NSA exploited Heartbleed bug

Joseph Santolan
14 April 2014

On Friday, Bloomberg News published a report citing two sources "familiar with the matter" revealing that the National Security Agency (NSA) was aware of the existence of the Heartbleed Internet security bug for two years and routinely exploited the bug to spy on private communications, rather than revealing and patching it.

On the same day, both the White House National Security Council (NSC) and the NSA issued categorical denials that they had any awareness of the existence of the Heartbleed bug prior to its public disclosure on April 7.

NSC spokeswoman Caitlyn Hayden told the press, "Reports that NSA or any other part of the government were aware of the so-called Heartbleed vulnerability before April 2014 are wrong." Director of National Intelligence James Clapper (who in March 2013 lied under oath during testimony before the Senate) also stated that the "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."

The Bloomberg News report, together with all the available evidence, points to the conclusion that the NSA knew of and exploited the Heartbleed bug from the beginning.

The Heartbleed bug is the result of five lines of poorly crafted code in an extension released in early 2012 to OpenSSL. OpenSSL is an open-source program responsible for the encryption of the majority of traffic on the Internet. Since its discovery and announcement on Monday, the Heartbleed bug has been widely described as the worst security breach in the history of the Internet.

The Heartbleed bug potentially exposed usernames, passwords, and essentially all private data communicated to affected servers. It also exposed the private keys of the servers themselves. Anyone in possession of these keys would be able to decrypt all traffic encrypted to any server using this key, including archived past traffic.

On Friday, the *New York Times* published an article claiming that Cloudflare, a Silicon Valley Internet firm, had run tests "this week" of servers operating with the vulnerable version of OpenSSL and had been unable to recover private keys. In fact, after only nine hours of testing, two separate teams of testers were able to recover the private keys of the affected servers. This revealed, according to reports, that the "worst case scenario" was real. However, the *Times* has not published an updated report.

OpenSSL is maintained by a core of four programmers, only one of whom works on the project full-time. It operates on a shoestring budget composed of individual donations.

Speaking to the *Sydney Morning Herald*, Robin Seggelmann, a programmer based in Germany, explained how he had crafted the code which, he claimed, inadvertently failed to include a routine bounds check—an error which the Heartbleed bug was able to exploit. This code containing the error was then reviewed by one other programmer, and the revision was committed in the first week of March 2012.

That a coding error such as Heartbleed would be missed by two volunteer programmers is entirely plausible. That it could be overlooked by the huge NSA cyber-spying apparatus for two years is not.

NSA whistleblower Edward Snowden has indicated that the mathematics on which the encryption is based, which relies on the rather elegant use of extremely large prime numbers, is secure. The NSA's efforts to break the encryption consists in crafting of deliberately bad code which is then incorporated into proprietary software, or in locating errors in existing open-source software which can be exploited.

These bugs are known as "zero-day" exploits,

because at the moment of their discovery the code is immediately vulnerable. In other words, programmers have zero days in which to craft a response. According to budget documents published by the *Washington Post*, the NSA spent $25 million in 2013 for the purchase of zero-day exploits from "private vendors."

These purchases are known as zero-day bounties. The NSA encourages programmers to hunt for bugs in software which, instead of being fixed, are delivered to the NSA for exploitation in return for cash.

The average price for a serious zero-day threat on the private market is several hundred thousand dollars. The amount spent on "zero-day" bounties last year alone indicates that the NSA is responsible for the failure to patch a huge number of bugs and security breaches in communications software.

According to Bloomberg News, the NSA employs approximately one thousand full-time personnel whose sole task is to scan through code for exploitable bugs. Much of this process is automated, as code is scanned for known weak points such as the "memcpy()" command used in the Heartbleed bug.

The near universal use of OpenSSL would likely have made it among the highest priority targets on the NSA zero-day hit list. The idea that such a simple and major error as the Heartbleed bug was not discovered by a thousand employees and a $25 million bounty program for two years strains credulity.

Thanks to documents released by Snowden, it is now well known that the NSA is sucking up and storing practically all traffic on the Internet using its various spying tools, including the XKeyscore tool. The ability to obtain the private keys from servers using the Heartbleed bug means that the NSA can decrypt all past traffic encrypted to the keys it obtains, even traffic from years before the bug was introduced.

Quoting senior administration officials, the *New York Times* reported on Saturday that as part of the so-called "reforms" of the NSA (the toothless measures being introduced in an effort to diffuse popular anger over the Snowden revelations), there would be a "bias" in the NSA towards revealing discovered zero-day exploits.

However, according to the same officials, the reforms provide that the NSA can refrain from revealing zero-day exploits in the event of "a clear national security or law enforcement need." Like all of the supposed NSA "reforms" being introduced by the Obama administration, a loophole is always provided that is big enough to swallow any content that the "reform" might otherwise have had.

In any event, despite the "bias" towards disclosure announced by the Obama administration—and notwithstanding the millions spent on bounties and the one thousand employees dedicated to locating exploits—the NSA has not disclosed a single discovered exploit to the public.

In its article Saturday, the *Times* quoted senior officials who stated that disclosing zero-day vulnerabilities would be the equivalent of "unilateral disarmament."

This phrase, which mirrors the language of nuclear weapons, confirms that the zero-day exploits that the NSA is collecting are viewed as "arms" for cyber-warfare. In fact, the NSA used four such zero-day vulnerabilities in a series of cyber-warfare attacks on Iranian nuclear centrifuges in an operation codenamed "Olympic Games." The NSA stockpiles these vulnerabilities to spy on the American and world public and for use against anyone that Washington is targeting for attack.

One of the key targets for cyber warfare is China. Documents released by Snowden have revealed that the NSA is targeting major Chinese corporations with digital espionage, including the telecommunications giant Huawei.

The senior intelligence official interviewed by the *Times* continued, "We don't eliminate nuclear weapons until the Russians do ... You are not going to see the Chinese give up on 'zero days' just because we do."

The NSA's exploitation of the Heartbleed bug confirms once again that the US intelligence apparatus is determined to spy on every aspect of life by any means possible. In the pursuit of this goal, basic democratic rights such as the Fourth Amendment protection against unreasonable searches and seizures are simply ignored.