Exclusive: Snowden persuaded other NSA workers to give up passwords - sources

Thu, Nov 7 2013

By Mark Hosenball and Warren Strobel

WASHINGTON (Reuters) - Former U.S. National Security Agency contractor Edward Snowden used login credentials and passwords provided unwittingly by colleagues at a spy base in Hawaii to access some of the classified material he leaked to the media, sources said.

A handful of agency employees who gave their login details to Snowden were identified, questioned and removed from their assignments, said a source close to several U.S. government investigations into the damage caused by the leaks.

Snowden may have persuaded between 20 and 25 fellow workers at the NSA regional operations center in Hawaii to give him their logins and passwords by telling them they were needed for him to do his job as a computer systems administrator, a second source said.

The revelation is the latest to indicate that inadequate security measures at the NSA played a significant role in the worst breach of classified data in the super-secret eavesdropping agency's 61-year history.

Reuters reported last month that the NSA failed to install the most up-to-date, anti-leak software at the Hawaii site before Snowden went to work there and downloaded highly classified documents belonging to the agency and its British counterpart, Government Communication Headquarters.

It is not clear what rules the employees broke by giving Snowden their passwords, which allowed the contractor access to data that he was not authorized to see.

Snowden worked at the Hawaii site for about a month last spring, during which he got access to and downloaded tens of thousands of secret NSA documents.

COVERING TRACKS

"In the classified world, there is a sharp distinction between insiders and outsiders. If you've been cleared and especially if you've been polygraphed, you're an insider and you are presumed to be trustworthy," said Steven Aftergood, a secrecy expert with the Federation of American Scientists.

"What agencies are having a hard time grappling with is the insider threat, the idea that the guy in the next cubicle may not be reliable," he added.

Officials with the NSA and the Office of Director of National Intelligence declined to comment due to a criminal investigation related to Snowden, who disclosed previously secret U.S. government mass surveillance programs while in Hong Kong in June and then fled to Russia where he was granted temporary asylum.

People familiar with efforts to assess the damage to U.S. intelligence caused by Snowden's leaks have said assessments are proceeding slowly because Snowden succeeded in obscuring some electronic traces of how he accessed NSA records.

The sources did not know if the NSA employees who were removed from their assignments were given other duties or fired.

While the U.S. government now believes it has a good idea of all the data to which Snowden could have accessed, investigators are not positive which and how much of that data Snowden actually downloaded, the sources said.

Snowden and some of his interlocutors, such as former Guardian writer Glenn Greenwald, have said that Snowden provided NSA secrets only to media representatives such as Greenwald, filmmaker Laura Poitras, and a reporter with the British newspaper.

They have emphatically denied that he provided any classified material to countries such as China or Russia.

The revelation that Snowden got access to some of the material he leaked by using colleagues' passwords surfaced as the U.S. Senate Intelligence Committee approved a bill intended in part to tighten security over U.S. intelligence data.

One provision of the bill would earmark a classified sum of money - estimated as less than $100 million - to help fund efforts by intelligence agencies to install new software designed to spot and track attempts to access or download secret materials without proper authorization.

The bill also requires that the Director of National Intelligence set up a system requiring intelligence contractors to quickly report to spy agencies on incidents in which data networks have been penetrated by unauthorized persons.

(Editing by Alistair Bell and Paul Simao)