Everything We Know About How the FBI Hacks People

Kim Zetter ⋮ 5-6 minutes ⋮ 5/15/2016

Recent headlines warn that the government now has greater authority to hack your computers, in and outside the US. Changes to federal criminal court procedures known as Rule 41 are to blame; they vastly expand how and whom the FBI can legally hack. But just like the NSA's hacking operations, FBI hacking isn't new. In fact, the bureau has a long history of surreptitiously hacking us, going back two decades.

That history is almost impossible to document, however, because the hacking happens mostly in secret. Search warrants granting permission to hack get issued using vague, obtuse language that hides what's really happening, and defense attorneys rarely challenge the hacking tools and techniques in court. There's also no public accounting of how often the government hacks people. Although federal and state judges have to submit a report to Congress tracking the number and nature of wiretap requests they process each year, no similar requirement exists for hacking tools. As a result, little is known about the invasive tools the bureau, and other law enforcement agencies, use or how they use them. But occasionally, tidbits of information do leak out in court cases and news stories.

A look at a few of these cases offers a glimpse at how FBI computer intrusion techniques have developed over the years. Note that the government takes issue with the word "hacking," since this implies unauthorized access, and the government's hacking is court-sanctioned. Instead it prefers the terms "remote access searches" and Network Investigative Techniques, or NIT. By whatever name, however, the activity is growing.

1998: The Short But Dramatic Life of Carnivore

The FBI's first known computer surveillance tool was a traffic sniffer named Carnivore that got installed on network backbones---with the permission of internet service providers. The unfortunately named tool was custom-built to filter and copy metadata and/or the content of communications to and from a surveillance target. The government had already used it about 25 times, beginning in 1998, when the public finally learned about it in 2000 after Earthlink refused to let the FBI install the tool on its network. Earthlink feared the sniffer would give the feds unfettered access to all customer communications. A court battle and congressional hearing ensued, which sparked a fierce and divisive debate, making Carnivore the Apple/FBI case of its day.

The FBI insisted to Congress that its precision filters prevented anything but the target's communications from being collected. But Carnivore's descriptive name seemed to defy that, and an independent review ultimately found that the system was "capable of broad sweeps" if incorrectly configured. The reviewers also found that Carnivore lacked both the protections to prevent someone from configuring it this way and the capability to track who did it if the configuration got changed.

By 2005, the FBI had replaced Carnivore with commercial filters, but was still using other custom-built collection tools in the Carnivore family. But all of these network surveillance tools had one problem, the same issue plaguing law enforcement agencies today: encryption. FBI agents could use tools to siphon all the data they wanted as it crossed various networks, but if the data was encrypted, they couldn't read it.

Enter key loggers designed to circumvent encryption by capturing keystrokes as a surveillance target typed, before encryption kicked in.

1999: How a Mob Boss Helped Birth the Fed's Computer Surveillance

Cosa Nostra mob boss Nicodemo Salvatore Scarfo, Jr., was the first criminal suspect known to be targeted by a government keystroke logger in 1999. Scarfo was using encryption to protect his communications, and the FBI used a key logger---which was likely a commercially made tool---to capture his PGP encryption key. Unlike key loggers today which can be remotely installed, however, the FBI had to physically break into Scarfo's office twice to install the logger on his computer and retrieve it, since Scarfo was using a dial-up internet connection that prevented authorities from reaching his computer remotely.

The FBI apparently went rogue in using the tool, however, because a government memo from 2002 (.pdf) recently obtained by MIT national security researcher Ryan Shapiro revealed that the Justice Department was irked that the Bureau had "risked a classified technique on an unworth [sic] target."

Previous Chapter Next Chapter