

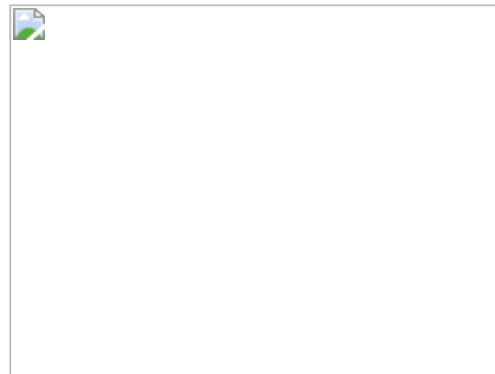
OpenPGP Keyservers Now Store Irremovable Torrent Magnet Links For Freedom Of Information Activists

BY ERNESTO ON

C: 28

BitTorrent has proven to be an ideal tool for pirates. The protocol's decentralized nature makes it impossible to interfere with transfers between users. Torrent sites and indexes are the only weak link in the chain, but there are novel solutions to that 'problem' as well, it appears.

BitTorrent is often praised for its decentralized nature. The file-transfers take place between users and there's no central service required.



That's also one of the main reasons why pirates embraced it.

There is a weak spot though. In order to download something, you need a torrent or magnet link. These are available through torrent sites which, as history has shown, can disappear overnight.

While it's unlikely that all torrent sites will be eradicated at once, we recently spotted a rather novel approach to this 'problem.' A few weeks ago OpenPGP keys with magnet links were added to SKS key servers.

These key servers are computers which store and index OpenPGP keys over the Internet. This helps users who rely on encrypted email, for example. The servers generally share the keys amongst each other in a pool and uploaded keys generally can't be removed.

The permanent storage of keys generally isn't an issue. However, when the system is used as a stealth resource to store magnet links to pirated content, this resilience is put in a different light.

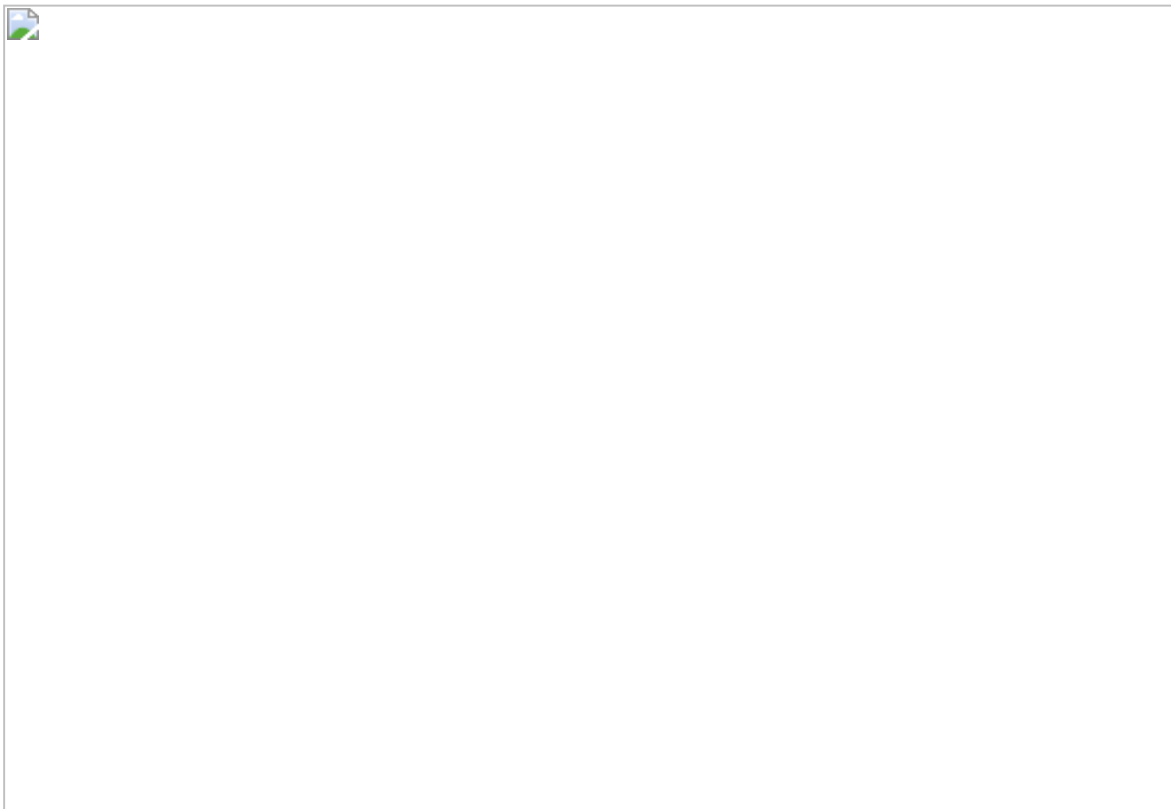
This is exactly what happened.

A few weeks ago a series of rather odd, but valid, PGP keys were uploaded to SKS key servers. These keys were not meant to encrypt email though, but as a safe storage for torrent magnet links.

As a result, popular key servers, including the ones hosted by research university [MIT](#) and [Surfnet](#), have transformed into pirate sites.

The magnet links, most of which point to pirated content, were added in the UID field. In examples we've seen, sometimes there were a hundred magnet links added to a single key entry. And with the search functionality of the key servers, these are easy to find.

Magnet links..



While there are over a thousand magnet links on these key servers now, there are a lot of duplicate entries. That makes it more of a gimmick than a usable tool for pirates, but still.

While key servers are not really an alternative to pirate sites yet, these magnet links have not gone unnoticed. We received the first

tip weeks ago and others spotted it too. The irremovable nature of these links is particularly intriguing.

MIT, for example, clearly states in its FAQ that it is impossible to remove keys once they're up.

TorrentFreak spoke about the issue with Kristian Fiskerstrand, who operates the sks-keyservers website. He notes that removing keys is not possible due to the nature of these servers.

"The keyserver network is intended as an add-by-anyone key store, and structurally these are valid OpenPGP keyblocks," Fiskerstrand says.

Only the owner of a private key can remove an entry. Keyservers are designed to keep their data online and share it with other servers. Similar to the blockchain, nothing is removed.

Fiskerstrand confirms that if copyright holders want these keys removed, they're out of luck.

"[E]ven if the copyright holders were having issues with it they should focus on removing the underlying data not any pointer that is far off the original data," Fiskerstrand notes.

That, however, brings us back to the beginning of this article.

Since BitTorrent transfers are decentralized there is no single source to go after. Copyright holders will have to go after each and every pirating torrent user individually...