The FBI Hacked Over 8,000 Computers In 120 Countries Based on One Warrant

6-7 minutes

In January, Motherboard reported on the FBI's "unprecedented" hacking operation, in which the agency, using a single warrant, deployed malware to over one thousand alleged visitors of a dark web child pornography site. Now, it has emerged that the campaign was actually an order of magnitude larger.

In all, the FBI obtained over 8,000 IP addresses, and hacked computers in 120 different countries, according to a transcript from a recent evidentiary hearing in a related case.

The figures illustrate the largest ever known law enforcement hacking campaign to date, and starkly demonstrate what the future of policing crime on the dark web may look like. This news comes as the US is preparing to usher in changes that would allow magistrate judges to authorize the mass hacking of computers, wherever in the world they may be located.

"We have never, in our nation's history as far as I can tell, seen a warrant so utterly sweeping," federal public defender Colin Fieman said in a hearing at the end of October, according to the transcript. Fieman is representing several defendants in affected cases.

Those cases revolve around the FBI's investigation into dark web child pornography site Playpen. In February 2015, the FBI seized the site, but instead of shutting it down, the agency ran Playpen from a government server for 13 days. However, even though they had administrative control of the site, investigators were unable to see the real IP address of Playpen's visitors, because users typically connected to it through the Tor network.

In order to circumvent that anonymity, the FBI deployed what it calls a network investigative technique (NIT), or a piece of malware. That malware, which included a Tor Browser exploit, broke into the computer of anyone who visited certain child pornography threads on Playpen. It then sent the suspect's real IP address back to the FBI.

According to court filings, the FBI obtained over 1,000 IP addresses of alleged US-based users. Over the past year, Motherboard has also found that the FBI hacked computers in Australia, Austria, Chile, Colombia, Denmark, Greece, and likely the UK, Turkey, and Norway too.

But, those are only a tiny handful of countries in which the FBI was hacking computers. According to the newly published transcript, the FBI hacked computers in at least 120 countries.

"The fact that a single magistrate judge could authorize the FBI to hack 8000 people in 120 countries is truly terrifying," Christopher Soghoian, principal technologist at the American Civil Liberties Union (ACLU) told Motherboard in a phone call. (Soghoian has testified for the defense in Playpen cases).

Bizarrely, the FBI also hacked what has been described as a "satellite provider," according to the transcript.

"So now we are into outer space as well," Fieman said in the hearing.

Image: United States District Court Western District of Washington at Tacoma

The Department of Justice has had an intense battle on its hands over the past few months, especially around the validity of the warrant used for this hacking operation. According to a filing from the Department of Justice, fourteen court decisions have found that the warrant was not properly issued pursuant to Rule 41 of the Federal Rules of Criminal Procedure, which governs how search warrants can be authorized.

The main issue has been that the judge who signed the warrant, Magistrate Judge Theresa C. Buchanan in the Eastern District of Virginia, did not have the authority to greenlight searches outside of her own district. In four cases, courts have then decided to throw out all evidence obtained by the malware because of the violation.

But, changes to Rule 41 will likely come into effect on December 1, meaning that magistrate judges will be allowed to authorize warrants just like the one used in the Playpen investigation.

The changes "give rank and file law enforcement officers way too much discretion to conduct hacking techniques within and outside the United States," Ahmed Ghappour, visiting assistant professor at UC Hastings College of Law, and author of the paper "Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web," told Motherboard in a phone call.

Soghoian added "With the changes to Rule 41, this is probably the new normal."

"We should expect to see future operations of this scale conducted not just by the FBI, but by other federal, state and local law enforcement agencies, and we should expect to see foreign law enforcement agencies hacking individuals in the United States, too," he added.

Indeed, in August Motherboard reported that Australian authorities had hacked criminal suspects in the United States. It is unclear whether a warrant was obtained.

The Department of Justice said it received Motherboard's request for comment, but did not provide a direct response in time for publication. However, the DoJ published a blog post on Monday further justifying the Rule 41 changes.

"We believe technology should not create a lawless zone merely because a procedural rule has not kept up with the times," Assistant Attorney General Leslie R. Caldwell of the Criminal Division wrote.

The FBI declined to comment.

As far as is publicly known, these mass hacking techniques have been limited to child pornography investigations. But with the changes to Rule 41, there is a chance US authorities will expand their use to other crimes too.

"That's the real question: are they going to use watering-hole attacks, are they going to use network investigative techniques to pursue, for example, visitors of the Silk Road, or visitors of a drug marketplace, or other types of illicit services?" Ghappour said.