Cloud-based Censorship Resistant I2P Reseeding

Sep 29, 2019 · 4 min read

From early March until April, 2019, we conducted measurements from 1.7K network locations located in 164 countries to examine the accessibility of four different I2P services: the official homepage, its mirror site, reseed servers, and active relays in the network. We could identify blocking attempts in five countries. China consistently hinders access to I2P by poisoning DNS resolutions of the I2P homepage and reseed servers; SNI-based blocking was detected in Oman and Qatar when accessing the I2P homepage over HTTPS; TCP packet injection was detected in Iran, Oman, Qatar, and Kuwait when visiting the mirror site via HTTP; and explicit block pages were discovered when visiting the mirror site from Oman, Qatar, and Kuwait. Our findings were presented at the 9th USENIX Workshop on Free and Open Communications on the Internet.

To remedy the SNI-based blocking problem, we recently set up an I2P reseed server over Cloudflare since this is the only provider currently supporting Encrypted SNI. To cope with the problem of several censors preventing users from using I2P by blocking access to the download homepage and reseed severs, we opt to mirror the latest I2P installation packages and reseed bundle on major cloud providers as this is one of the ways to hinder network filtering by making the cost of collateral damage as high as possible. The installation packages will be updated as soon as new version is released, while the reseed bundle will be updated periodically to provide censored users with currently active relays in the network. To that end, the censors will have to bare high collateral damage to block access to all of the aforementioned cloud service providers to prevent I2P users from manually reseeding. While the censors can also block access to active I2P relays contained in the reseed bundle, we did not notice such a blocking case in the wild.

To that end, censored users can download the installation packages and the latest reseed bundle from these cloud storage providers:

- Box: https://app.box.com/s/aednqugd5zf07mlg65wjeafay3b1qqbg
- Dropbox: https://www.dropbox.com/sh/3w9pn8l4269ky01/AACo-l7GpK2TYji5y5vOyQR7a
- Google Drive: https://drive.google.com/drive/folders/16VaXQ_1q_IjsMeGht5DjfxRKT1t8EW8Y
- OneDrive: https://1drv.ms/u/s!Agjj2p_MBHA0aZF3LWIYBEWbGDg

With the reseed bundle fetched from one of the above cloud storages, censored users can manually reseed from the I2P router console http://localhost:7657/configreseed (or http://localhost:7647/configreseed if the client is an I2P Browser bundle on MacOS) by clicking `Browse` to point to the reseed bundle under `Reseed from File`.

In addition to hosting on cloud storages, we also distribute the installation packages and the reseed bundle on the

InterPlanetary File System (IPFS), which is an emerging technology that powers the Distributed Web. Moreover, contents on IPFS are harder to block because content on IPFS is stored on several IPFS nodes distributed across the globe. Files stored on IPFS can be located by Content Identifiers (CID). In order to fetch files from IPFS, users can install IPFS on their machine, or use one of the public IPFS gateways, which can be found here.

To download a file or a directory, users can simply append the CID of that file/directory to the URL of the above public IPFS gateways. The CID of the directory, where the current I2Pv0.9.42 installation packages are stored, is `QmU1HJvxvzpizLHm84zg3yEYvaRvfPJWabj5ZGfWtejw2B`, and the CID of the I2P browser for MacOS `QmdNJ1zA7P6VSDmMZ8YhicgHKzzU8KhLaRTaNfQcnuzbHr`. Users can visit these URL to download installation packages:

- https://ninetailed.ninja/ipfs/QmU1HJvxvzpizLHm84zg3yEYvaRvfPJWabj5ZGfWtejw2B
- https://ninetailed.ninja/ipfs/QmdNJ1zA7P6VSDmMZ8YhicgHKzzU8KhLaRTaNfQcnuzbHr

For the reseed bundle, its CID can be obtained by querying the DNS `TXT` record of the domain `_dnslink.reseed.np-tokumei.net`. This `TXT` record is changed periodically as the content of the reseed bundle is also changed frequently. In Unix environment, users can use `dig` command to get the CID of the latest reseed bundle. For instance, at the time of composing this post, the `TXT` record was returned as follow.

```
dig +short _dnslink.reseed.np-tokumei.net TXT

output: "dnslink=/ipfs/QmTdoTuxdThXjDvDpQ5ihByXAaLxMQw1h3JNg3Lr16QDC3"
```

Users can simply take the above CID (i.e., `QmTd...`) and append it to any of the public IPFS gateways to download the reseed bundle. Then, from the I2P router console, the reseed bundle can be used for manual reseeding as shown above.

It is worth noting that censors can always interfere with the DNS resolution process above. Thus, it is desirable that the DNS resolution of `_dnslink.reseed.np-tokumei.net` should be conducted using DNS over HTTPS/TLS techniques. Alternatively, any online DNS lookup tool can also be used to obtain the most current CID of the reseed bundle, e.g., https://dnschecker.org/#TXT/_dnslink.reseed.np-tokumei.net.

If you run into problems accessing any URL provided above, feel free to contact me at `hoang.nguyenphong@protonmail.com` or DM me on Twitter `@NP_tokumei`, I will try my best to help as much as possible.

blog post censorship resistant I2P reseeding

Hoàng Nguyên Phong
PhD Candidate

Related

- Guidelines to set up an I2P reseed server over Cloudflare