Analisi delle tecniche di censura della piattaforma TOR

Giovanni Cerrato

E-privacy 2017

Lucca, 24 Giugno

BACKBOXLINUX

Gartner Cool Vendor 2016

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

Whoami

- Professionista nel campo della sicurezza informatica: vulnerability assessment, penetration test, malware analysis
- Senior Cyber Security Specialist
- Collaboratore Owasp Italy
- Autore per la rivista

giovanni.cerrato@aizoon.it

giovcerrato

Agenda

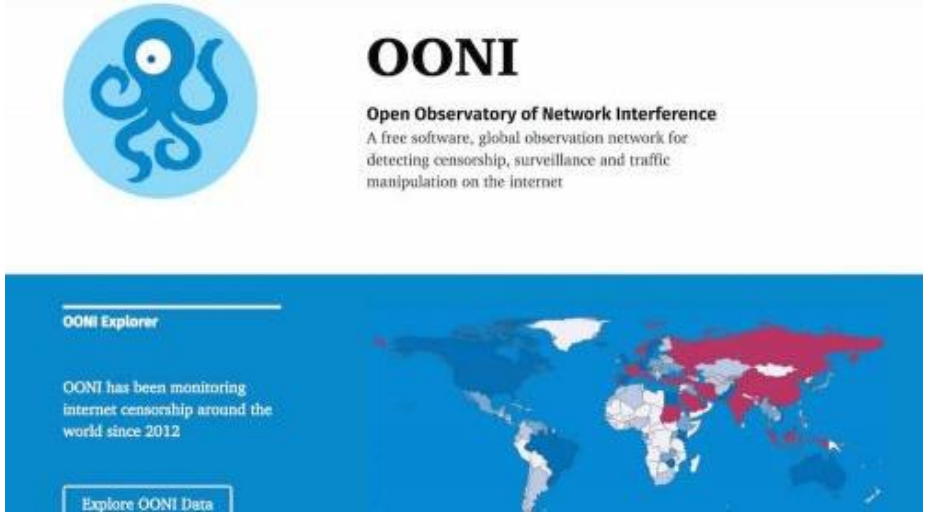
- Censura su Internet
- Tor
- Tor censorship
- Tecniche di evasione della censura

La censura su Internet

Per “censura su Internet" si intende il controllo o il blocco della pubblicazione di contenuti o dell'accesso ad essi nella rete Internet

- **Trigger:**
  - Hostname
  - IP address
  - Port number
  - Protocollo utilizzato
  - URL/keyword(s)
- **Esecuzione**
  - DNS redirection
  - Reset della connessione tra gli host
  - Modifica della richiesta (time out connessioni)
  - Alterazione della response: (eliminazione/aggiunta contenuti)
- **Posizione del modulo di censura**
  - Dns
  - Router
  - (Client)
  - (Server)

Osservatori sulla censura



OpenNet Initiative

HERDICT
HELP SPOT WEB BLOCKAGES

Università degli Studi di Napoli Federico II

Tor

- Scopo: Garantire anonimato e privacy in Internet
- Come lo fa: nascondendo l'indirizzo IP del fruitore
- Realizzazione pratica: traffico generato da un utente viene instradato in modo casuale attraverso più nodi della rete Tor
- La destinazione finale vedrà pervenire la richiesta da un nodo della rete Tor, e le sarà impossibile risalire all'origine

Tor Censorship

NEWS

Turkey Doubles Down on Censorship With Block on VPNs, Tor

LORENZO FRANCESCHI-BICCHIERAI
Nov 4 2016, 10:20pm

Turkey blocks access to Tor anonymising network

19 December 2016 | Technology

Share

People use Tor to browse the internet and communicate in private

Tor Censorship

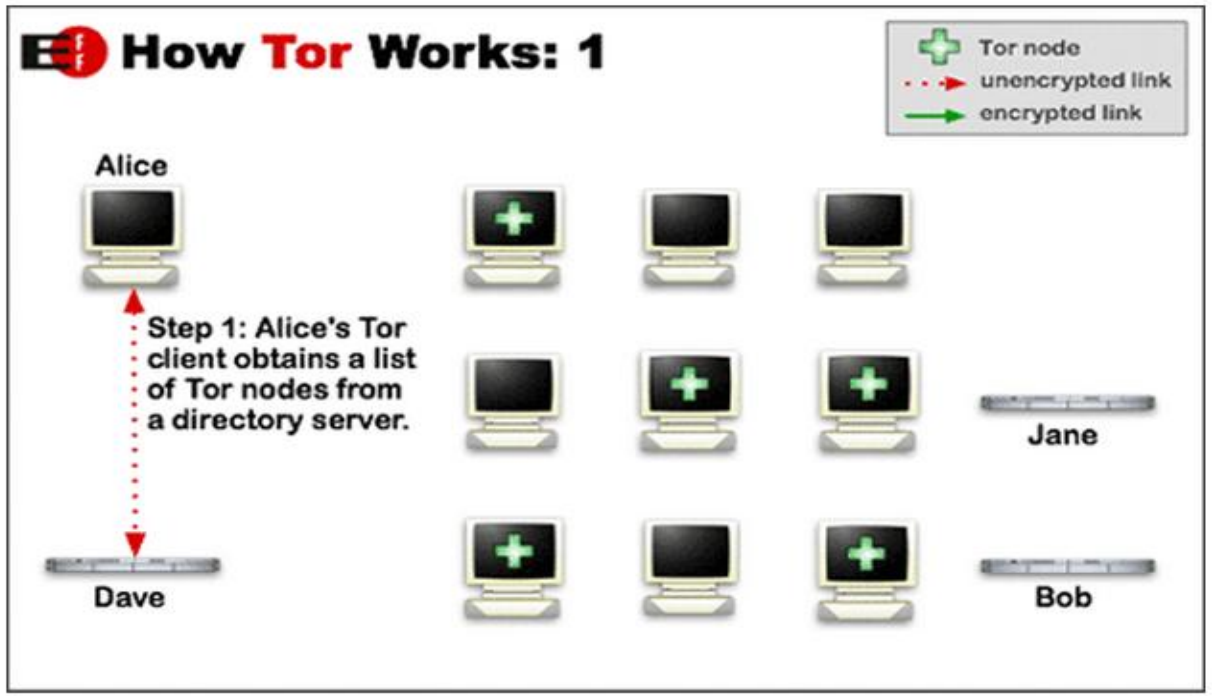
#EgyptCensors: Evidence of recent censorship events in Egypt

Maria Xynou (OONI), Vasilis Ververis (OONI), Arturo Filastò (OONI), Wafa Ben Hassine (Access Now), 2017-06-19 15:30:00 +0000 UTC

Websites	Link Egypt (AS24863)	Vodafone Egypt (AS36935)	TE (AS8452)
http://www.torproject.org	BLOCKED	BLOCKED	Unclear
https://www.torproject.org	BLOCKED	Unknown (N/A)	Unclear
http://bridges.torproject.org	BLOCKED	BLOCKED	ACCESSIBLE
https://bridges.torproject.org	BLOCKED	Unknown (N/A)	ACCESSIBLE
http://ooni.torproject.org	BLOCKED	BLOCKED	ACCESSIBLE
https://ooni.torproject.org	BLOCKED	Unknown (N/A)	Unknown (N/A)

Tor primo step

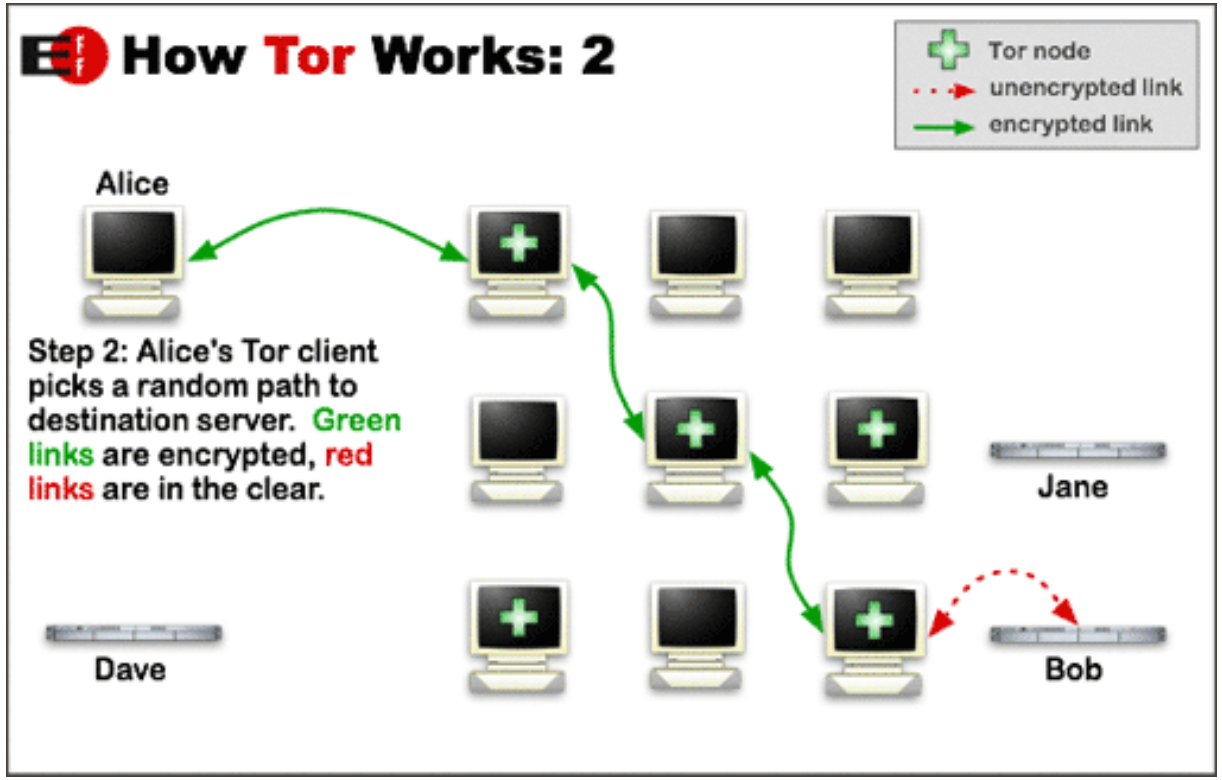
- Ottenere la lista dei nodi della rete con cui poter stabilire un circuito casuale contattando le directory authorities



Tratta da : https://www.torproject.org/about/overview

Tor secondo step

- Stabilire un percorso tra l'origine e la destinazione



Tratta da : https://www.torproject.org/about/overview

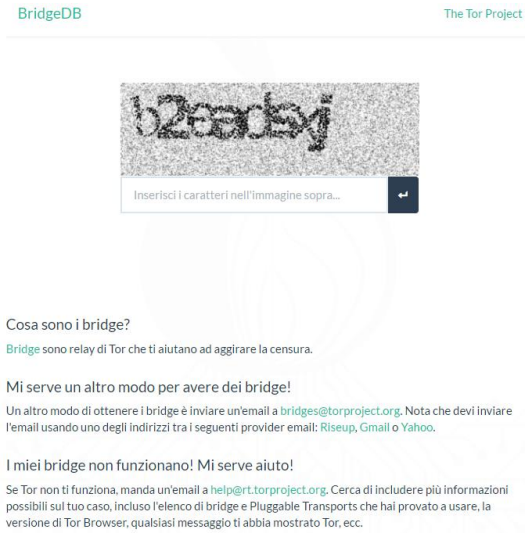
Tool ed esecuzione test

- Ispirato a :Philipp Winter, "Design Requirements for a Tor Censorship Analysis Tool ",Tor Tech Report
- Eseguito su nodi PlanetLab: un'architettura di nodi distribuiti in tutto il mondo che permettono l'esecuzione di test in scenari reali

https://www.planet-lab.org

Test di reperibilità del software e dei bridges

- Pagina indice?
- Accesso ai mirror?
- Connessione TCP?
- Connessione TLS?
- DNS fornisce risultati corretti?
- Gli host rispondono al ping?



- Test replicati per l'indirizzo relativo ai bridges (meccanismi di evasione)

DNS filtering and redirection

- Indirizzi forniti dal DNS sono corretti?
- Due nodi fornivano la stessa risoluzione DNS sia per bridges.torproject.org che per www.torproject.org

```
www.torproject.org. 261 IN A 154.35.132.70
www.torproject.org. 261 IN A 38.229.72.16
www.torproject.org. 261 IN A 138.201.14.197
www.torproject.org. 261 IN A 89.45.235.21
www.torproject.org. 261 IN A 82.195.75.101
```

```
bridges.torproject.org. 366 IN A 78.47.38.229
```

Test di raggiungibilità degli host

```
giovanni@Y:~$ ping -c2  www.torproject.org
PING www.torproject.org (38.229.72.16) 56(84) bytes of data.
64 bytes from aroides.torproject.org (38.229.72.16): icmp_seq=1 ttl=49 time=124 ms
64 bytes from aroides.torproject.org (38.229.72.16): icmp_seq=2 ttl=49 time=127 ms

--- www.torproject.org ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 124.865/126.015/127.165/1.150 ms
giovanni@Y:~$ ping -c2  www.torproject.org
PING www.torproject.org (154.35.132.70) 56(84) bytes of data.
64 bytes from archeotrichon.torproject.org (154.35.132.70): icmp_seq=1 ttl=48 time=122 ms
64 bytes from archeotrichon.torproject.org (154.35.132.70): icmp_seq=2 ttl=48 time=123 ms

--- www.torproject.org ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1002ms
rtt min/avg/max/mdev = 122.670/123.085/123.500/0.415 ms
```

- Connessione TCP?
- Connessione TLS?

```
giovanni@Y:~$ ping -c2 bridges.torproject.org
PING bridges.torproject.org (78.47.38.229) 56(84) bytes of data.
64 bytes from polyanthum.torproject.org (78.47.38.229): icmp_seq=1 ttl=49 time=23.7 ms
64 bytes from polyanthum.torproject.org (78.47.38.229): icmp_seq=2 ttl=49 time=21.6 ms

--- bridges.torproject.org ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 21.648/22.677/23.706/1.029 ms
```

Censura Directory Authorities

- Utilizzate nella fase di avvio
- "Cablate" nel software
- E' possibile scaricare il consenso(lista firmata di tutti i nodi della rete)?
  - Gli host rispondono al ping?

- Tutte le Directory Authorities censurate
  - No connessione
  - No Ping

Test censura relay della rete Tor

- Selezionato sottoinsieme di 851 classificati come:
  - Stabili, Veloci, Aggiornati
- Esclusi exit node
- Esclusi nodi non affidabili o ibernati
- Escluse le Directory Authorities

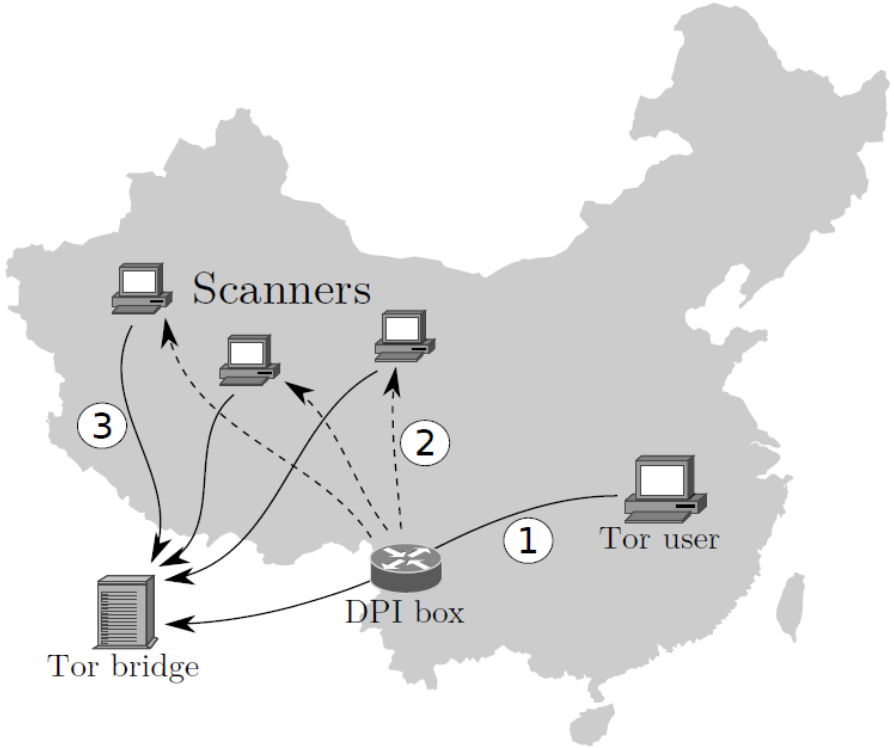
- Con quanti relay della rete Tor è possibile instaurare una connessione TCP?
  - In caso di blocco, a quante fonti informative sull'evasione del blocco riesco ad accedere?

Censura relay: risultati

- Mediamente solo con 50 relay su 851 andava a buon fine una connessione TCP
- Caso eclatante: 5 relay su 851

Censura Bridge

- How China is Blocking Tor
- Localizzare un bridge analizzando il traffico di rete?
- Pattern riconducibile ad una connessione Tor
- Scanner cercano di negoziare una connessione TOR col nodo destinazione del flusso
- Censura dei flussi diretti verso il nodo




```
c0 0a c0 14 00 39 00 38 c0 0f c0 05 00 35 c0 07
c0 09 c0 11 c0 13 00 33 00 32 c0 0c c0 0e c0 02
c0 04 00 04 00 05 00 2f c0 08 c0 12 00 16 00 13
c0 0d c0 03 fe ff 00 0a 00 ff
```

Listing 1.1. Tor cipher list inside TLS client hello.

Evasione censura

- Lotta continua tra censori e tecniche di evasione della censura

- Obfs4
- Meek: Tunnel HTTP
- SkypeMorph: Tunnel Skype Video
- Format-Transforming Encryption (FTE)
- ScrambleSuit

Conclusioni

- I regimi dittatoriali adoperano meccanismi di censura
- Iniziative per monitorare il grado di censura
- Meccanismi di censura della rete Tor
- Continua lotta tra censori e tecniche per l'evasione delle restrizioni

Riferimenti

- https://ooni.torproject.org/post/egypt-censors/
- https://afteegypt.org/right_to_know-2/publicationsright_to_know-right_to_know-2/2017/06/04/13069-afteegypt.html?lang=en
- https://ooni.torproject.org
- https://www.herdict.org
- https://opennet.net
- http://traffic.comics.unina.it/internetcensor.php
- https://www.torproject.org
- https://research.torproject.org/techreports/censorship-analysis-tool-2013-02-06.pdf
- https://www.cs.kau.se/philwint/static/gfc
- https://www.torproject.org/docs/pluggable-transports.html.en

aizoon® AUSTRALIA EUROPE USA
TECHNOLOGY CONSULTING

AUSTRALIA
Sydney NSW

EUROPE
Torino ITA | Cuneo ITA | Milano ITA | Genova ITA
Bologna ITA | Roma ITA | Bari ITA | Sheffield UK

USA
New York NY | Troy MI
Cambridge MA | Lewiston ME

www.aizoongroup.com
aizoon@aizoongroup.com
aizoon Technology Consulting
@aizoongroup