



A culmination of a unique set of technologies, SafeMedia's P2PD solutions provide the following benefits:

- Cost effective, zero installation, and pro-active protection against contaminated P2P networks
- Safely drops all contaminated P2P network traffic
- Reduces network bandwidth consumption
- Does not compromise user privacy
- Eliminates the risk of inadvertently disclosing classified national security information or confidential personal and business information associated with the use of contaminated P2P networks
- Eliminates the risk of viruses, Malware and spyware associated with the use of contaminated P2P networks
- Zero administration – automatically updates itself when needed and is self healing
- No discernable network latency impact

WHAT IS A CONTAMINATED P2P NETWORK?

SafeMedia Corporation has developed patent pending technologies that disaggregate contaminated peer-to-peer (P2P) networks. These networks are known to illegally contain copyrighted files, classified business information, national security data, and personal identification documents. SafeMedia's solutions allow non-contaminated P2P traffic and all other Internet traffic to pass freely with no latency.

P2P networks connect user computers to other users' computers or central P2P servers using software, called client software. There are specific characteristics that make certain P2P networks contaminated. A contaminated network:

- Is a "virtual" network
- Consists of many peers (users) and allow all peers to be active nodes on the network
- Allows the peer-owned network to pass 'free riding' traffic to other peers on the contaminated network, even if the peer owner of the network is not actively participating in upload or download processes
- Allow uploads as well as downloads to and from all other peers.
- Has no systematic procedures or programmable methodology to control the content on the network or what content peers upload or download
- Vary in size and content, depending on the number and quality of nodes (users) logged into it at any given time. The more users logged in the more files available to download
- Has at least; one tainted or illegal file on the network. The distributed contents may also contain copyright infringing digital files, classified business and national security data, and personal identification documents
- Has been designed to implement file sharing features that trick users into uploading infringing files inadvertently

- Contaminated P2P client software implants “Duping” schemes in their design. The vast majority of contaminated P2P clients are designed to effectively deploy their “users” as a means to achieve an illegal end; i.e., they trick users into inadvertently or unintentionally performing illegal acts. Some of those methods and techniques are:

- 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 infringing files to strangers, and in most cases without the user’s permission or knowledge.
- Most contaminated P2P clients use a feature built into the client software which is uniquely dangerous. This feature is called “Share-folder and Search-Wizard” that causes users to inadvertently share 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 usually implemented without user permission or knowledge.
- Most contaminated P2P clients use a feature built into the software named “Coerced-sharing features” which makes it almost impossible for an average 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.
- Most contaminated P2P clients use a feature built into the client software named “Partial-uninstallfeatures”. 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.

The definition of Contaminated P2P networks is derived from:

- The design of the software used to connect to the network, which is called “client” software.
- The operational characteristics of those contaminated P2P networks; which includes:
 - No ownership
 - No controls over the content of the network
 - No control or checks and balances on the status of the network
- The client software implements the basic concept self survival through increased uploads. A P2P network is only valuable to users if it has a large selection of files available to download, so developers automatically add upload capabilities to the client software so that everything a user has downloaded is now available for other users on the network to download. Without this mechanism, P2P clients would provide no value to those seeking files and would not expand and grow.

About Us

SafeMedia is a Florida corporation, founded by Mr. Safwat Fahmy in October 2003, the SafeMedia Corporation mission has been to provide an effective, cost efficient and easily implemented preventive solution to the unresolved issues of national security breaches, identity theft and the massive theft of copyrighted digital materials associated with the use of contaminated peer-to-peer networks, and to restore and preserve asset value to copyright holders.



SafeMedia Corporation

6531 Park of Commerce Blvd., Suite 180
Boca Raton, FL 33487
P: 561.989.1934
F: 561.989.1937
www.safemediacorp.com