TURNS OUT ALASKANS WON'T GET TO SEE RUSSIAN HACKER PYOTR LEVASHOV FROM THEIR WINDOWS

Earlier this month, DOJ got some good press by releasing the first known Rule 41 nationwide hacking warrant. It targeted Pyotr Levashov, who ran a big botnet infecting tons of Americans' computers. He was arrested on April 9 in Barcelona and DOJ shut down the botnet.

The good press continued when EFF lauded the way the Rule 41 hacking warrant was handled. I'm not aware that anyone has reviewed the Pen Register application that went along with the warrant, about which I have more concerns, but having EFF's blessing goes some way to rolling out a new authority without controversy.

Last week, DOJ announced the indictment, last Thursday, of Levashov. Whereas the Rule 41 warrant was submitted in Alaska, the indictment (and much of the investigation) was done in New Haven. Levashov was charged with eight different counts. Of note, the indictment includes two conspiracy-related charges against Levashov without naming any co-conspirators.

What I find interesting about all this is that there's a still sealed complaint, dated March 24, against Levashov in the New Haven docket, with its own affidavit.

So I'm wondering why the Rule 41 action was taken in Alaska whereas the prosecution (assuming Levashov is extradited) appears slotted for New Haven.

The Alaska affidavit makes abundant reference to the investigative activities in New Haven. It describes that New Haven FBI Agents tested the Kelihos malware, identified how Kelihos

harvested credentials, and tracked how Kelihos installed WinPCAP to intercept traffic.

It also includes a footnote describing other cases against Levashov.

> I am also aware that an indictment was filed in 2007 in the Eastern District of Michigan for conspiracy to commit electronic mail fraud, mail fraud, and wire fraud in violation of 18 U.S.C. $$ 371, 1037(a)(2)-(a)(B), 1037(b)(2)(C), 1341, and 1343 and several substantive counts of violating 18 U.S.C. $$ 1037(a)(2), 1037(b)(2)(C), and Section 2. That indictment remains pending. I am also aware that a criminal complaint filed in the U.S. District Court for the District of Columbia, which in 2009 charged LEVASHOV in his true name with two substantive counts of violating 18 U.S.C. $$ 1030(a)(5)(A)(i), 1030(a)(5)(B)(i), 1030(a)(5)(A)(i) and 1030(a)(5XBXV), as well as one count of conspiracy to commit these offenses in violation of 18 U.S.C. $ 371. These charges resulted from LEVASHOV's operating the Storm Botnet from January 2007 until September 22,2008. That botnet, like that which is the subject of this prosecution, sent spam to facilitate pump and dump schemes and the purchase of grey market pharmaceuticals. Because the government was unable to apprehend and detain LEVASHOV, it dismissed the complaint in 2014.

But it doesn't mention the complaint, which had already been filed, in CT — unless that's what the almost paragraph long redaction in the affidavit was.

One possible explanation for the jurisdictional oddity is just that DOJ could. To test their new authorities, perhaps, they chose to obtain a warrant in a totally different jurisdiction from the one they were prosecuting in, just to lay

out the precedent of doing so. And as noted, it's possible the big redacted passage in the AK affidavit explains all this.

I'd feel better about that if the FBI affidavit submitted in AK hadn't (possibly) hidden the already existing complaint in CT, though.

I've got a question into DOJ and will update if they provide an explanation. But for now, know that Alaska won't get to host a high profile hacking trial after all.

Upated, fixed DOJ announce date h/t EG.