NAPSTER – Should You Be Worried About It?

By: Thomas Kasmir Level One SANS GIAC

Napster in case you didn't know, is a server-based distributed file-sharing system designed primarily to allow clients to download, as well as serve, MP3 encoded music files. The program is available at http://www.napster.com/ for Windows 95/98/NT; and alternative implementations of "Napster-compatible" programs are also available, including "open source" Napster-compatible clients for Amiga, BeOS, Java, Linux, and MacOSX (see http://opennap.source-forge.net/)[1]

How It Works: Let's say that you are looking for "Fields of Gold" by Sting. You first make a request for that song in a search sent to a Napster server. The server would then search its index of files and return to you a list of matches. This returned list is actually a list of other clients like yourself, who claim to have that song on their systems. By connecting to one of their systems you could then download Sting's hit onto your own system. If you wish, when you first connect to Napster you could offer up a list of MP3 files that you would like to add to the server's index thus availing your collection to the rest of the Napster community.

A New Breed of Denial of Services?

Now legal consideration aside (of which there are many), you should know what the security ramifications are should any of your network users be Napster aficionados. If you are administering a network of any kind at an educational facility you already know how popular, and thus how much of a problem, the program can be. According to a report by Computerworld's Mitch Betts, many universities have banned student access to Napster.com after finding that 20% to 60% of their network bandwidth was being eaten up by the MP3 traffic at peak times.[2] So on this count we could feasibly categorize Napster as being guilty of Denial of Services. This new breed of DOS "attacks" however being of a kind that is initiated from within our networks by users seeking data from outside the network, as opposed to the traditional model wherein outside hackers seek to disrupt our services by attacking various vulnerabilities on our servers or routers.

A Secure Musical Community or Network Neighborhood For The Masses?

By now you may be wondering about the inherent dangers of your users converting portions of their hard drives into servers in order to share their musical libraries with the rest of the world. And here is where the controversy begins – you as the network administrator must weigh the evidence and decide what is right for your system. Let's begin with Napster's claim concerning the safety of its product.

Napster maintains that its systems are safe and that there haven't been any security issues to date. In fact one of its chief engineers, Eddie Kessler, director of engineering for Napster, maintains that any references to security problems are simply that - allusions with no basis in fact:

"These kind of veiled security risk references have come up since nine months ago when I joined the company. They are usually about what kind of security problem Napster could potentially have, but so far all such discussions haven't led to any real security hole." [3]

What makes such a claim possible is that it is Napster's policy to not allow any executable files to be traded on its systems, and in fact only accommodates files having legitimate MP3 headers.[4] There are ways to circumvent this directive however as we shall soon see.

Exploring The Risks

Chris Rouland, director of research at Atlanta-based Internet Security Systems, a leading computer security firm, considers the use of Napster "risky Internet behaviour".[4] If Napster's assertion that non-executable files are barred from its systems is true, then does the fact that users are opening up their computers to anonymous Web surfers constitute a real security risk?

Many a network or security administrator may consider that question a no-brainer as in, 'no way are we going to allow universal shares on user's PCs in our organization'. In some places however users exert tremendous pressure to be allowed to have their fun, and in the absence of any as of yet unreported security holes in Napster, a network admin may become convinced to allow the traffic in through the firewall, if at least only during after work hours.

What about that aforementioned ability to circumvent Napster's no-executables policy? Can such file types be planted and thus downloaded from the Napster system? Enter Wrapster - a program that will wrap any files – vbs and other executables included – in MP3 camouflage. According to the download blurb on ZDNet for Wrapster v.2.0: "This great, free file-sharing tool lets you archive any type of file into a bogus .mp3 file that shows up on the Napster Network as having a bit rate of 32kps and a frequency of 32,000Hz. Even though your file might contain pictures, documents, or movies, Napster is fooled into thinking it's a normal .mp3 file. The special bit rate/frequency lets anyone easily search for any Wrapster files that may be hiding on Napster servers."[5]

Now before you jump to the conclusion that your users may have directories full of viruses waiting to spring into action instead of what they thought were Metallica's greatest hits, realize that it's not that simple for a malicious Napsterite to trick another client into downloading his viral payload. Both parties must have Wrapster installed on their PCs and be using it to both wrap as well as unwrap the bogus MP3 tracks in order for this to happen. So while Microsoft Outlook may be an easier and more fertile platform than Napster when it comes to delivering malicious code, one cannot rule out the possibility of Napster as perhaps evolving towards a similar infamous fate based on its popularity and present intrusion into our systems.

It's also worth noting here that in one reported case a security expert has claimed to have found a way to exploit another Napster client's PC into exposing directories that it otherwise shouldn't have. Bruce Hubbert, director of West Coast operations at IFSec Inc., a security consulting group in New York, states that by using a buffer overflow (confusing command buffers with unacceptably high numbers the client PC can't understand) he was able to "trick Napster into displaying remote file directories that it shouldn't".[6]

Locking Out Napster

The most commonly used ports Napster uses are 4444, 5555, 6666, 7777, 8888, 8875. At the end of this paper I have included some sample packet captures of my own in order to see if these are indeed default ports. Now you might try blocking these ports at your firewall if you want to prohibit Napster traffic, but this is a far from foolproof since newer versions of Napster supposedly are designed to search for alternative open/unfiltered ports if the default Napster ones are blocked, and OpenNapster (an extension to the Napster protocol[7]) clients can be configured to use virtually any arbitrary port[8].

If port filtering proves ineffective perhaps a better method is to block the two main IP addresses that all Napster clients contact before being redirected to other subsidiary Napster servers. It's the job of these central servers to locate for the users the most optimal host on which they may begin querying the MP3 indices.
These servers are:
208.184.216.222
208.184.216.223[9]

If the client cannot reach those two IP Addresses there supposedly is no way for them to directly connect to any other Napster server. However for every hole plugged there will always be another one discovered, and in this case the way around this sort of IP blocking comes in the form of another program called Napigator. Napigator allows a client to locate other servers that pretty much function in the same capacity as Napster, but otherwise are non-Napster and have nothing to do with those above IP addresses. Since anyone can host a Napigator server you can see it's a battle of Sisyphean proportions should one elect to embark down the road of blocking access.

It's also worth mentioning that another way around port blocking or IP blocking is the use of Proxy servers. Here is a snippet from an online student guide geared to outwit the network admin who has successfully blocked the Napster protocol:
"The way this hack works is a bit round-about, but simple. Virtually no college worth its .edu blocks its FTP port 21. Building on this tidbit, an off-site friend installs on a spare PC copies of Napster, an FTP server (included with older versions of Windows' Personal Web Server) and a copy of VNC, a free remote-control program. With this infrastructure in place, whenever the Napster-blocked students feel the urge for an MP3 splurge, they can fire up their own VNC client and remotely direct the friend's PC to download MP3s to its local FTP directory. The students can then tap into their friend's FTP server and by circumventing their college firewall, scoop up all the MP3 files they just downloaded remotely."[10]

Packet Captures done on a Windows 2000 Pro PC using WINDUMP mid-October 2000
(I am on machine cs-gk-900)

Here is an initial 3-Way Handshake to Napster.
Napster is defaulting to Port 7777 in this case, while also maintaining a Port 80 HTTP connection ---

```
-----------------------
09:17:01.658216 cs-gk-900.1118 > 64.124.41.237.napster.com.7777: S 4081311328:4081311328(0) win
16384 <mss 1460,nop,nop,sackOK> (DF)
09:17:01.950577 64.124.41.35.napster.com.80 > cs-gk-900.1117: S 1999408833:1999408833(0) ack
4081259428 win 16060 <mss 1460,nop,nop,sackOK> (DF)
09:17:01.950642 cs-gk-900.1117 > 64.124.41.35.napster.com.80: . ack 1 win 17520 (DF)
------------------------
```

Napster now Pushes out some data during this same session but is also seen to use Port 8875 ---

```
09:17:01.951017 cs-gk-900.1117 > 64.124.41.35.napster.com.80: P 1:304(303) ack 1 win 17520 (DF)
09:17:01.951175 64.124.41.16.napster.com.8875 > cs-gk-900.1116: . ack 2 win 16060 (DF)
09:17:01.953201 64.124.41.237.napster.com.7777 > cs-gk-900.1118: S 1829715417:1829715417(0) ack
4081311329 win 32120 <mss 1460,nop,nop,sackOK> (DF)
09:17:01.953249 cs-gk-900.1118 > 64.124.41.237.napster.com.7777: . ack 1 win 17520 (DF)
09:17:01.953779 cs-gk-900.1118 > 64.124.41.237.napster.com.7777: P 1:46(45) ack 1 win 17520 (DF)
------------------------
```

Finally, the session is closed ---

```
09:38:40.397100 cs-gk-900.1118 > 64.124.41.237.napster.com.7777: F 2699:2699(0) ack 18336 win
17088 (DF)
09:38:40.629078 64.124.41.237.napster.com.7777 > cs-gk-900.1118: . ack 2700 win 32120 (DF)
09:38:40.645464 64.124.41.237.napster.com.7777 > cs-gk-900.1118: F 18336:18336(0) ack 2700 win
32120 (DF)
09:38:40.645537 cs-gk-900.1118 > 64.124.41.237.napster.com.7777: . ack 18337 win 17088 (DF)
```

Here's some traffic from a different session, this time with Napster defaulting to Port 8888.
In these packets you can observe Napster negotiating a song download from another client (cr3907-a.pr1.on.wave.home.com), to my machine (cs-gk-900) .
Note that the other client is using Port 6699.
Napster allows you to change this default port for downloading music if you wish. In the Napster program see the Preferences section: " Share files With Napster Users on TCP Port: XXXX" The default is Port 6699, but you can change that. Also, even if you choose to NOT serve up any MP3 files, you still need to declare a directory as a Napster Share in order to be able to download any music.

```
16:40:20.377427 64.124.41.227.napster.com.8888 > cs-gk-900.1126: . ack 152 win 31968 (DF)
16:40:20.377481 cs-gk-900.1594 > cr3907-a.pr1.on.wave.home.com.6699: . ack 264536 win 17520
<nop,nop,sack 48197@30 55801@30> (DF)
16:40:20.377494 cs-gk-900.1126 > 64.124.41.227.napster.com.8888: P 152:252(100) ack 1 win 17480
(DF)
16:40:20.397308 cr3907-a.pr1.on.wave.home.com.6699 > cs-gk-900.1594: P 272728:273316(588) ack 1
win 8662 (DF)
16:40:20.397376 cs-gk-900.1594 > cr3907-a.pr1.on.wave.home.com.6699: . ack 264536 win 17520
<nop,nop,sack 48197@30 56389@30> (DF)
16:40:20.417475 cr3907-a.pr1.on.wave.home.com.6699 > cs-gk-900.1594: P 264536:265124(588) ack 1
win 8662 (DF)
```

So we earlier said that --
"The most commonly used ports Napster uses are 4444, 5555, 6666, 7777, 8888, 8875".
We can see that this much is true, and in these scans we can also add at least a few more to the list: 8875, & 6699.

Conclusion – Allow It At Your Own Risk

If it's all beginning to sound like a losing battle, the network administrator can take heart in knowing that Napster traffic can at least be minimized. The savviest of users who can circumvent filtering or construct proxy servers are also unlikely to ever be fooled into running a VBS script folded into an MP3 wrapper. If your policy dictates that you must do all you can do to minimize risk, then it may serve you well to keep abreast of Napster and all its offspring.

While we have mostly discussed what Napster is as well as what you can do to try and block it, there hasn't been a lot of hard data showing it to be a bona fide security risk. If and until some incident takes place and receives ample press coverage, only the most proactive administrators may wish to presently consider it thus. Bandwidth saturation & MP3 storage requirements as well as legal considerations aside, Napster may not be on your security radar presently, but consider yourself warned. A program this ubiquitous, this powerful, and one that especially appeals to the enterprising spirit of today's young technically knowledgeable crowd bears careful watching.

[1] Computing News. "Napster/Napster-like Programs Not Music to All Ears" Spring 2000 URL: http://cc.uoregon.edu/cnews/spring2000/napster.html

[2] Betts, Mitch. "Internet Webcasts become corporate bandwidth hogs" 5 May 2000 URL: http://www.cnn.com/2000/TECH/computing/05/25/webcast.jam.idg/

3Reuters. "Security Guru: Napster A Security Risk" 20 July 2000 URL: http://www.zdnet.co.uk/news/2000/28/ns-16736.html

[4] ibid

[5] ZDNet. Wrapster download URL: http://www.zdnet.com/downloads/stories/info/0,,0018RM,.html

[6] Computerworld. "Napster Gaffes" 17v July 2000. URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO47133,00.html

[7] OpenNap. "Open Source Napster Server" URL: http://opennap.sourceforge.net/

[8]Computing News. "Napster/Napster-like Programs Not Music to All Ears" Spring 2000 URL: http://cc.uoregon.edu/cnews/spring2000/napster.html

[9] david.weekly.org. "The Napster Protocol" 4 October 2000 URL: http://david.weekly.org/code/napster.php3

[10] How-To-Guides. Top Secret Napster Tricks" URL: http://music.zdnet.com/guides/napstersecrets/page2.html