**What are WebRTC leaks?**

WebRTC implement STUN (Session Traversal Utilities for Nat), a protocol that allows to discover the public IP address. To disable it:

* Mozilla Firefox: Type "about:config” in the address bar. Scroll down to “media.peerconnection.enabled”, double click to set it to false.
* Google Chrome: Install Google official extension [WebRTC Network Limiter](https://chrome.google.com/webstore/detail/webrtc-network-limiter/npeicpdbkakmehahjeeohfdhnlpdklia).
* Opera: Type "about:config" in the address bar or go to "Settings". Select "Show advanced settings" and click on "Privacy & security". At "WebRTC" mark select "Disable non-proxied UDP".

**What are DNS leaks?**

In this context, with "DNS leak" we mean an unencrypted DNS query sent by your system OUTSIDE the established VPN tunnel.

**Why does my system leak DNS queries?**

In brief: Windows lacks the concept of global DNS. Each network interface can have its own DNS. Under various circumstances, the system process svchost.exe will send out DNS queries without respecting the routing table and the default gateway of the VPN tunnel, causing the leak.

**Should I be worried for a DNS leak?**

If you don't want that your ISP, and anybody with the ability to monitor your line, knows the names your system tries to resolve (so the web sites you visit etc.) you must prevent your system to leak DNS. If you feel that you're living in a human rights hostile country, or in any way the above mentioned knowledge may harm you, you should act immediately to stop DNS leaks.

**How does torrent detection work?**

To detect data from your torrent client we provide a magnet link to a fake file. The magnet contains an http url of a controlled by us tracker which archives the information coming from the torrent client.