FBI Spyware Has Been Snaring [some] Extortionists and [a few 5th rate] Hackers for Years

by Kevin Poulsen via Kismo - Wired *Thursday, May 21 2009, 11:25pm*
international / miscellaneous / other press

Cross-border legalities remain as major hurdle

> A sophisticated FBI-produced spyware program has played a crucial behind-the-scenes role in federal investigations into extortion plots, terrorist threats and hacker attacks in cases stretching back at least seven years, newly declassified documents show.

As first reported by Wired.com, the software, called a "computer and internet protocol address verifier," or CIPAV, is designed to infiltrate a target's computer and gather a wide range of information, which it secretly sends to an FBI server in eastern Virginia. The FBI's use of the spyware surfaced in 2007 when the bureau used it to track e-mailed bomb threats against a Washington state high school to a 15-year-old student.

But the documents released Thursday under the Freedom of Information Act show the FBI has quietly obtained court authorization to deploy the CIPAV in a wide variety of cases, ranging from major hacker investigations, to someone posing as an FBI agent online. Shortly after its launch, the program became so popular with federal law enforcement that Justice Department lawyers in Washington warned that overuse of the novel technique could result in its electronic evidence being thrown out of court in some cases.

"While the technique is of indisputable value in certain kinds of cases, we are seeing indications that it is being used needlessly by some agencies, unnecessarily raising difficult legal questions (and a risk of suppression) without any countervailing benefit," reads a formerly-classified March 7, 2002 memo from the Justice Department's Computer Crime and Intellectual Property Section.

The documents, which are heavily redacted, do not detail the CIPAV's capabilities, but an FBI affidavit in the 2007 case indicate it gathers and reports a computer's IP address; MAC address; open ports; a list of running programs; the operating system type, version and serial number; preferred internet browser and version; the computer's registered owner and registered company name; the current logged-in user name and the last-visited URL.

After sending the information to the FBI, the CIPAV settles into a silent "pen register" mode, in which it lurks on the target computer and monitors its internet use, logging the IP address of every server to which the machine connects.

The documents shed some light on how the FBI sneaks the CIPAV onto a target's machine, hinting

that the bureau may be using one or more web browser vulnerabilities. In several of the cases outlined, the FBI hosted the CIPAV on a website, and tricked the target into clicking on a link. That's what happened in the Washington case, according to a formerly-secret planning document for the 2007 operation. "The CIPAV will be deployed via a Uniform Resource Locator (URL) address posted to the subject's private chat room on MySpace.com."

In a separate February 2007, Cincinnati-based investigation of hackers who'd successfully targeted an unnamed bank, the documents indicate the FBI's efforts may have been detected. An FBI agent became alarmed when the hacker he was chasing didn't get infected with the spyware after visiting the CIPAV-loaded website. Instead, the hacker "proceeded to visit the site 29 more times," according to a summary of the incident. "In these instances, the CIPAV did not deliver its payload because of system incompatibility."

The agent phoned the FBI's Special Technologies Operations Unit for "urgent" help, expressing "the valid concern that the Unsub hackers would be 'spooked.'" But two days later the hacker, or a different one, visited the site again and "the system was able to deliver a CIPAV and the CIPAV returned data."

The software's primary utility appears to be in tracking down suspects that use proxy servers or anonymizing websites to cover their tracks. That's illustrated in several cases in the documents, including the 2004 hunt for a saboteur who cut off telephone, cable TV and internet service for thousands of Boston residents. The man's name is redacted from the documents, but the description of the case matches that of Danny Kelly, an unemployed Massachusetts engineer.

According to court records, Kelly deliberately cut a total of 18 communications cables belong to Comcast, AT&T, Verizon and others over a three month period. In anonymous extortion letters to Comcast and Verizon, Kelly threatened to increase the sabotage if the companies didn't begin paying him $10,000-a-month in protection money. He instructed the companies to deposit the cash in a new bank account and post the account information to a web page he could access anonymously.

When the FBI tried to track him down from his visits to the web page, they found he was routing through a German-based anonymizer. The FBI obtained a warrant to use the CIPAV on Feb. 10, 2005, and was apparently successful. Kelly went on to plead guilty to extortion, and was sentenced to five years probation.

The CIPAV also played a previously-unreported role in an investigation of a prolific computer hacker who made headlines after penetrating thousands of computers at Cisco, various U.S. national laboratories, and NASA's Jet Propulsion Laboratory in 2005. The FBI agent leading the case sought approval to plant a CIPAV through an undercover operative posing as a Defense Department contractor "with a computer network connected to JPL's computer network," according to one document. The FBI linked the intrusions to known 16-year-old hacker in Sweden.

And in 2005, FBI agents on the Innocent Images task force hit a wall when trying to track a sexual predator who'd begun threatening the life of a teenage girl he'd met for sex. The man's IP addresses were "from all over the world" — a sign of web proxy use. The bureau sought and won court approval to use the CIPAV on Aug. 9, 2005.

Other cases are less weighty. In another 2005 case, someone was unwisely using the name of the chief of the FBI's Buffalo, New York office to harass people online. The FBI got a warrant to use the spyware to track down the fake agent.

Additional cases include:

- In March 2006, the FBI investigated a hacker who took over a Hotmail user's account and acquired personal information. The hacker tried to extort the owner out of $10,000, demanding the victim create and fund an E-Gold account and e-mail the password to the hacker. The FBI obtained a search warrant allowing them to send the intruder a CIPAV instead, to uncover his or her location.
- In October 2005, an undercover agent working a case described as "WMD (bomb & anthrax)" communicated with the suspect via Hotmail, and sought approval from Washington to use a CIPAV to locate the subject's computer.
- In December 2005, FBI agents sought to use the spyware to track down another extortionist who sent an e-mail to a casino threatening violence.
- In June 2005, an intruder deleted a database at an unnamed company and demanded payment to restore it. The FBI prepared a search warrant affidavit and was ready to ask a judge for authorization to deliver the CIPAV through the hacker's Yahoo e-mail account. They were briefly thwarted when the intruder stopped communicating with the victim, but after a month of silence the hacker reestablished contact and, presumably, got the FBI's spyware for his trouble.

The documents appear to settle one of the questions the FBI declined to answer in 2007: whether the bureau obtains search warrants before using the CIPAV, or if it sometimes relies on weaker "pen register" orders that don't require a showing of probable cause that a crime has been committed. In all the criminal cases described in the documents, the FBI sought search warrants.

The records also indicate that the FBI obtained court orders from the Foreign Intelligence Surveillance Court, which covers foreign espionage and terrorism investigations, but the details are redacted.

The FBI released 152 heavily-redacted pages in response to Threat Level's FOIA request, and withheld another 623.

Update: The documents are now available for download here.

Image courtesy ABCNews.com

See Also:

- FBI Spyware: How Does the CIPAV Work? — UPDATE
- FBI's Sought Approval for Custom Spyware in FISA Court
- 'Thank You For Your Interest in the FBI'
- Appeals Court Clarifies: Government Spyware Not Protected in Ruling
- FBI's Magic Lantern Revealed
- FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats

how far in front is wee-willie-winkette? catch us if u can, fbi

http://www.wired.com/threatlevel/2009/04/fbi-spyware-pro/

Cleaves Alternative News. http://cleaves.lingama.net/news/story-1573.html