Justice Department seeks massive expansion of FBI hacking powers

Thomas Gaist
3 November 2014

The US Department of Justice (DOJ) is seeking a massive expansion of the Federal Bureau of Investigation's authority to conduct computer hacking operations against civilian PCs, tablets and smartphones, both within the US and internationally.

Proposed legal amendments submitted by the DOJ, currently under consideration by a little-known body called the Advisory Committee on Criminal Rules, would allow the FBI to effectively dispense with constitutional restrictions on its computer hacking operations, according to reports produced by the Center for Democracy and Technology (CDT) and other NGOs.

The DOJ proposes modifying Rule 41 of the Federal Rules of Criminal Procedure, which outlines the warranting process police agencies must follow to comply with the Fourth Amendment to the Constitution, a core element of the US Bill of Rights.

The DOJ amendment states that a central purpose of the new regulations is to allow FBI agents to "use remote access to search electronic storage media to seize or copy electronically stored information."

Up to now the FBI has been required, by legal regulations based on the Fourth Amendment, to submit individualized warrants showing that hacking the targeted machine was necessary to investigate a suspected criminal. The bureau has also been required to submit specific requests for every aspect of the surveillance operations it wants to execute against the machine (such as activating the camera, seizing or deleting a certain file, or sending a fake email).

Whereas Fourth Amendment-based regulations require that warrants be very specific, the new rules will allow FBI agents to rifle through the entire contents of targeted machines, including audio and video recordings, images captured by laptop cameras, and data from motion sensors and biometric tracking devices.

"While the particularity of a warrant under the 4th Amendment requires the government to specify exactly the materials they seek to search for and seize, the proposed amendment would grant access to a panoply of sensors on modern computing platforms," the CDT warns.

The Obama DOJ's "legal" recommendations would streamline the warranting process, allowing the FBI to launch mass hacking operations based on very general criteria that can be reinterpreted to suit the needs of the government.

"The proposed modification to Rule 41 would enable the US government to gain authorization from any district judge in the United States to spread invasive malware - code that may penetrate, search, and copy electronic media without user authorization – to potentially any computer worldwide," the CDT's official statement notes.

The bureau's malware programs give FBI agents unrestricted access to the hard drives and main computing functions of targeted machines, enabling them to perform every conceivable manipulation, including:

- stealing and deleting data;
- sending forged emails and other electronic messages;
- using stored photos to create fake online profiles;
- installing software;
- identifying the precise geographical location of the machine.

The most sophisticated and invasive forms of malware, sometimes referred to as "rootkits," are designed to overcome all antivirus protections and to thwart existing malware removal techniques, embedding themselves in machines permanently.

Boiled down, the bureau's malware allows it to completely hijack and remotely control targeted computers anywhere on the planet.

The scope of the hacking authority sought by the FBI is essentially infinite. As the CDT noted in its report, "The target device can be potentially any device attached to the Internet from personal computing devices to industrial control systems to Internet voting systems."

"We are talking here about giving the FBI the green light to hack into any computer in the country or around the world," commented technologist Chris Soghoian with the American Civil Liberties Union (ACLU).

The FBI has been developing an elite hacker unit, known as the "Secure Technologies Exploitation Group," since at least 2007, according to a leaked document cited by the ACLU's Soghoian.

The DOJ amendments propose to allow such comprehensive hacking operations by the government against any data-bearing devices that fall under any of three general criteria:

• They hold data that is "concealed through technological means";

• They have been "damaged" by any form of infectious software;

• They are connected with computer networks spanning five or more districts.

The vague and downright bizarre legal concepts advanced by the DOJ's lawyers grant the FBI authority to implant ultrasophisticated malware on millions and even hundreds of millions of servers, personal computers and Internet accessing devices worldwide. The CDT notes in its report that millions of computers can easily be targeted using these principles.

The "technological concealment" criterion would authorize FBI agents to sift through and sabotage any machine or network that utilizes widely used encryption or antisurveillance software, which is becoming standard practice for any organization remotely critical of the state or the capitalist class.

This criterion may even be used to justify hacking against Facebook users suspected of employing "concealment" by listing an inaccurate location on their profile.

The FBI's "damaged machine" criterion can be interpreted to include any machine already infected with even relatively weak or benign malware, a category that includes millions of machines worldwide if not more, according to the CDT.

Due to the proliferation of "botnets," or networks of machines, some numbering in the millions, that have been infected and "bound together" by a sophisticated networking virus, the "five districts networked" criterion will potentially enable the FBI to target millions of machines with a single warrant, according to the CDT.

DOJ further proposes that warrants issued on these grounds by judges in any given district be applicable across the US, a measure that will allow the bureau to go "shopping" for judges willing to sign off on surveillance, according to the CDT's official statement.

The proposed changes make clear that the new US cyber-policy would violate basic principles of international law, giving the FBI authority to "unilaterally conduct searches of electronic media outside US territory" and spy on foreign targets with impunity, according to the CDT.

The amendments represent "possibly the broadest expansion of extraterritorial surveillance power since the FBI's inception," according to a legal expert at the University of California Hastings College of the Law.

A recent report makes clear that the FBI is already engaged in covert and likely illegal electronic sting operations using malware.

The FBI already sets up electronic "honey pots" that automatically attempt to infiltrate malware onto every machine that visits a targeted web page, a tactic referred to casually as "drive by download," according to sources cited by *Wired* magazine this summer.

As part of a recently exposed 2007 "spear phishing" sting operation, the FBI created a fake Associated Press article and sent it to an individual under investigation in an effort to transfer malware to the target's computer.

Through the DOJ, the Obama administration is spearheading a vast expansion of the American state's effort to dominate and control the world's increasingly integrated information system.

The spate of reports hyping alleged Russian and Chinese efforts to hack US corporate and government servers has highlighted the geopolitical implications of this US global hacking agenda. This week, the *Wall Street Journal* cited claims made by Google and US intelligence that the Russian government has launched a systematic hacking campaign against a number of its border states and NATO governments since 2007, focusing on the Caucasus region and Eastern Europe.

According to sources cited by the *Journal*, Russian hackers have targeted US-based mercenaries operating in Ukraine, including Academi (formerly Blackwater) and Science Applications International Corp.

Whether or not they are true, these reports illustrate that US hacking operations are being prepared not just against millions of ordinary people, but also against rival powers armed with nuclear weapons.