Justice Dept: Trust Us to Not Abuse the CFAA, a Hacking Law We've Always Abused

Written by

JASON KOEBLER

STAFF WRITER

March 19, 2015 // 05:13 PM CET

President Obama and the Justice Department want Congress to revise a controversial computer hacking law to make it illegal to buy, sell, or rent botnets—the large networks of virus-infected computers that can be used to slow down network traffic, spam people, and brute-force their way into computer systems.

The language the White House wants to use to amend the Computer Fraud and Abuse Act makes it illegal to use more than 100 computers "without authorization." It also criminalizes not just password "trafficking," but the sharing of any "means of access" to computers "without authorization," which would include botnets. Problem is, there are legitimate uses for botnets that would technically become illegal if the law is revised.

A handful of researchers around the world have employed botnets as a means of learning how they work, what they can be used for, how they can be tracked, and how they can be created. Others have used them to reveal various vulnerabilities in computer systems or to map the internet.

"The expansion of the definition [to 'means of access'] may impact researchers who commonly scan public websites to detect potential vulnerabilities," the Electronic Frontier Foundation wrote in a blog post. "These researchers should not have to face a felony charge if a prosecutor thinks they should have known the site prohibited scanning."

The Justice Department's response to that concern is "trust us."

"Some commentators have raised the concern that this proposal would chill the activities of legitimate security researchers, academics, and system administrators," Leslie Caldwell, the DOJ's assistant attorney general wrote in a blog post Wednesday. "We take this concern seriously. We have no interest in prosecuting such individuals, and our proposal would not prohibit such legitimate activity."

Caldwell goes on to explain that there is language in the bill that would make it illegal only if the person “knew it was wrongful.” The EFF says that’s not enough, and a careful reading of the proposed language doesn’t seem to provide any specific protection to researchers.

It's hard to take the Department of Justice at its word when it says it will stick very close to the statute when it prosecutes those who use, buy, sell, and create botnets. Federal prosecutors have notoriously abused the language of the Computer Fraud and Abuse Act, at times stretching the definition of certain provisions of it to prosecute people who accessed computers doing nothing that even resembled hacking.

Internet activist Aaron Swartz was prosecuted for downloading a huge number of science papers from a database he had access to, internet troll Weev was prosecuted for exploiting a flaw in AT&T's website that gave out iPad users' email addresses, and others have been prosecuted merely for sharing passwords. The only charge that stuck for the "Cannibal Cop"—that he illegally used his access to a police database—was brought under the CFAA; what he did was creepy and dangerous, but not hacking.

"The [CFAA] has definitely been susceptible to abuse. It's been stretched in ways that are improper." Hanni Fakhoury, a staff lawyer for the Electronic Frontier Foundation, told me. "The malleability of the CFAA to provide a tool for law enforcement to prosecute cases like these suggests that the law is problematic."

The law, it seems, might be about to get a lot more malleable. We've seen Obama's administration take this tack of selective enforcement in the past, most notably with the Defense of Marriage Act, illegal immigration, and legal weed in Washington and Colorado. The question is, are we willing to trust his administration at his word? More importantly, do we want to continue to put ever-expansive laws on the books, knowing that the next president might not follow suit?

TOPICS: Computer Fraud and Abuse Act, power, justice department, CFAA, EFF, electronic frontier foundation, Aaron Swartz