Safety of the Tor network

A look at network diversity, relay operators, and malicious relays
Runa A. Sandvik

- Developer for the Tor Project
- Worked with/for Tor since GSoC 2009
- Frequent traveler
What this talk is about

• Is the Tor network a CIA honeypot?
• Are all relays malicious?
• Looked at all consensus files created between late 2007 and mid 2013
r OnionSoup CNImeTd8nvcBGTwfGZ2bCz8a7jw 6i1X8TC+YxGItibB352JRwVHEu8 2012-09-17 22:00:03 87.195.253.3 9001 9030
s Exit Fast Guard HSDir Named Running V2Dir Valid
v Tor 0.2.3.20-rc
w Bandwidth=5800
p accept 80,110,143,443,993,995
r OnionSoup CNImeTd8nvcBGTwfGZ2bCz8a7jw 6i1X8TC+YxGiTibB352JrwVHEu8 2012-09-17 22:00:03 87.195.253.3 9001 9030
s Exit Fast Guard HSDir Named Running V2Dir Valid
v Tor 0.2.3.20-rc
w Bandwidth=5800
p accept 80,110,143,443,993,995
r OnionSoup CNImeTd8nvcBGTwfGZ2bCz8a7jw 6i1X8TC+YxGIiTibB352JRwVHEu8 2012-09-17 22:00:03 87.195.253.3 9001 9030
s Exit Fast Guard HSDir Named Running V2Dir Valid
v Tor 0.2.3.20-rc
w Bandwidth=5800
p accept 80,110,143,443,993,995
r OnionSoup CNImeTd8nvcBGTwfGZ2bCz8a7jw 6i1X8TC+YxGtibB352JRwVHEu8 2012-09-17 22:00:03 87.195.253.3 9001 9030
s Exit Fast Guard HSDir Named Running V2Dir Valid
v Tor 0.2.3.20-rc
w Bandwidth=5800
p accept 80,110,143,443,993,995
Number of relays in all countries

The Tor Project – https://metrics.torproject.org/
High-level statistics

• 95,314 unique nicknames
• 1,595,879 unique IP address
• 230,595 unique fingerprints
• 195 different countries
Top countries

- The US
- Germany
- France
- Russia
- Netherlands
- United Kingdom
Top nicknames

- Popular nicknames: Unnamed, default, ididnteditheconfig, idideditheconfig, MgeniUser, anonymous

- anonymous (Germany, Sweden, US, Ukraine) versus Anonymous (US, Germany, Ukraine, Japan)

- A lot of Orbot relays in the Middle East
What is average?

- Uptime
- Lifetime
- Bandwidth
- Utilization
So it’s all good?

- China
- Russia
- Eastern European botnet
Network diversity

- Different relays owned by different people in different data centers in different parts of the world
Number of relays with relay flags assigned

The Tor Project – https://metrics.torproject.org/
Malicious relays

- SSL MITM
- sslstrip
- Plaintext only exit policy
- Anti-virus filter blocking sites
- Dropping TLS connections for multiple sites
Snakes on a Tor (SoaT)

- Scans the Tor network for misbehaving and misconfigured exit relays
- Several tests, including HTML, javascript, arbitrary HTTP, SSL, DNS scans
- A number of relays banned since 2010, but SoaT is currently not maintained
How to ban a relay

- *BadExit* flag set by directory authorities
- 36,356 unique IP addresses, tied to 264 unique nicknames, with the *BadExit* flag
Where do we go from here?