Global Information Assurance Certification Paper

Carnivore – Diagnostic Tool or Invasion of privacy?
Mario Figueroa
September 1, 2000

Introduction

The FBI has developed a tool called Carnivore to "covertly search for e-mails and other computer messages from criminal suspects" 13. They describe this tool as a diagnostic tool, but privacy groups call it an invasion of privacy. Many privacy groups are challenging the legality and use of such a tool.

Is Carnivore a crime-fighting tool allowing the FBI to arm themselves as well as the cyber criminals are now armed? Or is it a spying device to grab as much power as they can and have control over all individuals and corporations on the Internet? Has it been thoroughly tested on all kinds of systems for all kinds of data?

FBI's Carnivore

Carnivore is a software and hardware device that provides the FBI with the ability to intercept and collect data on the Internet. The device is installed at an Internet Service Provider (ISP) site. It can be configured to capture and save data from specific users or sites. The device acts like a "sniffer" or other network diagnostic tool. It can capture any kind of data, such as e-mail or FTP data.

The "sniffer" device known as Carnivore was developed by the FBI 's Engineering Research facility in Quantico, Virginia. The program is said to be very sophisticated and fast. According to Donald M. Kerr, Assistant Director at the FBI, this tool does not look for information like "bomb" or "drugs". Instead it monitors packets of data searching for particular snippets of information, such as an SMTP address. The FBI has been working on Carnivore for about 3 years now. It continually upgrades the software to make it run faster and make it more compatible with existing software and protocols.

The FBI has confirmed that Carnivore was built from an off-the-shelf "sniffer" program. They declined to say which one of the more than a dozen known products it might be. According to attorney Robert Corn-Revere who represents an ISP, the federal marshals who first approached his client with a court order, revealed the program it came from. He said the federal marshals revealed it came from a well-known product called EtherPeek, of AG Group Inc.. The FBI later denied that it was the EtherPeek product.

The FBI claims that the latest tweaking of the program gives them a unique opportunity to distinguish between data that can be lawfully intercepted and that which can not. They claim only information specified in a court order will be extracted and collected.

The software, according to a source from Ben Charney, a ZDNN reporter, runs on Windows NT. The FBI just describes it as running under the Microsoft Windows operating system. The device has been described as anywhere from a two-foot box, to a file cabinet looking box.

According to the FBI, Carnivore is subject to intense oversight from internal FBI controls, the U.S. Department of Justice, and by order of a Court. The FBI says there are significant penalties for misuse of this tool. "The illegal use of this is punishable by imprisonment of up to five years, a fine, or both."10.

The FBI doesn't think Carnivore will be susceptible to abuse by outsiders, since it requires "a certain amount of expertise" 2. The FBI web site states that they have shared information regarding Carnivore with the industry so standards can be developed for Internet interception as soon as possible. The particular industry sharing this information was not revealed on the FBI web site.

Why the controversy

Privacy groups, such as the Electronic Privacy Information Center (EPIC) have accused the FBI of not providing timely information, based on the Freedom of Information Act. EPIC is suing the FBI to provide code for Carnivore. In addition, the American Civil Liberties Union (ACLU) has also filed similar requests.

In a recent House Judiciary Committee meeting, an oversight hearing was held on the constitutional issues raised by Carnivore and it's use. At this hearing, the FBI acknowledged that Carnivore has been deployed at least 25 times since its inception, and 16 of those done this year.

House Judiciary Committee members were quick to raise questions about the name given the software package and about the checks and balances the agency has in place to prevent potential misuse of the system. Other judiciary members raised questions about why it took so long to come forward with information about Carnivore.

The FBI told House Judiciary members that the agency had agreed to submit the source code to an independent third party body for review. But the FBI and Department Of Justice (DOJ) refuse to give the source code to any industry groups in fear that it could be exploited.

The American Civil Liberties Union (ACLU) has characterized Carnivore as the FBI's latest piece of evidence that the FBI "is engaged in an 'unprecedented' power grab that threatens the privacy of all Americans." It likens the attack of Carnivore to letting the FBI go into each and every mailbag in a post office to find a criminal's letter. They claim that every user is subject to wiretapping using this device.

The ACLU is urging all people to let Congress and the President know how you feel about this invasion of privacy. They don't believe Carnivore is needed because ISP's can already provide the information the FBI is after, without scanning every person's messages. It is an attack on our Fourth Amendment, the ALCU writes.

The FBI counters that most ISPs do not have such capabilities or cannot do it in a secure manner. It is not enough to just clone a mailbox. It needs to intercept e-mail to and from particular users. It also sometimes requires other types of protocols, like instant messaging for example, that most ISPs cannot capture.

According to one ISP, Earthlink, the device installed on their system caused outages for many of their subscribers. They claim that the FBI had a court order that allowed the FBI to install the device on their systems. Earthlink had to install an older version of software to make it compatible with Carnivore. The older software caused many of their remote access servers to crash.

EarthLink now refuses to install any new devices on its network. According to EarthLinks director of technology, Steve Dougherty, "It has the potential to hurt our network, to bring pieces of it down." 11. He goes on to say that it could impact thousands of people.

Executives at EarthLink never really knew if the surveillance was limited to criminals or not. They were concerned about individuals not part of the investigation, and their privacy.

To these concerns, the FBI insists that Carnivore does not affect performance or stability of networks. They claim that Carnivore only monitors traffic that is relevant to the FBI investigation.

Summary

The FBI officials claim that Carnivore will only focus on private information about criminal suspects who are targets of an investigation. The FBI claims they need this type of technology to effectively investigate and prevent crimes on the Internet. Advocates claim that all information is tapped into not just some. And that the information is already available from ISPs so why do they need to gather it.

Giving up the source code could cause the FBI to be ineffective in gathering the necessary data for prosecutions. It is unlikely that they will reveal the inner workings of Carnivore to anyone but a trusted third party.

Privacy groups and some members of congress are worried about the potential for possible abuse from the use of Carnivore. Both Republicans and Democrats have raised concerns about how the surveillance software operates.

At least one ISP claims that Carnivore crashed parts of their system and caused outages to many of their users. They were forced to downgrade system software to get Carnivore to run.

References

1. Hopper, D. Ian *Associated Press Writer*. "Details of E-Mail Spy System Sought"

   1 August 2000.
   URL: HTTP://news.excite.com/news/ap/00801/23/fbi-snooping

2. FBI home page, no author given "Carnivore Diagnostic Tool"

   URL: HTTP://www.fbi.gov/programs/carnivore/carnivore2.htm

3. FBI home page, no author given "Internet and Data Interception Capabilities Developed by FBI" 24 July 2000

   URL: HTTP://www.fbi.gov/pressrm/congress/congress00/kerr072400.htm

4. Wired News Report. "Carnivore Eats Your Privacy" 11 July 2000

   URL: HTTP://www.wired.com/news/print/0,1294,37503,00.htm

5. Foley, Mary Jo. ZDNN " Congress isn't swallowing Carnivore" 24 July 2000

   URL: HTTP://www.zdnet.com/zdnn/stories/news/0,4586,2606899,00.html

6. Collingwood, John E. Assistant Director FBI "Letter to Mr. Gallagher, Editor of the Editorial Page, USA Today" 24 July 2000

   URL: HTTP://www.fbi.gov/programs/carnivore/letter1.htm

7. Collingwood, John E. Assistant Director FBI "Letter to Ms. Christine Bertelson, Editor of the Editorial/Opinion Page, St. Louis Post Dispatch" 25 July 2000

   URL: HTTP://www.fbi.gov/programs/carnivore/letter2.htm

8. By Reuters "Reno vows to look into 'Carnivore' delay" 3 August 2000

   URL HTTP://www.zdnet.com/zdnn/stories/news/0,4586,2611486,00.html

9. Charney, Ben, ZDNN "The technology behind FBI's 'Carnivore'" 19 July 2000

   URL HTTP://www.zdnet.com/filters/printerfriendly/0,6061,2605428-2,00.html

10. Congressional Statement Federal Bureau of Investigation

    Statement for the record of Donald M. Kerr, Assistant Director Laboratory Division Federal Bureau of Investigation on Internet and Data Interception Capabilities Developed by FBI Before the United States House of Representatives The Committee on the Judiciary Subcommittee on the Constitution Washington, D.C.
    URL: HTTP://www.fbi.prssrm/congress/congress00/kerr072400.htm

11. Wingfield, Nick. Bridis, Ted. King, Neil Jr. "EarthLink just says no to FBI's Carnivore" 14 July 2000

    URL HTTP://www.zdnet.com/zdnn/stories/news/0,4586,2603945,00.html

12. Wolf, Jim, Reuters "FBI yields on Carnivore code" 2 August 2000

    URL: HTTP://www.zdnet.com/filters/printerfriendly/0,6061,2611192-2,00.html

13. Grace Sharon "TIA Offers Background on FBI's Carnivore Demonstration" 18 July 2000

    URL HTTP://www.tiaonline.org/pubs/press_releases/2000/00-68.cfm

14. ACLU "Urge the President and Congress To Stop the FBI's Use of Privacy-Invading Software"
    URL: HTTP://aclu.org/action/carnivore106.html