

Lawyers: FBI Must Reveal Malware for Hacking Child Porn Users or Drop Its Case

Written by **JOSEPH COX** (/EN_UK/AUTHOR/JOSEPHCOX)

26 April 2016 // 12:35 AM CET



Image: Hungju Lu/Flickr (<https://www.flickr.com/photos/jefflen/399928915/in/photolist-BkJW8-5YdNsd-5uPRir-cEjPCY-pfxVwm-9JfEUJ-rxjC5s-dn66Qb-5Ang9a-6A2eev-f5MbTo-6fVHYf-cXXqXy-61NDgC-92T7f1-7qnFy8-jT5U21-q62TRu-fKcz6k-bDLeCD-5xD8Mu-pF7Zf1-dE6EjG-qKeP3u-b2Y1vX-bw1GF5-pvy3cp-Ni1RK-9A8uFb-bWtdhd-dgHw5g-bjVsqi-74SiKE-dEbuNm-pwSUGT-3jHoxV-4ipQTn-7BDyqR-556MQr-qc5XDu-6A2hZg-cMqQpf-87ABQn-qtsV6V-r7jBEn-B1JhnW-cs6BwA-8SDhJX-6hwHFW-cfXJUJ>)

Last month, the FBI pushed back against a court order (<https://motherboard.vice.com/read/fbi-is-pushing-back-against-judges-order-to-reveal-tor-browser-exploit>) to reveal the full malware code it used to hack suspected visitors of a dark web child pornography site.

Now, in a partially redacted motion filed on Monday, opposing lawyers are arguing that the government either needs to comply with the order and reveal its malware, or drop the case.

"The Government has now made plain that the FBI will not comply with the Court's discovery order," wrote Colin Fieman and Linda Sullivan, attorneys representing Jay Michaud, one of those arrested as part of the FBI's investigation into child pornography site (<https://motherboard.vice.com/read/the-fbis-unprecedented-hacking-campaign-targeted-over-a-thousand-computers>) Playpen.

Michaud was arrested after the FBI deployed a network investigative technique (NIT)—the agency's term for a hacking tool, or malware—in order to identify the site's users.

Michaud's lawyers add that if the FBI continues its stalemate, then the judge should throw out the case himself

The FBI has been resisting an order to reveal the code for this NIT since February, when a judge said "you can either produce [the discovery] or move to dismiss."

Defense lawyers have echoed that ultimatum.

"The consequences are straightforward: the prosecution must now choose between complying with the court's discovery order and dismissing the case," Fieman and Sullivan continue.

The motion was in response to a sealed filing from the government, which asked the judge to reconsider providing the malware code to the defense. Several large sections of the defenses' latest filing are redacted, as it quotes parts of the government's own motion. (The attorneys are also seeking to have the government's argument unsealed.)

There are parts that hint at what arguments the government has made, however. "It has flatly refused to adopt additional security measures for discovery that would address any legitimate security concerns," the attorneys write, indicating that the government may have argued that any exposure of the NIT, even to defense lawyers under a protective order, could put the malware at risk of being distributed more widely.

Experts have previously said (<https://motherboard.vice.com/read/the-fbi-may-be-sitting-on-a-firefox-vulnerability>) that, judging by the effort that the FBI is going to in order to keep its hacking tool under wraps, it may still work.

The attorneys then point to similar cases where the FBI would rather lose convictions than divulge details of its surveillance techniques. With regards to Stingrays, devices that are capable of tracking cellphones (<https://motherboard.vice.com/tag/Stingrays>) and sometimes intercepting communications, "the FBI in fact ordered local prosecutors to dismiss cases or reduce felonies to minor charges rather than comply with discovery orders," they write.

They also note that the number of Playpen users increased dramatically while the FBI was operating the site (<https://motherboard.vice.com/read/judge-rules-fbi-running-child-porn-site-for-13-days-was-not-outrageous-conduct-playpen>) in order to deliver its NIT. The two possible reasons given are that the FBI deliberately drew new users to the site, or that a small tweak in the homepage made by the administrator before the site was seized could have led users to not understand that they were about to log into a child pornography site. Both of these theories are unsubstantiated, however.

Last week, in a related case, a judge threw out evidence (https://motherboard.vice.com/read/in-a-first-judge-throws-out-evidence-obtained-from-fbi-malware) obtained via the NIT. That reasoning (https://motherboard.vice.com/read/why-a-judge-threw-out-evidence-from-an-fbi-mass-hacking-campaign-playpen-NIT), however, had little to do with the malware itself or any discovery issues, and instead circled around the one warrant (https://motherboard.vice.com/read/here-is-the-warrant-the-fbi-used-to-hack-over-a-thousand-computers) used to authorise the FBI's hacking campaign.

As for the Michaud case, the defense indicate that the FBI really has no intention of handing over its malware code.

"The FBI has announced that it will not comply with the Court's discovery order," the attorneys write.

Michaud's lawyers add that if the FBI continues its stalemate, then the judge should throw out the case himself.

Case 3:15-cr-05351-RJB Document 179 Filed 04/25/16 Page 1 of 26

JUDGE ROBERT J. BRYAN

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT TACOMA

<p>1</p> <p>2</p> <p>3</p> <p>4</p> <p>5</p> <p>6</p> <p>7</p> <p>8 UNITED STATES OF AMERICA,</p> <p>9 Plaintiff,</p> <p>10 v.</p> <p>11</p> <p>12 JAY MICHAUD,</p> <p>13 Defendant.</p> <p>14</p> <hr style="width: 100%;"/>	<p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p> <p>)</p>	<p>No. CR15-5351RJB</p> <p>CONSOLIDATED RESPONSE TO</p> <p>GOVERNMENT MOTION FOR</p> <p>RECONSIDERATION; RESPONSE TO</p> <p>MOTIONS FOR EX PARTE AND IN</p> <p>CAMERA PROCEEDINGS; AND</p> <p>SECOND DEFENSE MOTION TO</p> <p>DISMISS INDICTMENT</p> <p>FILED UNDER SEAL¹</p>
---	---	---

TOPICS: Playpen (/en_uk/tag/Playpen), FBI (/en_uk/tag/FBI), jay michaud (/en_uk/tag/jay+michaud), network investigative technique (/en_uk/tag/network+investigative+technique), NIT (/en_uk/tag/NIT), hacking (/en_uk/tag/hacking), law enforcement (/en_uk/tag/law+enforcement), Federal Bureau of Investigation (/en_uk/tag/Federal+Bureau+of+Investigation)

Contact the author by email (mailto:josephcox@riseup.net) or Twitter (https://twitter.com/josephfcox).

You can reach us at letters@motherboard.tv (mailto:letters@motherboard.tv). Want to see other people talking about Motherboard? Check out our letters to the editor (http://motherboard.vice.com/tag/letters+to+the+editor).