TORRENT POISONING: Antipiracy and Anonymity

Ashish Kumar Sharma[1], Amit Dabas[2]
[1,2]Department of Cyber Forensics & Information Security,
Ganga Institute of Technology and Management,
Kablana, Jhajjar, Haryana, India

Abstract: **In this paper we have thoroughly analyzed one of the most prominent file sharing Bit-Torrent protocol based on P2P network architecture which has been used as a major platform of pirating the copyrighted materials and imposing a threat of security as well, besides being a worthy tool of file sharing that supports almost all type and formats of data.**

Available tools and techniques used to support Antipiracy and Security are deeply analyzed that have been used so far by the law enforcement agencies and practitioners. So many attacks are discovered on the torrent systems and have been used to secure the antipiracy but there are also some legal complexities comes into the system while addressing the issues depending upon to which country they belongs. It is important to know the source and destination pair information but new methods are also discovered for being Anonymous used by legal and illegal way both and there are still new terminologies are being discovered to provide some solid solutions to these issues.

Keywords— Piracy, poisoning

I. INRODUCTION

Peer to Peer (P2P) network file sharing system is system where files of any type and size are shared by dividing the whole file into chunks (small parts) distributed over number of peers. Peers are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes. Peers make a portion of their resources, such as processing power, disk storage or network bandwidth, directly available to other network participants, without the need for central coordination by servers or stable hosts.Peers are both suppliers and consumers of resources, in contrast to the traditional client-server model in which the consumption and supply of resources is divided. Emerging collaborative P2P systems are going beyond the era of peers doing similar things while sharing resources, and are looking for diverse peers that can bring in unique resources and capabilities to a virtual community thereby empowering it to engage in the greater tasks beyond those that can be accomplished by individual peers, yet that are beneficial to all the peers. [1]

BitTorrent is a protocol specially developed on distributed Peer to Peer network file sharing system. BitTorrent is one of the most common protocols for transferring large files. To send or receive files the user must have a BitTorrent client; a computer program that implements the BitTorrent protocol.The best-known BitTorrent tracker is The Pirate Bay.Programmer Bram Cohen, a former University at Buffalo graduate student in Computer Science,designed the protocol in April 2001 and released the first available version on 2 July 2001, and the final version in 2008. BitTorrent clients are available for a variety of computing platforms and operating systems including an official client released by Bit Torrent, Inc. [2]

In Aug-2011, the SDPO (Seoul District Prosecutors Office) announced that it had been investigating whether some web storage service providers were distributing illegal content. According to the announcement, two companies with annual sales of US$25 million and US$15 million had the same owner. It was claimed that they operated a specialized company for uploading illegal content independently from the service companies and swindled copyright owners out of license fees (about US$15 million). In July of 2013, Contra Piracy, a claimed non-profit group, said they had monitored 2,919 individuals infringing the movie on more than 280,000 occasions. In order to stop these infringements they need the identities of the file-sharers from ISPs. As usual, Swiss-based Contra Piracy isn't the creators of the movie. Instead the outfit obtained "enforcement rights" from Los Angeles-based Hannibal Pictures to pursue the action. With around US$8 million in settlements potentially on the table, it was certainly a deal worth doing. While piracy techniques are becoming more intelligent and advanced, copyright protection technologies and tools for acquiring digital evidence important to study the prevention of copyright infringement on P2P software such as BitTorrent. In particular, to prevent large-scale damage from continued illegal distribution, we must develop a system that can quickly block unauthorized downloads.[3]

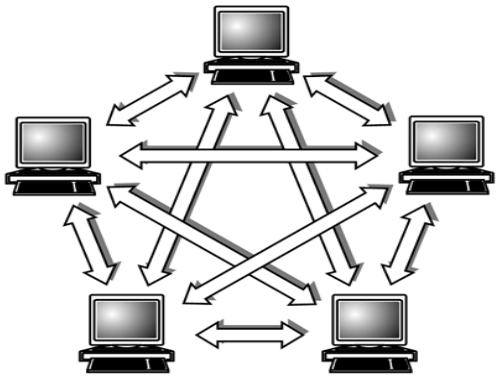

Figure 1: peer to peer network

II. TORRENT POISONING

Torrent poisoning is intentionally sharing corrupt data or data with misleading file names using the BitTorrent protocol. This practice of uploading fake torrents is sometimes carried out by anti-piracy organizations as an attempt to prevent the peer-to-peer (P2P) sharing of copyrighted content, and to gather the IP addresses of downloaders.[4]

Methods:-

1. Decoy insertion

Decoy insertion also known as content poisoning is one of the most popular method by which corrupted versions of a particular file are inserted into the network. This deters users from finding an uncorrupted version and also increases distribution of the corrupted file.A malicious user pollutes the file by converting it into another format that is indistinguishable from uncorrupted files (e.g. it may have similar or same metadata). In order to entice users to download the decoys, malicious users may make the corrupted file available via high bandwidth connections. This method consumes a large amount of computing resources since the malicious server must respond to a large quantity of requests. As a result, queries return principally corrupted copies such as a blank file or executable files infected with a virus. [4]

2. Index poisoning

In this method the index of the files are manipulated or altered by the malicious users. The index allows users to locate the IP addresses of desired content. Therefore making it difficult to locate the file to peers. The attacker inserts a large amount of invalid information into the index to prevent users from finding the correct resource. Invalid information could include random content identifiers or fake IP addresses and port numbers. When a user attempts to download the corrupted content, the server will fail to establish a connection due to the large volume of invalid information. Users will then waste time trying to establish a connection with bogus users thus increasing the average time it takes to download the file.The index poisoning attack requires less bandwidth and server resources than decoy insertion. Furthermore, the attacker does not have to transfer files nor respond to requests. For this reason, index poisoning requires less effort than other methods of attack. [4]

3. Spoofing

Some companies that disrupt P2P file sharing on behalf of content providers create their own software in order to launch attacks. MediaDefender has written their own program which directs users to non-existent locations via bogus search results. As users typically select one of the top five search results only, this method requires users to persevere beyond their initial failed attempts to locate the desired file. The idea is that many users will simply give up their search because of frustration.[4]

4. Interdiction

This method of attack prevents distributors from serving users and thus slows P2P file sharing. The attacker's servers constantly connect to the desired file, which floods the provider's upstream bandwidth and prevents other users from downloading the file.[4]

5. Selective content poisoning

Selective content poisoning (also known as proactive or discriminatory content poisoning) attempts to detect pirates while allowing legitimate users to continue to enjoy the service provided by an open P2P network. The protocol identifies a peer with its endpoint address while the file index format is changed to incorporate a digital signature. A peer authentication protocol can then establish the legitimacy of a peer when they download and upload files. Using identity based signatures, the system enables each peer to identify pirates without the need for communication with a central authority. The protocol then sends poisoned chunks to detected pirates requesting a copyright protected file only. If all legitimate users simply deny download requests from known pirates, pirates could usually accumulate clean chunks from colluders (paid peers who share content with others without authorization). However, this method of content poisoning forces pirates to discard even clean chunks, prolonging their download time.[4]

6. Eclipse attack

The eclipse attack also known as routing-table poisoning instead of poisoning the network, targets requesting peers directly. In this attack, the attacker takes over the peer's routing table so that they are unable to communicate with any other peer except the attacker. As the attacker replicates the whole network for the targeted peer, they can manipulate them in a number of ways. For example, the attacker can specify which search results are returned. The attacker can also modify file comments. The peer's requests can also be directed back into the network by the attacker and can also be modified.It also checks data randomly for any errors found in that.[4]

7. Uncooperative-peer attack

In this attack, the attacker joins the targeted swarm and establishes connections with many peers. However, the attacker never provides any chunks (authentic or otherwise) to the peers. A common version of this attack is the "chatty peer" attack. The attacker establishes connection with targeted peers via the required handshake message, followed by a message advertising that they have a number of available chunks. Not only does the attacker never provide any chunks, they also repeatedly resend the handshake and message. These attacks prevent downloads as, essentially, the peer wastes time dealing with the attacker, instead of downloading chunks from others.[4]

III. COUNTERMEASURES

The methods of attack described above are not particularly effective on their own, as for each measure effective countermeasures have evolved. These measures must be combined in order to have a significant impact on illegal

peer-to-peer file sharing using Bit Torrent protocols and Torrent files.

- Bit Torrent is highly resistant to content poisoning (as opposed to index poisoning), as it is able to verify individual file chunks. Overall, Bit Torrent is one of the most resistant P2P file sharing methods to poisoning.
- By Torrent users being members of Private Tracker websites (where one has to be a member of the Torrent tracker website) -- poisoned torrents can be quickly labeled and deleted and the person responsible can be banned from the site(s).
- Public torrent tracker sites have enabled the ability to report if a torrent has been poisoned (or is fake or malicious in any way). Thus torrent files shared by public trackers can have similar levels of quality assurance as Private Tracker websites.
- Tracker technology as well as Bit Torrent client programs have improved over time, and many kinds of spoofing that were possible in the past are no longer possible.
- Bit Torrent used to exclusively be a TCP-IP protocol, but this is no longer true. Use of UDP, with the uTP protocol has made TCP Man in the Middle attacks more difficult to nearly impossible.
- Public or Private tracker websites have selectively switched over to using SHTTP for the distribution of their web text and image content. By using SHTTP for the website content (versus tracker communications) many poisoning techniques are rendered impossible.

IV. ANONYMITY

With an increasing number of BitTorrent users seeking solutions to hide their identities from the outside world, privacy services have seen a spike in customers recently. Below we've listed some of the most-used services that allow BitTorrent users to hide their IP-addresses from the public.The services discussed in this post range from totally free to costing several dollars a month. The general rule is that free services are generally slower or have other restrictions, while paid ones can get you the same speeds as your regular connection would. [5]

1. *VPN*

VPN is one of the best way to ensure privacy while using BitTorrent. For a few dollars a month VPNs route all your traffic through their servers, hiding your IP address from the public. Some VPNs also offer a free plan, but these are significantly slower and not really suited for more demanding BitTorrent users.Unlike the other services listed in this article, VPNs are not limited to just BitTorrent traffic, they will also conceal the source of all the other traffic on your connection too. BTGuard, Torguard and PrivateInternetAccess are popular among BitTorrent users, but a Google search should find dozens more. It is recommended to ask beforehand if BitTorrent traffic is permitted on the service of your choice.[5]

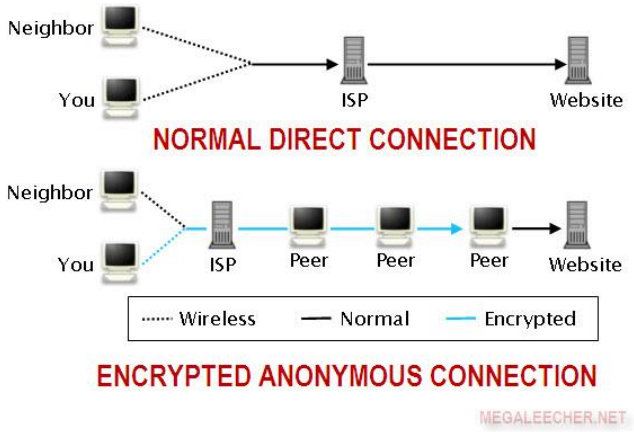

Figure 2: anonymity through VPN

2. *BTGuard*

BTGuard is a proxy service that hides the IP-addresses of its users from the public. The service works on Windows, Mac, Linux and as the name already suggests, it is set up specifically with BitTorrent users in mind. Besides using the pre-configured client, users can also set up their own client to work with BTGuard. It works with all clients that support "Socks V5″ proxies including uTorrent and Vuze. In addition, BTGuard also includes encryption tunnel software for the real security purists.

Torrent Privacy is another proxy service for BitTorrent users, very similar to that of BTGuard. It offers a modified uTorrent client that has all the necessary settings pre-configured. The downside to this approach is that it is limited to users on Windows platforms. TorrentPrivacy is operated by the TorrentReactor.net team and has been in business for more than two years.[5]

3. *Anomos*

Anomos is a pseudonymous, encrypted multi peer-to-peer file distribution protocol. It is based on the peer/tracker concept of BitTorrent in combination with an onion routing anonymization layer, with the added benefit of end-to-end encryption, is how the Anomos team describes its project.Anomos is one of the few free multi-platform solutions for BitTorrent users to hide their IP-addresses. The downside is that it's not fully compatible with regular torrent files as Anomos uses its own atorrent format. Another drawback is that the download speeds are generally lower than regular BitTorrent transfers.[5]

4. *Seedbox*

A seedbox is BitTorrent jargon for a dedicated high-speed server, used exclusively for torrent transfers. With a seedbox users generally get very high download speeds while their IP-addresses are not shared with the public. Once a download is finished users can download the files to their PC through a fast http connection. FileShareFreak periodically reviews several good seedbox providers.[5]

V. CONCLUSION

While comparing the various attacks used to support antipiracy and the methods involved to sustain anonymity one can apply enforcement to protect his copyrighted work but none of them have been proven most efficient as there are countermeasures of torrent protocols but lot of work is still going on in this direction and a global framework is desirable. So these methods and techniques are giving a greater help to Cyber Law and Enforcement Agencies to enforce the legality to the use of antipiracy. Although it is clear that the torrent software are not illegal as they are very useful in information and data sharing but pirating the copyrighted materials over these networks are illegal.

REFERENCES

[1] http://en.wikipedia.org/wiki/Peer-to-peer.
[2] http://en.wikipedia.org/wiki/BitTorrent.
[3] 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
[4] http://en.wikipedia.org/wiki/Torrent_poisoning
[5] https://torrentfreak.com/5-ways-to-download-torrents-anonymously/2/