FBI keeping hack tools under wraps (+video)

Herald Democrat (Sherman, Texas)

April 1, 2016 Friday

Length: 1190 words

Byline: Paresh Dave and David Pierson Los Angeles Times

Body

LOS ANGELES - Even when courts compel law enforcement agencies to reveal the ways they hack into technology products, it's criminal suspects - not the makers of hardware or software - who are most likely to learn the details.

As Apple Inc. considers legal tactics that could force the FBI to share how it unlocked an iPhone belonging to one of the San Bernardino, Calif., shooters, a federal court case in Washington illuminates how the judicial process can leave the tech world in the dark.

The case involves the Tor browser, which is popular among activists, dissidents, journalists - and those who want to mask their identities when surfing online. The FBI hacked the browser as part of a sweeping child pornography investigation that led to 1,300 suspects.

In one of the cases, a judge has ordered that the FBI give defense attorneys details about the software flaw that allowed the FBI to identify suspect Jay Michaud of Vancouver, Wash., whose prosecution has been at the forefront of the investigation. But prosecutors on Tuesday opposed the ruling in a heavily redacted document.

They say the defense already has enough information to analyze the operation. And former federal prosecutors say disclosing the vulnerability takes away the ability to use the technique to nab more offenders.

But technology developers and privacy activists fear that consumers' safety could be put at risk if the Tor issue turns out to be an unpatched bug.

The tension will manifest in ″much more litigation to understand the techniques used to capture individuals,″ said Michael Zweiback, an attorney at Alston & Bird and former chief of the Justice Department's cybercrimes section.

The issue will not go away as the FBI's growing interest in probing the Internet for criminal activity will require using ″techniques that are more proactive - that are recognized exploits - to get access to information,″ Zweiback said.

In the Washington case, federal agents briefly seized control of Playpen, a secretive online forum, accessible through Tor, where more than 214,000 members traded what authorities describe as sexually

explicit photos and videos, including of children. The FBI learned the Internet protocol addresses of Playpen visitors by using a software bug linked to Tor to defeat the browser's security measures.

Public defenders for Michaud, who is charged with possession of child pornography, say they can't fully vet the legality of the FBI's investigation without knowing how the agency hacked Tor. While the government has turned over details about the software that identified his address, it hasn't shared information about how that tracking tool was introduced.

Prosecutors and experts say what matters is that the hack didn't tamper with Michaud's data.

"Getting through the lock doesn't matter, as long as the information on the other side of the door isn't affected," Zweiback said, comparing digital searches with physical ones.

Colin Fieman, an attorney for Michaud, told a judge in his case last month that the government's objections to revealing the vulnerability were "puzzling." The information wasn't classified or confidential, he said, according to a court transcript.

Law enforcement generally seeks to protect its hacking methods as long as possible because the techniques' usefulness shrinks when the public or manufacturers are aware, Zweiback said.

Fieman said only his technological expert would examine the hacking tool.

"We are not looking to circulate this stuff," he told the court. "We just need to look at it."

Last month, U.S. District Judge Robert Bryan ruled in favor of Fieman and Michaud. But prosecutors this week asked Bryan to reconsider, saying that the additional information wouldn't address the defense's concerns. Justice and FBI officials didn't have immediate comment.

Fieman in an email Wednesday said he disagreed with the government's assertion that law enforcement privilege "should trump a defendant's constitutional rights to an effective defense and fair trial."

Though his team may eventually gain access to details of the FBI method, Tor has little recourse. Suing the government to get the same information is unlikely to end well, legal experts said.

Kate Krauss, director of communications and public policy for the Cambridge, Mass.-based nonprofit that develops and operates the browser, said her colleagues suspect that the issue exploited by the FBI has been fixed, but they want to confirm that.

"We're watching with interest," Krauss said over a voice call on the encrypted chat app Signal. "We're the gold standard for online anonymity software, and we're committed to keeping the security stronger."

It's a desire shared by Apple too. Attorneys for the Cupertino, Calif., company say they plan to insist that the government explain how, with the help of an undisclosed outside group, investigators bypassed an iPhone 5c's security - the same device authorities had maintained couldn't be opened without Apple's assistance.

Krauss said Tor, just like the tech industry at large, prefers that people who find vulnerabilities in products privately report them so they can be fixed before they are turned against users. But law

enforcement and counterterrorism agencies maintain a narrow set of bugs are better left untouched for investigative purposes.

Apple and Tor may never confirm the FBI's tactics. But the publicity around the two incidents could lead judges overseeing similar cases to ask more questions, said Robert Cattanach, a former Justice Department attorney who specializes in cybersecurity for the law firm Dorsey & Whitney.

″You have skeptical judges and criminal defense lawyers using San Bernardino to exploit ways to get under the FBI's skin if nothing else,″ Cattanach said. ″Even the most neutral federal judge is going to give pause when the FBI makes representations.″

Michael Vatis, a former official with the Justice Department and FBI, now a partner at Steptoe & Johnson, said any time that the FBI uses a technical vulnerability in a case, details of it are kept under seal. But Cattanach said there were instances, though rare, when the FBI revoked cases because it was asked to share hacking methods, even just to defendants and their attorneys. He declined to provide details.

Attorneys said the question of when authorities must bare all is set to explode in significance. The FBI and police will need to rely increasingly on taking advantage of technical flaws to ferret out cybercriminals as tech companies introduce stronger security protections.

″There's been some frustration at the FBI that they're operating with one hand tied behind their back,″ Cattanach said. ″They've since realized that if you're going to beat the bad guys at their own game, you've got to play the game.″

But in improving capabilities, the FBI has turned into yet another security research group that tech firms want to learn from.

″There is a great deal of irony … that the FBI is being asked to reveal their work now″ in the Michaud case, Vatis said.

Visit the Los Angeles Times at *www.latimes.com*

Distributed by Tribune Content Agency, LLC.

Classification

Language: ENGLISH

Publication-Type: Newspaper

Subject: LAW ENFORCEMENT (90%); INVESTIGATIONS (90%); SPECIAL INVESTIGATIVE FORCES (90%); CRIMINAL INVESTIGATIONS (89%); SEX OFFENSES (89%); FEDERAL INVESTIGATIONS (89%); CHILD PORNOGRAPHY (88%); PORNOGRAPHY (88%); LAW

COURTS & TRIBUNALS (78%); COMPUTER CRIME (78%); LAWYERS (78%); CYBERCRIME (78%); JUSTICE DEPARTMENTS (78%); LITIGATION (78%); CHILDREN (74%); PUBLIC DEFENDERS (73%); JUDGES (73%)

Company: APPLE INC (84%); ALSTON & BIRD LLP (58%)

Industry: COMPUTER SOFTWARE (89%); INTERNET & WWW (89%); COMPUTER CRIME (78%); LAWYERS (78%); CYBERCRIME (78%); LITIGATION (78%); HIDDEN WEB (78%); SOFTWARE DEFECTS (77%); PUBLIC DEFENDERS (73%); MOBILE & CELLULAR TELEPHONES (72%); NETWORK PROTOCOLS (50%)

Geographic: SAN BERNARDINO, CA, USA (79%); LOS ANGELES, CA, USA (79%); WASHINGTON, USA (79%); CALIFORNIA, USA (79%); UNITED STATES (92%)

Load-Date: April 4, 2016