THE RUSSIAN METADATA IN THE SHADOW BROKERS DUMP

When I first noted, back in April, that there was metadata in one of the Shadow Brokers dumps, I suggested two possible motives for the doxing of several NSA hackers. First (assuming Russia had a role in the operation), to retaliate against US indictments of Russian hackers, including several believed to be tied to the DNC hack.

> A number of the few people who've noted this doxing publicly have suggested that it clearly supports the notion that a nation-state — most likely Russia — is behind the Shadow Brokers leak. As such, the release of previously unannounced documents to carry out this doxing would be seen as retaliation for the US' naming of Russia's hackers, both in December's election hacking related sanctions and more recently in the Yahoo indictment, to say nothing of America's renewed effort to arrest Russian hackers worldwide while they vacation outside of Russia.

But leaving the metadata in the documents might also make the investigation more difficult.

> [F]our days before Shadow Brokers started doxing NSA hackers, Shadow Brokers made threats against those who've commented on the released Shadow Brokers files specifically within the context of counterintelligence investigations, even while bragging about having gone unexposed thus far even while remaining in the United States.
>
> Whatever else this doxing may do, it will also make the investigation into

> how internal NSA files have come to be plastered all over the Internet more difficult, because Shadow Brokers is now threatening to expose members of TAO.

With that in mind, I want to look at a Brian Krebs piece that makes several uncharacteristic errors to get around to suggesting a Russian-American might have been the guy who leaked the files in question.

He sets out to read the metadata I noted (but did not analyze in detail, because why make the dox worse?) in April to identify who the engineer was that had NSA files discovered because he was running Kaspersky on his home machine.

> In August 2016, a mysterious entity calling itself “The Shadow Brokers” began releasing the first of several troves of classified documents and hacking tools purportedly stolen from “The Equation Group,” a highly advanced threat actor that is suspected of having ties to the U.S. National Security Agency. According to media reports, at least some of the information was stolen from the computer of an unidentified software developer and NSA contractor who was arrested in 2015 after taking the hacking tools home. In this post, we’ll examine clues left behind in the leaked Equation Group documents that may point to the identity of the mysterious software developer.

He links to the WSJ and cites, but doesn’t link, this NYT story on the Kaspersky related breach.

> Although Kaspersky was the first to report on the existence of the Equation Group, it also has been implicated in the group’s compromise. Earlier this year, both *The New York Times* and *The*

> *Wall Street Journal* cited unnamed U.S. intelligence officials saying Russian hackers were able to obtain the advanced Equation Group hacking tools after identifying the files through a contractor's use of Kaspersky Antivirus on his personal computer. For its part, Kaspersky has denied any involvement in the theft.

Then he turns to NYT's magnum opus on Shadow Brokers to substantiate the claim the government has investigations into three NSA personnel, two of whom were related to TAO.

> The Times reports that the NSA has active investigations into at least three former employees or contractors, including two who had worked for a specialized hacking division of NSA known as Tailored Access Operations, or TAO.
>
> [snip]
>
> The third person under investigation, The Times writes, is "a still publicly unidentified software developer secretly arrested after taking hacking tools home in 2015, only to have Russian hackers lift them from his home computer."

He then turns to the Shadow Brokers' released metadata to — he claims — identify the two "unnamed" NSA employees and the contractor referenced in The Times' reporter."

> So who are those two unnamed NSA employees and the contractor referenced in The Times' reporting?

From there, he points to a guy that few reports that analyzed the people identified in the metadata had discussed, A Russian! Krebs decides that because this guy is Russian he's likely to run Kaspersky and so he must be the guy who lost

these files.

> The two NSA employees are something of a known commodity, but the third individual — Mr. Sidelnikov — is more mysterious. Sidelnikov did not respond to repeated requests for comment. Independent Software also did not return calls and emails seeking comment.
>
> Sidelnikov's LinkedIn page (PDF) says he began working for Independent Software in 2015, and that he speaks both English and Russian. In 1982, Sidelnikov earned his masters in information security from Kishinev University, a school located in Moldova — an Eastern European country that at the time was part of the Soviet Union.
>
> Sildelnikov says he also earned a Bachelor of Science degree in "mathematical cybernetics" from the same university in 1981. Under "interests," Mr. Sidelnikov lists on his LinkedIn profile Independent Software, Microsoft, and The National Security Agency.
>
> Both The Times and The Journal have reported that the contractor suspected of leaking the classified documents was running Kaspersky Antivirus on his computer. It stands to reason that as a Russian native, Mr. Sildelnikov might be predisposed to using a Russian antivirus product.

Krebs further suggests Sidelnikov must be the culprit for losing his files in the Kaspersky incident because the guy who first pointed him to this metadata, a pentester named Mike Poor, said a database expert like Sidelnikov shouldn't have access to operational files.

> "He's the only one in there that is not Agency/TAO, and I think that poses important questions," Poor said. "Such as why did a DB programmer for a

> software company have access to operational classified documents? If he is or isn't a source or a tie to Shadow Brokers, it at least begets the question of why he accessed classified operational documents."

There are numerous problems with Krebs' analysis – which I pointed out this morning but which he blew off with a really snotty tweet.

First, the NYT story he cites but doesn't link to notes specifically that the Kaspersky related breach is unrelated to the Shadow Brokers leak, something that I also pointed out was logically obvious given how long the NSA claimed Hal Martin was behind the Shadow Brokers leak after the government was known to be investigating the Kaspersky related guy.

> It does not appear to be related to a devastating leak of N.S.A. hacking tools last year to a group, still unidentified, calling itself the Shadow Brokers, which has placed many of them online.

Krebs also misreads the magnum opus NYT story. The very paragraph he quotes from reads like this:

> The agency has active investigations into at least three former N.S.A. employees or contractors. Two had worked for T.A.O.: a still publicly unidentified software developer secretly arrested after taking hacking tools home in 2015, only to have Russian hackers lift them from his home computer; and Harold T. Martin III, a contractor arrested last year when F.B.I. agents found his home, garden shed and car stuffed with sensitive agency documents and storage devices he had taken over many years when a work-at-home habit got out of control, his lawyers say. The

> third is Reality Winner, a young N.S.A. linguist arrested in June, who is charged with leaking to the news site The Intercept a single classified report on a Russian breach of an American election systems vendor.

That is, there aren't "two unnamed NSA employees and [a] contractor referenced in The Times' reporting." The paragraph he refers to names two of the targets: Hal Martin (the other TAO employee) and Reality Winner. Which leaves just the Kaspersky related guy.

Krebs seemed unaware of the WaPo versions of the story, which include this one where Ellen Nakashima (who was the first to identify this guy last year) described the engineer as a Vietnamese born US citizen. Not a Russian-American, a Vietnamese-American.

Mystery solved Scoob! All without even looking at the Shadow Brokers' metadata. There's one more part of the Krebs story which is weird — that he takes the same non-response he got from the known NSA guys doxed by Shadow Brokers from Sidelnikov as somehow indicative of anything, even while if he had been "arrested" as Krebs' headline mistakenly suggests, then you'd think his phone might not be working at all.

There's more I won't say publicly about Krebs' project, what he really seems to be up to.

But the reason I went through the trouble of pointing out the errors is precisely because Krebs went so far out of his way to find a Russian to blame for … something.

We've been seeing Russian metadata in documents for 17 months. Every time such Russian metadata is found, everyone says, Aha! Russians! That, in spite of the fact that the Iron Felix metadata was obviously placed there intentionally, and further analysis showed that some of the other Russian metadata was put there intentionally, too.

At some point, we might begin to wonder why we're finding so much metadata screaming "Russia"?

Update: After the Vietnamese-American's guilty plea got announced, Krebs unpublished his doxing post.

> A note to readers: This author published a story earlier in the week that examined information in the metadata of Microsoft Office documents stolen from the NSA by The Shadow Brokers and leaked online. That story identified several individuals whose names were in the metadata from those documents. After the guilty plea entered this week and described above, KrebsOnSecurity has unpublished that earlier story.