Who's Afraid of Carnivore? Not Me!

Richard F. Forno
<rforno@infowarrior.org>

Essay 2000-05

Recently, the FBI has become embroiled into the controversy surrounding its latest attempt to bring law enforcement into the Information Age. The "Carnivore" project is the Bureau's attempt to collect information on electronic suspects and computer criminals in the dark reaches of cyberspace…..their version of a combination TRAP AND TRACE and PEN REGISTER carried over from the 'old fashion' days of POTS, or Plain Old Telephone Service. The ACLU, EFF, EPIC, Congressional committees, and even segments of the American technocracy are up-at-arms over this questionable law enforcement device, and even more dubious of the goofy explanations provided by FBI front-men as to how it is employed. From where I sit, it looks like the FBI wants to get into the "Enemy of the State" spook-tech game like everyone thinks NSA participates in.

This article will discuss some differences between Carnivore's access to electronic information and the methods (and limitations) of traditional law enforcement access to "old school' communications systems. Then, we're going to discuss how easy it is to circumvent the Carnivore system and still keep our communications secret from all prying eyes….no matter how sophisticated the FBI thinks Carnivore is.

CARNIVORE

The FBI's website (http://www.fbi.gov/programs/carnivore/carnivore.htm) calls Carnivore a "diagnostic tool" versus an electronic eavesdropping device. In reality, Carnivore is indeed a network diagnostic tool (a network analyzer or "sniffer"), but to imply that Carnivore's primary use is as a "diagnostic tool" is stretching the Bureau's already-thin credibility a bit too far. That's like a criminal claiming that the gun he shot someone with was not a gun but a "tool" to eject hot lead into a wall. The goal of Carnivore is to allow the FBI to quickly gather information from an ISP without having to go through that ISP's management each time to obtain it, as is commonly done via subpoena.

Donald Kerr, Assistant Director at the FBI, told a Congressional panel recently that

> the Carnivore device works much like commercial "sniffers" and other network diagnostic tools used by ISPs every day, except that it provides

the FBI with a unique ability to distinguish between communications which may be lawfully intercepted and those which may not. For example, if a court order provides for the lawful interception of one type of communication (e.g., e-mail), but excludes all other communications (e.g., online shopping) the Carnivore tool can be configured to intercept only those e-mails being transmitted either to or from the named subject.

His statement also mentions that Carnivore

is a very specialized network analyzer or "sniffer" which runs as an application program on a normal personal computer under the Microsoft Windows operating system. It works by "sniffing" the proper portions of network packets and copying and storing only those packets which match a finely defined filter set programmed in conformity with the court order. This filter set can be extremely complex, and this provides the FBI with an ability to collect transmissions which comply with pen register court orders, trap & trace court orders, Title III interception orders, etc.

Let's stop and analyze this claim. The FBI has a Windows-based tool that can be configured to differentiate between "legitimate" and "extraneous" traffic that it intercepts at a given ISP. This will -- according to the FBI testimony – provide federal law enforcement folks the same ability to intercept electronic communications (e-mail, web surfing, instant messages, etc.) than they currently have in the world of the POTS telephone systems. Right. And my Aunt Sally is a world-class hacker master. Let's see why.

The Carnivore system is allegedly a single "item" or black-box "device' placed at each ISP to monitor communications as authorized by court order. Where is this box placed at the ISP? Hanging it off the gateway router or bastion network means that this poor Windows box will have to intercept GIGABYTES of raw data in real-time unless it is pre-configured to only monitor certain ports such as SMTP, POP, or IRC. However, Carnivore – like all sniffers -- still collects "everything" associated with those protocols – however, as was testified to by senior FBI agents, only reveals (under court order) the "header information" of a suspects to the FBI. So while, they are only using "header" information that was collected (as shown below) under an authorized investigation, what is done with the rest of the information (such as the content or e-mail attachments) collected alongside the headers?

Is Carnivore unique? Does it take rocket science to create a Carnivore-type system? Hardly. Many companies use sniffers to enforce acceptable use policies or for routine internal administrative matters and do not as a matter of course look at content, only source, destination, and protocol of the packets being monitored. There are tons of freeware, shareware, and commercial network sniffers available on the market. In fact, it's already reported that EtherPeek is the FBI's tool driving Carnivore.

Kerr's Congressional testimony continues…

> It is important to distinguish now what is meant by "sniffing." The problem of discriminating between users' messages on the Internet is a complex one. However, this is exactly what Carnivore does. It does NOT search through the contents of every message and collect those that contain certain key words like "bomb" or "drugs." It selects messages based on criteria expressly set out in the court order, for example, messages transmitted to or from a particular account or to or from a particular user.

Either the FBI is kidding themselves, or they are trying to pull a fast one here. Let's look at how EtherPeek (or any network sniffer, for that matter) works. What follows below are two captured packets from my EtherPeek analyzer of an e-mail message I sent to myself. Note that the sniffer was configured to only sniff e-mail information via SMTP protocols. Let's take a look:

```
–@ïJ–––†…–[ |––E–      00 40 95 4a 0f e0 00 a0 c9 ea 5b 7c 08 00 45 00
 –(:F––/–~– a¶–––      02 28 3a 46 00 00 2f 06 7e 0a 20 61 a6 07 0a ff
 –––n–––ïL–îÕƒ?P–       00 19 00 6e 08 04 db 95 4c e7 94 cd c4 3f 50 10
 Ä–t–––Received:       80 00 74 e1 00 00 52 65 63 65 69 76 65 64 3a 20
 from stmpy-2.cai      66 72 6f 6d 20 73 74 6d 70 79 2d 32 2e 63 61 69
 s.net ([205.252.      73 2e 6e 65 74 20 28 5b 32 30 35 2e 32 35 32 2e
 14.72])––             31 34 2e 37 32 5d 29 0d 0a 20 20 20 20 20 20 20
     by prserv.net      20 20 20 62 79 20 70 72 73 65 72 76 2e 6e 65 74
 (in4) with ESMT      20 28 69 6e 34 29 20 77 69 74 68 20 45 53 4d 54
 P––        id        50 0d 0a 20 20 20 20 20 20 20 20 20 20 69 64 20
 <200007301539311     3c 32 30 30 30 30 37 33 30 31 35 33 39 33 31 31
 0400igs2le>; Sun     30 34 30 30 69 67 73 32 6c 65 3e 3b 20 53 75 6e
 , 30 Jul 2000 15     2c 20 33 30 20 4a 75 6c 20 32 30 30 30 20 31 35
 :39:31 +0000––Re     3a 33 39 3a 33 31 20 2b 30 30 30 30 0d 0a 52 65
 ceived: from [10     63 65 69 76 65 64 3a 20 66 72 6f 6d 20 5b 31 30
 .215.0.21] (x2-a      2e 32 35 35 2e 30 2e 32 35 5d 20 21 11 52 2h 6a
 mailer.org [201.      6f 72 77 61 72 64 2e 6f 72 67 20 5b 32 30 39 2e
 8.231.35] (may b     38 2e 32 31 31 2e 32 35 5d 20 28 6d 61 79 20 62
 e forged))–––by      65 20 66 6f 72 67 65 64 29 29 0d 0a 09 62 79 20
 stmpy-2.cais.net     73 74 6d 70 79 2d 32 2e 63 61 69 73 2e 6e 65 74
  (8.10.1/8.9.3)      20 28 38 2e 31 30 2e 31 2f 38 2e 39 2e 33 29 20
 with ESMTP id e6     77 69 74 68 20 45 53 4d 54 50 20 69 64 20 65 36
 UfddQ34343–––for     55 46 64 64 51 33 34 33 34 33 0d 0a 09 66 6f 72
  <rforno@YYY.net      20 3c 72 66 6f 72 6e 6f 40 69 62 84 v6 e6 65 74
 >; Sun, 30 Jul 2     3e 3b 20 53 75 6e 2c 20 33 30 20 4a 75 6c 20 32
 000 11:39:39 -04     30 30 30 20 31 31 3a 33 39 3a 33 39 20 2d 30 34
 00 (EDT)–––(enve     30 30 20 28 45 44 54 29 0d 0a 09 28 65 6e 76 65
 lope-from rforno     6c 6f 70 65 2d 66 72 6f 6d 20 72 66 6f 72 6e 6f
 @YYY.net)––Messa     40 61 62 6v 22 1e 65 74 29 0d 0a 4d 65 73 73 61
 ge-Id: <20000730     67 65 2d 49 64 3a 20 3c 32 30 30 30 30 37 33 30
 1539.e6UFddQ3434     31 35 33 39 2e 65 36 55 46 64 64 51 33 34 33 34
 3@stmpy-2.cais.n      33 40 73 74 6d 70 79 2d 32 2e 63 61 69 73 2e 6e
 et>––X-Mailer: M     65 74 3e 0d 0a 58 2d 4d 61 69 6c 65 72 3a 20 4d
 icrosoft Outlook     69 63 72 6f 73 6f 66 74 20 4f 75 74 6c 6f 6f 6b
```

From this "capture" of an SMTP packet, EtherPeek/Carnivore/any network sniffer can see various server names, IP addresses, and related e-mail header information. From this can be learned from where mail was being sent from, how it was relayed, and other interesting information in this e-mail header.

```
–@ïJ–––†…–[|––E–     00 40 95 4a 0f e0 00 a0 c9 ea 5b 7c 08 00 45 00
 –P:N––/–~~ a¶–––    01 50 3a 4e 00 00 2f 06 7e da 20 61 a6 07 0a ff
 –––n–––ïN–îÕƒ?P–     00 19 00 6e 08 04 db 95 4e e7 94 cd c4 3f 50 18
 Ä–~†––tion - 4.5    80 00 7e a0 00 00 74 69 6f 6e 20 2d 20 34 2e 35
   (0410)––Date: S   20 28 30 34 31 30 29 0d 0a 44 61 74 65 3a 20 53
 un, 30 Jul 2000      75 6e 2c 20 33 30 20 4a 75 6c 20 32 30 30 30 20
 11:41:47 -0400––     31 31 3a 34 31 3a 34 37 20 2d 30 34 30 30 0d 0a
 Subject: This is    53 75 62 6a 65 63 74 3a 20 54 68 69 73 20 69 73
  another secret     20 61 6e 6f 74 68 65 72 20 73 65 63 72 65 74 20
 message––From: "     6d 65 73 73 61 67 65 0d 0a 46 72 6f 6d 3a 20 22
 Richard Forno" <      52 69 63 68 61 72 64 20 46 6f 72 6e 6f 22 20 3c
 rforno@YYY.net>–      72 66 6f 72 6e 6f 40 69 62 9c 2e 6e 65 74 3e 0d
 –To: rforno@YYY.     0a 54 6f 3a 20 72 66 6f 72 6e 6f 40 69 62 8r 2e
 net––Mime-versio     6e 65 74 0d 0a 4d 69 6d 65 2d 76 65 72 73 69 6f
 n: 1.0––X-Priori     6e 3a 20 31 2e 30 0d 0a 58 2d 50 72 69 6f 72 69
 ty: 3––Content-t     74 79 3a 20 33 0d 0a 43 6f 6e 74 65 6e 74 2d 74
 ype: text/plain;     79 70 65 3a 20 74 65 78 74 2f 70 6c 61 69 6e 3b
  charset="US-ASC     20 63 68 61 72 73 65 74 3d 22 55 53 2d 41 53 43
 II"––Content-tra     49 49 22 0d 0a 43 6f 6e 74 65 6e 74 2d 74 72 61
 nsfer-encoding:      6e 73 66 65 72 2d 65 6e 63 6f 64 69 6e 67 3a 20
 7bit––––Secret S      37 62 69 74 0d 0a 0d 0a 53 65 63 72 65 74 20 53
 ecret!!––––.––––      65 63 72 65 74 21 21 0d 0a 0d 0a 2e 0d 0a 00 00
 ––                   00 00
```

From this next packet, the program has pulled down the complete e-mail header <u>and</u> also the content of the message ("Secret Secret!!") in both ASCII text and hex. If you use the Snooptrace feature of EtherPeek, you can assemble these two items into:

```
Received: from stmpy-2.cais.net ([205.252.14.72])  by prserv.net (in4) with ESMTP id
<2000073015393110400igs2le>; Sun, 30 Jul 2000 15:39:31 +0000
Received: from [10.215.0.21] (x2-amailer.org [201.8.231.35] (may be forged))
by stmpy-2.cais.net (8.10.1/8.9.3) with ESMTP id e6UFddQ34343
for <rforno@YYY.net>; Sun, 30 Jul 2000 11:39:39 -0400 (EDT)(envelope-from rforno@YYY.net)
Message-Id: <200007301539.e6UfddQ34343@stmpy-2.cais.net>
X-Mailer: Microsoft Outlook Express WindowsEdition (0410)
Date: Sun, 30 Jul 2000 11:41:47 -0400
Subject: This is another secret message
From: "Richard Forno" <rforno@YYY.net>
To: rforno@YYY.net
Mime-version: 1.0
X-Priority: 3
Content-type: text/plain; charset="US-ASCII"
Content-transfer-encoding: 7bit

Secret Secret!!
```

The FBI claims they will only use Carnivore's scanning for court-ordered intercepts of ISP traffic. Based on what we just saw, it is clear that Carnivore provides a wealth of information BEYOND just the "header" information, and that Carnivore-type tools can indeed perform keyword searches of its captured information! As shown above, common, off-the-shelf (COTS) programs such as EtherPeek can only filter traffic so far. To find the e-mail addresses of their suspects, they would have to run a "search" function to sift through the volumes of data to locate the many instances of that particular e-mail address in the archive of packets intercepted.

If the FBI – using Carnivore in a hypothetical case– is looking to obtain ONLY the e-mail addresses sent to and from an ISP account (as shown above) and not the content of such messages, they will still see what is shown above, however, they must discard whatever else is captured beyond the e-mail addresses in question. But do they? Or, will they?

This is where Carnivore differs from traditional wiretaps and pen traces. In the "old days" of telco intercepts, a TRAP AND TRACE and PEN REGISTER request enabled law enforcement to see what numbers were dialed to and from a given number. Let's call these "REFERENCE POINTS." These were approved by either by a US Attorney or a federal judge. A separate approval (or court order) was required to conduct a WIRETAP to actually intercept and monitor the communications between the two parties identified in the TRAP AND TRACE. Let's refer to the WIRETAP as "INTERCEPTED CONTENT."

It should be understood that the standards of proof to conduct these two distinct actions (REFERENCE POINTS v. INTERCEPTED CONTENT) are vastly different from each other. In particular, the ability to conduct a WIRETAP requires a much higher standard of proof that such illegal activity is being conducted over the phone, while a TRAP AND TRACE or PEN REGISTER have less stringent approval requirements since these latter two techniques do NOT provide intercepted content, only reference points to the communications themselves. Therefore, individuals' privacy is not (in theory) easily subject to violations by illegal wiretaps and content monitoring.

Traditionally, WIRETAPS have been required to be conducted and physically-monitored by a person (agent) to insure that only the conversations of the person(s) covered by the court order could be recorded. On the other hand, Carnivore, like its name, takes in everything it sees and doesn't require human intervention. Here's an example of a potential problem with Carnivore to support this argument:

> A court order has been issued to intercept the telephone conversations of Suspect X. One of Suspect X's children makes a phone call from the line being monitored. Under the current rules, the agent running the WIRETAP

must discontinue the recording and monitoring of the (in this case) child's phone call.

Under Carnivore, a court order is issued to intercept the header information of Suspect X's e-mail (as testified to recently on the Hill.) One of Suspect X's children uses his computer, and possibly his e-mail identity (perhaps a shared family e-mail address), to send a message to a school friend. With Carnivore's capabilities, the FBI now has the complete text of all messages (see above) sent to/from that account regardless of who sent them. And, with Carnivore, there is no direct human (agent) monitoring the flow of intercepted communications to insure that only the suspect's communications are being stored and not someone else's.

The fact that the FBI claims to <u>only take the headers</u> begs the question, "what happens to the rest of the data Carnivore collects?" Carnivore thus encompasses the three areas of traditional intercepts, TRAP AND TRACE, PEN REGISTER, and CONTENT WIRETAP in one package that could easily be abused or used in a manner inconsistent with the spirit of the laws making such abuses difficult and illegal.

Enter Carnivore. This is a combination of a TRAP AND TRACE and WIRETAP in either real-time or near-real time. The use of one technology (in this case, our network sniffer, EtherPeek) provides both the TRAP AND TRACE function and WIRETAP functions! Granted, the FBI still claims it will not exceed its authority in using Carnivore's sniffing capabilities, but let's examine another all-too-possible scenario where Carnivore may be abused:

Suspect X uses e-mail to contact Suspect Y. The FBI receives a court order to use Carnivore to "only" obtain the various e-mail addresses used by both X and Y during the past month to communicate information about their illegal activities in trafficking pirated software. As shown above, Carnivore also intercepts the content of all messages exchanged between X and Y.

The FBI testified on the Hill that they will use Carnivore only for "header information" or as authorized, however, the Carnviore archive contains all the information intercepted. For purposes of this scenario, let us assume that some of the messages exchanged talk about how one of the suspects is engaged in the distribution of stolen credit card numbers

<u>Using the content of these messages would be beyond the scope of the original court order authorizing the interception of the e-mail addresses of the suspects.</u> Two chances for abuse present themselves at this time. First, the FBI could have drafted a fairly-general justification for a Carnivore intercept that could allow them to use the contents of the intercepted messages. Secondly, while the FBI might not "use" the information archived, that information could quite possibly be used

for "theoretical" or deep-background material to develop additional leads or charges against the suspect or develop another avenue to target the suspect or his alleged accomplices without proper investigation. This reminds me of how notorious mobster Al Capone was arrested – not for being a mobster, but on charges of federal income tax evasion. Indeed, Carnivore provides a wealth of information to the FBI that gives them considerable surveillance powers in the digital age, but opens up the very real possibilities that such powers may be abused by case agents. Should it ever be proven that Carnivore was abused in such a fashion, the FBI will be in a very difficult position to defend their actions in this area. The fact that the FBI is reluctant to allow public and/or peer review of its Carnivore technology only further implies that it is not the appropriate solution the FBI claims it is.

Traditionally, REFERENCE POINTS (TRAP AND TRACE or PEN REGISTERS) and INTERCEPTED CONTENT (WIRETAPS) required different and specific procedures and approvals before use. The goal was to implement a "two-key solution" to get complete intercept information on a suspect, and reduce the chances of abusing the WIRETAP ability of law enforcement via a "single source" solution for intercepts. However, Carnivore is indeed a single-source method for the FBI to obtain complete information on a suspect's Internet communications. Carnivore is a point-and-click system and thus probably very easy to use and re-configure. Considerable oversight and objective examination must be given the uses and limitations of this "total snooping solution" device being pitched by the FBI.

COUNTER-CARNIVORE

As I hinted at earlier, Carnivore is a joke to anyone who deems themselves a hacker, cracker, computer-criminal, or power user. As such, I don't consider Carnivore much of a threat to me personally, but I do fear for how easy it is to abuse of the Carnivore system and infringe on personal liberties.

First, everyone should know that e-mail is inherently insecure and ripe for eavesdropping. Thus, one should never send sensitive material via e-mail if they want to insure such material stays secret. As such, countering Carnivore is simple, and only the foolish criminal would be caught by Carnivore.

Following are some common-sense ways to beat Carnivore-type systems. In fact, these are some helpful hints for anyone who wants to help guard their electronic privacy in today's digital world:

Set up a VPN. Use an encrypted point-to-point tunnel, SSH, or SSL to encrypt your link to your mailserver. For example, Hotmail supports SSL-based secured Web sessions. A sniffer looking at the traffic to your computer will only see SSL gibberish as it is collected.

Do A Systems Audit. Vigilant system administrators run routine network scans on their networks for administrative and security purposes. Any good system administrator – particularly a security-minded one - would consider the discovery of a new undocumented system on his network a security violation and proceed to investigate it. Heck, I'd even take it offline. If it's a Carnivore box, what happens then? Whose investigation did I just mess up in the name of good systems security practices?

Use out-of-band communications. The best way to hide information is in plain sight. Don't use common ports for mail servers or chat sessions, but map them to more common traffic. Just as the Russian hackers used port 80 (http) to move sensitive material out of DoD networks last year right under the noses of the firewalls, figure out a way to use a covert channel inside a well-used port. The bad guys will be hard-pressed to intercept and parse (in real-time at least) the one or two e-mail notes sent along the gigabytes of Web traffic flowing into your company via port 80.

Frequency Hop. Don't just use e-mail. Have multiple e-mail accounts from multiple sources (POP3, IMAP, APOP, Web-based). Get multiple dial-up accounts and personae. Use IRC, Instant Messaging, *Nix console chats, one-time accounts, and combinations of these forms of communication. Set a defined schedule for what medium and for how long you will use that medium for, and see how long it takes for Carnivore to catch up with you. Or, use text editors to exchange messages, and FTP them to various sites. Then switch to AIM. Then e-mail. Then IRC on a particular channel. The possibilities are endless!

My Favorite. When all else fails, stick with e-mail and encrypt it. But, based on what I've heard from folks involved in computer crimes, the worst thing an investigator can see when using a sniffer or reading intercepted electronic communication is the following: "--- BEGIN PGP MESSAGE ---". Use PGP to send self-extracting files to your associates, encrypt files and exchange them via FTP, and so forth.

It's unlikely that Big Internet Business will continue to develop network infrastructure components that don't have "hooks" for law enforcement use in the future, just as how phone switches today have the ability for law enforcement to "plug in" as necessary under court order. Therefore, it's up to the individual to find ways to insure their communications are secure and free from prying eyes using such tools and techniques as mentioned above, PGP, Zero Knowledge, and other tools yet-to-be-developed.

The best solution is to make sure that whatever you deem as sensitive information is encrypted BEFORE IT LEAVES your desktop computer and the area where YOU CONTROL IT. Waiting for a server to encrypt something places you at risk. Point-to-point encryption of communication channels like VPNs or e-mail are your best bets to insure secure modes of communication.

All Carnivore will do is keep honest folks honest. Power users who value their online privacy and cyber-criminals with half a clue already know how to get around it.