Activists to FBI: Show Us Your Warrant for Mass Hack of TorMail Users

5-6 minutes

Mass hacking is now one of the FBI's established tactics for fighting crime on the dark web. In February 2015, the agency hit at least 4,000 computers all over the world in an attempt to identify visitors of a child pornography site.

But questions remain about another FBI operation from 2013, in which the agency may have hacked users of a dark web email service called TorMail even if they weren't suspects of a crime. Now, the American Civil Liberties Union (ACLU) is trying to unseal the court docket sheet containing the search warrant used to deploy malware against users of the service. If the ACLU were then to get access to the warrant itself, it may reveal the true scale of the FBI's controversial hacking campaign.

TorMail was a site based on Freedom Hosting, a web host that provided easy-to-set-up Tor hidden services. In 2013, the FBI seized Freedom Hosting; according to media reports at the time, anyone visiting a Freedom Hosting site was met with a "Down for Maintenance" message. Researchers soon found that that page contained malicious code designed to de-anonymise users of the Tor Browser. The error page was also displayed to users of TorMail, one former user previously told Motherboard.

> "The sealing of docket sheets with warrants authorizing the use of malware prevents … critical public debate from happening"

The *Washington Post* recently confirmed that the FBI used a "network investigative technique" or NIT—the agency's term for a hacking tool—on the TorMail site. According to the article, the FBI had obtained a warrant to hack the owners of certain email accounts suspected of being involved in child pornography, and anonymous sources claimed that, with this approach, only suspects who had been linked to child pornography would be hacked.

But journalists, dissidents, and other individuals used TorMail too, and it seems that the error page was presented to every TorMail user—raising questions about how broad the operation really was.

"That the FBI engaged in a bulk hacking operation against all visitors to TorMail, which had many lawful, valid uses, raises serious concerns about the appropriateness of bulk hacking, and the extents to which courts should be authorizing and supervising such operations," reads the motion to unseal the docket, which was written by ACLU attorneys Brett Kaufman, Nathan Wessler, and David Rocah and filed last week.

Read More: The FBI May Have Hacked Innocent TorMail Users

Information that might help answer those sorts of questions and others are likely included in the search warrant. Although the warrant is referenced in other court documents, a copy of it has never been made publicly available.

"It is unclear, for instance, how many individuals' computers were infected, in which Districts, and what information was obtained," the ACLU writes.

The TorMail warrant is of particular interest because public documentation of FBI mass hacking operations so far only deal with clearly illegal sites, such as child pornography platforms.

"To date, the only publicly accessible warrants authorizing the FBI to engage in bulk hacking have targeted websites that are dedicated to the distribution of child pornography, and, as a result, the government has been able to assert probable cause that everyone visiting the sites is engaged in a crime. The TorMail website, in contrast, was not dedicated to the distribution of child pornography—it was a free, anonymous email service that had many users who were using it to protect their lawful private communications," the attorneys write.

The ACLU says the FBI has never sought explicit legislative authority to use hacking technologies in its investigations, despite using them for around 15 years. It argues that if policy makers, activists and technologists are going to have any sort of effective public debate around law enforcement use of malware, this search warrant should be in the public domain.

"The breadth and potency of malware as a law-enforcement tool raises concerns that can only be properly debated if legislators and the general public are aware of instances in which it is being used, the ways in which law enforcement seeks to use it, and the extent of judicial supervision," the motion reads. "The sealing of docket sheets with warrants authorizing the use of malware prevents this critical public debate from happening, in violation of the public's right of access."

Now, it's up to the US District court of Maryland, Baltimore, where the motion was filed, to decide whether to unseal the docket or not.

Correction: A previous version of this article incorrectly stated that the ACLU had filed a motion to unseal the FBI's search warrant. The ACLU is trying to unseal the docket sheet which contains the search warrant. We regret the error, and have updated the article appropriately.