FBI commits crime to entrap American citizens; Operates half of child porn websites

written by NARSOL | November 12, 2016

By Bryan Clark . . . Earlier this year we brought you an in-depth exposé of how, for 12 days in February and March, the Federal Bureau of Investigation (FBI) ran the world's largest child porn site, Playpen. According to newly unsealed documents, Playpen wasn't the only site containing child pornography on FBI servers.

The piece above can handle the in-depth explaining (if you're interested), but it went down like this: the FBI seized the site, ran it on government servers for 13 days and attempted to ensnare pedophiles through malware. The malware, known in law enforcement as a "network investigative technique" (NIT), tried to infiltrate layers of security TOR users employ when accessing the dark web. In at least a few cases, it worked.

According to an FBI affidavit:

> *In the normal course of the operation of a web site, a user sends "request data" to the web site in order to access that site. While Websites 1-23 operate at a government facility, such request data associated with a user's actions on Websites 1-23 will be collected. That data collection is not a function of the NIT. Such request data can be paired with data collected by the NIT, however, in order to attempt to identify a particular user and to determine that particular user's actions on Websites 1-23.*

Put simply, "websites 1-23" were operated at a government facility for an undefined period in an attempt to snag potential child predators.

Sarah Jamie Lewis, a security researcher, told Ars Technica: "it's a pretty reasonable assumption" that the FBI was, at one point, running nearly half of all known child porn sites hosted on Tor-hidden services. Lewis runs OnionScan, an analysis tool that uses bots to map out the dark web and look for vulnerabilities. She began her researching in April of this year, and as of August, she's mapped 29 unique child porn-related sites on Tor-hidden servers.

The issue – aside from the FBI's above-the-law approach at investigation – is the use of a single warrant to hack thousands of computers. The Playpen investigation netted some 1,300 unique internet protocol (IP) addresses. Of these, fewer than 100 cases made their way to court, and judges in Iowa, Massachusetts, and Oklahoma ruled that the FBI's investigation techniques violated current laws of federal procedure.

Other judges have taken issue with the unlawful search but failed to go as far as suppressing the evidence collected. (Please continue reading this article in The Next Web)