breaches affecting tens of millions of Americans have been reported at health insurance firms such as Anthem and CareFirst, members of the Blue Cross Blue Shield Association—which cover many federal government employees.

ThreatConnect said its analysis shows similar software and signatures in both the OPM incident and the health care breaches, suggesting these could be part of the same effort to compile intelligence data.

"We believe there is enough technical evidence to say there is an overlap" between the health care and government workforce data breaches, Barger said.

Anup Ghosh, founder and chief executive of the security firm Invincea, said the incidents suggest a long-term plan "building dossiers on targets of interest."

Combining the data in personnel records with detailed health information provides "very personal and private information," Ghosh said.

"This has people's vulnerabilities. It gives (foreign agents) leverage."

And because public disclosure of these breaches often takes time, Ghosh said he anticipates additional news about hacks affecting US government employees.

"I'm confident you will see more," he said.

Most of the breaches are the result of "spearphishing" using an email that appears to come from a legitimate person and gets the recipient to click on a link that enables the intrusion, Ghosh said.

He noted that the federal government is vulnerable because most defense software is "based on legacy technology from the 1990s" that fails to stop the attacks.

Some of the newer systems aim for real-time monitoring and

containment when a network is breached.

"You can't stop people from clicking on links," he said.

"But you can put the malware in virtual containers in a disposable environment."