Hacker group releases malware codes attributed to National Security Agency

Nick Barrickman
18 August 2016

On Monday, a hacker group calling itself the Shadow Brokers released malware files and code it claimed to have taken from hackers employed by the US National Security Agency (NSA). The codes, described by the group as a "state sponsor tool set" for spying and exploiting breaches in computer networks of foreign governments and companies, were released in two bundles--one a freely accessible trove and the other an encrypted bundle containing "the best files," which would be auctioned to the public for $500 million.

"There is a lot of consensus among technical experts that the cybertools were indeed stolen from the NSA, most likely from an external command and control server created to launch hacking operations that couldn't be traced back to the US," former NSA General Counsel Stewart Baker told NBC News.

The Shadow Brokers group claims to have taken its nearly 300 megabyte collection of malware from an NSA-affiliated hacker team known as the Equation Group. According to the Russian security firm Kaspersky Labs, the Equation Group is "a threat actor that surpasses anything known in terms of complexity and sophistication of techniques."

"How much you pay for enemies cyber weapons [sic]?" asks Shadow Brokers in a crudely worded statement on its web page, referring to the NSA. "We find cyber weapons made by creators of stuxnet, duqu, flame," continues the statement.

The Equation Group is the maker of the Stuxnet worm, a computer virus that was used to infect Iran's nuclear centrifuges, significantly hampering the latter's ability to develop its energy sector. The *New York Times* reported that the exposed cache of malicious computer code was used "to break through network firewalls and get inside the computer systems of competitors like Russia, China and Iran." The NSA has yet to comment on the evident breach of its security system.

The malware programs were mostly dated to June 2013, the month that NSA whistleblower Edward Snowden revealed massive illegal spying operations conducted by the US intelligence apparatus around the world. The NSA conducted a systematic revamping of its security protocol after Snowden made these revelations and many of the programs made available by the Shadow Brokers are considered obsolete today.

Both the *Times* and the *Washington Post* published prominent news pieces on Wednesday, two days after the leak, seeking, without presenting any factual substantiation, to attribute the breach to the Russian government. Both quoted from statements made on social media by Snowden, who said that "circumstantial evidence and conventional wisdom indicates Russian responsibility."

Snowden suggested the alleged Russian move was "more diplomacy than intelligence, related to the escalation around the DNC hack." This was a reference to the campaign of the Democratic Party and much of the US media to blame the Russian government for last month's leak of Democratic National Committee emails showing corrupt efforts by the party leadership to undermine the primary campaign of Vermont Senator Bernie Sanders. The presidential campaign of Democratic candidate Hillary Clinton and the party establishment, with the tacit support of Sanders, have charged that the leaks amount to an intervention into the US election by Russian President Vladimir Putin aimed at tipping the result in favor of his agent, Republican candidate Donald Trump.

Snowden said the Russian government likely wanted to send "a warning that someone can prove US responsibility for any attacks that originated from this

malware server," and that this could prove damaging "particularly if any of those operations targeted elections."

The acknowledgment by the corporate media of massive spying, hacking and cyber warfare by the NSA against governments and corporations all over the world underscores the hypocrisy of the current efforts to brand Putin and the Russian government as international pariahs and rogue forces for their alleged hacking into Democratic Party computer servers.

Other experts in cyber security have cast doubt on the claims of Russian involvement in the Shadow Brokers hacks. "There are so many unknowns here, and a lot of people in the hacking community don't think this is the Russian government," said journalist James Bamford, the author of authoritative books and articles exposing the illegal activities of the NSA. He told NBC News that "even the NSA probably doesn't know who did this."

Former NSA General Counsel Baker suggested that "the more disastrous and less likely scenario is that someone has hacked US infrastructure and extracted large files," and likely has the ability to do so again.