GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials Bootcamp Style (Security 401)"
at http://www.giac.org/registration/gsec

Controversial Carnivore, A Threat to Privacy?
Kurt Steiner
September 5, 2000

In the past few months the news media has thoroughly covered the new wiretapping device implemented by the Federal Bureau of Investigation (FBI). The moniker Carnivore denotes a laptop device which is connected to an Internet Service Provider (ISP) system to gather packets of data in hopes of finding incriminating evidence of a suspected terrorist, drug cartel, or other high level criminals. The device has been used twenty five times in the last eighteen months including ten national security and six domestic criminal cases this year. FBI officials will not comment on the success of Carnivore's use since all cases are pending trial.

The specifics of Carnivore remain at large a mystery. Industry and privacy advocates have requested the source code and documentation be revealed. Bureau officials now regret the device's name which has inflamed the issue more. Carnivore was derived from and earlier version of the packet sniffing system by the name Omnivore since it sniffed all the data it was connected to. Later the filtering was streamlined to a more manageable level thus becoming the pickier eater Carnivore.

Carnivore when attached to an ISP's network runs a packet sniffing program to select the data specified by a required federal court order from the ISP's data stream where the system is attached. The Bureau claims that Carnivore only looks at the to and from Internet Protocol (IP) addresses of the packets being scanned and then only the ones specified by the court order are retrieved. The agency claims no other data is recorded or examined. The FBI has declined to comment on whether Carnivore evolved from commercial packet sniffing software EtherPeek sold by AG Group of Walnut Creek, CA.

"According to the AG Group Web site, EtherPeek is a 32-bit Ethernet packet-level network traffic protocol analyzer and debugging tool designed to capture packets on an Ethernet network or a switched network such as the Internet. EtherPeek includes an application called EtherHelp that appears to have the same capabilities as those the FBI claims for Carnivore. EtherHelp captures all network traffic or a specific portion of that traffic in the form of packets according to the product data. Packets captured are not displayed in EhterHelp but can be saved in a file, which can then be forwarded to support personnel for analysis by EtherPeek, which can then display the saved packets."

Both Electronic Privacy Information Center (EPIC) and the American Civil Liberties Union (ACLU) have filed actions under the Freedom Of Information Act (FOIA) requesting documents disclosing the methods which describe the operating details of CARNIVORE. Initially the FBI refused stating there are over 3,000 pages of documentation to shift through and intertwined in this is classified data and sensitive proprietary information from contractors who helped to develop Carnivore. After mounting public pressure and extensive media coverage, Attorney General Janet Reno has implemented a plan to have a university panel investigate Carnivore and report it's findings.

The Department of Justice (DOJ) posted a 63-page document on its web site soliciting for university contractor to review Carnivore's use. Contractors have been asked to submit their bids by September 6th. Attorney General Reno will select a contractor and the contract will be awarded by 25 September. The final version of the report of findings is due out mid December. EPIC is doubtful full technical details will be made in the review findings and all questions surrounding Carnivore will not be answered. Others point out that this review will only apply to the current version of the software being used. Bureau sources say that Carnivore is constantly being updated to improve its capabilities.

According to the solicitation the government wants to know: " If the operators obey the law, will Carnivore provide agents with all the information they ought to see, but only that information? Will Carnivore risk harming an Internet service provider's network? Does Carnivore introduce new risks the FBI agents or others will gain intentional unintentional access to electronic communications they have no right to see? Are Carnivore's operational procedures and built-in protections adequate to prevent such unauthorized access?"

The issue of computer user privacy is now center stage. Peter Sachs, President of ICONN.net, an ISP in New Haven, Connecticut testified before a congressional subcommittee warning of Carnivores threat to the Fourth Amendment. Based on his knowledge of ISP operations he voiced his concern that Carnivore does intrude on ISP users privacy rights and the issues of liability of the ISP when asked to connect Carnivore to its system. Mr. Sachs warned of possible threat of an ISP's system security when Carnivore is connected since the only vigilance of the systems operation is by the FBI's full remote control of Carnivore. The ISP has no ability to monitor connections of Carnivore when in use unlike that of a phone company running and monitoring 100 percent of a traditional wiretap. He questioned the FBI's need to use this system since any ISP has the ability, with as little as two lines of code, to provide law enforcement with Emails of suspects without having to possibly infringe on the privacy of innocent ISP

© SANS Institute 2000 - 2005 Author retains full rights.

users. ISPs have concerns in what their possible liabilities might be having the device connected and the device gathering data not specified in a court order. To date one ISP lost a court battle when they refused to allow Carnivore to be connected.

Currently law enforcement can legally obtain a court order granting a wire tape of a single phone line of a criminal suspect once sufficient evidence has been ascertained that this would prove beneficial in pursuing the suspect. Once granted the single wire tape is connected and controlled solely by the phone company. However with Carnivore the device is connected to an ISP and controlled remotely by the FBI. Carnivore monitors the data flow of the ISP's system unlike the single line phone tap. This is an overwhelming amount of data sniffed by the device. Even if it is monitoring the to and from Internet Protocol (IP) addresses of Email the question of innocent users privacy still surfaces.

Who is monitoring the FBI who is monitoring all this data? The FBI argues that the federal judge issuing the Carnivore tap is responsible to overseeing the FBI's operation just like the same judge would monitor the operation a conventional wiretap. A judge usually sets a review of a wiretap every week to ten days. Concerns arise with Carnivores ability to possibly gobble up private email of innocent users of an ISP which has a Carnivore system connected to it. The FBI counters that Carnivore filters out only the data that is authorized by the court order. The question then arises if it's filtered the data being filtered could be access and abused.

Organized crime has sufficient funds to use high tech equipment and implement encryption to counter Carnivore, as does the public in general. Concerns are that the FBI might have technology in Carnivore to break some forms of encryption. What is unknown is the key length they are able to break if at all. The mystery and the unknown are what is feeding the media frenzy and privacy advocates. Until questions are better answered we will see these concerns continue.

In conclusion, there are currently 20 Carnivore systems maintained at Quantico, VA when not in use. The FBI says they are only used when absolutely needed. The request for a university panel investigation into the specific details of the system operating abilities has been initiated. Many points and counterpoints have been volleyed across the media net to further create a mystery which needs to be solved with the release of hard facts by a reliable source. In the meantime, with the availability of encryption for public use many ask what the big concern of Carnivore is. Most Americans do not use encryption when sending Email or take advantage of anonymous browsers yet they say they are concerned of their privacy. Maybe they should start.

Resources:

"2000 Electronic Privacy Information Center Civil Action No. 00-1849 JR."
URL: http://www.epic.org (30 Aug., 2000)

Bridis, Ted and King, Jr., Neil. "FBI Lobbies To Show Carnivore Doesn't Eat Privacy." Wall Street Journal Europe July 21, 2000.
URL: http://www.infowar.com/class_1/00/class1_072100c_j.shtml (30 Aug., 2000)

FBI Programs and Initiatives - Carnivore Diagnostic Tool.
URL: http://www.fbi.gov/programs/carnivore/carnivore2.htm (31 Aug., 2000)

Collingswood, John E. Letter to Editor USA Today, July 24, 2000.
URL: http://www.fbi.gov/programs/carnivore/letter1.htm (31 Aug.,2000)

Sachs, Peter William. "Statement – ISP Testifies Carnivore Dangerous". Statement of Peter William Sachs before the Subcommittee on the Constitution of the Committee on the Judiciary United States House of Representatives. July 24, 2000.
URL: http://www.infowar.com/law/00/law_072600j_j.shtml (30 Aug., 2000)

Collingswood, John E. Letter to Editor St. Louis Post Dispatch, July 25, 2000.
URL: http://www.fbi.gov/programs/carnivore/letter2.htm (31 Aug., 2000)

FBI Press Room - Congressional Statement – 2000 – Internet and Data Interception Capabilities Developed by FBI, July 24, 2000.
URL: http://www.fbi.gov/pressrm/congress/congress00/kerr072400.htm (31 Aug., 2000)

Kiefer, Francine. "Is cybermonitoring eating away at privacy? FBI's 'Carnivore' tracks criminals' e-mail; critics worry it may be used against others." The Christian Science Monitor. July 26, 2000.

© SANS Institute 2000 - 2005 Author retains full rights.

Electronic Privacy Information Center Press Release on Carnivore lawsuit, August 2, 2000.
URL: http://www.epic.org/privacy/litigation/carnivore_release.html (30 Aug., 2000)

Harrison, Ann. "Carnivore: How Much Bite Behind the Bark?". Computerworld. August 07, 2000.
URL: http://www.computerworld.com/cwi/Printer_Friendly_V.../0,1212,NAV63_STO48051-,00.htm (31 Aug., 2000)

Collingswood, John E. Letter to Editor Los Angeles Times, August 7, 2000.
URL: http://www.fbi.gov/programs/carnivore/letter3.htm (31 Aug., 2000)

Stout, David. "Major University to Be Asked to Review F.B.I.'s Carnivore". The New York Times. August 10, 2000.
URL: http://www.nytimes.com/library/tech/00/08/biztech/articles/11/cnd-carnivore.html (30 Aug., 2000)

Vise, David A. "Carnivore Going to Review U." Washington Post Staff Writer August 11, 2000.
URL: http://www.infowar.com/law/00/law_081100b_j.shtml (30 Aug., 2000)

Weiss, Todd R. "FBI to release documents on Carnivore system in 45 days" Computerworld. August 17, 2000.
URL: http://www.computerworld.com/cwi/Printer_FriendlyVer!../0,1212,NAV47_Sto48694-00.htm (01 Sep., 2000)

McClure, Stuart and Scambray, Joel. Security Watch "FBI's Carnivore highlights the need for public-source review, strong encryption" Infoworld. August 18, 2000.
URL: http://www.infoworld.com/cgi-bin/deleteframe.pl?story=/articles/op/xm.../000821opswatch.xm (30 Aug., 2000)

The Associated Press. "Group Objects to F.B.I. Release of Carnivore Information" August 18, 2000.
URL: http://www.nytimes.com/library/tech/00/08/biztech/articles/18carnivore.html (30 Aug., 2000)

Barnes, Cecily. "DOJ sets rules for Carnivore wiretap investigation" CNET News.com. August 24, 2000. URL: http://dailynews.yahoo.com/htx/c.../doj_sets_rules_for_carnivore_wiretap_investigation_1.htm (31 Aug., 2000)

Sniffen, Michael J. "Chewing Out Carnivore" The Associated Press. August 25, 2000.
URL: http://www.abcnew.go.com/sections/tech/DailyNews/carnivore000825.html (29 Aug., 2000)

"Justice Dept. posts Carnivore review details" USA Today. August 25, 2000.
URL: http://www.usatoday.com/life/cyber/tech/cti445.htm (30 Aug., 2000)

Reuters. "Justice Department Releases Guidelines for Carnivore Review" The New York Times. August 25, 2000.
URL: http://www.nytime.com/library/tech/00/08/biztech/articles (30 Aug., 2000)

© SANS Institute 2000 - 2005 Author retains full rights.

Last Updated: April 23rd, 2017

Upcoming Training

Click Here to
{Get CERTIFIED!}

Community SANS Virginia Beach SEC401*	Virginia Beach, VA	Apr 24, 2017 - Apr 29, 2017	Community SANS
SANS Baltimore Spring 2017	Baltimore, MD	Apr 24, 2017 - Apr 29, 2017	Live Event
SANS Riyadh 2017	Riyadh, Saudi Arabia	May 06, 2017 - May 11, 2017	Live Event
SANS Security West 2017	San Diego, CA	May 09, 2017 - May 18, 2017	Live Event
SANS Northern Virginia - Reston 2017	Reston, VA	May 21, 2017 - May 26, 2017	Live Event
SANS Melbourne 2017	Melbourne, Australia	May 22, 2017 - May 27, 2017	Live Event
SANS London May 2017	London, United Kingdom	May 22, 2017 - May 27, 2017	Live Event
SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
SANS Atlanta 2017	Atlanta, GA	May 30, 2017 - Jun 04, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Jun 05, 2017 - Jun 10, 2017	Community SANS
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
Community SANS Philadelphia SEC401	Philadelphia, PA	Jun 19, 2017 - Jun 24, 2017	Community SANS
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event