The FBI's 'Unprecedented' Hacking Campaign Targeted Over a Thousand Computers

WRITTEN BY JOSEPH COX (/AUTHOR/JOSEPHCOX)

January 5, 2016 // 04:00 PM EST

In the summer of 2015, two men from New York were charged (http://www.reuters.com/article/us-usa-crime-childporn-idUSKCN0PI2CH20150708) with online child pornography crimes. The site the men allegedly visited was a Tor hidden service, which supposedly would protect the identity of its users and server location. What made the case stand out was that the Federal Bureau of Investigation (FBI) had used a hacking tool to identify the IP addresses of the individuals.

The case received some media attention (https://motherboard.vice.com/read/the-fbi-hacked-a-dark-web-child-porn-site-to-unmask-its-visitors), and snippets of information about other (http://www.silive.com/news/index.ssf/2015/09/dark_web_child_porn_probe_snar.html), related arrests (http://www.columbian.com/news/2015/jul/14/gaiser-teacher-arrested-on-child-porn-charge/) started to spring up as the year went on. But only now is the true extent of the FBI's bulk hacking campaign coming to light.

In order to fight what it has called one of the largest child pornography sites on the dark web, the FBI hacked over a thousand computers, according to court documents reviewed by Motherboard and interviews with legal parties involved.

"This kind of operation is simply unprecedented," Christopher Soghoian, principal technologist at the American Civil Liberties Union (ACLU), told Motherboard in a phone interview.

A new bulletin board site on the dark web was launched in August 2014, on which users could sign up and then upload whatever images they wanted. According to court documents, the site's primary purpose was "the advertisement and distribution

of child pornography." Documents in another case would later confirm that the site was called "Playpen."

Just a month after launch, Playpen had nearly 60,000 member accounts. By the following year, this number had ballooned to almost 215,000, with over 117,000 total posts, and an average of 11,000 unique visitors each week. Many of those posts, according to FBI testimony, contained some of the most extreme child abuse imagery one could imagine, and others included advice on how sexual abusers could avoid detection online.

An FBI complaint described the site as "the largest remaining known child pornography hidden service in the world."

communications of users of "Website A." Before, during, and after its seizure by law enforcement, law enforcement agents viewed, examined and documented the contents of "Website A." Approximately 1300 true internet protocol (IP) addresses were identified during this time, one of which was user name, "xxxxoi1" (the complete user name has been redacted, but is known to your affiant) operating on IP address 73.20.54.250.

A section of one of the complaints involved in the Playpen investigation, showing that 1300 true IP addresses were obtained.

A month before this peak, in February 2015, the computer server running Playpen was seized by law enforcement from a web host in Lenoir, North Carolina, according to a complaint filed against Peter Ferrell, one of the accused in New York. (Data hosts in Lenoir contacted by Motherboard declined to comment. One of them, CentriLogic, wrote "We have no comment on the matter referenced by you. Our obligations to customers and law enforcement preclude us from responding to your inquiry.")

But after Playpen was seized, it wasn't immediately closed down, unlike previous dark web sites that have been shuttered (https://motherboard.vice.com/read/the-silk-road-is-shut-down-and-the-owner-is-in-custody) by law enforcement. Instead, the FBI ran Playpen from its own servers in Newington, Virginia, from February 20 to March 4,

reads a complaint filed against a defendant in Utah. During this time, the FBI deployed what is known as a network investigative technique (NIT), the agency's term for a hacking tool.

> “There will probably be an escalating stream of these [cases] in the next six months or so”

While Playpen was being run out of a server in Virginia, and the hacking tool was infecting targets, “approximately 1300 true internet protocol (IP) addresses were identified during this time,” according to the same complaint.

The legal counsel for one of the accused believes that the number of eventual cases may even be slightly higher.

“Fifteen-hundred or so of these cases are going to end up getting filed out of the same, underlying investigation,” Colin Fieman, a federal public defender handling several of the related cases, told Motherboard in a phone interview. Fieman, who is representing Jay Michaud, a Vancouver teacher arrested (http://www.columbian.com/news/2015/jul/14/gaiser-teacher-arrested-on-child-porn-charge/) in July 2015, said his estimate comes from what “we've seen in terms of the discovery.”

“There will probably be an escalating stream of these [cases] in the next six months or so,” Fieman added. “There is going to be a lot in the pipeline.”

Fieman has three cases pending in his defenders office, he said. According to court documents, charges have also been filed against defendants in Connecticut, Massachusetts, Illinois, New York, New Jersey, Florida, Utah, and Wisconsin.

In court filings, Fieman describes the use of this broad NIT as an “extraordinary

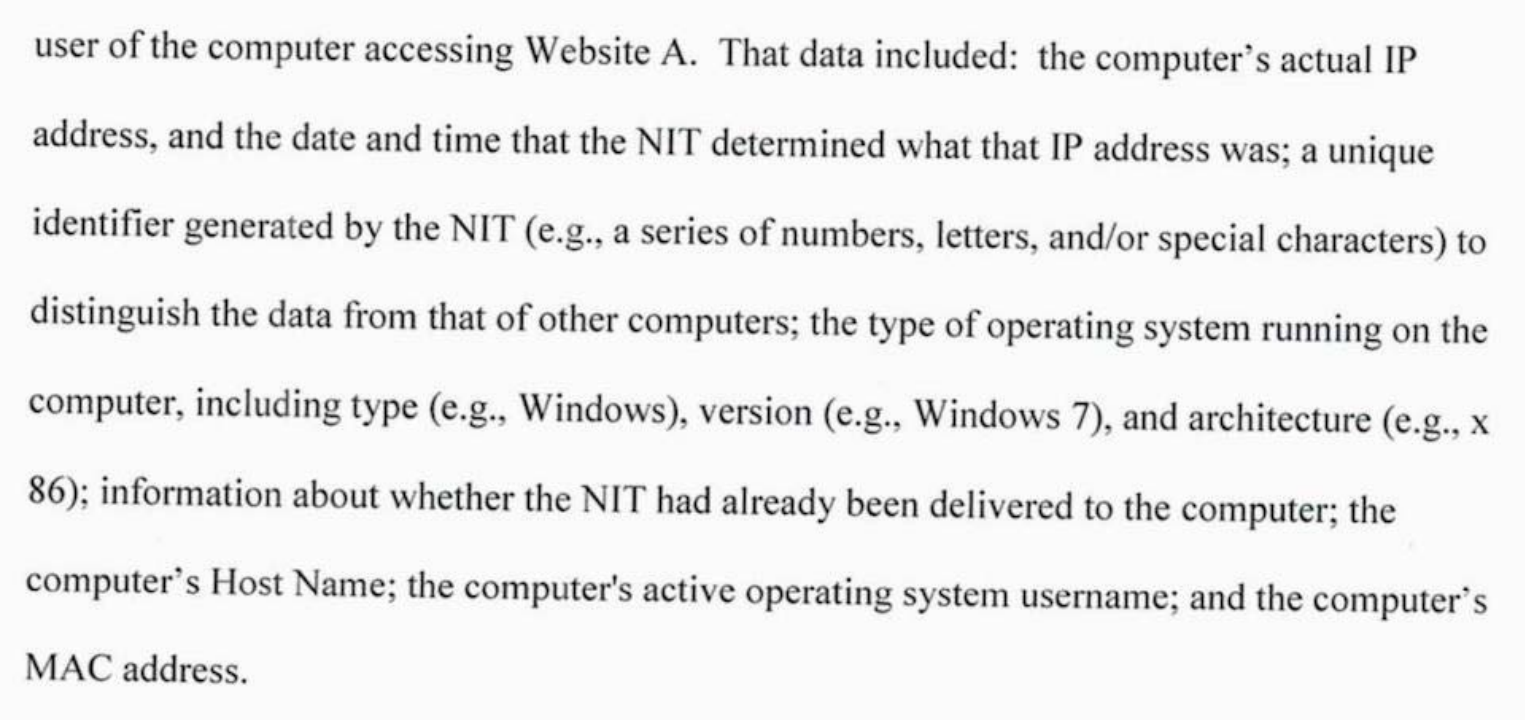
expansion of government surveillance and its use of illegal search methods on a massive scale."

NITs come in all sorts of different forms, and have been used since at least 2002 (http://www.wired.com/2009/04/fbi-spyware-pro/). Malware has been delivered (https://www.washingtonpost.com/business/technology/2013/12/06/352ba174-5397-11e3-9e2c-e1d01116fd98_story.html) to bomb threat suspects via phishing emails, and the FBI has also taken over hosting services and surreptitiously exploited a known bug in Firefox (http://www.wired.com/2013/09/freedom-hosting-fbi/) to identify users connecting with the Tor Browser Bundle.

In 2011, "Operation Torpedo" was launched, which saw the agency place an NIT on the servers of three different hidden services hosting child pornography, which would then target anyone who happened to access them. The NIT used a Flash application (http://www.wired.com/2014/12/fbi-metasploit-tor/) that would ping a user's real IP address back to an FBI controlled server, rather than routing their traffic through the Tor network and protecting their identity.

When WIRED reported (http://www.wired.com/2014/08/operation_torpedo/) on that operation in 2014, "over a dozen alleged users of Tor-based child porn sites" were headed for trial. And within a two-week period, the FBI reportedly collected IP addresses for at least 25 of the site's US visitors.

But the case of Playpen appears to be much, much broader in scope.


user of the computer accessing Website A. That data included: the computer's actual IP address, and the date and time that the NIT determined what that IP address was; a unique identifier generated by the NIT (e.g., a series of numbers, letters, and/or special characters) to distinguish the data from that of other computers; the type of operating system running on the computer, including type (e.g., Windows), version (e.g., Windows 7), and architecture (e.g., x 86); information about whether the NIT had already been delivered to the computer; the computer's Host Name; the computer's active operating system username; and the computer's MAC address.

A section of an affidavit in support of application for a search warrant, as part of the Playpen case, showing what sort of data the NIT sent to the FBI.

"We're not talking about searching one or two computers. We're talking about the government hacking thousands of computers, pursuant to a single warrant," said Soghoian, the ACLU technologist.

With earlier cases, the FBI's broad NIT attacks had used already known and patched vulnerabilities. But because the Tor Browser Bundle had no auto-update mechanism (http://www.wired.com/2014/08/operation_torpedo/) in August 2013—around the time of one of the FBI's attacks—only those users who bothered or remembered to patch their systems were safe. Evidentially, some people forgot.

The same might be true of the Playpen NIT: automatic updates to the Tor Browser Bundle were introduced in August 2015, months after the FBI had already obtained over a thousand IP addresses.

"There is no public information revealing whether or not the FBI used a zero-day in this case, or an exploit that targeted a known flaw," Soghoian said.

It’s not totally clear exactly how it was deployed, but the warrant allowed for anyone who logged into the site to be hacked.

Some clues about the Playpen NIT exist however. The NIT is likely different to the one used in Operation Torpedo because according to court filings that one is “no longer in use.” As for how the Playpen NIT operates, it’s not totally clear exactly how it was deployed, but the warrant allowed for anyone who logged into the site to be hacked.

“Basically, if you visited the homepage, and started to sign up for a membership, or started to log in, the warrant authorised deployment of the NIT,” Fieman said. From here, the NIT would send a target's IP address, a unique identifier generated by the NIT, the operating system running on the computer and its architecture, information about whether the NIT had already been deployed to the same computer, the computer's Host Name, operating system username, and the computer's MAC address.

Experts say that the true nature of NITs—that is, as powerful hacking tools—is kept from judges when law enforcement ask for authorisation to deploy them.

“Although the application for the NIT in this case isn't public, applications for NITs in other cases are (http://www.wired.com/2014/08/operation_torpedo/#slide-2),” said Soghoian. “Time and time again, we have seen the Department of Justice is very vague in the application they're filing. They don't make it clear to judges what they're actually seeking to do. They don't talk about exploiting browser flaws, they don't use the word 'hack.'”

“And even if judges know what they're authorizing, there remain serious questions about whether judges can lawfully approve hacking at such scale,” Soghoian added.

Magistrate Judge Theresa C. Buchanan in the Eastern District of Virginia, who signed the warrant used for the NIT, did not respond to questions on whether she understood that the warrant would grant the power to hack anyone who signed up to Playpen, or whether she consulted technical experts before signing it, and her office said not to expect a reply.

But Fieman said that the warrant “effectively authorizes an unlimited number of searches, against unidentified targets, anywhere in the world.”

While Soghoian warned about what this scale of hacking may signal for the future of policing. “This is a scary new frontier of surveillance, and we should not be heading in this direction without public debate, and without Congress carefully evaluating whether these kind of techniques should be used by law enforcement," he said.

The FBI did not provide a response in time for publication.

Plenty of questions remain about this law enforcement hacking operation, such as the exact wording used in the authorisation for the NIT, the technical aspects of the NIT itself, and how many computers were targeted outside of the United States.

The UK's National Crime Agency (NCA), which often receives intelligence from the FBI, told Motherboard in a statement that "The NCA does not routinely confirm or deny the receipt of specific intelligence for reasons of operational security. We work closely with international partners both in law enforcement and industry to share intelligence and work collaboratively to bring those involved in the sexual exploitation of children to account." Europol, Europe’s law enforcement agency, did not respond to a request for comment.

Regardless, in taking down one of the biggest dark web child pornography sites, the FBI also engaged in likely the largest law enforcement hacking campaign to date.

--

TOPICS: hacking (/tag/hacking), cybercrime (/tag/cybercrime), porn (/tag/porn), pornography (/tag/pornography), child pornography (/tag/child+pornography), FBI (/tag/FBI), Federal Bureau of Investigation (/tag/Federal+Bureau+of+Investigation), Operation Torpedo (/tag/Operation+Torpedo), tor (/tag/tor), IPs (/tag/IPs), features (/tag/features), Playpen (/tag/Playpen), servers (/tag/servers), NIT (/tag/NIT)

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).

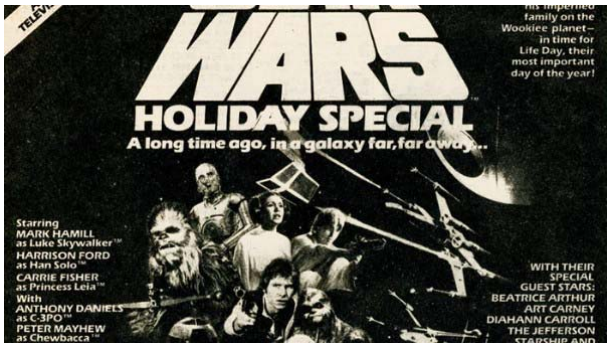
RECOMMENDED

Chaos Communication Congress Hackers Invaded Millions of Servers With a Poem (/read/chaos-communication-congress-hackers-invaded-millions-of-servers-with-a-poem?trk_source=recommended)

Malware Found Inside Downed Ukrainian Grid Management Points to Cyberattack (/read/malware-found-inside-downed-ukrainian-power-plant-points-to-cyberattack?trk_source=recommended)

The Dark Web Hacking Forum 'Hell' Is Back Online (/read/the-dark-web-hacking-forum-hell-is-back-online?trk_source=recommended)

Encryption and Other Tricks Are Making Malvertising Harder to Hunt (/read/encryption-and-other-tricks-are-making-malvertising-harder-to-hunt?trk_source=recommended)



We Talked to a Famous Adult Actress About the Promise of Virtual Reality Porn (/read/we-talked-to-a-famous-adult-actress-about-the-promise-of-virtual-reality-porn?trk_source=recommended)

That Time the 'Star Wars Holiday Special' Predicted VR Porn (/read/that-time-the-star-wars-holiday-special-predicted-vr-porn?trk_source=recommended)

print