IJIAET International Journal of Innovative Analyses and Emerging Technology

| e-ISSN: 2792-4025 | http://openaccessjournals.eu | Volume: 1 Issue: 3

Torrent Poisoning: Antipiracy and Anonymity

Megha Yadav[1], Ms. Shalini Bhadola[2], Ms. Kirti Bhatia[2], Rohini Sharma[3]

[1]Master of Technology in Computer Science, MDU, India,
[2]Depatrment of Computer Science & Engineering, Satkabir Institute of Technology And Management, MDU, India
[3]Assistant Professor, Government College for Women, Rohtak, India

Abstract: A P2P network architecture based on Bit Torrent is one of the most popular protocols today, which has been used as a popular method of copyright infringement by pirates and as a method of file transfer that works with almost any data type and format.

An evaluation of the tools and techniques utilized by law enforcement agencies and practitioners to support antipiracy and security is performed. There are a number of legal complexities to consider when dealing with torrent systems that have been attacked many times and used to secure antipiracy, but there are also certain geographic differences that come into play on which country they belong to and how they're handled. However, there are also new ways to remain anonymous even with the source and destination pair information. A new set of terms have been discovered to aid in coming up with good solutions to these problems, and they can be used legally as well as illegally.

Key words: Piracy, Poisoning.

INRODUCTION:-

In Peer-to-Peer (P2P) network file sharing, a large file is broken down into smaller chunks (small pieces) and distributed across multiple peers.In this application, peers have the same privilege, capacity, and rights.During peer-to-peer connection, each node communicates with the other.Rather than requiring central coordination by servers or stable hosts, peers make certain resources available directly to each other.Peers provide as well as consume resources, as opposed to the traditional client-servlet model in which resources are consumed and supplied.P2P collaborative systems are changing peer learning models by focusing on peers doing the same thing while sharing resources, and looking for diverse peers who can bring their own skills, expertise, and resources to the community, allowing each participant to accomplish more than they could individually.[1]

File sharing systems distributed over P2P networks use BitTorrent, a protocol. File transfers using BitTorrent are among the most common protocols. Bit Torrent clients, which implement the Bit Torrent protocol, are required for the user to send and receive files. Most people are familiar with The Pirate Bay, a BitTorrent tracker. A student at the University at Buffalo at the time, Bram Cohen, designed the protocol in April 2001.On 2 July 2001, the first version of the software was released, and the final version was released in 2008. An official Bit Torrent client is available for nearly every computing platform and operating system, including Linux, Mac and Windows. [2]

A Seoul District Prosecutor's Office (SDPO) investigation into illegal content distribution by cloud storage services initiated in August 2011. 25 million dollars in annual sales for a company and a company with annual sales of $15 million both had the same owner, according to the announcement. Their alleged misconduct involved running an illegal content uploading company, independent of the service companies, and stealing license fees (about US$15 million) from content owners. The Contra Piracy group, which claims to be non-profit, reported monitoring 2,919 individuals for infringing the movie over 290,000 times in July of 2013. Identifying the file-sharers from ISPs is crucial to stopping these infringements. The movie was not created by Swiss-based Contra Piracy. Los Angeles-based Hannibal Pictures granted the outfit enforcement rights in order to pursue the action. It was certainly a deal worth doing with up to US$8 million in settlements at stake. In addition to copyright protection technologies and tools for acquiring digital evidence, technologies aimed at protecting copyright on P2P programs like BitTorrent, are becoming more sophisticated and sophisticated as piracy techniques become more sophisticated. The implementation of an effective system to block unauthorized downloads is essential to preventing large-scale damage from continued illegal distribution. [3]

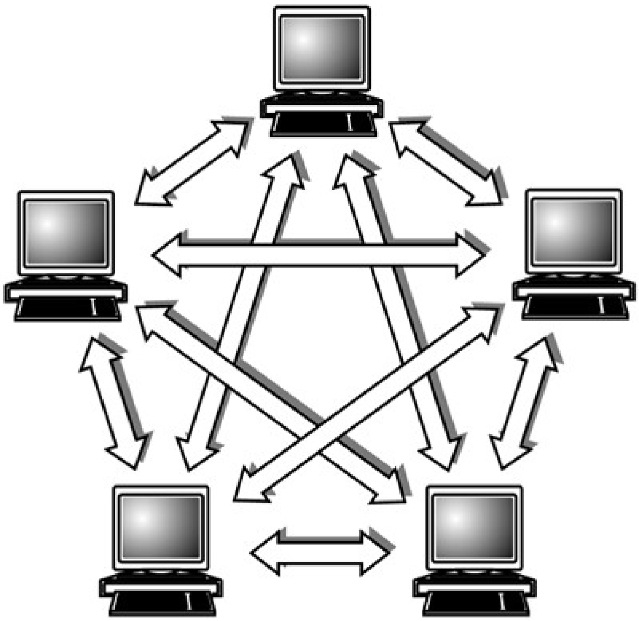

Figure 1: peer to peer network

TORRENT POISONING:

By using BitTorrent, Torrent poisoning involves the deliberate sharing of corrupt or misleading data.These torrent upload methods are sometimes used by anti-piracy organizations to stop peer-to-peer (P2P) sharing of intellectual property and to gather IP addresses of downloaders.[4]

Methods:-

1. Decoy insertion

Viruses are normally spread either by decoy insertion or content poisoning. Both methods are used to introduce corrupted versions of a file into a network.A malicious user makes the corrupted file indistinguishable from an uncorrupted version by modifying it into another format that is easily accessible to users (e.g. similar metadata).Malicious users may turn to high bandwidth connections in order to lure users into downloading the corrupted file.Because the malicious server must process many requests at once, this method consumes a significant amount of resources.The result of these queries is predominantly corrupted copies, such as blank files for instance, or executables infected by viruses. [4]

2. Index poisoning

The malicious users manipulate or alter the index of the files using this method. Users can locate desired content through the index. As a result, peers have a hard time finding the file. In order to prevent users from finding the correct resource, Incorrect information is inserted into the index by the attacker. False IP addresses and port numbers are examples of invalid information. Because of the large volume of invalid information, the server will not be able to connect to the user when they attempt to download the corrupted content. This will cause the average download time to increase since users will need to spend time establishing connections with bogus users. Index poisoning attacks also use less bandwidth and server resources. Files need not be transmitted or requests must be responded to by the attacker.Index poisoning is, therefore, a more effort-efficient method than other methods.[4]

3. Spoofing

For the purpose of disrupting P2P file sharing, some companies develop their own software.By using bogus search results, MediaDefender redirects users to non-existent sites.If users fail to locate the file within the first few attempts, they need to persist to find it, since they typically select only one of the top five search results.Many people will simply stop searching due to frustration, so we expect to see a lot of users give up on searching.[4]

4. Interdiction

P2P file sharing is slowed by this attack method since distributors are unable to serve users.It prevents other users from downloading the file because the attacker uses the connection to the desired file continuously to flood the host's upstream bandwidth.[4]

5. Selective content poisoning

In such an approach, pirates are prevented from accessing open P2P networks, but legitimate users remain able to access content poisoned selectively (also called proactive content poisoning or discriminatory content poisoning).Peers are identified by endpoint address in the protocol, while a digital signature is added to file indexes.Upon downloading and uploading, peers can be authenticated and their legitimacy establishes.A peer-to-peer identification system using identity-based signatures makes it possible to identify pirates without communicating with any central authority.To prevent copyright infringement, poisoned chunks are then sent to detected pirates.Pirates could generally collect clean chunks from colluders (paid peers who send content to other peers without authorization) if legitimate users simply refused download requests from known pirates.Pirates have to discard even clean chunks using this method, which prolongs their download time.[4]

6. Eclipse attack

By concentrating the attack on requesting peers rather than the entire network, the eclipse attack is also known as routing-table poisoning.This attack involves overriding the peers' routing tables to prevent the peer from communicating with anyone but the attacker.The attacker can manipulate the targeted peer in a variety of ways because he copies the entire network.By specifying which search results to return, the attacker can, for instance, control what shows up.A file comment can also be modified by an attacker.In addition to redirecting the peer's requests and modifying them, the attacker can also find out what errors there are by randomly checking data. [4]

7. Uncooperative-peer attack

With this strategy, the attacker connects to a large number of peers within a swarm.As a result, no incoming chunks (authentic or otherwise) are delivered to the peers by the attacker."Chatty peer" attacks are a common form of this attack.A message announcing that there are a number of available chunks is sent by the attacker following the handshake message.Additionally, the attacker repeatedly resends the handshake and message, even when no chunks are provided.By definition, these attacks prevent downloads, since the peer does not download chunks from others instead of dealing with the attacker.[4]

COUNTERMEASURES:

As each method of attack has evolved with time, effective countermeasures have emerged to counter these methods of attack.Torrent files and BitTorrent protocols should have a substantial effect on illegal file-sharing,these measures need to be combined.

- As Bit Torrent is capable of verifying individual files in chunks, it doesn't suffer from content poisoning (unlike index poisoning).P2P file sharing methods such as BitTorrent are among the least susceptible to tampering.
- If Torrent users become members of Private Tracker sites (where one must become a member of a Private Tracker) to handle poisoned torrents (the user is banned from the Tracker site) the torrents can be immediately tagged, deleted, and the person responsible banned.
- A number of torrent tracker websites have added the ability to report poisoned torrents (or malicious torrents of any kind).
- By sharing torrent files on public trackers, torrent data can be managed at similar quality assurance levels to that of private tracker websites.
- In the past, spoofing was possible with tracker technology and Bit Torrent client programs, but now such methods are not possible.
- TCP-IP used to be the only protocol that Bit Torrent used. However, this isn't true any more.TCP Man in the Middle attacks have been made much more difficult to prevent through the use of UDP.
- SHTTP is being used selectively by public and private tracker websites to distribute their web text and image content. Many poisoning techniques are eliminated by using SHTTP (rather than tracker communications) for the website's content.

ANONYMITY:

BitTorrent users have been using privacy services in record numbers lately, as they seek out solutions for hiding their identities. There are several services available for BitTorrent users who would like to hide their IP addresses.Depending on the service, it is either free or charges.Paid services usually offer quicker connections than free ones, whereas free ones have limitations. [5]

1. VPN

BitTorrent users can ensure their privacy most effectively by using a VPN. VPNs hide your IP address by routing all of your traffic over their servers for a few dollars per month. There are usually many downsides to using free plans such as slow speeds and not being able to adjust the BitTorrent settings.VPNs don't just encrypt your BitTorrent traffic, they also hide your entire internet connection, which is different from the other services listed here.A Google search will reveal dozens of other alternatives to BTGuard, Torguard, and Private Internet Access. To be sure that the service you choose permits BitTorrent traffic, our recommendation is to ask beforehand.[5]

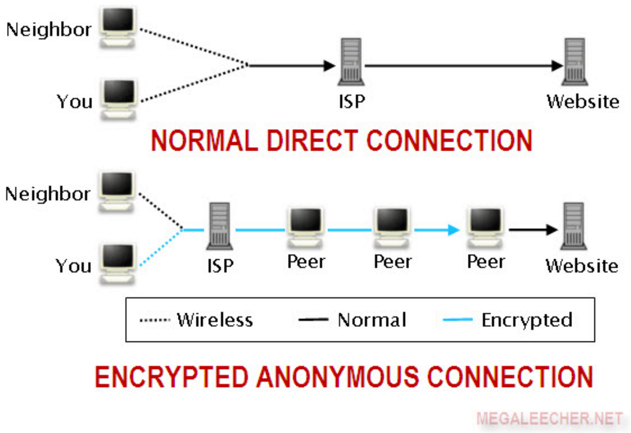

Figure 2: anonymity through VPN

2. BTGuard

This service provides its users with a way to mask their IP addresses.It is designed specifically for BitTorrent users and works on Windows, Mac, and Linux.It is possible to set up your own client in addition to using the preconfigured client.uTorrent and Vuze, among others, support the "Socks V5" proxy protocol. BTGuard also incorporates real security purists with encryption tunnel software.

A proxy service for BitTorrent users like BTGuard would be Torrent Privacy.The client comes with a modified version of uTorrent preconfigured with all the necessary settings.The downside is that this approach can only be used by Windows users.Since 2013 TorrentPrivacy has been operating by the team at TorrentReactor.net.[5]

3. Anomos

In simple terms, Anomos is a distribution protocol for peer-to-peer file sharing that is anonymous, encrypted, and multi-peer.The Anomos team describes its product as a peer-to-peer tagging project integrating onion routing anonymization with single-chain encryption as a free multi-platform solution which enables hide your IP address when using BitTorrent.Anomos uses its own version of torrent files, so it is incompatible with regular torrents.There is another disadvantage of BitTorrent transfers in that they tend to be slower than regular BitTorrent transactions.[5]

4. Seedbox

Known as a seedbox, a torrent server uses high-speed transfers exclusively to transfer torrents.An advantage of seedboxes is that users' IP-addresses are not shared with the public, while they generally get high download speeds.Easily download computer files to their PCs over fast https connections after a download is complete.Several good seedboxes are reviewed by FileShareFreak on a regular basis. [5]

CONCLUSION:

A comparative analysis of different attacks and the methods carried out to protect an anonymous user while defending his copyrighted work has been conducted. However, none of these methods has been proven most efficient as there are countermeasures for torrent protocol, but a global approach is desirable. Cyber Law and Enforcement Agencies are able to enforce the lawfulness of antipiracy through these methods and techniques. It is obvious that the use of torrent software is not illegal as they provide a great means for sharing data and information, however, pirating copyrighted materials over these networks is against the law.

REFERENCES

1. Jungjae Lee and Jongweon Kim “**Piracy Tracking System of the BitTorrent”** International Journal of Security and Its Applications Vol.7, No.6 (2013), pp.191-198 http://dx.doi.org/10.14257/ijsia.2013.7.6.20