Global Information Assurance Certification Paper

Carnivore: The Price To Pay For Security

Tory Lorenz
December 12, 2001
GIAC Practical Version 1.2f

America is the land of the free and the home of the brave. As Americans we pride ourselves in having freedoms and liberties that citizens of other countries can only dream about. Yet, do we take this freedom too far? Are people turning on the government that prides itself in protecting our freedom? In doing so, are we preventing our government from being able to do its job in protecting our security and us? My paper is going to bring to light the issue of the FBI's Carnivore (a computer security tool used to monitor internet services), what exactly carnivore does, and why I believe it is an essential new piece to the fight against any kind of unlawful act committed with a Personal Computer. This powerful tool has so many uses in keeping our computer safe and with keeping our lives safe. Computer security and national security are becoming one and the same. So many aspects of our daily lives now center around our computers, that if we don't use the proper tools to protect them, we are not protecting ourselves. You can put in firewalls, write policies, never tell a soul what your password is, and do all that is possible to keep your network safe, but if there are not tools to keep the internet safe crime will still take place. I am going to show Carnivore's fight before the tragic events of September 11, 2001, and how the American people are looking at this tool in the aftermath. Carnivore is a tool used by the Federal Bureau of Investigation to protect American citizens, not to exploit them.

Carnivore should not be thought of so much as a privacy issue as it should a security issue. The major fight against the use of Carnivore is coming from people who think that privacy is more important than security. Groups like Stop Carnivore "do not think privacy needs to be compromised in the name of security." (http://www.stopcarnivore.org/corpeceinterview.htm.) They think that Carnivore is a complete violation of the public's Fourth Amendment rights and that there is absolutely no reason that our society should allow Carnivore to be used. In reading their above mentioned article it seems that Lance Brown has been misinformed. He is making wonderful points about people's security not being invaded and yet the things he is accusing Carnivore of doing have all been disputed by the FBI and other agencies. The bad part about that is one person can cause such an uprising that security could be ignored because nobody wants to step on the wrong toes. The public needs to know that in order for their computers, networks, and lives to be secure, diagnostic tools as powerful as Carnivore, need to be used. Carnivore can help prevent horrible acts from occurring. The good seems to outweigh the bad.

In the United States Bill of Rights, the Fourth Amendment states:

> "*The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches*

and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

Many people who object to the use of Carnivore believe that they're Fourth Amendment right is violated. The concern is that the Federal Bureau of Investigation is obtaining more information than warranted. The belief is that the FBI is obtaining person e-mail that belongs to people that have nothing to do with ongoing investigations. There are also beliefs that there is a great chance of misuse by the FBI of the Carnivore system because of the sensitive information they are able to retrieve. The public is afraid misuse is a real issue.

The Federal Bureau of Investigation has been very secretive about what exactly Carnivore is and how it works. They have released documents with tons of blacked out items. Fear of the unknown is what frightens the public. As Americans, we need to step back and think what exactly do we know about how other tools are used to fight crime and keep our security? When was the last time we were completely informed in what our military was doing in the fight against terrorism? Do we know exactly what the Marines' plan of action is to find the terrorists? No. Do we know exactly what the Army has been told they can and cannot bomb? No. So why is it such a problem that we don't know exactly what the FBI is using to fight cyber-crime and keep our networks safe? If in depth information about the make-up of Carnivore is released, are we going to rest better knowing that the bad guys now know exactly how this powerful computer security tool works? No, because the criminals are going to be able to figure out how to get around Carnivore faster and with worse outcomes, they could even possible misuse Carnivore themselves.

As Americans, we need to have faith in what our government is using to protect our cyber security. It's time to support our elected officials and stand behind them in their decisions of what is the best way to prevent crime. They shouldn't have to fight the public to use these powerful tools. Internet service providers globally use a variety of sniffers without any objections from clients. Carnivore by another name is a sniffer. The definition of sniffer obtained from "Webopedia" is, "a program or device that monitors data traveling over the net. Sniffers can be used both for legitimate network functions or for stealing information off a network. Unauthorized sniffers can be extremely dangerous to a network's security because they are virtually impossible to detect and can be inserted almost anywhere." (http://www.webopedia.com/TERM/s/sniffer.html)

The Federal Bureau of Investigation released the computer security system Carnivore in 1999. According to the "Carnivore FAQ" document the FBI says that, "Carnivore is a computer-based system that is designed to allow the FBI, in cooperation with an Internet Service Provider (ISP), to comply with court orders requiring the collection of certain information about e-mails or other electronic communications to or from a specific user targeted in an investigation." (http://www.robertgraham.com/pubs/carnivore-faq.html") It works much like many sniffer products that are being used by ISPs all the time. The

main difference between Carnivore and other tools is that Carnivore is able to separate the information that can be used according to the court orders the FBI obtains and the information that cannot be used according to the court order. I found many explanations of how exactly Carnivore works, on the Robertgraham.com Website, on the FBI Website, and in the congressional Statement issued by Donald M. Kerr. I decided to summarize the one that I found at the site "HowStuffWorks". You can find a complete explanation at: (http://www.howstuffworks.com/carnivore.html)

1. The FBI has a reasonable suspicion that someone is engaged in criminal activities and requests a court order to view the suspect's online activity.
2. A court grants the request for a full content-wiretap of e-mail traffic only and issues an order.
3. The FBI contacts the suspect's Internet service provider and requests a copy of the back-up files of the suspect's activity.
4. The ISP does not maintain customer-activity data as part of its back up.
5. The FBI sets up a Carnivore computer at the ISP to monitor the suspect's activity.
6. The FBI configures the Carnivore software with the IP address of the suspect so that Carnivore will only capture packets from this particular location. It ignores all other packets.
7. Carnivore copies all of the packets from the suspect's system without impeding the flow of the network traffic.
8. Once the copies are made, they go through a filter that only keeps the e-mail packets.
9. The e-mail packets are saved on the Jaz cartridge
10. Once every day or two, an FBI agent visits the ISP and swaps out the Jaz cartridge. The agent takes the retrieved cartridge and puts it in a container that is dated and sealed. If the seal is broken, the person breaking it must sign, date and reseal it –otherwise, the cartridge can be considered "compromised".
11. The surveillance cannot continue for more than a month without an extension from the court. Once complete, the FBI removes the system from the ISP.
12. The captured data is processed using Packeteer and Coolminer. ("Coolminer and Packeteer are used to reconstruct the raw data scooped up in the initial phase by Carnivore" (http://www.zdnet.com/sdnn/stories/news/0,4586,2641902,00.html)
13. If the results provide enough evidence, the FBI can use them as part of a case against the suspect.

If that does not make you feel comfortable with the FBI's use of Carnivore there are a few more details that should be pointed out. Carnivore is used only in cases when an Internet service provider is unable to obtain the information that the court order asks for. Another important point is that Carnivore's most powerful feature is that it limits the e-mail messages that are viewed by agent's eyes to those that are strictly defined in the court order. The fact that a warrant for the contents of your e-mail can only be issued by a Federal District Judge is also proof that our government is really looking out for the rights of people. The warrant has to specify who the suspect is, what lines will be tapped, and what kind of information is being captured for the investigation. This means that the FBI cannot just go get a warrant to tap your e-mail and then look for your wrongdoings. The FBI has to have probable cause to use Carnivore. The FBI has to have proof that a

specific person is using a specific line for wrong-doing that are already taking place and the FBI is just collecting the evidence to help convict the criminal.

On the FBI's website it states that, "Carnivore is not susceptible to abuse because it requires expertise to install and operate, and such operations are conducted, as required in the court orders, with close cooperation with the ISP's." (http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm) The FBI has to get permission from an ISP in order to place the Carnivore box on the ISP box. They cannot just barge in and do as they wish. It is a joint effort of trust that helps catch cyber-criminals, not just the FBI using their own tools without the ISP's. Intense scrutiny of the use of Carnivore by the FBI comes from many different groups of government including: internal FBI controls, the U.S. Department of Justice, and by the courts. The potential of misuse is always there, as with any powerful tool placed in the wrong person's hands. In his letter to the United States Senate, FBI agent Donald M. Kerr states, "If an FBI employee were to attempt to acquire such content or information using Carnivore without obtaining a court order or appropriate consent, it would be a serious violation of the law – a federal felony, thereby subjecting the employee to criminal prosecution, civil liability, and termination." (http://www.fbi.gov/congress/congress00/kerr090600.htm) Agents are aware that if they obtain evidence without following the proper procedures, they can cause the whole case to be dismissed in court.

Carnivore can be used to fight many different types of crime, including: terrorism, child pornography/exploitation, espionage, information warfare, fraud and hacking. In his letter to the United States Senate, FBI agent Donald M. Kerr states that, "Cyber terrorism-the use of Cyber tools to shut down critical national infrastructures (such as energy, telecommunications, transportation, or government operations) for the purpose of coercing or intimidating a government or civilian population – is emerging as a very real threat." (http://www.fbi.gov/congress/congress00/kerr090600.htm) He also gave great examples of why the threats of these crimes are real and why Carnivore is an essential part in fighting these crimes:

> "**TERRORISM:**
> Terrorist groups are increasing using new information technology and the Internet To formulate plans, raise funds, spread propaganda, and communicate securely Using computerized files, e-mail, and encryption.
>
> **ESPIONAGE:**
> It should not surprise anyone to hear that foreign intelligence services Increasingly view the Internet and computer intrusions as useful tools for Acquiring sensitive U.S. government and private sector information.
>
> **INFORMATION WARFARE:**
> Knowing that they cannot match our military might with conventional weapons, nations see cyber attacks on our critical infrastructure or military operations as a way to hit what they perceive as America's Achilles heel – our

growing dependence on information technology in government and commercial operations" (http://www.fbi.gov/conress/congress00/kerr090600.htm)

We can prevent these acts from getting out of hand by using Carnivore as a cyber security defense.

In two of the articles I read while doing my research, "Statement for the Record of Donald M. Kerr on Carnivore Diagnostic Tool" and "Carnivore FAQ", I found references to Osama bin Laden and the al Qa'ida organization along with references to bombings of the World Trade Center. The mentioning of bombings of the World Trade Center may have been just an eerie coincidence. The fact that Osama bin Laden was referenced proves that the public helped prevent the FBI from being able to fight terrorism at all possible angles needed. The mention of bin Laden proves that the government has known for some time that he is a threat to America and that he was using the Internet and his personal computer for hurtful, wrongdoings. In fact, Agent Donald Kerr makes a reference to him in his letter to the United States senate, which doesn't seem odd today, since the whole world knows who bin Laden is, but Agent Kerr's letter was written September 6, 2000. If Americans would not have been so worried about their own privacy and more concerned with their nations security, both on and off the computers, would the World Trade Center and Pentagon attacks have been prevented? If the FBI could have put Carnivore on the ISP's that bin Laden and his followers were using could they have saved thousands of lives? The FBI knew a year ago that bin Laden was using e-mail for wrong doings. We should've been able to stop him then, but couldn't because the public doesn't see that computer security and national security are becoming one in the same. Not it's too late the damage is done.

Since the attacks on America, there have been two new bills brought forward for approval in the fight against computer related crimes. First is the "Combating Terrorism Act of 2001", "which enhances police wiretap powers and permits monitoring to more situations." (http://www.wired.com/news/politics/0,1283,46852,00.html) This act states, "that any U.S. attorney or State Attorney General can order the installation of the FBI's Carnivore surveillance system". The second one is the "Public Safety and Cyber Security Enhancement Act of 2001". It states that, "the courts shall enter an ex parte order authorizing the installation and use of a pen register or a trap and trace device if the court finds the attorney for the Government has certified to the court that the information likely to be obtained by such installation and use is relevant to an ongoing criminal investigation. Such order shall, upon service of such order, apply to any entity providing wire or electronic communication service in the United States whose assistance may facilitate the execution of the order." (http://rs9.loc.gov/cgi-bin/query/D/c107:4:.temp/~c107cwBmjA:) This means the FBI no longer has strict policies thy need to follow in obtaining information with Carnivore. If they come across more information than what was in the original court order, thy may be able to use it in their criminal case.

Before September 11, 2001, there were very strict laws surrounding Carnivore. The FBI had to jump through numerous hoops in order to use it. After September 11, 2001, the

FBI has been granted free reign to place Carnivore wherever needed to help prevent future attacks. It is too bad the loss of lives was needed to prove this security tool is essential in protecting us.

The services provided by Carnivore out number the disservice that the public thinks it causes. If this tool will help monitor Internet activities and decrease cyber-crimes, then it is worthwhile whatever privacy is lost. The allegation of privacy invasion among our government is unbearable. Since Carnivore is considered a good service in the aftermath of September 11, the public should be provided the necessary information in order to educate them on the great possibilities of Carnivore. This paper proves that Carnivore is not a price to pay for privacy it is a great loss if we don't use it for our security.

BIBLIOGRAPHY

McCullagh, Declan. "Senate Oks FBI Net Spying" WiredNews.com September 14, 2001 http://www.wired.com/news/politics/0,1283,46852,00.html (December 26, 2001)

McCullagh, Delan. "Anit-Attack Feds Push Carnivore" Wirednews.com September 12, 2001 http://www.wired.com/news/politics/0,1283,46747,00.html (December 26, 2001)

Collingwood, John E. "Letter from Assistant Director John Collingwood to Members of Congress on Carnivore Diagnostic Tool" Federal Bureau of Investigation August 16, 2000 http://www.fbi.gov/congress/congress00/collingwood081600.htm (November 27, 2001)

Graham, Robert. "Carnivore FAQ (Frequently Asked Questions)" RobertGraham.com September7, 2000 http://www.robertgraham.com/pubs/carnivore-faq.html (November 26, 2001)

Various "107th Congress 1st Session H.R. 2915" Senate and House of Represenatives September 20, 2001 http://rs9.loc.gov/cgi-bin/query/D?c107:4:./temp/~c107cwBmjA:: (November 26, 2001)

Various "107th Congress 1st Session S. 1568" Senate and House of Represenatives October18, 2001 http://rs9.loc.gov/cgi-bin/query/D?c107:6:./temp/~c107cwBmjA:: (November 26, 2001)

Brown, Lance. "Stop Carnivore NOW!" Stop Carnivore.org 2000 http://www.stopcarnivore.org/corpeceinterview.htm (December 26, 2001)

Meeks, Brook. "FBI's Carnivore hunts in a pack" MSNBC October 18, 2000 http://www.zdnet.com/zdnn/stories/news/0,4586,2641902,00.html (November 26, 2001)
Konrad, Rachel. "New documents shed more light on FBI's 'Carnivore'" CNET News.com November 16, 2000 http://news.cnet.com/news/0-1005-202-3731884.html (November 26, 2001)
Evans, James "Despite New Name, Carnivore Still Bites" IDG News Service March 9, 2001 http://www.pcworld.com/resource/printable/article/0,aid,43963,00.asp (November 27, 2001)
Meeks, Brock N. "FBI's Carnivore has partners" MSNBC October 17, 2000 http://www.msnbc.com/news/477749.asp (November 26, 2001)
McLaughlin, Matt. "FBI's upgrade of Carnivore includes a new name" Government Computer News Staff February 12, 2001 http://www.washtech.com/cgi (December 26, 2001)
Kerr, Donald M. "Statement for the Record of Donald M. Kerr, Assistant Director Laboratory Division Federal Bureau of Investigation on Carnivor Diagnostic Tool" Federal Bureau of Investigation September 6, 2000 http://www.fbi.gov/congress/congress00/kerr090600.htm (November 27, 2001)
Various "sniffer" Webopedia 2001 http://www.webopeida.com/TERM/s/sniffer.html (December 27,2001)
Various "Carnivore Diagnostic Tool" Federal Bureau of Investigation 2000 http://www.fbi.gov/hq/lab/carnivore/carnivore2.htm (November 27, 2001)
Tyson, Jeff "How Carnivore Works" HowStufWorks 2000 http://www.howstuffworks.com/canivore.htm (November 26, 2001)

Last Updated: July 24th, 2017

Upcoming Training

SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
Community SANS Pasadena SEC401 @ NASA	Pasadena, CA	Aug 23, 2017 - Aug 30, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Sep 11, 2017 - Oct 12, 2017	Mentor
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS
Community SANS Columbia SEC401	Columbia, MD	Sep 18, 2017 - Sep 23, 2017	Community SANS
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Boise SEC401	Boise, ID	Sep 25, 2017 - Sep 30, 2017	Community SANS
Baltimore Fall 2017 - SEC401: Security Essentials Bootcamp Style	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	vLive
Community SANS New York SEC401	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS London September 2017	London, United Kingdom	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Charleston SEC401	Charleston, SC	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Arlington, VA	Oct 04, 2017 - Nov 15, 2017	Mentor