

What is contaminated P2P network?

SafeMedia defines a contaminated P2P network as a contaminated virtual network with the following characteristics:

1. A P2P contaminated network consists of many public peers who have distributed contents.
2. Contaminated networks allow all peers to be active nodes on the network.
3. Contaminated networks use the peer-owned network to pass free riding traffic to other peers on the contaminated network
4. Contaminated networks allow uploads as well as downloads to and from other peers.
5. Contaminated networks vary in size and content, depending on the number and quality of nodes logged into it.
6. Contaminated networks have tainted or illegal content. The distributed contents contain copyrighted infringing digital files.
7. Contaminated networks do not have any measures to control the content on the network or on the peers' content.
8. Contaminated networks use specifically designed client software to connect and operate with the one or more of the contaminated networks, using one or more specific P2P protocol.

Further more, contaminated P2P networks can be identified by further examination of the client software (programs) used in connecting to those networks. There are almost 550 software clients available to contact and communicate with contaminated P2P networks. Almost all of the clients share common characteristics^[1]: those clients induce the users to infringe copyrights. In their design and operations, they use a “Duping” scheme. These P2P clients are designed to deploy their “users” as a means to achieve an illegal end. They trick users into inadvertently or unintentionally performing illegal acts. Some of those methods and techniques are:

1. File sharing programs (P2P client software) have repeatedly deployed features that had a known propensity to trick users into uploading infringing files inadvertently.
2. Most Contaminated P2P clients have deployed a feature (redistribution) that will, by default, cause users of the program to upload (or “share”) all files that they download. This feature allows users to distribute illegal files to strangers, and in most cases without the user’s permission or knowledge.

^[1] Filesharing Programs and “Technological Features to Induce Users to Share”: A Report to the United States Patent and Trademark Office: v 1.1 November, 2006

3. Most contaminated P2P networks use a feature built into the client software which is uniquely dangerous. This feature is called “Share-folder and Search-Wizard”. This feature causes users to share inadvertently not only infringing files, but also sensitive personal files like tax returns, financial records, and documents containing private or even classified data. This feature is implemented without user permission or knowledge.
4. Most contaminated P2P networks use a feature built into the client software named “Coerced-sharing features” which makes it almost impossible for a normal user to disable sharing of the folder used to store downloaded files. In most cases, the sharing caused by this feature will be recursive: The program will share not only the files stored in the folder selected to store downloaded files, but also all files stored in any of its subfolders.
5. Most contaminated P2P networks use a feature built into the client software named “Partial-uninstall features”. This feature ensures that if users uninstall the file sharing programs from their computers, the process will leave behind a file that will cause any subsequent installation of any version of the same program to share all folders shared by the “uninstalled” copy of the program. Whenever a computer is used by more than one person, this feature ensures that users cannot know which files and folders these programs will share by default.