GlobalResearch
Center for Research on Globalization

FBI Wants to Hack Computers Globally, Seeks Search Warrant Expansion

By RT
Global Research, November 06, 2014
RT

Region: USA
Theme: Intelligence, Police State & Civil Rights

The Justice Department is looking to remove restrictions on the FBI's ability to hack into and monitor computer systems everywhere by easing the requirements necessary for it to obtain a search warrant.

Currently, law enforcement agencies can only receive warrants authorizing computer searches if the physical location of the computer in question falls within the corresponding jurisdiction of the judge they are appealing to. If the computer is outside of the judge's jurisdiction, a warrant is not usually granted.

Now, however, the Justice Department wants to change this limitation, which is called Rule 41. It has asked a judicial advisory committee to allow judges to grant search warrants and permit electronic surveillance regardless of where a computer is located – within or outside of the United States,

Here's why, according to the National Journal, which reported on the story:

> "Law-enforcement investigators are seeking the additional powers to better track and investigate criminals who use technology to conceal their identity and location, a practice that has become more common and sophisticated in recent years. Intelligence analysts, when given a warrant, can infiltrate computer networks and covertly install malicious software, or malware, that gives them the ability to control the targeted device and download its contents."

Image: The Justice Department in Washington (Reuters / Gary Cameron)

The proposal has unsurprisingly upset many civil liberties advocates, who claim changing Rule 41 in this manner would potentially violate the Fourth Amendment, which protects Americans from unreasonable search and seizures by the government.

The panel, known as the Advisory Committee on Criminal Rules, held a hearing on the issue on Wednesday, where opponents of the rule change expressed their views. Asked what other methods would be preferable for hunting down increasingly sophisticated cyber criminals, Amie Stepanovich of the digital freedom group Access said the Justice Department should go through Congress.

“I empathize that it is very hard to get a legislative change,” she said. “However, when you have us resorting to Congress to get increased privacy protections, we would also like to see the government turn to Congress to get increased surveillance authority.”

That sentiment was echoed by the American Civil Liberties Union the day before, and the group was also present at Wednesday’s hearing.

“If the proposed amendment is adopted, it will throw the doors wide open to an industry peddling tools to undermine computer security, and make the U.S. government an even bigger player in the surveillance software industry,” ACLU Staff Attorney Nathan Wessler wrote on Tuesday.

> Govt’s proposed change to rules on search warrants cld be a major boost to zero-day market, making us all less safe. https://t.co/Hmi7T6w4BQ
>
> — ACLU National (@ACLU) November 4, 2014

In its report, the ACLU noted that changing the rule could also promote the use of “zero-day” exploits, which are completely unknown to software manufacturers yet used by governments to get around security systems and enable surveillance.

“Governments pay big bucks – reportedly into the hundreds of thousands of dollars – to acquire [zero-day exploits], resulting in a largely unregulated market for these tools,” Wessler wrote. “Since the use of a given zero-day exploit depends on the continued existence of the vulnerability it’s exploiting, governments withhold their existence from the manufacturer.”

This isn’t the first time law enforcement has expressed a desire to retain its surveillance capabilities. Following decisions by Apple and Google to enable data encryption on their new devices, FBI Director James Comey criticizedthe moves, saying they will ultimately impede police ability to track and capture criminals.

“There will come a day — well it comes every day in this business — when it will matter a great, great deal to the lives of people of all kinds that we be able to with judicial authorization gain access to a kidnapper’s or a terrorist or a criminal’s device,” Comey said in September. “I just want to make sure we have a good conversation in this country before that day comes.”

Articles by: RT