The FBI Used Classified Hacking Tools in Ordinary Criminal Investigations

Joseph Cox ⋮ 6-7 minutes ⋮ 3/29/2018

The FBI's Remote Operations Unit (ROU), tasked with hacking into computers and phones, is one of the Bureau's most elusive departments. But a recent report from the Office of the Inspector General (OIG) for the Department of Justice has now publicly acknowledged the unit's existence seemingly for the first time. The report also revealed that the ROU has used classified hacking tools—techniques typically reserved for intelligence purposes—in ordinary criminal investigations, possibly denying defendants the chance to scrutinize evidence, as well as destabilizing prosecutors' cases against suspects.

"Using classified tools in criminal cases is risky for all sides," Ahmed Ghappour, associate professor of law at Boston University School of Law, and who has researched law enforcement hacking extensively, told Motherboard in a Twitter message.

Videos by VICE

The ROU is part of the FBI's Operational Technology Division (OTD), which handles the Bureau's more technical surveillance methods. The OIG's report says ROU "provides computer network exploitation capabilities" and has "engineers and vendors who attempt to develop techniques that can exploit mobile devices." A previous *Wall Street Journal* report said the FBI can use malware to remotely activate microphones on Android devices.

In 2013, then American Civil Liberties Union (ACLU) principal technologist Chris Soghoian uncovered ROU's existence by piecing together LinkedIn profiles and sections of documents released through the Freedom of Information Act. Soghoian found that an Eric Chuang heads the ROU, and it appears Chuang is still leading the unit now—the OIG report mentions the current head became chief in 2010.

While most of the OIG's new report focuses on how the FBI did not fully explore its technical options for accessing the iPhone of one of the San Bernardino terrorists in 2016, several sections shine more light on the ROU, and how they are using their hacking tools. One mentions the ROU chief, based on long standing policy, sees a "line in the sand" against using national security tools in criminal cases—this was why the ROU initially did not get involved at all with finding a solution to unlocking the San Bernardino iPhone. Indeed, it's important to remember that as well as a law enforcement agency, the FBI also acts as an intelligence body, gathering information that may be used to protect the country, rather than bring formal charges against suspects.

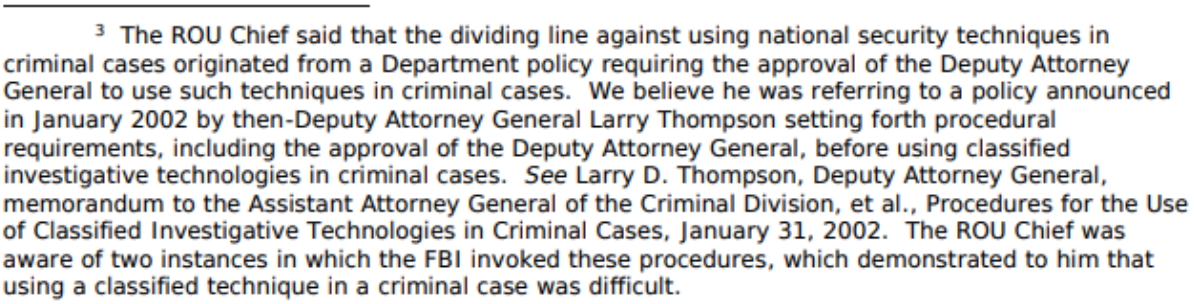
Got a tip? You can contact this reporter securely on Signal on +44 20 8133 5190, OTR chat on jfcox@jabber.ccc.de, or email joseph.cox@vice.com.

But that line can be crossed with approval of the Deputy Attorney General to use the more sensitive techniques in ordinary investigations, the report adds.

"The ROU Chief was aware of two instances in which the FBI invoked these procedures," a

footnote in the report reads. In other words, although it seemingly only happened twice, the FBI has asked for permission to use classified hacking techniques in a criminal case.

It's not clear which two cases the ROU Chief is referring to. However, the FBI previously deployed a Tor Browser exploit to over 8,000 computers around the world, including some in China, Russia, and Iran, based on one, legally contentious warrant. At the time of the operation in February 2015, the tool was unclassified. But as Motherboard found using court records, the following year the FBI moved to classify the exploit itself for reasons of national security, despite the case being a criminal child pornography investigation.



[3] The ROU Chief said that the dividing line against using national security techniques in criminal cases originated from a Department policy requiring the approval of the Deputy Attorney General to use such techniques in criminal cases. We believe he was referring to a policy announced in January 2002 by then-Deputy Attorney General Larry Thompson setting forth procedural requirements, including the approval of the Deputy Attorney General, before using classified investigative technologies in criminal cases. *See* Larry D. Thompson, Deputy Attorney General, memorandum to the Assistant Attorney General of the Criminal Division, et al., Procedures for the Use of Classified Investigative Technologies in Criminal Cases, January 31, 2002. The ROU Chief was aware of two instances in which the FBI invoked these procedures, which demonstrated to him that using a classified technique in a criminal case was difficult.

Caption: A section of the OIG report discussing the ROU and the chief's position on national security and criminal investigations.

Motherboard's recent investigation into the exploit industry found that an Australia-based company called Azimuth Security, along with its partner Linchpin Labs, has provided exploits to the FBI, including one for breaking through the Tor Browser.

Using classified tools in a criminal investigation may pose issues for both prosecutors and defendants. If the FBI used a classified technique to identify a suspect, does the suspect find out, and have a chance to question the legality of the search used against them?

"When hacking tools are classified, reliance on them in regular criminal investigations is likely to severely undermine a defendant's constitutional rights by complicating discovery into and confrontation of their details," Brett Kaufman, a staff attorney at the ACLU, told Motherboard in an email. "If hacking tools are used at all, the government should seek a warrant to employ them, and it must fully disclose to a judge sufficient information, in clear language, about how the tools work and what they will do," he added.

And on the flip side, if the FBI uses a classified and sensitive tool in an ordinary case, and has to reveal information about it in court, the exploit may then be fixed by the affected vendor, such as, say, Apple. Some may seen that as a positive, but the FBI might have to drop their charges against a criminal as well.

"It's also a risk for the government, who may be ordered to disclose classified information to the defense to satisfy due process, or face dismissal of the case," Ghappour said.

With the mentioned Tor Browser attack, a judge ordered the FBI to give defense counsel the code of the exploit; the FBI refused, meaning the evidence the related malware obtained was thrown out altogether.

A spokesperson for the FBI declined to comment on the ROU's cross-over into criminal cases, and instead pointed to page 16 of the report, which reads, in part, that "FBI/OTD has realigned mission areas for several Units in preparation for a larger re-organization."