WHY WOULD FSB OFFICER DMITRY DOKUCHAEV USE A YAHOO EMAIL ACCOUNT TO SPY FOR RUSSIA?

At the Atlantic, I expanded on this post to explore how Russia has to do by hacking what the US can do using Section 702. As I lay out, for a lot of foreign spying involving US tech companies, Russia has to do things like phish or hack Yahoo's servers to gain the kind of access the NSA gets just by asking nicely.

But as Jeffrey Carr notes in this post, that's not true for unencrypted communications that originate in Russia. FSB — the agency where alleged Yahoo hackers Dmitry Dokuchaev and Igor Sushchin worked — have access to anything that originates in Russia.

> To put it another way, the FSB has total information awareness on every type of communication that originates in Russia or passes through Russian servers.

Carr uses that detail to argue that this probably means Dokuchaev — who was charged by Russia with treason in December — and Suschin were operating on their own.

> [W]hy would the FSB, with their vast resources and legal authorities, need to collect information on Russian targets in Russia via Yahoo?
>
> The obvious answer is — they don't. And since all of the defendants with the exception of one person are either criminals or charged by the Russian government with treason, the Yahoo breach was most likely the act of corrupt FSB employees and criminal

> hackers rather than an official FSB operation.

Now, many if not most accounts identified in the indictment (I made a list of the described targets in this post) wouldn't be officially available, because they're located in countries adjoining Russia or the US.

But there are a few other details that do support Carr's argument.

First, in addition to Yahoo and Google accounts, the conspirators targeted a Russian webmail service — probably Yandex.

> In or around April 2016, the conspirators sought access to an account of a senior officer at a Russian webmail and internet-related services provider (the "Russian Webmail Provider"). On or about April 25, 2016, DOKUCHAEV successfully minted a cookie to gain access to the victim user's account.

Admittedly, FSB might not want to go to Yandex (or whichever provider it is) to ask for information on one of their senior officers, but nevertheless, this information should be available officially in Russia. Another passage that describes the Russian webmail service lists only Russian targets, though that section also includes Google targets, so those may have been the GMail accounts of Russians unavailable in Russia.

In addition, the day after the indictment, Sushchin got fired from Renaissance Capital (which is owned by Nets owner Mikhail Prokhorov), where he was embedded. That suggests his was not an official embed noticed to the company (though it still may have been a legitimate FSB placement).

Most interesting of all is that Dokuchaev used US resources to conduct the hack. He had a Paypal account, which he presumably used to pay

Karim Baratov.

> All funds which constitute proceeds that are held on deposit in PayPal account number xxxxxxxxxxxxxx2639, held by DOKUCHAEV;

And, according to the G&M (and this is the most amazing part), Dokuchaev used a Yahoo account to communicate with Baratov.

> Mr. Dokuchaev is alleged in the court documents to have used a Yahoo e-mail account to contact Mr. Baratov and hire him to get the log-in information for about 80 accounts belonging to victims of the Yahoo hack.

I get why you wouldn't email Baratov from your Dokuchaev@FSB.ru account, because that would alert Canadian and US authorities he was working with Russian spies. But surely a Russian spy knows enough not to communicate via an account that is readily available to US authorities under Section 702, even if the conspirators' persistent presence in the Yahoo servers might alert you to such surveillance? Even if you wanted to use an account in North America there are surely better options.

In other words, there are a lot of reasons to believe that Dokuchaev was making more effort to keep this activity out of easy reach of Russian authorities then he did to hide it from the US.