Quick Find Search News For SEARCH

News Home Top News Photos Videos Business Technology Entertainment Sports World Odd

FBI Confirms 'Magic Lantern' Project Exists

Updated:□Wed,□Dec□12□6:08□PM□EST

By Elinor Mills Abreu

SAN FRANCISCO (Reuters) - An FBI spokesman confirmed on Wednesday that the U.S. government is working on a controversial Internet spying technology, code-named "Magic Lantern", which could be used to eavesdrop on computer communications by suspected criminals.

"It is a workbench project" that has not yet been deployed, said FBI spokesman Paul Bresson. "We can't discuss it because it's under development."

The FBI has already acknowledged that it uses software that records keystrokes typed into a computer to obtain passwords that can be used to read encrypted e-mail and other documents as part of criminal investigations.

Magic Lantern reportedly would allow the agency to plant a Trojan horse keystroke logger on a target's PC by sending a computer virus over the Internet, rather than require physical access to the computer as is now the case.

Malicious hackers have been known to use e-mail or other remote methods for installing spying technology, security experts said.

When word of Magic Lantern leaked out in published reports in November, civil libertarians said the program could easily be abused by overzealous law enforcement agencies.

When asked if Magic Lantern would require a court order for the FBI to use it, as existing keystroke logger technology does, Bresson said: "Like all technology projects or tools deployed by the FBI it would be used pursuant to the appropriate legal process."

Major anti-virus vendors this week said they would not voluntarily cooperate with the FBI and said their products would continue to be updated to detect and prevent viruses, regardless of their origin, unless there was a legal order otherwise.

Doing so would anger customers and alienate non-U.S. customers and governments, they said, adding that there had been no requests by the FBI to ignore any viruses.

The FBI set a precedent in a similar case by asking Internet service providers to install technology in their networks that allows officials to secretly read e-mails of criminal investigation targets.

While the FBI requires a court order to install its technology, formerly called "Carnivore," some service providers reportedly comply voluntarily, while court orders are relatively easy to get, civil libertarians argue.

Given the hijacking attacks of Sept. 11, it is also conceivable that the U.S. government would enlist the aid of private companies to combat terrorism and help its war effort, said Michael Erbschloe, vice president of research at Computer Economics, which analyzes the impact of viruses.

"In previous wars, including World War II, the government had the power to call on companies to help; to commandeer the technology," said Erbschloe, author of "Information Warfare: How to Survive Cyber Attacks."

"If we were at war the government would be able to require technology companies to cooperate, I believe, in a number of ways, including getting back door access to information and computer systems."