How the NSA Shot Itself In the Foot By Denying Prior Knowledge Of Heartbleed Vulnerability

Zack Whittaker | Zdnet | April 12th 2014

In 2012, during a classified but widely-known operation at Fort Meade, MD, government cryptographers and developers downloaded the OpenSSL source code, as it does with dozens of other software published on the Web. The operation's objective was to find weaknesses in the library and exploit those vulnerabilities as part of wider efforts by the intelligence agency to conduct mass-scale surveillance.

fter the code was downloaded and compiled, the developers were soon able to pinpoint a programming flaw in the code, which would have allowed the agency to collect usernames and passwords far quicker, more efficiently, and at a lower cost than its bulk data collection programs, notably its fiber cable tapping operation named Upstream.

Executives and senior officials heralded it as one of the biggest vulnerability discoveries in the intelligence agency's recent history. A single programming flaw that it could exploit and use to tap directly into the communications of hundreds of millions of users, and gain system administrative privileges to vacuum up every shred of data it could find. Not just once, but at will, and it was untraceable.

It was the NSA's golden goose.

Except, none of that happened, according to a statement by the U.S.' director of national intelligence, James Clapper, who said on Friday following the Bloomberg report citing two

people familiar with the situation. “NSA was not aware of the recently identified vulnerability in OpenSSL, the so-called Heartbleed vulnerability, until it was made public in a private sector cybersecurity report.”

“Reports that say otherwise are wrong,” he added, noting that the U.S. government “relies” on OpenSSL to protect its users on government websites. “If the… government, including the intelligence community, had discovered this vulnerability prior to last week, it would have been disclosed to the community responsible for OpenSSL.”

Either one of two things happened: Bloomberg got screwed over by its sources, or the U.S. government is outright lying and clambering to save face with the already disgruntled public.

Clapper’s response instead disclosed a seismic vulnerability in the intelligence agency’s own mission, to “protect U.S. national security systems and to produce foreign signals intelligence information.”

Clapper has, either intentionally (though more likely inadvertently) revealed the agency’s own core internal weaknesses and deficiencies probably more so than any other revelation leaked by whistleblower Edward Snowden, who remains responsible for the biggest global intelligence leak in post-World War II history.

The NSA’s job, first and foremost, has been blown up by the Snowden leaks in a specific and precise way than the agency’s simplistic “protect America” rhetoric – from tapping fiber cables, demanding data from Silicon Valley servers, intercepting wireless transmissions, and exploiting vulnerabilities and flaws in common encryption standards in order to vacuum up all the data things.

[read full post here]