Dissecting Tor Bridges: a Security Evaluation of Their Private and Public Infrastructures

Srdjan Matic, Carmela Troncoso, Juan Caballero
Internet Censorship
Onion Routing

Vanilla Tor Protocol

Relay

Relay

Relay

Relay

101.182.129.111

http://facebook.com
Tor Bridges

- IP not available in consensus
- First hop
- Pluggable transports (PTs)
- Public or private
- Default bridges
Our Goals

- Perform first systematic study of the security of the Tor bridge infrastructure
  - Public bridges
  - Private bridges
  - Private proxies
Known Tor Issues

Two issues known to Tor project since October 2010

1. Vanilla Tor Certificates
   – Vanilla Tor uses TLS handshake
   – Easy to spot certificates
   – It won’t be fixed

2. Open OR Port
   – Bridges have open OR Port with Vanilla Tor
   – Even if they do not offer Vanilla Tor
   – Difficult to fix
Intro

Approach

Public Bridge Analysis

Private Bridge Analysis
Datasets

**SHODAN**
- Scan 200+ ports with multiple protocols
- 19 ports scanned with TLS
- Indexed data available

**Censys**
- Scan 6 ports with TLS
- Raw + indexed data available

**CollectTor**
- Node-level data on public bridges + relays
- Some bridge data sanitized

**Is there sensitive data not anonymized?**
Discovering Bridges

1. Finding candidate IP addresses
2. Filtering relays
3. Verifying IP addresses
4. Identifying private proxies
5. Classifying as public or private bridge
Outline

Intro

Approach

Public Bridge Analysis

Private Bridge Analysis
April 2016:
- 5.3K active public bridges
- 2.3K bridges with clients

Different population metrics!
Bridge Stability

Current censor block policies that remove blocks every 25 hours are **very polite!!!**
PT Deployment

April 2016

- 77.1% vanilla
- 6.5% obf3+obf4+ssuit
- 6.3% obf3+fle+obf4+ssuit
- 4.4% obf3+fle+obf4+ssuit
- 3% obf3+obf4
- 1.6% obf3+ssuit
- 1.4% obf4
- 1.2% OTHER

Conflicting security properties!
Top-3 OR ports are used by 71% of public bridges.

Scanning on those ports reveals majority of bridges!
Bridge Ranking

Not all bridges are equally important

How well is country-level blocking working?
How well is blocking of specific PT working?
Which bridges should censor target next?

<table>
<thead>
<tr>
<th>CC</th>
<th>Used Brid.</th>
<th>Top 20 (Default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>cn</td>
<td>712</td>
<td>45.6% (44.0%)</td>
</tr>
<tr>
<td>ir</td>
<td>941</td>
<td>86.6% (86.1%)</td>
</tr>
<tr>
<td>sy</td>
<td>74</td>
<td>76.9% (68.0%)</td>
</tr>
<tr>
<td>uk</td>
<td>943</td>
<td>84.1% (84.0%)</td>
</tr>
<tr>
<td>us</td>
<td>1,496</td>
<td>58.7% (56.7%)</td>
</tr>
<tr>
<td>All</td>
<td>2,213</td>
<td>91.71% (91.4%)</td>
</tr>
</tbody>
</table>

91% traffic used default bridges!
Censor can disconnect users in reaction to an event
Outline

Intro

Approach

Public Bridge Analysis

Private Bridge Analysis
### Bridge Discovery (April 2016)

- Deanonymized 35% public bridges with clients
- Found 684 private bridges
- Found 645 private proxies
- 35% bridges private, 65% public

<table>
<thead>
<tr>
<th>Port</th>
<th>SC</th>
<th>Source</th>
<th>Disc.</th>
<th>Verified</th>
<th>Public</th>
<th>Private</th>
<th>Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>443</td>
<td>9</td>
<td>Censys</td>
<td>2,448</td>
<td>1,315 (1,122)</td>
<td>897 (860)</td>
<td>263 (262)</td>
<td>164</td>
</tr>
<tr>
<td>993</td>
<td>2</td>
<td>Censys</td>
<td>19</td>
<td>16 (13)</td>
<td>11 (11)</td>
<td>3 (2)</td>
<td>2</td>
</tr>
<tr>
<td>995</td>
<td>3</td>
<td>Censys</td>
<td>14</td>
<td>14 (13)</td>
<td>10 (10)</td>
<td>3 (3)</td>
<td>1</td>
</tr>
<tr>
<td>444</td>
<td>1</td>
<td>Shodan</td>
<td>14</td>
<td>12 (101)</td>
<td>8 (97)</td>
<td>1 (4)</td>
<td>4</td>
</tr>
<tr>
<td>8443</td>
<td>1</td>
<td>Shodan</td>
<td>191</td>
<td>156 (149)</td>
<td>148 (148)</td>
<td>1 (1)</td>
<td>7</td>
</tr>
<tr>
<td>9001</td>
<td>1</td>
<td>Shodan</td>
<td>2,001</td>
<td>1047 (587)</td>
<td>165 (166)</td>
<td>415 (421)</td>
<td>468</td>
</tr>
<tr>
<td>9002</td>
<td>1</td>
<td>Shodan</td>
<td>23</td>
<td>19 (5)</td>
<td>1 (1)</td>
<td>4 (4)</td>
<td>14</td>
</tr>
<tr>
<td>All</td>
<td>17</td>
<td>All</td>
<td>4,684</td>
<td>2,554 (1,986)</td>
<td>1,239 (1,292)</td>
<td>684 (694)</td>
<td>645</td>
</tr>
</tbody>
</table>
Bridge Cluster Types

1,343 clusters, 75% singletons

77% Proxies and Backend in same AS
Proxies do not provide IP diversity
Conclusion

- **Public Bridges**
  - Bridges with clients live 4 months, no IP changes → Blocking
  - PTs with conflicting security properties
  - Top-3 OR ports 71% public bridges → Patch CollecTor
  - 91% bridge traffic uses default bridges → Defeats purpose
  - Bridge Ranking enables targeted attacks

- **Bridge discovery**
  - Deanonymized 35% of public bridges
  - Found 684 private bridges + 645 private proxies
  - 35% bridges are private
  - Clusters of bridges+proxies deployed → Little IP diversity

- **Open OR Port needs fixing**
Public Bridges Analysis

(1) Bridge Population
(2) Bridge Stability
(3) PT Deployment

(4) OR Port Distribution
(5) Bridge Ranking
(6) CollecTor Security Analysis
Private Bridge & Proxy Analysis

(1) Population

We first need to discover private bridges!

(2) Clusters

Cluster Types
Private Proxies

(3) Hosting

IP diversity
AS diversity
Bridge Clustering & Ranking

• Cluster bridges from same owners
  1. Same fingerprint
  2. Similar nicknames
  3. Same contact information
  4. Similar verified IP address
  5. Similar IP address in descriptor

• Rank Bridges
  – Not all bridges equally important
Related Work

• Design secure Pluggable Transports
  – Obfs4, Skypemorph, BridgeSPA, StegoTorus, ScrambleSuit

• Techniques to discover bridge IP
  – Ling et al., McLachlan and Hopper, Zmap
Ethical Considerations

- Approved by IMDEA’s ethics review board
- Disclosed to Tor project at submission
- We only use leaks/info from public datasets
- No access to any user traffic
- No malicious Tor nodes added
- No deanonymized bridges revealed
- No data release
Internet Censorship

The Great (Fire)Wall of China

YouTube, Twitter, Yahoo, Facebook

Tor, I2P, OpenVPN, SuperVPN, PureVPN, SocksProxy
fingerprint

= SHA1( )