IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

IN RE: AIMSTER COPYRIGHT LITIGATION	: :	MASTER FILE No. 01 C 8933 MDL 1425 Judge Marvin E. Aspen

DECLARATION OF DANIEL FARMER IN SUPPORT OF PLAINTIFFS' MOTION FOR ORDER TO SHOW CAUSE RE CONTEMPT

I, DANIEL FARMER, the undersigned, declare:

1 I have been retained by Plaintiffs as an expert in this action. I make this declaration in support of Plaintiffs' Motion for Order to Show Cause re Contempt. I have personal knowledge of the following facts and, if called and sworn as a witness, could and would testify competently thereto.

Qualifications

2. I currently serve as an independent computer security consultant. In addition, I am currently writing a book on computer security and spend a great deal of my time performing research on forensic computing and large, high-speed computer networks.

served the principal technical expert for the laintiffs in the entitled In Re Napster, Inc. Copyright Litigation, Case Nos. MDL-00-136 MHP C99-83 MHP C00-007 MHP, and C0 -0926 MHP In that capacity, worked extensively with and analyzed the Napster application and website participated hearings with the concerning the system questions regarding

4. also served the principal technical expert as the plaintiffs In re Aimster Copyright Litigation, No 8933 MDL 425. In that capacity, worked extensively with and analyzed the Aimster application and website, and submitted declaration used support Plaintiffs' Motion for Preliminary Injunction.

5. In 999 testified in United States District Court for the Eastern District of ennsylvania in ALCU v. Reno, No. 99-1324 involving the Child On-line Protection Act.

6. From 1997 1999 the head of Internet security, well the network security architect of EarthLink, responsible for the design and implementation of security policies, firewalls, the internal security infrastructure, well the maintenance and continual monitoring of host and network activity on our large internal network and the with whom communicate. Any and all issues (including products, services, and connectivity) that dealt with Internet security approved by me, including e-commerce and any other aspects involving authentication, validation, or online transactions

Prior EarthLink. worked for several years pair of Fortune 500 companies Sun Microsystems, the largest UNIX system manufacturer the world, and Silicon Graphics, Inc the graphics workstation company. At both companies charge of the technical aspects of computer and network security well conducting security and network research. also re-designed and re-architected Microsystem firewall, and consulted internally and for customers.

In 990 started working for Computer Emergency Response ("CERT"). CERT venture funded by the Defense Advanced Research Projects Agency, entity that originally created because of an Internet worm kind of computer virus) in 988 and designed facilitate the flo of security information and provide emergency assistance any person or organization on the Internet. At CERT, coordinated support CERT customers that experiencing computer security emergencies and in charge of disseminating vulnerability information to vendors and getting them to announce and fix their security problems.

Before at CERT worked for Purdue University and some small software companies programmer and computer consultant. been computing professionally for 20 years have done security consulting for banks, computer companies, and Internet organizations for the past half-dozen years, and often speak computer conferences, academic and research facilities, and government institutions.

10. In 1989, I wrote COPS (the Computer Oracle and Password System), the first publicly available Internet security tool. COPS provides a variety of ways to test and report on the security of a UNIX system.

Seven years ago I co-authored SATAN (the Security Administrator's Tool for Analyzing Networks.) SATAN is a program that analyzes and reports on the security of a computer network. COPS and SATAN are the most popular and widely used security analysis tools ever written. Several companies used the ideas in these tools to create commercial products. Titan, another security tool I co-authored, was released in December of 1998. Titan fixes a variety of security problems and can help administrators create firewalls and implement their organization's technical security policy.

12. In February of 1997, I was one of a panel of experts who presented a briefing on computer and network security to the U.S. House of Representatives Committee on Science, Subcommittee on Technology, discussing the need to protect the confidential nature of communications and to ensure that proprietary data would remain uncompromised.

13. I have published several papers on computer security and networks, most notably on security analysis, software tools, analysis of the Internet, and on current issues with unsolicited commercial email (UCE, or spam.) A few years ago, I created and hosted the first Security Summit, an annual weekend retreat where some fifty of the top security, cryptography, and network researchers gather to discuss and attempt to solve some of the more pressing issues with security on the Internet.

14. Over the course of the past twelve years, I have been interviewed as an expert on nearly every major television, radio, and print news outlet (NBC, CBS, ABC, CNN, PBS, Time, Newsweek, The Wall Street Journal, NYT, etc.), and was interviewed and profiled by Scientific American as one of the top experts in Internet security.

15. I have written the following papers:

The COPS Security Checker System – June 1990 USENIX Proceedings

COPS – Fall 1990 Purdue Technical Report

Improving the Security of Your Site by Breaking Into It – 1993 Internet white paper

SATAN, an unusual application of Web technology – Nov 1995 NLUUG Proceedings

Shall we dust Moscow? – 1996 Internet security paper

From the Trenches: One ISPs Response to the Problem of Spam – April 1998, Login journal.

Titan – December 1998, LISA USENIX Proceedings

Gazing Computer Security with 2020 Vision December 999 Internet white paper

6. have been the Internet for 20 years. and administrate and control all aspects (WWW, Usenet news, email, etc.) for several domains.

Defendants Have The Ability To Stop All File Trading on Madster

My general knowledge and experience, as well as specific experiments have done the Madster system, indicate that (a) Madster depends on few key computers in the madster domain to operate its trading system.; (b) systems could be turned off easily; and (c) if the systems turned off, file trading the Madster system would One of the key of experiments conducted is described below

8. signed up for the Madster service on November or 12, 2002 (paying $4.95 for month of service) because could not find the Madster program available for download anywhere for free. then downloaded the version of the program offered by Madster and installed it on computer A. Before running the Madster software turned computer program that recorded all the network traffic that from computer A to the of the world. then able to create an account and log onto the Madster service, and to search for and download files. The network traffic recorder showed that when logged and searched for files, computer A sent network traffic to systems on the Madster network. then exited the Madster program, logging off the Madster system.

19. By modifying my network parameters, I then turned off the capability of computer A to talk to any system on the Madster network; however, computer A was still able to communicate to any other system on the Internet. I then attempted to log back onto the Madster network. This was unsuccessful. I then turned back on machine A's capability to talk to the Madster.com network and was able to log on, search for music, and download content as before.

20. While still logged onto the Madster network I once again modified my network parameters so that computer A could not talk to any system on the Madster network. Attempts to search for songs were now impossible. Downloading content by clicking on recordings that were previously searched for was also impossible.

21. From these and other experiments I have concluded: that Madster operates three types of servers that exist in the madster.com domain, and that without the ability of users to communicate with these servers, the Madster system will not operate, and users will not be able to trade files:

a. Domain Name Service (DNS) servers. These servers translate IP numbers into names (like madster.com.).

b. Web servers. These servers deliver web content to users perusing the world wide web with an Internet browser, such as Microsoft Internet Explorer or Netscape Navigator. Madster's web servers provide the content on the Madster website (including the Club Madster "Top 40")and allow downloads of the Madster client software, i.e., the software that Madster users use to trade files.

c. Madster servers. These servers allow Madster users to connect and log on to the service, search for files on the computers of other users connected to the Madster system, and to download files from other Madster users.

22. Based on my knowledge and experience, the Madster system can be halted easily in several ways, including simply turning off the power to the servers that Madster operates; disconnecting those servers from the network; stop running the programs that allow Madster users to connect, log on, and search for and download files; or terminating the Internet connectivity provided by Madster's ISP (which I have determined is Qwest Communications), so that the Internet cannot communicate with the madster.com domain.

23. In conclusion, it appears that if the Madster-controlled systems were halted, which can be done easily, the Madster file sharing service would cease to function.

I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct and that this declaration was executed on November 18, 2002, at San Francisco, California.

Daniel Farmer