Center for Information Security
www.cis.utulsa.edu The University of Tulsa®

01001010100101010101010011001010101010000101010101010101010100010100100

Risks of P2P File Sharing

John Hale

Alex Barclay

Center for Information Security
Department of Computer Science
University of Tulsa, Tulsa, OK 74104

P2P File Sharing Risks: Environmental Context

- Massive user base
  - Kazaa; over 214 million downloads
  - eDonkey; 2.58 million users per day
  - BitTorrent; consumes over 53% of P2P bandwidth (6 month Cachelogic study)
- P2P file sharing - business model
  - Promote a large network of users and files
  - Embed adware/spyware in client distributions
- Network software managed by end-users

Spyware, Adware and Pests

- Spyware – software that collects and transmits information (e.g. clickstream behavior) about users surreptitiously
- Adware – software that sends targeted advertisements to users, sometimes using dubious techniques, e.g., ad hijacking
- Pests – Any unwanted software
- Tricks of the trade
  - “System message” popups
  - Pop-under windows
  - Faux windows (embedded as images in an HTML file)
  - Leveraging auto-start mechanisms
  - Installation as Browser Helper Objects (BHOs)
  - Resetting browser home pages

Spyware and Pests in P2P Clients

- Recent scan of several P2P clients using Spybot and AdAware found spyware and pests in…
- Kazaa
  - Cydoor, Peerpoints, Altnet, TopSearch
  - GAIN Network (Claria), MyWay.speedbar
- eDonkey
  - Webhancer, GloPhone, WebSearch Toolbar, New.net
- Morpheus
  - Fastclick, Advertising.com, Huntbar, IBIS Toolbar
- Note: Notice often provided to users at install-time

P2P Client Vulnerabilities

- **Kazaa ADM ActiveX Buffer Overflow (2004)**
  - http://www.securityfocus.com/bid/11101
  - **Buffer overflow in Altnet Download Manager distributed in Kazaa and Grokster – a malicious web page would give an attacker control of a box**
- **TorrentTrader SQL Injection (2004)**
  - http://www.securityfocus.com/bid/11087
  - **Input validation error allows attackers to inject arbitrary SQL queries, e.g. to claim an administrator’s password**
- **Gator ActiveX Control Vulnerability (2002)**
  - http://www.securityfocus.com/bid/4161
  - **Gator software installation control allows download of arbitrary code from a malicious website**

P2P Client Vulnerabilities

- **eDonkey URL Buffer Overflow (2002)**
  - **http://www.securityfocus.com/bid/4951**
  - **The eDonkey 2000 Windows client includes a URL handler, ed2k://. The handler for eDonkey 2000 is vulnerable to a buffer overflow condition. Maliciously constructed URLs can crash the user's browser or execute arbitrary code on the victim client. »**
- **Bearshare Server Directory Traversal (2001)**
  - **http://www.securityfocus.com/bid/5888**
  - **BearShare is prone to directory traversal attacks, which allows remote attackers to browse the filesystem of the host running the software.**
  - **http://www.bearshare.com/help/citizen.htm**
  - **‘You don't need to get rid of your firewall completely, you just need to "drill a hole" in it for BearShare. It won't decrease your security because BearShare doesn't contain any security holes. Please read BearShare Firewall Tutorial for instructions how to configure your firewall.’**

P2P Viruses and Worms

- Viruses and worms that target P2P environments do exist
- Common P2P virus techniques
  - Copying itself into shared folders under camouflaged names to lure download/execution
  - Adjusting shared folders
  - Dropping backdoors
- Known P2P viruses
  - Swen, Fizzer, Lirva, Benjamin, KwBot, Bodiru, etc.
  - Kazaa and eDonkey are popular targets

P2P Viruses and Worms

- The potential is compelling
- P2P software
  - Vulnerabilities in clients and bundled software
  - Massive peer-wise connectivity
- Digital content
  - Active content and embedded URLs
  - Vulnerable media readers (JPEG vulnerability)
- Remediation factors are unfavorable
  - Size of install-base
  - Level of administrator awareness

Recommendations

- **Be selective and informed about the software you install**
- **Read the EULAs**
- **Monitor your configurations (of shared folders, etc.)**
- **Use spyware detection and removal software regularly**