RUSLAN STOYANOV AND TWO DEGREES OF SEPARATION FROM PROTECTED CRIMINAL HACKERS

Ruslan Stoyanov, the former head of cyber investigations at Kaspersky and now in prison fighting accusations of treason, got some press yesterday when letters he sent to his lawyers got released by a Russian TV station, Dozhd. Moscow Times covered Stoyanov's accusation that Russia exchanges intelligence related hacking for impunity for foreign cybercrimes.

> "The essence of the deal is that the state gets access to the technologies and information of 'cyberthieves,' in exchange for allowing them to steal abroad with impunity," Stoyanov said, claiming that this agreement has lead to "a new crime wave" perpetuated by "patriotic thieves."
>
> Stoyanov also warned that hackers are liable to turn their attention back to Russia, once their "patriotic fervor" wears off.

Dozhd's coverage is here, which makes one additional focus of Stoyanov's letters clear: Stoyanov pits the dangers to Russia of formerly protected hackers engaging in crimes within Russia against his own value to Russia in taking down the Lurk hackers last year. As Stoyanov's report from last year claims, Lurk's members managed to steal over 3 billion rubles before they were arrested with the help of Kaspersky.

It's a nice play to the public, Stoyanov's attempt to challenge Russia's accusations of treason by pointing out that protected criminal

hackers pose a greater threat to Russia.

But there's a problem with it (though one of which Stoyanov may be unaware).

Stoyanov's arrest for treason has been tied to that of FSB officers Sergei Mikhailov and Dmitry Dokuchaev. The best public (and, I believe, partial) explanation for their arrest so far is that the arrest arose, in part, out of an old grudge from spammer Pavel Vrublevsky, who believed Mikhailov and Stoyanov shared information on his operations with the FBI.

But that explanation pre-dates the unsealing of the indictment against four people — including Dokuchaev — for the hack of Yahoo from 2014 to 2016. In the indictment's description of Dokuchayev and in some of its description of the alleged hacks, it describes an FSB officer 3 who, because he is described as "supervisory," is likely Mikhailov (which, as I suggested in my original post on this, raises interesting questions about why he wasn't also charged).

> DMITRY ALEKSANDROVICH DOKUCHAEV, also known as "Patrick Nagel," was a Russian national and resident. DOKUCHAEV was an FSB officer assigned to Second Division ofFSB Center 18, also known as the FSB Center for Information Security. He was an associate ofFSB officer IGOR SUSHCHIN; another, supervisory FSB officer known to the Grand Jury ("FSB Officer 3"), who was the senior FSB official assigned to Center 18; and other FSB officers known and unknown.
>
> [snip]
>
> From at least in or around December 2015 until May 2016, the conspirators sought access to accounts ofthe former Minister ofEconomic Development of a country bordering Russia ("Victim A") and his wife ("Victim B"). DOKUCHAEV, SUSHCHIN, and BELAN worked with FSB Officer 3 to access_Victims A and B's accounts by minting cookies and to share information

> obtained from those accounts. In one instance, on or about December 18, 2015, FSB Officer 3 provided SUSHCHIN with information regarding a company controlled by Victims A and B. On or about December 21, 2015, DOKUCHAEV sent a cookie for Victim B's account to SUSHCHIN, who then later that day sent DOKUCHAEV a report on Victims A and B. On or about May 20, 2016, BELAN minted a cookie for the same Victim B account.

And the rest of the indictment describes how Dokuchaev, in particular, worked closely with prominent criminal hacker Alexsey Belan to access Yahoo. The indictment even describes how they helped Belan avoid legal troubles in Russia.

> One of the criminal hackers, BELAN, has been the subject of an Interpol "Red Notice" and listed as one of the Federal Bureau ofInvestigation's ("FBI") "Most Wanted" hackers since 2012. BELAN resides in Russia, within the FSB' s jurisdiction to arrest and prosecute. Rather than arrest him, however, the FSB officers used him. They also provided him with sensitive FSB law enforcement and intelligence information that would have helped him avoid detection by law enforcement, including information regarding FSB investigations of computer hacking and FSB techniques for identifying criminal hackers.

That is, Dokuchaev and, at least by presumed extension, Mikhailov, are allegedly involved in precisely the thing Stoyanov is trying to distinguish himself against, protecting prominent hackers so as to use their skills for FSB's goals.

But then, there are also the reasons to ask whether all that Dokuchaev, at least, was doing was official FSB business. On top of targeting a

Russian email provider (which is probably Yandex) via unofficial means, Dokuchaev used a number of tools, such as Yahoo and Paypal, that would be readily accessible to *American* authorities, but inaccessible to Russian authorities. Which, if he was spying against Russian authorities themselves, might explain why Russia would arrest Dokuchaev for treason.

Along with Stoyanov.

As I said, there's no reason to assume Stoyanov knows that Dokuchaev just got credibly accused of using Belan to help hack Yahoo. The Yahoo indictment likely got minimal attention in Russia to begin with, and it's not clear how much access to the media Stoyanov has in prison in any case.

But while his accusation against Russian authorities served its presumed purpose of making a media splash, both in Russia and internationally, given that he was accused of treason along with a guy who does just what he's claiming, it's not clear how much it helps his case (except perhaps to distinguish himself from those he got charged with).