GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

GIAC GSEC Practical Assignment 1.4, option 1
Stopping P2P: How to Rid Your Network of Unwanted P2P Traffic
Russell Meyer
July 30th 2002

Introduction

Peer-to-Peer (P2P) file sharing software like Napster, Morpheus and most recently KaZaA has exploded in popularity over the last several years. As of July 2002, KaZaA reports its software has been downloaded over 100 million times. At any given time as many as 2 million users are sharing 300 million plus files on the Internet using the FastTrack P2P network (the same network that KaZaA, Grokster and older versions of Morpheus use). These file sharing programs have grown from just sharing music files (Napster) that are 3 or 4 megabytes in size to sharing several different media types including video files that can be 700 - 800 megabytes (KaZaA for example). These mini file servers are running on computers on school, government, and business networks that were not designed for such traffic. Computers running P2P file sharing software raise several security and business concerns including: the release of confidential information, viruses and trojan infection and propagation, legal and liability issues concerning the 'sharing' of copyrighted material or pornography and misuse of company resources including employee time. These reasons and a misunderstanding of P2P software and P2P configuration (Good, p.1) are all reasons for blocking or at least limiting P2P traffic. The following will examine 3 steps you can take to rid your network of unwanted P2P traffic. This paper will focus on KaZaA, at this time one of the most popular P2P programs in use but many of these issues apply to all P2P software. This paper will not address P2P software in general or specific P2P threats, a list of articles on P2P software and security policies from the SANS reading room is included at the end of this paper. This paper is broken down into 2 parts, creating a P2P policy (Administrative) and enforcing the P2P policy (Technical) .

Part I: Administrative

Write and get the P2P policy approved first

The problem with unwritten rules.
Every organization has unwritten rules governing computer use but this is not the best way to protect a network from P2P software and traffic A well through out, written and approved policy on P2P file sharing software should be your first line of defense. It is difficult to enforce 'unwritten rules' across departments or large organizations. Different managers will have different priorities and may think it unnecessary or even counterproductive to censer their people's computer use. They may be more concerned in keeping their people happy and productive, not to "do your job". Managers have to deal with new rules and procedures from

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

upper management every day and they may see this as just another 'IT problem' that they should not have to deal with. Instead of trying to deal with each manager, it is much better to start with the top and then once the policy has been approved, go back to the managers and educate them, they are more likely to following written procedures approved by upper management then your wish.

Identify and articulate the problem.
You need to gather information on the impact of current P2P traffic on your organization and network. If P2P traffic is already an issue on the network, measure the size and severity of the problem. Define the scope of the problem in order to determine the P2P policy you need (a school may allow P2P usage after hours but not during the school day, the policy should address this). Too often policies are too broad to be enforced. The policy of "no unauthorized software installed on PCs" falls flat on its face if no one can produce an current list of all approved software and a procedure for getting new software added or allow for exceptions. Without a good way to measure and therefore enforce the policy, the policy will be ignored when convenient. You should have concrete examples of the dangers of using P2P software (see other SANS P2P articles listed at the end of the paper for a complete list of security threats). Past problems with viruses, trojans or information loss are excellence reasons for creating and getting an effective P2P policy approved.

Start with the IT department.
Before you draft a P2P policy, you should build a consensus within the IT department since they will be the ones helping you implementing the policy. Most people in IT will quickly recognize the dangers of P2P software but at the same time the technical folks might be the biggest users of P2P software. They have the technical savvy and access to extra hardware to use. Explain the problem, show them the resources consumed, point out the security issues and the cost. Most IT people have a logical mind set and will see the problem. They may have just turned a blind eye to the problem in the past or assume since they are the IT department, they can handle any problems or assume the 'rules' don't apply to them. Once you have explained the problem and your intention of creating a written policy, they will usually fall into line. It may be worth while to get them to draft the policy, people are more willing to follow and rules if they have a hand in creating them.

Writing the policy.
The P2P policy should be added to your existing security policy or internet usage policy. The following is a sample from the University of Missouri. As you can see, while the University does not explicitly disallow P2P software or its use, it does cover the problems related to P2P software and traffic.

> 2. Prohibited Uses or University Computer Resources:
>
> a. Unauthorized or excessive personal use. Use may be excessive if it overburdens a network, results in substantial use of system capacity, or otherwise subjects the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

institution to increased costs or risks (employees additionally may be subject to discipline for unauthorized or excessive personal use of computer resources.)

b. Uses that interfere with the proper functioning of the University's information technology resources.

c. Uses that unreasonably interfere with the ability of others to make use of University computer resources.

d. Attempting to gain or gaining unauthorized access to the computer system, or files of another.

e. Use of University computer resources to infringe the intellectual property rights of others.

f. Use of University computer resources for personal profit, except as permitted under the University's conflict of interest policy (University).

The above policy is just one example of a policy covering P2P software and traffic. There are several SANS resources listed at the end of the paper that provide sample polices as well as references to other resources. When drafting the policy, always keep in mind that upper management must approve it.

Laying the groundwork.
After getting input from the IT department and writing a draft of the policy, it is time to lay the groundwork for getting the policy approved. Start with other managers at your level, especially ones that will be directly affected by the P2P policy, make sure they how what you are doing and why. Ask for and then listen to their input. Determine who might be a problem and address their concerns. Try and get them to see the problem and show how the IT department is trying to fix it before it becomes a bigger problem. If you can't get them on your side, make sure they are at least neutral or risk having them fight you in the background.

Finding a mentor or sponsor.
In larger organizations, you might not have access to the people who need to approve the P2P policy. Even if you are the head of the IT department or CIO, you might not have access or you might not be the best one to 'make a case for change'. Ask yourself "Who is most affected by P2P software usage?" The department that is most effected by P2P usage should be a supporter of what you are trying to do. If payroll is having problems getting the payroll checks cut every month or if admissions can't process student schedules or records like they did before P2P grew in popularity, or the executives have problems receiving E-mail you have a compelling business reason and a spokesperson that is not from the IT department. Consider approaching those who seem to hold sway over others in the decision process. Talk to them about the problem and what IT is trying to do about it. Let all the decision makers know what you are trying to do and address any concerns they have before it comes up for formal review. Get the CIO on board or other decision makers (owners, administrators, civil

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

servants, etc…). Identify the holdouts and try and convert them. This may be the time to make small changes in the policy in order to get the policy approved.

Getting it approved by upper management.
Make sure you have enough support to get it passed the first time. The next chance you will get to add or change the P2P policy is after everything blows up due to P2P (network becomes unusable since it is so slow) or a P2P side effect (a new virus outbreak infects so many of your computers that the virus gets named for your organization). Preventive steps are better then the cure. Include onetime as well as ongoing costs of the P2P policy (i.e. new firewall, training or packet shaping software). Offset these costs against the cost of the problems and issues that P2P creates. Be prepared to document hard (like increased Internet traffic costs) and soft (hidden support costs and downtime) costs and back up your numbers. If you are going to use new software or hardware to reduce or eliminate P2P traffic, make sure you have tested the new solution and have a firm idea of the costs and realistic performance figures. It is a mistake to raise the alarm without having a solution and the costs of that solution in mind. Management needs to be aware of what the problems, potential problems and liability exposure (Risk). While the issue and solution may seem simple to you, non-technical people need to be shown the problem. Use simple terms and carefully explain your concerns and the costs of allowing P2P traffic on the network. Use case studies like "Rollins College Muzzles The Napster Mongrel" at http://www.commweb.com/article/printableArticle?doc_id=COM20010425S0014 to show what other organizations have done. Managers are most likely to approve a 'tried and true' solution then a new one. If P2P traffic is already an issue on your network, you can demonstrate the network congestion by using your day-to-day business software like e-mail with and without P2P traffic. To show security holes, run the netstat utility on a computer running P2P software to show just how many other computers on the Internet are connected to the computer behind the firewall. Multiply your example by the number of computers in your organization to show the potential problem. If increased network traffic is not affecting day-to-day applications and the security argument does not sway management, try pointing out the issue of liability. Remember not to appear to be a doomsayer, this is a problem that can be addressed, the network is not going to stop if you do not get exactly the policy you have worked for. Be prepared for alternative solutions to the P2P problem like buying more bandwidth (P2P application will use all the bandwidth they can) or keeping up with Anti-Virus updates (you do already, the P2P software is another attack vector.) It might be out of your hands at this point, make sure your mentor is fully informed of all aspects of the issue and any last minute changes. If you have followed the steps listed above, there should not be any surprises, everyone will be aware of the problem, your solution and will approve the new P2P policy.

I have a P2P policy, now what?
Just because you have a policy eliminating or reducing P2P software and traffic, don't expect it to disappear from the network overnight. There is little reason to

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

think the P2P problem will disappear the day after the P2P policy is approved. Try these steps next:

- Make sure the P2P policy is readily available to all effected by it, post it your organization's internal web site. Some organizations force users to accept the new policy during network logon.
- Go over the new policy with other IT managers and staff and make sure everyone understands the new policy. Reiterate the dangers, security issues, bandwidth usage, costs and potential organization liability if someone was to download or post copyrighted material or pornography using P2P software on the company computers. Mention the consequences of unauthorized P2P use. Remind them that they set an example for the rest of the organization in terms of computer use.
- Start the process of educating other managers. Let them know of the new policy and where they can get a copy. Explain the reasons for it and how it will help them (less wasted time, fewer computer calls to the helpdesk due to viruses or Trojans, faster response time for day-to-day applications, etc…). Let them know how the policy is going to be measured and enforced and what the penalties could be. Encourage them to let their people know about the new policy and the reasons for it.
- Encourage people you talk to ask questions, but be ready to respond to questions regarding checking existing computers and removing any P2P software found. They will want to know about any exceptions to the policy and may have 'what if' questions.
- Measure and report P2P traffic and desktop compliance on a regular basis. This will keep the policy fresh in everyone's mind. Use the pre-policy measurement you took as a baseline and report on going results to upper management on a regular basis. If P2P traffic was a problem before, hopefully network throughput will show improvement and a decrease in P2P traffic.
- If P2P traffic does not drop significantly or go away, determine who is still using P2P software and why, address their reasons and talk to their supervisors. If this still does not work, maybe it is time for enforcement.

Part 2: Technical

Blocking or limiting P2P traffic on the network.
A P2P policy does not usually eliminate P2P traffic by itself, it must be enforced by blocking P2P traffic. While this is the first step for many organizations, it should come after a well-implemented P2P policy. If the policy is not enough, it is time to back it up with network and or client based solutions. You have been using network based solutions to monitor P2P traffic so you have a good idea where the P2P traffic is coming from and who is using it (if you don't, see below). It is now time to use the same filtering technology to block or limit the P2P traffic. Make sure the IT department and upper management or administration know

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

what you are doing and why. Blocking or limiting P2P traffic should come as no surprise to anyone.

Using TCP/IP scanners to identify P2P users.
Before you start blocking P2P traffic, you should have a good idea who is using it. You can use nmap (or nmapNT for the Windows NT and Windows 2000 port of nmap) or other TCP/IP port scanning software to scan internal computers to discover which computers are running P2P software and sharing files. For the scan to return a positive: [1] you need to know the port or IP address that the P2P software uses and [2] the computers being scanned must be on and running the P2P software. NOTE: In the case of KaZaA, file sharing can be on or off, in either case the computer is listening on port 1214. For example, to scan the class C network 192.168.1.0 for users running KaZaA or other FastTrack network software using port 1214 without pinging the host, the nmap command would be "nmap –P0 –p 1214 192.168.1.1/24" or "nmapnt –P0 –p 1214 192.168.1.1/24" on computers running NT or Windows 2000. This is an easy and inexpensive way to catch computers in the act. Once the computer has been identified, action can be taken or at least documented for future use. This scan can be automated to run on a regular bases and the results logged to a text file. Scanning can set off Intrusion Detection Systems (IDS) and can result in an unwelcome visit or phone call from IT security. Remember to get written permission before using any scanner on a production network.

Using a network analyzer to identify P2P traffic.
You can use a network analyzer like Sniffer Pro from Network associates to capture traffic on the network based on port, IP address or on application signatures. Laura Chappell has written several step-by-step articles on P2P traffic analysis including 2 that give the reader detailed instructions on capturing traffic from popular P2P programs, including KaZaA, Morpheus and Gnutella. Take a look at "Capturing Peer-to-Peer Applications" at http://www.ncmag.com/2001_12/securityd1/index.html and "Just Say Gno!" at http://www.ncmag.com/2001_09/gnutel91/index.html. Remember, a network analyzer can only capture packets it can see. In a switched or routed network environment, you will have to make arrangements to connect your analyzer to a network port that mirrors the port that the traffic you want to analyze passes through. Always get written permission before using a network analyzer on a production network. Many organizations and government offices prohibit using a network analyzer without permission on the network due to confidential nature and security issues capturing network traffic raises.

Blocking traffic at the firewall.
Stopping P2P traffic at the firewall is a good choice. You could also block the P2P traffic by segmenting the internal network if the P2P problem is located in just one area, for example in the case of a campus network the dorms might be the hot stop for P2P traffic so it might be worth while to block P2P traffic to and

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

from the dorms. The same holds true for a specific building or a remote site that will not abide by the P2P policy.

Port blocking.
Configure your firewall to block ports known to be used by P2P software. Port blocking will work for some P2P software with known ports but will not work with P2P software that does not use a specific port (i.e. Imesh) or can use common ports like 80 (HTTP), 23 (Telnet), 25 (SMTP) or 110 (POP3). Several P2P programs use the same P2P network so blocking one P2P program will block other P2P programs as well. If you find traffic on your network using an unfamiliar port, you can download the current list of assigned port numbers from www.iana.org.

Cisco PIX firewall example.
While different firewalls will have different commands for port blocking, the following is an example of port and IP address blocking on the Cisco PIX 5xx firewalls running PIX IOS versions 5.0 or above. This will block P2P traffic using the FastTrack P2P network; the same network that KaZaA, Grokster and older versions of Morpheus use. NOTE: Blocking IP addresses or range of addresses is one way of blocking P2P traffic but the addresses can change even easier then the ports can so if you decide to block IP addresses, someone will need to maintain the list of blocked IPs.

Access-list 100 remark deny access to the KaZaA web site
Access-list 100 deny ip 0.0.0.0 0.0.0.0 www.kazaa.com* 255.255.255.255

Access-list 100 remark deny access to the Morpheus web site and the entire 206.142.53 network.
Access-list 100 deny ip 0.0.0.0 0.0.0.0 www.morpheus.com* 255.255.255.255

Access-list 100 remark deny tcp port 1214
Access-list 100 deny tcp 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 eq 1214

Access-list 100 remark apply access-list 100 to both the “inside” and “outside” interfaces
Access-group 100 in interface inside
Access-group 100 in interface outside

There are dozens of P2P networks on the Internet, with more appearing every day. The following is a list of some of the more popular P2P programs with common ports and IP addresses used:

P2P Software	TCP Ports to filter	IP Addresses to filter
MusicCity Morpheus	1214	www.morpheus.com*

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

KaZaA Media Desktop	1214	www.kazaa.com*
AudioGalaxy	40,000 – 49,999	www.audiogalaxy.com*
Imesh		www.imesh.com*
Gnutella Network	6346, 6347, 6348, 6355	
Gnutella – BearShare		www.bearshare.com*
Gnutella – LimeWire		www.limeware.com*
Gnutella – ToadNode		www.toadnode.com*
WinMX	6699	www.winmx.com*
Napster		www.napster.com*
Napigator		www.napigator.com*
eDonkey2000	4661,4662, 4663	www.edonkey2000.com*

The Fast Track network includes Morpheus and KaZaA clients.
The Gnutella network includes BearShare, LimeWire and ToadNode clients.

* Due to SANs policy, the IP addresses of the P2P sites and servers can not be listed. A partial work around for this is to ping the DNS name to determine the IP address of the P2P program. For example "ping www.kazaa.com".

Linux firewalls.
A PC running Linux can be configured as an inexpensive P2P firewall. If you are interested in using Linux as your firewall for P2P traffic, there are several good articles by Josh Ballard at http://www.oofle.com/index.htm including "Firewalling with Linux and IPChains" at http://www.oofle.com/docs/linuxipchains.doc or if you are running a Linux with 2.4.x kernel version or higher "Linux IPTables Firewalling" at http://www.oofle.com/iptables/index.htm. These require a PC with 2 NICs and the know-how to recompile the Linux kernel. For more information on IPChains, check out the Linux HOWTO at http://www.ibiblio.org/mdw/HOWTO/IPCHAINS-HOWTO.html and the "Linux 2.4 Advanced Routing Howto" for more information on to iproute2, traffic shaping and netfilter at http://www.ibiblio.org/mdw/HOWTO/Adv-Routing-HOWTO.html.

Using bandwidth quotas.
Some schools have used bandwidth quotas and then "throttle down" users that exceed their quota. While researching this paper, it seems that schools are more likely to impose quotas and throttle bandwidth usage instead of outright blocking traffic with the use of port or IP blocking or packet inspection. Bruce Curtis produced a detailed presentation of how North Dakota State University implemented a quota system "Network Quotas for Individuals – A better answer to the P2P bandwidth problem?" This presentation can be found at http://www.greatplains.net/activities/meetings/meeting-20020418/presentations/BruceCurtis/BruceCurtis.ppt The University of Texas at Austin also uses quotas to manage bandwidth usage in the dorms. Their policy (https://resnet.utexas.edu/policy/meter.html) addresses such things as IP phone service, P2P applications and even allowing residents to monitor their bandwidth usage in near real time. Quotas can also be setup to apply only to Internet rather

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

then intranet traffic and only apply during specific times of the day. For example, allowing unlimited bandwidth between the hours of 2 and 6 AM.

QoS or giving the 'legitimate' traffic priority.
One of the issues with a quota system is that such a system assumes that high bandwidth users are using the bandwidth for non-school or business activities. This can raise issues for legitimate high bandwidth issues like video production or processing large amount of raw data over the network. In these cases, it might be more appropriate to control bandwidth based on the application or protocol rather then the amount of bandwidth used. Quality of Service (QoS) is a term used to identify and prioritize traffic based on protocol and stateful packet inspection. This can control P2P software like Imesh that uses port roaming that defeats port blocking. Using a QoS system such as Packeteer's PacketShaper or Cisco's Network-Based Application Recognition (NBAR) allows administrators to limit the amount of bandwidth P2P traffic consumes. Oregon State University uses a PacketShaper and quota system to rein in student bandwidth consummation (http://rcn.orst.edu/bandwidth_faq.php).
QOS devices are expensive and will take some expertise to setup and maintain but can pay for themselves with reduced WAN and Internet traffic costs. A recent (6/02) review of several QOS devices like PacketShaper can be found at http://www.nwfusion.com/reviews/2002/0603rev.html. An overview of Cisco's NBAR can be found at http://www.cisco.com/warp/public/cc/so/neso/ienesv/cxne/nbar_ov.htm).

Blocking P2P traffic at the client, locking down the desktop.
One of the best ways to block P2P traffic on the network is to simply not allow users to install P2P software. "Locking down" the desktop will prevent a host of desktop issues but usually results in support issues as well as problems with users who feel that the computer they are using is 'theirs' (it might be, on a college network). While government and private business should make it clear the computer the employee is using is not a 'personal computer' but a company computer, that issue is outside the scope of this paper. Newer desktop and network operating systems like Windows 2000 and Windows XP allow the administrator to lock down the desktop therefore preventing users from installing P2P applications. There are also several network management systems like Zenworks and Intel LANDesk that will allow you to lock down the desktop. You can also find after market desktop lockdown software by using your favorite search engine and searching for "desktop lockdown software". These programs will allow you to lockdown the desktop so users cannot install unauthorized software like P2P programs. If the problem already exists, you will have to identify the computers using P2P software.

Identifying computers that have P2P software installed.
You may need to scan existing computers for known P2P software. This can be done via batch files and login scripts, scanning administrator shares, network operation system add-ons like SMS, Zenworks, Intel LANDesk that allow the

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

administrators to inventory the software installed on the computers. Once the software has been identified it can be remotely deleted, disabled or the user can be informed and asked to remove it. Computers can also be scanned for the files that P2P software shares. Finding large numbers of .MP3s, .AVIs, or other file types can be indicative of P2P software misuse. Scanning should be done on a regular basis and a summary of the reports compiled to document the P2P issues.

Conclusion.
Use the steps above to prevent or at least minimize the P2P traffic on your network. Use passive means such as the security policy and user education first and then use active means to enforce the security policy. Once the security policy has been approved and the network and computers configured, you still need to continue monitoring traffic and desktops in order to prevent new versions of P2P traffic from taking over the network.

© SANS Institute 2000 - 2002, Author retains full rights.

Further SANS P2P and Security Policy Reading

Peer-to-Peer Networking
Billy Evans October 29, 2001
http://rr.sans.org/threats/peer2.php

Post Napster: Peer-to-Peer Revisited
Sean Mays, February 20, 2001
http://rr.sans.org/policy/post_napster.php

A Review of Peer-to-Peer Network Insecurities in Business Applications: Should you take the Risk?
Joanne Kossuth, February 17, 2001
http://rr.sans.org/win/review.php

An Overview of Gnutella
Brenda L. Batkins, July 27, 2001
http://rr.sans.org/threats/gnutella.php

How to Identify and "Contain" Some of the Information Security Problems Created by Unique Business Environments
John Cupps, August 10, 2001
http://rr.sans.org/casestudies/infosec_problems.php

The SANS Security Policy Project
http://rr.sans.org/policy/policy_list.php
http://www.sans.org/newlook/resources/policies/policies.htm

Building and Implementing an Information Security Policy
Martyn Elmy-Liddiard, April 30, 2002
http://rr.sans.org/policy/building.php

Developing Security Policies: Charting an Obstacle Course
Rosemary Sumajit, April 4, 2002
http://rr.sans.org/policy/course.php

Herding Cats 101: Development & Implementation of Security Policies at a University
Jodi Ito, November 22, 2000
http://rr.sans.org/policy/herding.php

Acceptable Use: Whose Responsibility Is It?
Patti Lawrence, March 20, 2002
http://rr.sans.org/acceptable/responsibility.php

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Firewalls & Perimeter Protection
http://rr.sans.org/firewall/firewall_list.php

The Packet Filter: A Basic Network Security Tool
Dan Strom, September 25, 2000
http://rr.sans.org/firewall/packet_filter.php

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

Ballard, Josh. "Firewalling with Linux and IPChains" URL: http://www.oofle.com/docs/linuxipchains.doc (July 24th 2002)

Ballard, Josh. "Linux IPTables Firewalling" URL: http://www.oofle.com/iptables/index.htm (July 24th 2002)

Berg, Al. "P2P, or Not P2P?" Information Security February 2001. URL: http://www.infosecuritymag.com/articles/february01/cover.shtml (19 June 2002).

Bruce Curtis. "Network Quotas for Individuals – A better answer to the P2P bandwidth problem?" April 4th 2002 URL: http://www.greatplains.net/activities/meetings/meeting-20020418/presentations/BruceCurtis/BruceCurtis.ppt (July 24th 2002)

Chappell, Laura. "Security Alert: Capturing Peer-to-Peer Applications." Novell Connection December 2001 URL: http://www.ncmag.com/2001_12/securityd1/index.html (19 June 2002).

Chappell, Laura. "Security Alert: Just Say Gno!" Novell Connection December 2001 URL: http://www.ncmag.com/2001_09/gnutel91/index.html (19 June 2002).

Harrison, Ann. "Another take on limiting P2P traffic." Network World Fusion April 3rd 2002. URL: http://www.nwfusion.com/newsletters/fileshare/2002/01297785.html (June 21 June 2002).

Godfrey, Paul. "KaZaA / Morpheus Denial of Service Attack (Flood)" SecuriTeam September 16th 2001 URL: http://www.securiteam.com/exploits/5XP0D1F5FM.html (July 18th 2001)

Good, Nathaniel S.; Krekelberg, Aaron. "Usability and privacy: a study of KaZaA P2P file- sharing." HPL-2002-163 June 5th 2002 URL: http://www.hpl.hp.com/techreports/2002/HPL-2002-163.pdf (July 18th 2002)

Harrison, Ann. "Controlling P2P in the enterprise." Network World Fusion April 18th 2002. URL: http://www.nwfusion.com/newsletters/fileshare/2002/01276381.html (June 21 2002)

Harrison, Ann. "Choking off file trading in the enterprise." Network World Fusion April 6th 2002. URL: http://www.nwfusion.com/newsletters/fileshare/2002/01246732.html (June 21 2002)

© SANS Institute 2000 - 2002, Author retains full rights.

Hubert, Bert. "Linux Advanced Routing & Traffic Control HOWTO" v1.12 July 20th 2002. URL: at http://www.ibiblio.org/mdw/HOWTO/Adv-Routing-HOWTO.html

Hurwicz, Michael "Emerging Technology: Peer-To-Peer Networking Security" Network Magazine Febuary 6th, 2002 URL: http://www.networkmagazine.com/article/NMG20020206S0005 (July 19th 2002)

KaZaA home page. URL: www.KaZaA.com (July 24th 2002)

Kirby, Rob. "Business Case: Rollins College Muzzles The Napster Mongrel." Commweb April 25th 2001 URL: http://www.commweb.com/article/printableArticle?doc_id=COM20010425S0014 (July 18th 2002)

Lee, Eric "Morpheus File Sharing Software Discloses Files Not Selected For Sharing to Remote Users in Certain Configurations" SecurityTracker August 1st 2001 URL: http://www.securitytracker.com/alerts/2001/Jul/1002113.html (July 18th)

Loney, Matt. "KWBot worm hits KaZaA " ZDNet July 8th 2002 URL: http://www.zdnet.com.au/newstech/security/story/0,2000024985,20266500,00.htm (July 19th 2002)

Russell, Rusty, "Linux IPCHAINS-HOWTO" v1.0.8 July 4th 2000 URL: http://www.ibiblio.org/mdw/HOWTO/IPCHAINS-HOWTO.html v1.0.8, Tue Jul 4 14:20:53 EST 2000

Stevenson, David. "Secret Network Angers KaZaA Users." Tech TV April 10th 2002 URL: http://www.techtv.com/news/internet/story/0,24195,3380237,00.html (July 18th)

Sunday, Jesse "Morpheus Peer-to-Peer Software Discloses User Name Information to Remote Users" SecurityTracker September 1st 2001 URL: http://www.securitytracker.com/alerts/2001/Sep/1002311.html (June 18th 2002)

Truelove, Kelly and Chasin, Andrew "Morpheus Out of the Underworld" OpenP2P.com July 2nd 2001 URL: http://www.openp2p.com/pub/a/p2p/2001/07/02/morpheus.html?page=1 (July 18th 2002)

"University of Missouri Acceptable Use Policy" University of Missouri Septempter 14th 2000 URL: http://www.system.missouri.edu/uminfo/rules/facilities/110005.htm (July 24th 2002)

© SANS Institute 2000 - 2002, Author retains full rights.