Past, Present, Future of Anonymous Publishing Infrastructure

Fabio Pietrosanti
e-privacy 2012
naif@globaleaks.org
Milano 21-06-2012
Tor Hidden Services

- Anonymity for the server
- eqt5g4fuenphqinx.onion
- End-to-end encryption
Why use Hidden Service?

- Avoid retaliation for what you publish
- Securely serve content
- Protect against seizures/location
Tor2web

- Exchange clients anonymity for usability
- Connects Tor Hidden Services with the surface web
- You can setup an anonymous site and impact the whole net
- site:tor2web.org 52k link on google
Tor2web 1.0

Tor is a software project that lets you use the Internet anonymously. tor2web is a project to let Internet users access anonymous servers.

Here's how it works: Imagine you've got something that you want to publish anonymously, like the Federalist Papers or leaked documents from a whistleblower. You publish them via HTTP using a Tor hidden service; that way your anonymity is protected. Then people access those documents through tor2web; that way anyone with a Web browser can see them.

Getting started

Whenever you see a URL like http://duskgytldkxiug6.onion/, that's a Tor hidden Web service. Just replace .onion with .tor2web.org to use the tor2web proxy network. Example:

https://duskgytldkxiug6.tor2web.org/

This connects you with tor2web, which then talks to the hidden service via Tor and relays the response back to you.

WARNING: tor2web is only intended to protect publishers, not readers. You won't get the level of anonymity, confidentiality, or authentication that you would get if you were using a Tor client yourself. Using tor2web trades off security for convenience; install Tor for better results. (More details...)

More information

- How do I run my own tor2web proxy?
- Is this legal?
- What about mirroring?
- How can Tor make this better?

Example sites

- Search Google
- The Federalist Papers
- WikiLeaks

Thursday, June 21, 2012
Tor2web 1.0 issues

- Exposed to abuse complaints
- Misuse of HS to spread of illicit content
- No disclaimer
- No reporting system
- High latency -> Little usability
- The leads to server takedown
In 2010 there were at one point 3 Tor2web nodes.

In April 2011, there was only one server left.

In June 2011, the last of the 3 original Tor2web nodes went offline.
You are visiting a Tor Hidden Service Website through Tor2web Proxy.

Tor2web servers are not hosting this web content you are viewing. Tor2web can identify the IP of visitors of this site, we strongly suggest to access this site directly with Tor Browser Bundle to increase your anonymity and efficiency.

If you feel this website violate some kind of user policy or ethical code, you can fill an Abuse Complain.
If you want to report a bug or a problem, you can Send us an Error Notification.

Click here to hide this disclaimer.

This is the example page for Tor's rendezvous points system.
Read Thomas Paine's Common Sense.
Or read The Federalist papers, which were also originally published anonymously.
Tor2web 2.0 improvements

• Tell the audience the content is not hosted
• Abuse complaint reporting system
• Dynamic URL rewriting
Tor2web 2.0 issues

- Usability aspect not dealt with (white-page effect)
- Not easily deployed
- Crappy code
- Trust issue with sharing of *.tor2web.org SSL private key
Tor2web 3.0

- Reimplementation funded by RFA F2C and managed by Hermes Association within GlobaLeaks Project
- Distribute responsibility
- Rewrite the code
- Get more Tor2web node!
• A tor2web node does not need anonymity
• To improve performance reduce the number of hops
• An experimental implementation will be in tor 0.2.3.x
Multi-domain distribution

- To run a tor2web node currently we need to entrust you with the wildcard SSL cert
- You should be able to run tor2web on xxxx.your_domain.org
- There can be a list of all supported tor2web domains
Unique and Temporary URL

• Separate the linker to content from the server
  • I request xxxx.tor2web.org
  • Just for me get’s generated yyyyy.tor2web.org (or also yyyyy.something.org)
  • If someone else visits at a latter time yyyyy.tor2web.org it is expired
  • This also avoids hot-linking
Legal Help

• Terms of Services
  • Any lawyers willing to help?
Let’s talk.


tor2web 2.0: [https://github.com/globaleaks/tor2web-2.0](https://github.com/globaleaks/tor2web-2.0)

Tor2web Cataclysm Edition: [https://github.com/globaleaks/Tor2web-3.0](https://github.com/globaleaks/Tor2web-3.0)
Past, Present, Future of Anonymous Publishing Infrastructure

Fabio Pietrosanti
e-privacy 2012
naif@globaleaks.org
Milano 21-06-2012