The FBI Doesn't Want To Share Details On The Exploit It Deployed While Running A Child Porn Site

Techdirt

April 4, 2016 Monday 5:08 PM EST

Length: 1036 words

Byline: Tim Cushing

Body

Apr 04, 2016(Techdirt: *http://www.techdirt.com* Delivered by Newstex) The FBI will not[1] be talking about the Network Investigative Technique (NIT) it used[2] to obtain information about anonymous visitors to the child porn site it seized and ran[3] for two weeks while the NIT did its work. A recently-filed declaration[4] (uploaded by USA Today's Brad Heath[5] and pointed out by the ACLU's Chris Soghoian[6]) by the FBI tells the court the defense will learn nothing from being provided details on the NIT's inner workings, especially since the agency isn't willing to turn these details over to Jay Michaud's lawyers. As Special Agent Daniel Alfin explains it, the defense's tech expert has misrepresented the NIT's form and function to the court. I have also reviewed the declaration of Mr. Tsyrklevich, the defense expert, dated January 13, 2016 and noted a number of statements that are inaccurate and/or require clarification.

I will address several of these in great detail below but will begin by noting one overarching misconception in that declaration. Specifically, Tsyrklevich attempts to redefine the NIT as something containing multiple components. The NIT, however, consists of a single component -- that is, the computer instructions delivered to the defendant's computer after he logged into Playpen that sent specific information obtained from his computer back to the FBI. This is hardly surprising, considering the tech expert hasn't had an opportunity to examine the FBI's software. But because the defense is wrong about the NIT, the FBI argues it shouldn't be allowed to figure out how wrong it is -- or figure out what it may have gotten right by examining other evidence. Tsyrklevich claims that he requires access to the government's ″exploit″ to determine if the government ″executed additional functions outside the scope of the NIT warrant.″ He is wrong. Discovery of the ″exploit″ would do nothing to help him determine if the government exceeded the scope of the warrant because it would explain how the NIT was deployed to Michaud's computer, not what it did once deployed. This is the FBI playing games with words, albeit words perhaps poorly chosen by Michaud's lawyer. The FBI is claiming the only ″exploit″ was the delivery of the NIT payload, but not the payload itself. Michaud would like access to details on the latter (the payload), but the FBI is claiming the defense expert is only seeking details on the former. Continuing in that vein, the FBI agent says additional info on the exploit would do nothing to help determine whether the NIT exceeded the scope of the warrant because all the ″exploit″ did was allow the FBI to access information about Michaud's computer. It's circular reasoning that allows the FBI to skirt questions about the information it pulled from the computers it attached itself to while running the Playpen website. The FBI's declaration then goes even further, stating that all the information Michaud's lawyer needs can be found in the information the agency has already handed over. The FBI doesn't want to discuss its ″server component″ (where information

exchanged with suspects' computers was stored). Agent Alfin claims the defense can verify the legitimacy of the FBI's claims about data supposedly originating from Michaud's computer by comparing the information already handed to it by the agency with what will presumably be another copy of the same information previously handed to it by the agency. Specifically, the government has offered to provide a copy of the data stream sent by Michaud's computer to the government as a result of the execution of the NIT. Tsyrklevich can compare the information sent to the government by the NIT to the information provided in discovery to verify that what the government recorded from Michaud's computer is in fact what was sent by Michaud's computer. And how will Michaud know this new copy of the information isn't just a reprint of the old copy? Well, apparently because the FBI agent says it's totally legit. I have reviewed that data stream and, as explained below, confirmed that the information sent by Michaud's computer as a result of the NIT matches the information that is stored on the government's servers. Feel better? The FBI obviously isn't going to hand over information on its means and methods without a fight, making its NITs just another tech component it won't talk about in court. It has managed to keep discussions of Stingrays[7] out of court for several years and now it's doing everything it can to protect more recently-discovered innovations -- even if it means cutting defendants and judges out of the loop.The FBI could hand these details over to the defense and judges without having to hand them over to the general public (via in camera presentations, sealed submissions or the use of redactions) but it would rather keep even those components of the justice system in the dark. Permalink[8] | Comments[9] | Email This Story[10] [1]: *https://www.techdirt.com/articles/20160219/06072533647/judge-child-porn-case-says-fbi-must-turn-over-details-hacking-tool.shtml* [2]: *https://www.techdirt.com/articles/20160107/06414333264/fbi-deploying-large-scale-hacking-with-little-to-no-judicial-oversight.shtml* [3]: *https://www.techdirt-.com/articles/20160126/14535433436/courts-pretty-much-ok-with-fbis-occasional-stints-as-child-porn-distributors.shtml* [4]: *https://assets.documentcloud.org/documents/2778488/Show-Temp.pdf* [5]: *https://twitter.com/bradheath* [6]: *https://twitter.com/csoghoian/status/714638979098763264* [7]: *https://www.techdirt.com/articles/20150515/08573531016/fbi-says-it-has-no-idea-why-law-enforcement-agencies-are-following-terms-stingray-non-disclosure-agreements.shtml* [8]: *https://www.techdirt.com/articles/20160401/06514734076/fbi-doesnt-want-to-share-details-exploit-it-deployed-while-running-child-porn-site.shtml* [9]: *https://www.techdirt.com/articles/20160401/06514734076/fbi-doesnt-want-to-share-details-exploit-it-deployed-while-running-child-porn-site.shtml#comments* [10]: *https://www.techdirt.com/articles/20160401/06514734076/fbi-doesnt-want-to-share-details-exploit-it-deployed-while-running-child-porn-site.shtml?op=sharethis*

Classification

Language: English

Publication-Type: Web Blog

Journal Code: DIRT-0001

Subject: SPECIAL INVESTIGATIVE FORCES (89%); INVESTIGATIONS (78%); INTERNET CRIME (72%); CHILD PORNOGRAPHY (57%); PORNOGRAPHY (57%)

Organization: FEDERAL BUREAU OF INVESTIGATION (94%)

Industry: INTERNET CRIME (72%); COMPUTER SOFTWARE (70%)

Geographic: UNITED STATES (79%)

Load-Date: April 4, 2016