WIKIPEDIA

Computer and Internet Protocol Address Verifier

Computer and Internet Protocol Address Verifier	
Original author(s)	Federal Bureau of Investigation
Type	Spyware

The **Computer and Internet Protocol Address Verifier** (**CIPAV**) is a data gathering tool that the Federal Bureau of Investigation (FBI) uses to track and gather location data on suspects under electronic surveillance. The software operates on the target computer much like other forms of illegal spyware, whereas it is unknown to the operator that the software has been installed and is monitoring and reporting on their activities.[1]

The CIPAV captures location-related information, such as: IP address, MAC address, open ports, running programs, operating system and installed application registration and version information, default web browser, and last visited URL.[1]

Once that initial inventory is conducted, the CIPAV slips into the background and silently monitors all outbound communication, logging every IP address to which the computer connects, and time and date stamping each.[1]

The CIPAV made headlines in July, 2007, when its use was exposed in open court during an investigation of a teen who had made bomb threats against Timberline High School in Washington State,[1] and again in 2014 when it was shown that a fake news story was created to go along with it.[2]

FBI sought approval to use CIPAV from Foreign Intelligence Surveillance Court in terrorism or spying investigations.

See also

- Backdoor (computing)
- ECHELON
- FinFisher
- Magic Lantern (software)
- MiniPanzer and MegaPanzer
- Network Investigative Technique
- Policeware
- R2D2 (trojan)
- Tailored Access Operations
- Wiretapping

References

1. "FBI's Secret Spyware Tracks Down Teen Who Made Bomb Threats" (https://web.archive.org/web/20080516201251/http://www.wired.com/politics/law/news/2007/07/fbi_spyware). Wired Magazine. 2007-07-18. Archived from the original (https://www.wired.com/politics/law/news/2007/07/fbi_spyware) on May 16, 2008.
2. "Editor outraged after FBI created a fake news story on a lookalike Seattle Times webpage to catch suspect calling in school bomb threats" (http://www.dailymail.co.uk/news/article-2811568/FBI-creates-fake-news-story-bogus-website-resembling-Seattle-Times-catches-suspect-calling-series-BOMB-threats-high-school.html), *Daily Mail*, October 28, 2014

External links

- http://blog.wired.com/27bstroke6/2009/04/fbi-spyware-pro.html

- http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9131778&source=NLT_AM
- https://www.eff.org/deeplinks/2011/04/new-fbi-documents-show-depth-government
- http://www.infosecurity-magazine.com/view/33825/did-the-fbi-use-cipav-against-tor/

Retrieved from "https://en.wikipedia.org/w/index.php?title=Computer_and_Internet_Protocol_Address_Verifier&oldid=839991894"

This page was last edited on 7 May 2018, at 01:19 (UTC).