Tor2web: exposing the darknet on Internet

Giovanni Pellerano, E-Privacy, Florence June 8 2013

Who am I?

- Giovanni Pellerano
- Independent Security Researcher
- Co-Founder of Hermes Association
- Actually involved in development of:
  - GlobaLeaks
  - Tor2web

Speech Outline

- Background on Tor Hidden Services (HS)
- Tor2web 0.1, concept and issues
- Actual Tor2web status
- Discussion on current issues and ideas

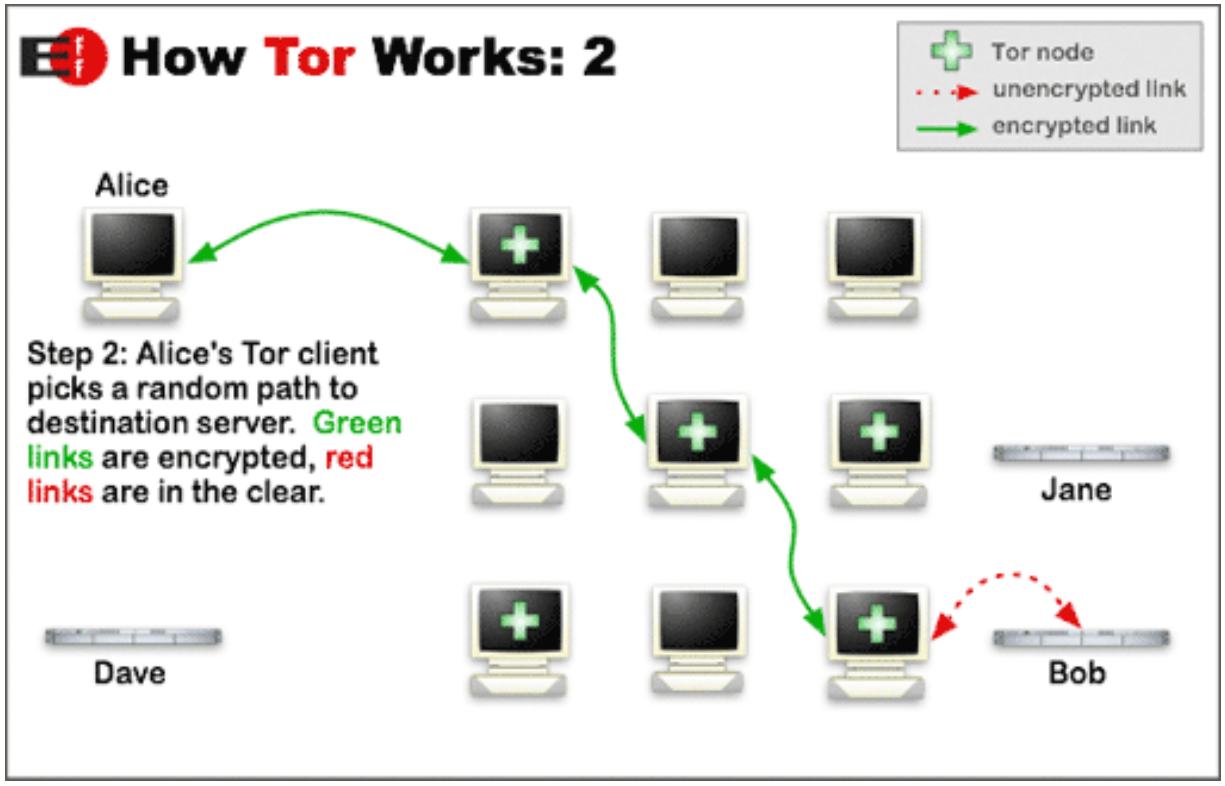
Tor?

The Onion Router (Tor) is a software that builds an overlay network over Internet.

- originally developed with the U.S. Navy in mind, for the primary purpose of protecting government communications

- it's first function is to provide a way to establish an anonymous connection from an anonymous client to a public server.

Tor



Details can be found at:
https://www.torproject.org/about/overview.html.en

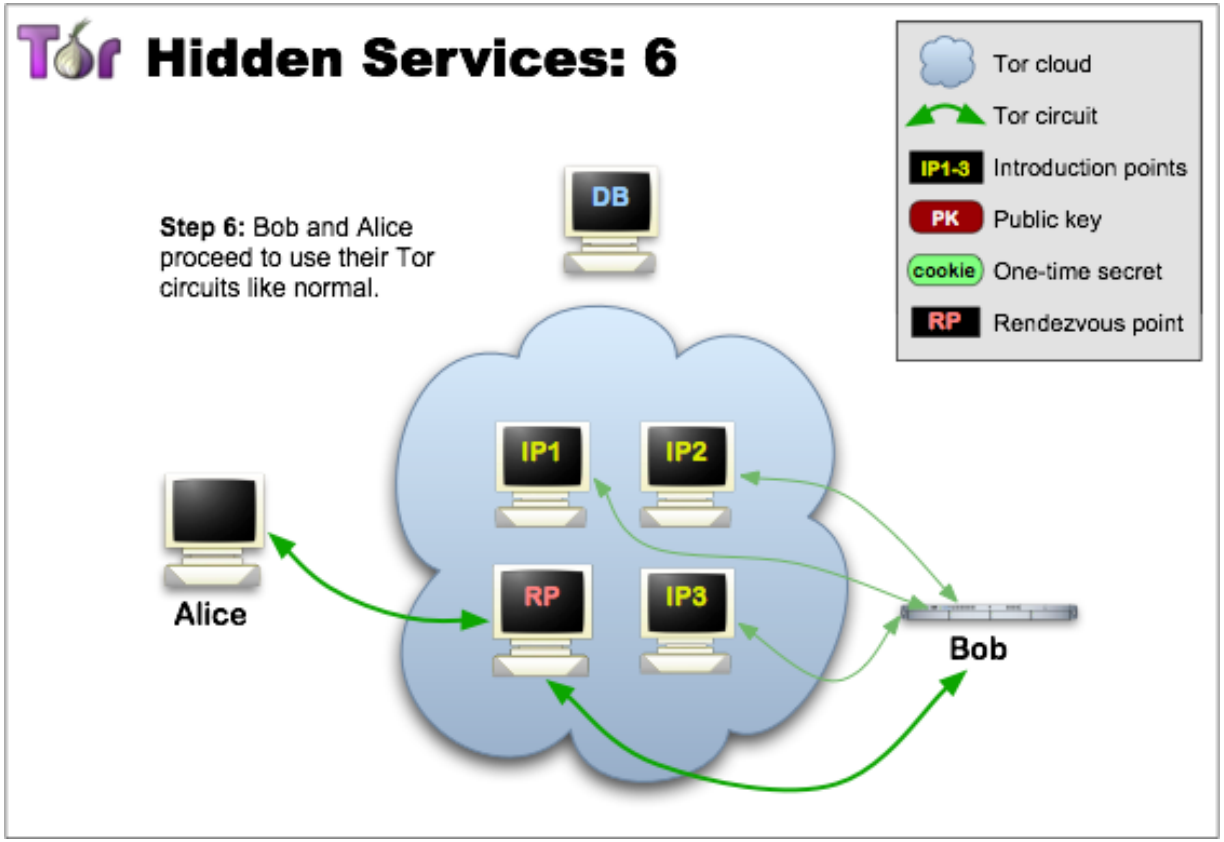
Tor Hidden Services?

A Tor Hidden Services (HS) is a technology that provides:

- Anonymity for servers
- End-to-end encryption

- It employs an URL like naming in order to provide addressing. e.g., http://eqt5g4fuenphqinx.onion

Tor HS



Details can be found at:
https://www.torproject.org/docs/hidden-services.html.en

Why use Tor Hidden Services?

- Avoid retaliation for what you publish
- Securely serve content
- Stealth Hidden Services

  To even prove the existence of the HS a client must share a secret with it

Limits to Tor HS contents usability

A software is needed to access the Tor darknet:

- A Browser configured to use Tor as Socks Proxy
- Minor simplification: TBB, an all-in-one bundle.

A user can't know of the presence of an HS in the darknet if nobody talks him about it:

- Ok this is a Tor design choice,
- … but what if we allow anonymous contents to be indexed by **Google**?!

What is Tor2web? (1/3)

- An other interesting idea of the Aaron Swartz

http://www.aaronsw.com/weblog/tor2web

What is Tor2web? (2/3)

A proxy that exploits a trade-off between security and anonymity in order to achieve usability

- The idea is to connect Tor Hidden Services with the surface Web
- With Tor2web, an Hidden Service could disclose its contents impacting the Internet

What is Tor2web? (3/3)

Instead of contacting http://eqt5g4fuenphqinx.onion directly, the user asks Tor2web to get the content by using https://eqt5g4fuenphqinx.tor2web.org

On behalf of the user, Tor2web asks the resource to the HS by using Tor (Tor is installed only on Tor2web node).

→ users access HS resources using a common Browser.

Tor2web 1.0 Issues (1/2)

Minor issues: **Performance**

- Tor has already it's own big latency.

- t2w 1.0 was a simply Proxy based on Apache + Mod Proxy.
- It lacked of any network optimization.

Tor2web 1.0 Issues (2/2)

Main Issue: **Legal Responsibility**

No disclaimer and no reporting system
→ Misuse of HS to spread of illicit content
→ Exposed to abuse complaints
→ The leads to **server takedown**

Tor2web 1.0 Bodycount

- 2010: three nodes compose Tor2web network
- April 2011: only one server left
- June 2011: no nodes alive :(

Fighting performance issues... (1/2)

Tor2web Mode:

A Tor2web node is public by design so it does not need anonymity while contacting HS!

=> The rendez-vous point can be at 1 hop from the Tor2web node without impacting on the HS threat model

=> a special patch is included in Tor since 0.2.3.9-alpha

Fighting performance issues... (2/2)

A certain number of network optimizations:

- Persistent socks connections
- From store & forward to streaming proxy
- Use of compression when possible

future optimizations are discussed here:

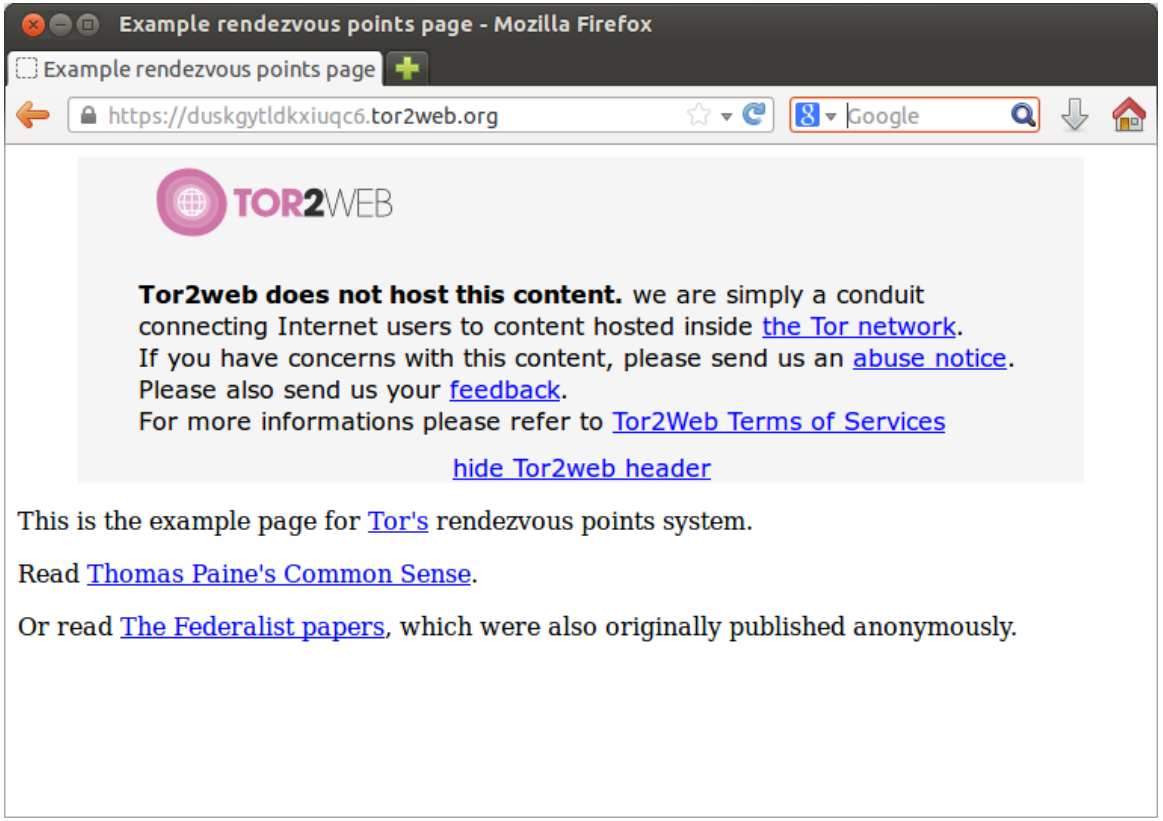
https://github.com/globaleaks/Tor2web-3.0/issues?state=open

Fighting legal issues...

- A complaints mailing list has been created.
- A banner is injected to HTML contents and permits complaints notifications.
- A robots.txt is injected to avoid Crawlers Indexing the HS (temporary solution for Child Pornography)
- A blocklist system is in force and allows node administrators to filter out specific HSs or some of their contents.

Fighting legal issues...

Tor2web Today:



The Tor2web 3.0 Network

6 Servers, 4 Domains

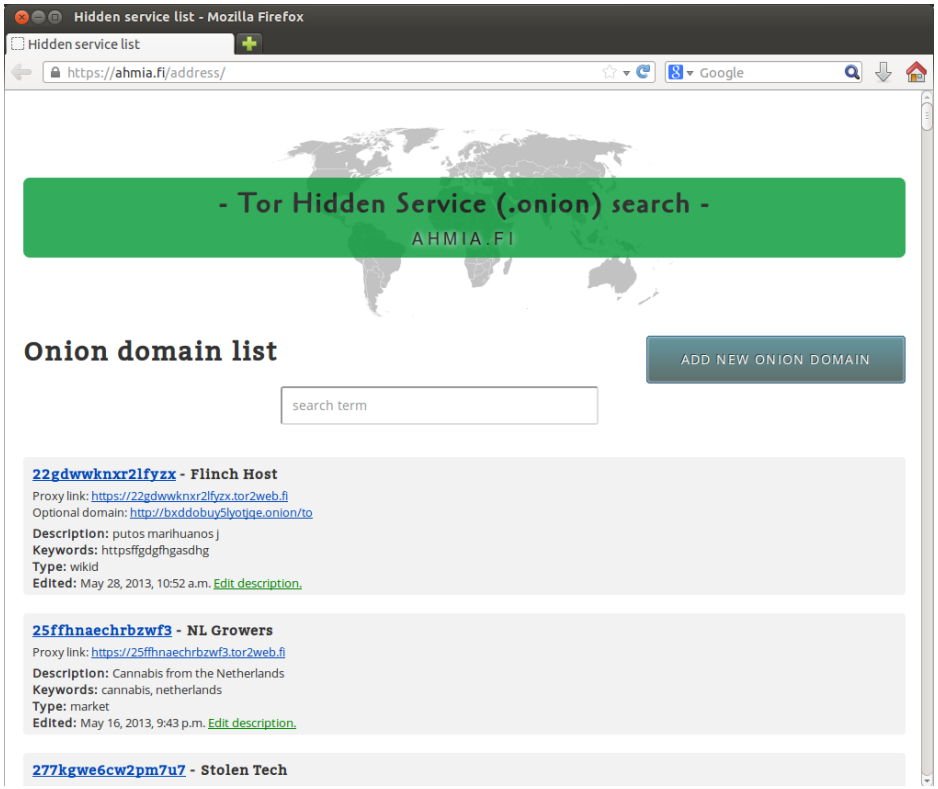
*.tor2web.org
*.tor2web.fi ← managed by Ahmia
*.tor2web.blutmagie.de ← managed by O.Selke with no block
*.onion.sh ← managed by my unknown friend: “hey anon!”

All instances indipendently managed.

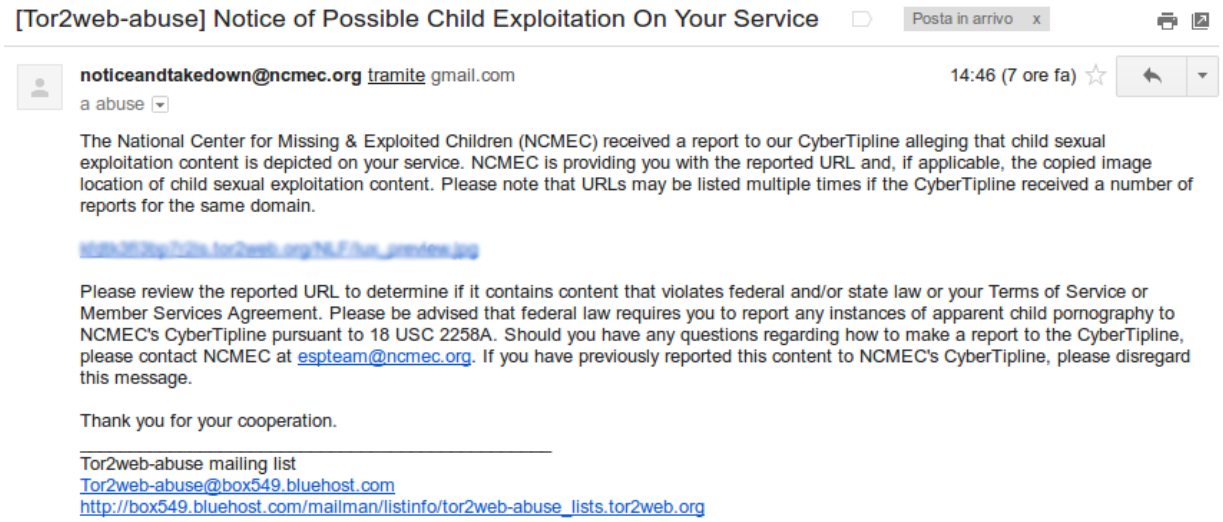
Network actually handled only in terms of alternatives suggestions.

The Tor2web 3.0 Network

Ahmia.fi Onion Search Engine



Recent Complaints, Different Visions.



[Tor2web-abuse] Notice of Possible Child Exploitation On Your Service

Posta in arrivo x

noticeandtakedown@ncmec.org tramite gmail.com 14:46 (7 ore fa)

a abuse

The National Center for Missing & Exploited Children (NCMEC) received a report to our CyberTipline alleging that child sexual exploitation content is depicted on your service. NCMEC is providing you with the reported URL and, if applicable, the copied image location of child sexual exploitation content. Please note that URLs may be listed multiple times if the CyberTipline received a number of reports for the same domain.

[redacted]

Please review the reported URL to determine if it contains content that violates federal and/or state law or your Terms of Service or Member Services Agreement. Please be advised that federal law requires you to report any instances of apparent child pornography to NCMEC's CyberTipline pursuant to 18 USC 2258A. Should you have any questions regarding how to make a report to the CyberTipline, please contact NCMEC at espteam@ncmec.org. If you have previously reported this content to NCMEC's CyberTipline, please disregard this message.

Thank you for your cooperation.

Tor2web-abuse mailing list
Tor2web-abuse@box549.bluehost.com
http://box549.bluehost.com/mailman/listinfo/tor2web-abuse_lists.tor2web.org

A lot of complaints are always coming and manual filtering is needed so that it continue to be dangerous to host a Tor2web node.

It's a common idea that Tor2web shouldn't apply any censorship (but currently it's needed ...)

Recent Complaints, Different Visions.

http://tor2web.org/legal

One of the protections we actually declare is 17 USC 512 a part of the Digital Millennium Copyright Act (DMCA).

For these protections to apply, we must satisfy the conditions in 17 USC 512(a) but ...

- (2) the transmission, routing, provision of connections, or storage is carried out through an automatic technical process without selection of the material by the service provider;
- (5) the material is transmitted through the system or network without modification of its content.

Legal Help Needed

"Legal Proof "Terms of Services are lacking.

→ Any lawyers willing to help?

Mailing List: tor2web-talk@lists.tor2web.org

http://box549.bluehost.com/mailman/listinfo/tor2web-talk_lists.tor2web.org

Thanks for the attention.

Questions?

giovanni.pellerano@logioshermes.org