NSA Whistleblowers: Hack of NSA Hacks Was Likely An Inside Job

The mainstream press is accusing Russia of being behind the release of information on the NSA's dirty hacking tools.

Washington's Blog asked the highest-level NSA whistleblower in history, William Binney – the NSA executive who created the agency's mass surveillance program for digital information, who served as the senior technical director within the agency, who managed six thousand NSA employees, the 36-year NSA veteran widely regarded as a "legend" within the agency and the NSA's best-ever analyst and code-breaker, who mapped out the Soviet command-and-control structure before anyone else knew how, and so predicted Soviet invasions before they happened ("in the 1970s, he decrypted the Soviet Union's command system, which provided the US and its allies with real-time surveillance of all Soviet troop movements and Russian atomic weapons") – what he thinks of such claims.

Binney told us:

> The probability is that an insider provided the data.
>
> I say this because the NSA net is a closed net that is continuously encrypted. Which would mean, that if someone wanted to hack into the NSA network they would not only have to know weaknesses in the network/firewalls/tables and passwords but also be able to penetrate the encryption.
>
> So, my bet is that it is an insider. In my opinion, if the Russians had these files, they would use them not leak them or any part of them to the world.

Similarly, former NSA employee, producer for ABC's World News Tonight, and long-time reporter on the NSA James Bamfordnotes:

> If Russia had stolen the hacking tools, it would be senseless to publicize the theft, let alone put them up for sale. It would be like a safecracker stealing the combination to a bank vault and putting it on Facebook. Once revealed, companies and governments would patch their firewalls, just as the bank would change its combination.

A more logical explanation could also be insider theft. If that's the case, it's one more reason to question the usefulness of an agency that secretly collects private information on millions of Americans but can't keep its most valuable data from being stolen, or as it appears in this case, being used against us.

***

The reasons given for laying the blame on Russia appear less convincing, however. "This is probably some Russian mind game, down to the bogus accent," James A. Lewis, a computer expert at the Center for Strategic and International Studies, a Washington think tank, told the *New York Times*. Why the Russians would engage in such a mind game, he never explained.

Rather than the NSA hacking tools being snatched as a result of a sophisticated cyber operation by Russia or some other nation, it seems more likely that an employee stole them. Experts who have analyzed the files suspect that they date to October 2013, five months after Edward Snowden left his contractor position with the NSA and fled to Hong Kong carrying flash drives containing hundreds of thousands of pages of NSA documents.

So, if Snowden could not have stolen the hacking tools, there are indications that after he departed in May 2013, someone else did, possibly someone assigned to the agency's highly sensitive Tailored Access Operations.

In December 2013, another highly secret NSA document quietly became public. It was a top secret TAO catalog of NSA hacking tools. Known as the Advanced Network Technology (ANT) catalog, it consisted of 50 pages of extensive pictures, diagrams and descriptions of tools for every kind of hack, mostly targeted at devices manufactured by U.S. companies, including Apple, Cisco, Dell and many others.

Like the hacking tools, the catalog used similar codenames.

***

In 2014, I spent three days in Moscow with Snowden for a magazine assignment and a PBS documentary. During our on-the-record conversations, he would not talk about the ANT catalog, perhaps not wanting to bring attention to another possible NSA whistleblower.

I was, however, given unrestricted access to his cache of documents. These included both the entire British, or GCHQ, files and the entire NSA files.

But going through this archive using a sophisticated digital search tool, I could not find a single reference to the ANT catalog. This confirmed for me that it had likely been released by a second leaker. And if that person could have downloaded and removed the catalog of hacking tools, it's also likely he or she could have also downloaded and removed the digital tools now being leaked.

And Motherboard reports:

"My colleagues and I are fairly certain that this was no hack, or group for that matter," the former NSA employee told Motherboard. "This 'Shadow Brokers' character is one guy, an insider employee."

The source, who asked to remain anonymous, said that it'd be much easier for an insider to obtain the data that The Shadow Brokers put online rather than someone else, even Russia, remotely stealing it. He argued that "naming convention of the file directories, as well as some of the scripts in the dump are only accessible internally," and that "there is no reason" for those files to be on a server someone could hack. He claimed that these sorts of files are on a physically separated network that doesn't touch the internet; an air-gap.

***

"We are 99.9 percent sure that Russia has nothing to do

> with this and even though all this speculation is more sensational in the media, the insider theory should not be dismissed," the source added. "We think it is the most plausible."
>
> ***
>
> Another former NSA source, who was contacted independently and spoke on condition of anonymity, said that "it's plausible" that the leakers are actually a disgruntled insider, claiming that it's easier to walk out of the NSA with a USB drive or a CD than hack its servers.
>
> Michael Adams, an information security expert who served more than two decades in the US Special Operations Command, agreed that it's a viable theory.
>
> "It's Snowden junior," Adams told Motherboard. "Except he doesn't want to end up in virtual prison in Russia. He's smart enough to rip off shit, but also smart enough to be unidentifiable."

This wouldn't be the first time Russia has been framed for hacking.

http://www.zerohedge.com/news/2016-08-26/nsa-whistleblowers-nsa-hack-was-likely-inside-job