This is how the government is catching child porn users; Investigators are using techniques more typically used by hackers to find criminals on the dark Web.

Washington Post Blogs

January 21, 2016 Thursday 6:07 PM EST

washingtonpost.com

Length: 1503 words

Byline: Ellen Nakashima

Body

The user's online handle was Pewter, and while logged onto a website called Playpen, he allegedly downloaded images of young girls being sexually molested.

Pewter had carefully covered his tracks. To reach the site, he first had to install free software called Tor, the world's most widely-used tool for giving users anonymity online.

In order to uncover Pewter's true identity and location, the FBI quietly turned to a technique more typically used by hackers. The agency, with a warrant, surreptitiously placed computer code, or malware, on all computers that logged into the Playpen site. When Pewter connected, the malware exploited a flaw in his browser, forcing his computer to reveal its true Internet protocol address. From there, a subpoena to Comcast yielded his real name and address.

Pewter was unmasked last year as Jay Michaud, a 62-year-old administrator in the Vancouver, Wash., public schools. With a second warrant, agents searched the suspect's home and found a thumb drive that allegedly contained multiple images of children engaged in sex acts. Last July, Michaud was arrested and charged with possession of child pornography.

Michaud's is the lead case in a sweeping national investigation into child porn on the so-called dark Web, the universe of sites that are off Google's radar and where users can operate with anonymity.

As criminals become savvier about using technology such as Tor to hide their tracks, investigators are turning to hacking tools to thwart them. In some cases, law enforcement is placing malware on sites that might have thousands of users. Some privacy advocates and analysts worry that in doing so, investigators may also wind up hacking and identifying the computers of law-abiding people who are seeking to remain anonymous, people who can also include political dissidents and journalists.

″As the hacking techniques become more ambitious, failure in execution can lead to large-scale privacy and civil liberties abuses at home and abroad,″ said Ahmed Ghappour, a professor at the University of California Hastings College of Law. ″It's imperative that Congress step in to regulate exactly who and how law enforcement may hack.″

But Justice Department officials said that the government investigates crime based on evidence of illegal activities. ″When we obtain a warrant, it's because we have convinced a judge that there is

probable cause that we'll be able to find evidence in a particular location," said a senior department official, who spoke on condition of anonymity under ground rules set by the department.

In the Playpen case, the government activated malware on a site with 215,000 members as of last February and obtained Internet protocol addresses of 1,300 computers. Out of that group, the government said it has charged 137 people.

"It's a lot of people," said Colin Fieman, a public defender in Tacoma representing Michaud. "There never has been any warrant I've seen that allows searches on that scale. It is unprecedented."

Michaud is arguing that his charges be dismissed on grounds that the government's use of the tool violated the Fourth Amendment. Fieman argues that some people might have gone to the site seeking to express fantasies, which while repugnant, are legal. The site, he said, doesn't clearly advertise itself as devoted to child pornogaphy.

He likened the government's warrant to a "general warrant," referring to the British practice during the colonial era of allowing government searches without any individualized suspicion.

The judge in Michaud's case is scheduled on Friday to hear several motions that could result in the dismissal of charges against him.

"This is a gray area in the law," said Thomas Brown, a former federal prosecutor in the Southern District of New York who handled cases involving the use of hacking techniques. "It's another instance where you've got technology outstripping the law."

Fieman also said that rules established by the federal courts, grounded in constitutional principles, require that a warrant be deployed in the district in which it is issued - in this case, the Eastern District of Virginia. Michaud's computer was in Vancouver.

But prosecutors argue that the technique is lawful and that in general a warrant may be issued even when the location to be searched is unknown, as long as there is probable cause that the search will turn up evidence of a crime.

"The Supreme Court has made clear that the Fourth Amendment . . . does not preclude use of warrants where the purpose of the search is to discover the location of the place to be searched," said David Bitkower, then a deputy assistant attorney general, in a Dec. 2014 letter to a federal courts committee weighing changes to the rule that governs how search warrants are issued.

In the Playpen case, the government argued that it had probable cause to search the computers of anyone who navigated to the site - whether one person or 10,000 people - on the grounds that the site was devoted to child porn and anybody who knew how to get to it likely did so with the intent to view the content. The site can't be found through a Google search and can only be reached by users who know its exact, algorithm-generated Web address and are using special software that connects to the Tor network.

In such a case, "we have an obligation to investigate all 10,000 [people], not just one," prosecutor Keith Becker told Judge Robert J. Bryan of the U.S. District Court at a hearing in the Western District of Washington at Tacoma in December.

[Meet the woman in charge of the FBI's most controversial high-tech tools]

The FBI seized Playpen last year, and after operating it for two weeks, shut it down. During those two weeks, according to court documents, it deployed what it obliquely calls a ″network investigative technique,″ or NIT, to capture the IP address of anyone who logged into the website.

″In general, the constitution doesn't say that we have to stop investigating just because we need to use a computer technique to identify suspects rather than opening a letter or entering a private house,″ said the senior department official. ″The law doesn't give online pedophiles immunity from court-authorized search warrants just because they're using modern software.″

Fieman also argued that the government itself violated the law when it seized Playpen last year and then rather than shut it down immediately or find ways to reroute visitors, continued to operate the child porn site.

″What the government did is comparable to flooding a neighborhood with heroin in the hope of snaring an assortment of low-level drug users,″ Fieman said in a motion to dismiss filed in November.

Justice Department spokesman Peter Carr said that ″at no time in an operation like this does the FBI post any images, videos or links to images of child pornography.″ Any such postings are done by website users, not the FBI, he said. Also, he said, immediately shutting down a website would prevent law enforcement from identifying the offenders and frustrate efforts to identify and rescue child victims from abuse.

Without using the hacking technique, officials say, it would be very difficult to locate pedophiles who go to great lengths to hide their tracks.

The issue, said Ghappour, the law professor, is not the use of the malware per se, but ″whether hacking warrants are written narrowly enough to guarantee that only those culpable set the trigger [to launch the NIT], and consequently get hacked,″ he said. ″Given the scale of these operations, the smallest mistake could result in hundreds, if not thousands, of privacy violations.″

Privacy advocates concerned about the government doing mass hacks point to the case of TorMail, an anonymous email service, now shuttered. TorMail, which despite the name is not affiliated with the group behind Tor, was used by a range of people, from criminals to dissidents and journalists.

In the summer of 2013, reports surfaced of people trying to log in to TorMail and finding a Down for Maintenance message instead, and finding suspicious-looking code included in the TorMail Web page. Security researchers who analyzed the code concluded that it was likely placed there by the FBI.

At the time, the government would not confirm that the bureau was behind the hack. This week, people familiar with the investigation confirmed the FBI had used an NIT on TorMail. But, they said, the bureau obtained a warrant that listed specific email accounts within TorMail for which there was probable cause to believe the true user was engaged in illicit child pornography activities. In that way, the sources said, only suspects whose accounts had in some way been linked to involvement in child porn would have their computers infected.

An FBI official said the bureau recognizes that the use of the NIT is ″intrusive″ and should only be used ″in the most serious cases.″ He said the FBI uses the tool only against offenders who are ″the worst of the worst.″

ellen.nakashima@washpost.com

Classification

Language: ENGLISH

Publication-Type: Web Blog

Subject: ARREST WARRANTS (90%); PORNOGRAPHY (90%); INVESTIGATIONS (90%); SEX OFFENSES (90%); LAW ENFORCEMENT (89%); PROBABLE CAUSE (89%); CHILD PORNOGRAPHY (78%); CRIMINAL INVESTIGATIONS (78%); SEXUAL ASSAULT (78%); ARRESTS (78%); CHILD SEXUAL ABUSE (78%); EDUCATION SYSTEMS & INSTITUTIONS (77%); JUSTICE DEPARTMENTS (76%); COMPUTER CRIME (75%); SEARCH & SEIZURE (75%); SUBPOENAS (74%); CHILDREN (73%); LAW SCHOOLS (73%); PUBLIC DEFENDERS (71%); PRIVACY RIGHTS (63%); COLLEGE & UNIVERSITY PROFESSORS (60%)

Company: GOOGLE INC (84%)

Ticker: GOOG (NASDAQ) (84%)

Industry: MALICIOUS SOFTWARE (90%); HIDDEN WEB (90%); COMPUTER EQUIPMENT (89%); COMPUTER SOFTWARE (78%); EDUCATION SYSTEMS & INSTITUTIONS (77%); COMPUTER CRIME (75%); LAW SCHOOLS (73%); PUBLIC DEFENDERS (71%); FLASH DRIVES (70%); NETWORK PROTOCOLS (69%); COLLEGE & UNIVERSITY PROFESSORS (60%)

Geographic: WASHINGTON, USA (79%); CALIFORNIA, USA (73%)

Load-Date: January 21, 2016