The Shadow Brokers Mess Is What Happens When the NSA Hoards Zero-Days

Andy Greenberg ⋮ 7-9 minutes ⋮ 8/17/2016

When the NSA discovers a new method of hacking into a piece of software or hardware, it faces a dilemma. Report the security flaw it exploits to the product's manufacturer so it gets fixed, or keep that vulnerability secret---what's known in the security industry as a "zero day"---and use it to hack its targets, gathering valuable intelligence. Now a case of data apparently stolen from an NSA hacking team seems to show the risks that result when the agency chooses offense over defense: Its secret hacking tools can fall into unknown hands.

On Wednesday, networking equipment firms Cisco and Fortinet warned customers about vulnerabilities revealed in data posted to the web days earlier by an anonymous group calling itself Shadow Brokers. The group claimed it obtained the data by hacking of an elite espionage team known as Equation Group and linked to the NSA. Shadow Brokers described its haul as a cache of encrypted "cyberweapons" that it would auction to the highest bidder. The data dump also contained an unencrypted sample with 300 megabytes of information including hacking software---known as "exploits"---designed to target networking appliances from Cisco, Fortinet, Juniper and TopSec.[1]

Based on Fortinet and Cisco's urgent warnings in response to the exploits' leak, it appears that some of those exploits had in fact been secret zero-day flaws. That raises the likelihood that the data was in fact stolen from NSA hackers---a view increasingly held by security experts analyzing the data.

More broadly, it also raises new questions about the NSA practice of keeping zero days secret rather than reporting them to affected companies. "There's always that delicate balance: how do they accomplish their mission, hack their adversaries, and still protect the rest of us?" asks Jeremiah Grossman, a prolific web security researcher and chief of security strategy at the firm SentinelOne. "The longer you haven't reported it, the higher the likelihood it will eventually leak."

Though the stolen cache of data contained dozens of exploits, many matching previously known NSA hacking techniques referred to in documents leaked by Edward Snowden, Cisco has only warned customers about two of them, and recommended a configuration change to prevent the more serious of the two that would allow attackers in some circumstances to take control of its network security appliances. Fortinet warned customers that another of those leaked exploits affected versions of its security equipment sold before 2012, and recommended they update their software.

A Cisco spokesperson confirmed that the NSA hadn't previously reported the vulnerability the company is now addressing. Given that the data stolen by Shadow Brokers appears to be three years old, that could mean the NSA may have used the hacking technique in secret for years---and possibly allowed it to fall into the hands of its adversaries for just as long.[2]

Grossman argues that demonstrates the need for a more public debate over when the NSA should hoard zero days and when it should disclose them to vendors in order to improve the overall security of the internet. "I think they should be encouraged to have zero days at their disposal to accomplish their mission," says Grossman. "But they should have a well-defined time after which they need to release them so we can properly defend ourselves."

NSA Director Michael Rogers said in late 2014 that the NSA reports the majority of the vulnerabilities it finds. "By orders of magnitude, the greatest numbers of vulnerabilities we find, we share," he told an audience at Stanford University. Not long after, National Security Council cybersecurity coordinator and Obama adviser Michael Daniel told WIRED that "there's often this image that the government

has spent a lot of time and effort to discover vulnerabilities that we've stockpiled in huge numbers....The reality is just not nearly as stark or as interesting."

But the Shadow Brokers' leak appears to be evidence of just that sort of zero-day stockpile, albeit of an unknown size. And the fact that it may have been compromised for years adds more fuel to criticism of the NSA. As Berkeley security researcher Nicholas Weaver wrote on Twitter, "If the NSA discovered [this] breach in 2013 and never told Cisco/Fortinet, this is VERY BAD. If they didn't know, this is VERY BAD." ACLU lead technologist Chris Soghoian went so far as to suggest the incident will lead to a congressional investigation:

The Electronic Frontier Foundation's Andrew Crocker, who has investigated the federal government's policies about its collection and use of zero days, was wary of commenting before more facts about the source and nature of the Shadow Brokers breach could be confirmed. But he reiterated that "there needs to be a public conversation about whether to retain or disclose vulnerabilities."

For Cisco, the incident may represent an unpleasant flashback to 2014, when Edward Snowden's leaks revealed that the NSA was intercepting shipments of its equipment to install spyware. Then-CEO John Chambers wrote a letter to Obama at the time, arguing that the NSA's practices had compromised his business. "We simply cannot operate this way," Chambers wrote. "We need standards of conduct...to ensure that appropriate safeguards exist that serve national security objectives, while at the same time meet the needs of global commerce."

The Obama administration, for its part, told the New York Times in 2014 that it ordered the NSA to disclose the security flaws it discovers in computer systems in most cases, but to hold those flaws in secret when they can be used to serve "a clear national security or law enforcement need." And Dave Aitel, a former NSA analyst who now runs the security firm ImmunitySec, contends that the sort of exploits exposed in the Shadow Brokers breach do hold exactly that sort of national security value. "Remote access on Cisco [equipment] sounds like it has national-security-level value to me," says Aitel, who has posited in a blog post that the data was in fact stolen from the NSA and that the Shadow Brokers group was likely Russian. "We don't know what valuable intelligence was gathered through the use of this technology, but you can be assured it was worth spending the time to create it. When you have 300 megabytes of code that's this carefully crafted, you didn't do that for fun."

Aitel argues that as controversial as it may be, the NSA needs exactly these sorts of secret network exploitation capabilities to do its job. "Imagine if you didn't have any Cisco exploits," he says. "You'd be unable to report on terrorist movements, on Russian and Chinese movements....This is the necessary bread and butter of getting intelligence work done in this day and age. We need to get used to it."

[1]*Correction 8/17/2016 11pm EST: An earlier version of this story misstated how many days had passed since the Shadow Brokers posted their stolen data on the web.*

[2]*Correction 8/18/2016 8:30am EST: An earlier version of the story stated that Cisco has issued a patch for the more serious of the two vulnerabilities, when in fact it's only recommended a configuration change to customers.*