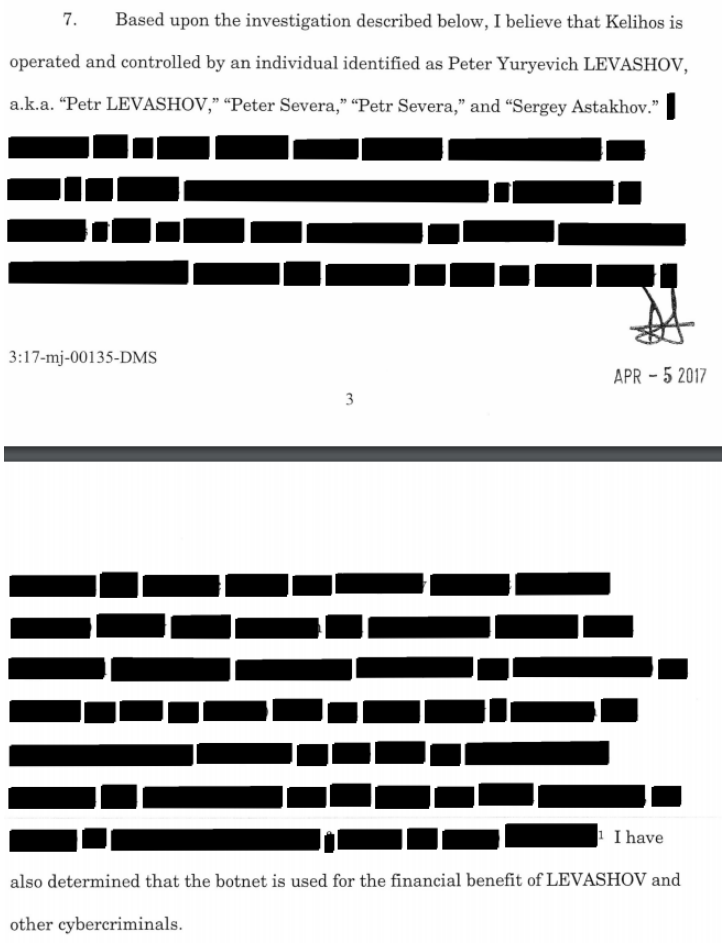
ANOTHER RUSSIAN HACKER (PROBABLY) NOT AFFILIATED WITH THE DNC HACK

When news came out that the Russian hacker Pyotr Levashov had been arrested in Barcelona, people assumed, based in part on what Levashov allegedly told his wife after being questioned, that he had a role in the DNC hack. (Update: Here's the RT story that reported it, which doesn't appear to have been posted on the UK or US RT sites, and which doesn't exactly correlate to some of the reports. Here's the complaint.)

> RT quoted Maria Levashova as saying armed police stormed into their apartment in Barcelona overnight, keeping her and her friend locked in a room for two hours while they quizzed Levashov.
>
> She said when she spoke to her husband on the phone from the police station, he told her he was told he had created a computer virus that was "linked to Trump's election win."
>
> Ms Levashova didn't elaborate, and the exact nature of the allegations weren't immediately clear.

DOJ has released the application associated with the Rule 41 search warrant they're using to take down Levashov's Kelihos botnet, and the unredacted part of the application supports no such thing. There is one paragraph with a mostly redacted description of how his customers use his botnet.



7. Based upon the investigation described below, I believe that Kelihos is operated and controlled by an individual identified as Peter Yuryevich LEVASHOV, a.k.a. "Petr LEVASHOV," "Peter Severa," "Petr Severa," and "Sergey Astakhov." [redacted]

[redacted]

3:17-mj-00135-DMS

APR – 5 2017

3

[redacted]

[redacted][1] I have also determined that the botnet is used for the financial benefit of LEVASHOV and other cybercriminals.

The rest of the application is consistent with Levashov working with pharma spammers, ransomware crooks, and those seeking money laundering online mules (though that's not inconsistent with Levashov cooperating with Russian intelligence in some way).

As noted, the government is using a Rule 41 warrant to redirect computers Levashov's botnet has hijacked to send their traffic into a sinkhole, along with a Pen Register to cover obtaining the IP addresses of the infected computers. The justification for using Rule 41 is that his botnet operates peer to peer. I expect we'll see more analysis about the necessity of using Rule 41 for this purpose. In any case, while some of the more sophisticated investigation of this case was done in New Haven, and while there are reportedly Connecticut computers that have been infected by the botnet, for some reason the case is being charged in Anchorage, AK (though there are definitely victims there, too, and the AK-based Agent who wrote the application also had a role

in the investigation). As more Rule 41 cases get charged we'll see some interesting jurisdictional questions.

The one other surprising part of this indictment is how crappy this guy's operational security is. The Luxembourg based IP address he used with his botnet tied to his iCloud account, which in turn tied through a common IP to his Google account, which in turn tied to his Foursquare account. All of this was done under his own or closely associated names.

Which might work fine if you were a Russian based hacker that did enough favors for the state to remain safe from prosecution. Until such time as you decide to take your wife and kid on a vacation to Spain.

One more point: When credential thief Yevgeniy Nikulin was arrested in Prague in October, the Russians quickly filed a competing arrest request for a minor 2009 bank account hack. The competing requests are being weighed by a Czech judge as we speak, but it seemed that the Russian request was an attempt to keep Nikulin out of US custody.

Thus far, there has been no hint of anything similar happening with Levashov.