**Information Bulletin**
**Title:** Unauthorized Peer to Peer (P2P) Programs on Government Computers
**Date:** April 19, 2005

**ATTENTION:** Federal Departments and Agencies, State Homeland Security Advisors, Security Managers, Federal and State Chief Information Officers and Information Technology Managers, and Information Sharing and Analysis Centers (ISACs).

**Based on this notification, no change to the Homeland Security Advisory System (HSAS) level is anticipated; the current HSAS national level is YELLOW-ELEVATED.**

## OVERVIEW

Peer-to-peer (P2P) file sharing systems provide Internet users with the ability to share files on their computers with up to millions of other people. In doing so, the software makes it possible for people to accidentally share personal files or sensitive data. P2P programs have been found to allow easier access to government computer systems for theft of sensitive documents and use of government resources, due to unauthorized installation and use of this software on government systems. Recent news media reports stated P2P allowed sensitive government documents to get into the public domain. There are documented incidents of P2P file sharing where Department of Defense (DoD) sensitive documents have been found on non-US computers with no protection against hostile intelligence services.

This Information Bulletin is designed to support the Office of Management and Budget (OMB) P2P control policies. Federal computer systems or networks (as well as those operated by contractors on the government's behalf) must not be used for the downloading of illegal and/or unauthorized copyrighted content in accordance with Office of Management and Budget (OMB) Memo M-04-26 on File Sharing Technology. Multiple organizations have ongoing investigations into disclosure of sensitive or classified material due to P2P. State and local government network administrators, and network administrators of private sector networks, are advised to discourage use of file sharing software on their networks for similar reasons.

### *What Is P2P?*

*P2P applications allow computer users to directly access files from one another's hard drive. The most popular P2P software is free and open source. Common P2P uses include song and movie file sharing, gaming and instant messaging.*

## DETAILS

P2P file sharing potentially compromises computer systems. The use of this software creates vulnerabilities which can be exploited by providing a means of introducing malicious code and other illegal material. The software can allow inadvertent sharing of files by vulnerabilities due to mis-configured P2P software. Also, the use of P2P can result in network intrusions and the theft of sensitive data. Recent information indicates there is a military investigation concerning security violations in which classified material has been wrongfully disclosed using P2P. Similarly, Department of Defense (DoD) and other federal government organizations have discovered the presence of P2P software on compromised systems while investigating cyber intrusions.

One example of a P2P program is Kazaa, a popular music sharing program owned by an overseas company. The P2P programs can download various file types, not only media files. A file shared with P2P can then be stored and shared again from any other P2P computer in the world. This can allow sensitive U.S. government data to become located in foreign countries. Often government computer users have installed P2P programs without realizing the potential threat, and this was the reason that Office of Management and Budget (OMB) Memo M-04-26, dated September 8, 2004, on File Sharing Technology was produced.

## SUGGESTED PROTECTIVE MEASURES

Information Technology managers should review procedures and institute policies controlling outside software on government computers as required in OMB Memo M-04-26. Blocking of known P2P application ports will not prevent all P2P applications. Due to the increased use of non-standard ports in P2P communications, administrators must move beyond simple blocking of known ports at the perimeter and focus on examining individual hosts for these applications. The following ports are a small sample that should be reviewed for indications of unnecessary traffic or volume which may indicate a P2P problem:

| **P2P application** | **Port** |
|---|---|
| Bittorrent | default 6881-6889 TCP/UDP |
| edonkey | fully configurable default 4662/TCP, 5737/UDP |
| Gnutella | default 6346/6347 TCP/UDP |
| Morpheus | default 6346/6347 TCP/UDP |
| Kazaa | default 1214 TCP/UDP |
| EMule | fully configurable default 4662/TCP 4672/UDP |
| WinMx | fully configurable default 6699/TCP 6257/UDP |
| Limewire | default 6346/6347 TCP/UDP |
| Napster | client default 6699 TCP alternate 6600-6699 TCP |
| BearShare | default 6346 TCP/UDP |

Additionally, firewalls and IDS systems can be configured to block and/or alert on the presence of P2P traffic. Government information technology managers should review policies to ensure that unauthorized non-government owned software is not residing on government computers.

## CONCLUSION

Few government computers have an operational reason for running P2P software. These applications represent a vulnerability that cannot be afforded without a strong justification. A check of systems can result in greatly increasing the security of the network.

**DHS encourages recipients to report specific information related to cyber incidents or vulnerabilities to the National Cyber Security Division/United States Computer Emergency Readiness Team (US-CERT) at: Webpage: www.us-cert.gov , email: soc@us-cert.gov, or Phone: +1-888-282-0870 (24-hour hotline). Recipients should report information concerning suspicious or criminal activity to the local FBI Joint Terrorism Task Force (JTTF) – the FBI regional phone numbers can be found online at http://www.fbi.gov/contact/fo/fo.htm – and the Homeland Security Operations Center (HSOC). The HSOC can be reached via telephone at 202-282-8101 or by email at HSCenter@dhs.gov. For information affecting the private sector and critical infrastructure, contact the National Infrastructure Coordinating Center (NICC), a sub-element of the HSOC. The NICC can be reached via telephone at 202-282-9201 or via email at NICC@dhs.gov. When available, each report submitted should include the date, time, location, type of activity, number of people and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact (POC).**

**For comments or questions related to the content or dissemination of this document, please contact the DHS/IAIP/IA-R – Information Management staff at DHS.IAIP@dhs.gov.**

# Appendix A: Technical Notes

**P2P can be used to control other exploited machines for coordinated attacks.** One example of this software problem was discussed in US-CERT technical article dated 18 March 2004 pertaining to Phatbot Trojan. Phatbot is an Internet Relay Chat (IRC) bot normally running on Microsoft Windows systems, however, this malicious code may affect other operating systems. Phatbot can propagate using several methods. It scans for NETBIOS shares and attempts to use common username and password combinations to gain access to the remote machine. Phatbot can also propagate by exploiting unpatched vulnerabilities in the Microsoft Windows operating system including vulnerabilities in WebDAV, DCOM, and the Windows Workstation service. It also has the ability to infect a system by taking advantage of the backdoor installed when a system is infected with W32/MyDoom and by exploiting a vulnerability in Dameware.

Once a system is infected, Phatbot will attempt to join an existing IRC channel or P2P network. An attacker can control infected systems by issuing commands to this IRC channel or by sending messages to this P2P network. Phatbot contains an extensive list of commands that provide control over the victim's system. Affected systems allow the remote user to have full access to the file system and the ability to execute arbitrary code on the victim's system. Additionally, Phatbot will attempt to terminate a large number of security related processes (i.e, firewall, anti-virus). This is an excellent example of why P2P creates a risk of losing control of your computer system.