WHY IS WIKILEAKS READING FROM SHADOWBROKERS' KASPERSKY SCRIPT?

A few weeks ago, when ShadowBrokers was telling the world they should pay attention to my journalism, I was noting that TSB's complaints about the Intelligence Community claim it obtained NSA files from Kaspersky were bogus. TSB himself had made such insinuations early in the year.

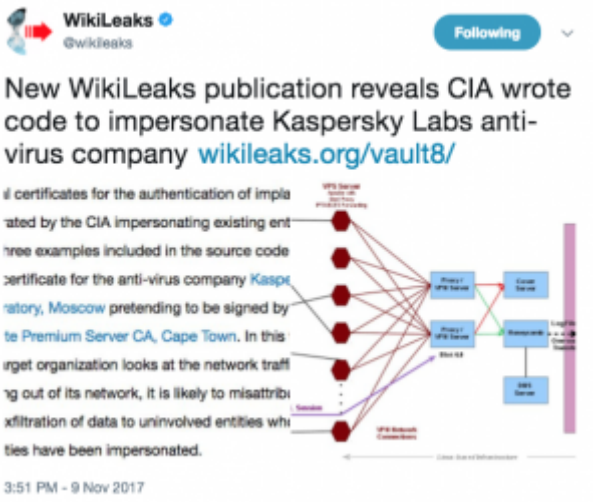
> TSB tries to claim that the Kaspersky stories are a US government attempt to explain how TSB got the files he is dumping. But as I have pointed out — even the NYT story on this did — it doesn't make sense. That's true, in part because if the government had identified the files the TAO hacker exposed to Kaspersky in spring 2016 as Shadowbrokers', they wouldn't have gone on to suggest the files came from Hal Martin when they arrested him. Mind you, Martin's case has had a series of continuations, which suggests he may be cooperating, so maybe he confessed to be running Kaspersky on his home machine too? But even there, they'd have known that long before now.
>
> Plus, TSB was the first person to suggest he got his files from Kaspersky. TSB invoked Kaspersky in his first post.
>
> > We find cyber weapons made by creators of stuxnet, duqu, flame. Kaspersky calls Equation Group. We follow Equation Group traffic.
>
> And TSB more directly called out Kaspersky in the 8th message, on January

> 8, just as the US government was unrolling its reports on the DNC hack.
>
> > Before go, TheShadowBrokers dropped Equation Group Windows Warez onto system with Kaspersky security product. 58 files popped Kaspersky alert for equationdrug.generic and equationdrug.k TheShadowBrokers is giving you popped files and including corresponding LP files.
>
> The latter is a point fsyourmoms made in a post and an Anon made on Twitter; I had made it in an unfinished post I accidentally briefly posted on September 15.

Today, as part of its roll-out of a plan to release, in TSB fashion, the source code behind CIA's hacking tools, WikiLeaks is similarly focusing on Kaspersky. WikiLeaks released the code for Hive, which it describes as,

> a back-end infrastructure malware with a public-facing HTTPS interface which is used by CIA implants to transfer exfiltrated information from target machines to the CIA and to receive commands from its operators to execute specific tasks on the targets.

In its second tweet advertising the new dump, it focused not on the functionality of the code, but on CIA's use of certificates appearing to be Kaspersky AV to exfiltrate its data.



As WikiLeaks explains:

> Digital certificates for the authentication of implants are generated by the CIA impersonating existing entities. The three examples included in the source code build a fake certificate for the anti-virus company Kaspersky Laboratory, Moscow pretending to be signed by Thawte Premium Server CA, Cape Town. In this way, if the target organization looks at the network traffic coming out of its network, it is likely to misattribute the CIA exfiltration of data to uninvolved entities whose identities have been impersonated.

The Kaspersky bit is nowhere near the most interesting thing about the release, but it nevertheless is a focus where it hadn't been when WikiLeaks first introduced Hive.

It seems, then, that WikiLeaks is picking up where TSB's most recent post left off — not just in dumping US intelligence community toys for others' use, but to do so while using Kaspersky to confuse issues.

I find the move all the more interesting given the two references TSB made to WikiLeaks' own dumps, as I laid out in March (at a time when it seemed TSB was done leaking).

> Several days after Shadow Brokers first announced an auction of a bunch of NSA tools last August, Wikileaks announced it had its own "pristine" copy of the files, which it would soon release.

> Wikileaks never did release that archive.
>
> On January 7-8, Shadow Brokers got testy with Wikileaks, suggesting that Wikileaks had grown power hungry.

> Shadow Brokers threw in several hashtags, two of which could be throw-offs or cultural references to a range of things (though as always with pop culture references, help me out if I'm missing something obvious). The third — "no more secrets" — in context invokes Sneakers, a movie full of devious US intelligence agencies, double dealing Russians, and the dilemma of what you do when you've got the power that comes from the ability to hack anything.
>
> Moments later, Shadow Brokers called out Wikileaks, invoking (in the language of this season's South Park) Wikileaks' promise to release the file.

> Of course, within a week, Shadow Brokers had reneged on a promise of sorts. Less than an hour before calling out Wikileaks for growing power hungry, Shadow Brokers suggested it would sell a range of Windows exploits. Four days later, it instead released a limited (and dated) subset of Windows files — ones curiously implicating Kaspersky Labs. All the "bullshit political talk," SB wrote in a final message, was just marketing.
>
> > Despite theories, it always being about bitcoins for TheShadowBrokers. Free dumps and bullshit political talk was being for marketing attention.
>
> And with that, the entity called Shadow Brokers checked out, still claiming to be in possession of a range of (dated) NSA hacking exploits.

We seem to have come full circle since that moment, with WikiLeaks picking where TSB left off in his last post. Which raises real questions about what this conversation has been about for the last year.

Update: William Ockham notes that Trust No One is a reference to the X Files generally as well as one episode focusing on electronic surveillance.