PRESS RELEASE

FOR IMMEDIATE RELEASE

Madrid, October 13 2011

Unrevealing the dark side of BitTorrent

With tens of millions of users, download events every day, 60% of Europe's upstream traffic and 20% of its downstream traffic, BitTorrent is the world's most popular P2P file-sharing application and represents a significant portion of current Internet traffic. . This level of popularity, however, not only attracts regular file-sharing users but others with malicious intentions.

Authors: Michal Kryczka of Institute IMDEA Networks and Rubén Cuevas of University Carlos III of Madrid

Research carried out by Institute IMDEA Networks, University Carlos III of Madrid and Institut Telecom Sud Paris, "TorrentGuard: stopping scam and malware distribution in the BitTorrent ecosystem", focused on the phenomenon of fake and malicious content publication in the BitTorrent ecosystem. It examined thirty thousand torrents published on the PirateBay portal over a period of two weeks. The results revealed that 35% of the torrents analyzed were associated with fake content. This means that every third torrent has different content to that described in its title.

PirateBay, BitTorrent's most popular portal, deletes any torrent found to be fake, along with the user account that published the content. Fake torrents are recognized by downloaders who report back to PirateBay, which in turn removes the torrent and the user account. Despite this detection/deletion

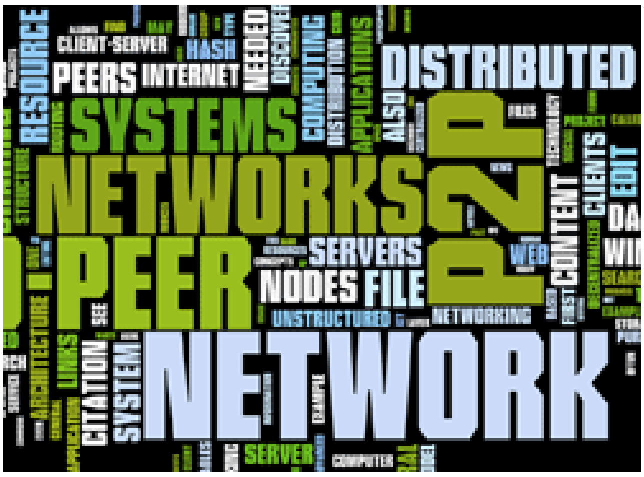
The Pirate Bay
Buscar Torrents | Explorar Torrents | Torrents Recientes | Shows de TV | Musica | Top 100
Preferencias
Idiomas
☑ Todos ☐ Todo ☐ Video ☐ Aplicaciones ☐ Juegos ☐ Otros
Búsqueda Pirata
Voy a tener suerte
Como descargo?
Iniciar sesión | Registrar | Language / Elegir idioma | Acerca de... | Amenazas Legales | Blog
Contactanos | Usage policy | Downloads | Doodles | Nube de Búsquedas | Tag Cloud | Forum | TPB T-shirts
Slopsbox | Bayfiords | BayImg | PREDator | Follow TPB on Twitter
4.862.316 usuario registrados. Ultimo subido 12:04:04.

mechanism, every fourth download from BitTorrent contains fake content. This creates a serious threat that is yet to be dealt with.

The study reveals that just 20 publishers are responsible for injecting 90% of the fake content that appears in the BitTorrent ecosystem. Most of these publishers employ dedicated servers from foreign companies in order to have sufficient resources for their activities, as well as to hide their identities. A great deal of effort is spent on distributing this fake content, as the portals delete each account from which the content is published, and new accounts must continually be created. The study also describes different techniques used by publishers to attract downloaders to their content. These include using the title of popular movies or falsifying the performance statistics of a torrent to make it appear more popular. This level of investment in both time and resources can only be explained by the strong motivations that drive the distribution of fake content.

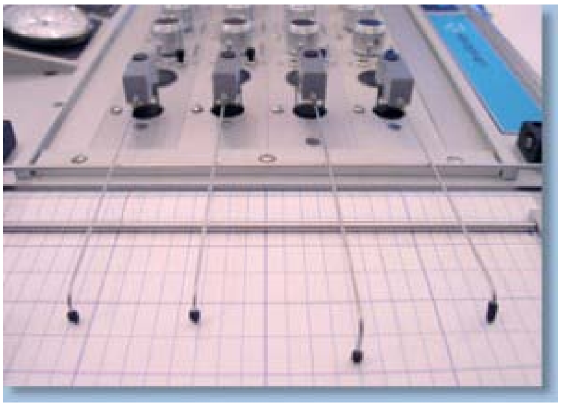
The researchers looked in detail at a large amount of fake content in order to identify these motivations. Their analysis showed that fake publishers fit one of three different profiles. Sixty-five percent exploit the popularity of the BitTorrent system to rapidly propagate malware among thousands of users. The content published may be malware itself, but there are also publishers using more sophisticated techniques. They publish movies with catchy titles, which open in a player showing pop-up windows. These request that the user install new codecs, providing a URL link to where they may be downloaded. Security and anti-virus software reports the file containing the false codecs as malware.

On the other hand, 35% of fake publishers are scammers. They use the torrent ecosystem to attract people to their websites, where different types of scams are carried out. For example, victims may be requested to provide their credit card number or to participate in premium SMS contests. Money, then, motivates these publishers. The result is that a very small fraction of fake torrents originate from anti-piracy agencies. Contrary to the two previous types of publishers, who pursue dishonest ends, anti-piracy agencies publish fake versions of the copyrighted content they want to protect. The measures undertaken by anti-piracy agencies are limited by the amount of content (under request from a company) and the time available (in the weeks before and after the content, e.g. movie, is released).



P2P file-sharing represents a significant portion of current Internet traffic

In order to protect themselves against fake torrents, the researchers implemented and evaluated software known as “TorrentGuard”. This program uses the PirateBay portal to collect IP addresses being used to distribute fake content. These addresses are then blacklisted. The software also monitors each torrent published on PirateBay and marks it as fake if a blacklisted IP address was used to serve its content. Using this method, it is possible to identify fake content shortly after it is first published, speeding up the detection process. The software is publicly available and can be accessed both through a website and a popular BitTorrent client's plugin. Widespread use of this tool may prevent up to 35 million downloads of fake content every year, helping reduce the number of computer infections and scam episodes faced by BitTorrent users.

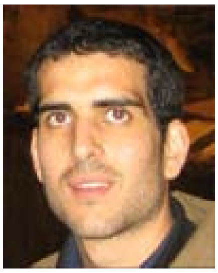


The software proposed in this study has a similar purpose to that of a poligraph.

The study was carried out by Michal Kryczka from Institute IMDEA Networks, Rubén Cuevas, Roberto González and Arturo Azcorra from Carlos III University in Madrid, and Ángel Cuevas from Institut Telecom Sud Paris (France).

Michal Kryczka

Institute IMDEA Networks



Rubén Cuevas

Universidad Carlos III de Madrid

ABOUT INSTITUTE IMDEA NETWORKS

Institute IMDEA Networks is an international research institute supported by the Regional Government of Madrid and the European Union. The Institute brings together distinguished and young scientific researchers from all over the world to develop cutting-edge science and technology in the field of networking. In order to ensure a truly international perspective, the Institute's working language is English. Promoting interdisciplinary collaboration, the Madrid-based Institute works in partnership with leading businesses and scientists from around the globe. By generating new knowledge and understanding through its activities, the Institute supports the continued development of Madrid and Spain as a centre for international scientific and technological research.

www.networks.imdea.org

CONTACT INFORMATION – FOR INFORMATION PURPOSES ONLY

We ask you kindly not to publish the following contact details. Thank you for your cooperation.

If you would like more information about this topic, please call or email:

Contact:

Rebeca De Miguel, Operations Support Manager
Tel: +34 91 481 6977
Email: rebeca.demiguel@imdea.org

Institute IMDEA NETWORKS
Avda del Mar Mediterraneo, 22
28918 – Leganés
Madrid (Spain)

General enquiries:

Tel: +34 91 481 6210
Email: info.networks@imdea.org