

Blocking Resistance in Tor

Presented by Justin Samuel

Compiled from:

“Design of a blocking-resistant anonymity system”
Roger Dingledine and Nick Mathewson

“Tor and circumvention: Lessons learned”
Roger Dingledine

Censorship Resistance

- Tor: designed for anonymity.
- **Additional usage: censorship resistance.**
 - China
 - Iran
 - Many others

Censorship Threat Model

- Governments
- Complete blocking not a goal
 - Necessary to have a working Internet
- Reprisal *mostly* targeted at producers of restricted information, not consumers

Censor's Technical Approach

- Currently:
 - Block by string matches in TCP
 - Block destination IP address or port
 - Intercept DNS requests
- **Arms race.**
 - Western companies (Nokia, Cisco, Siemens, etc.) are selling censorship tools (e.g. DPI) to these countries

Blocking Tor

- Block directory authorities
- **Block all the relay IP addresses in the directory**
- **Filter based on Tor's network fingerprint**
- Prevent users from finding the Tor software

Blocking-resistance in Tor

- Planning started years before blocking
 - In some cases, Tor's website blocked but not Tor
- High-level solution:
 - More relay addresses
 - Better ways to distribute them
 - Make Tor traffic look “normal”

Bridge Relays

- Leverage large, sympathetic user base
- **Allow Tor clients to be relays into the Tor network**
 - Called “bridges”
- Bridges advertise themselves to a bridge directory authority
 - Different from standard directory authority

Finding a First Bridge

- Remember:
 - Different users have different ways of initially bypassing filters
 - Users know other people (social graphs)
- **Types of bridges:**
 - **Independent** (no central discovery)
 - **Public bridges** (central discovery)

Public Bridge Distribution Strategies

- **Divide bridges into pools**, each pool with a different distribution strategy
 - Time-release
 - IP address of requesting user
 - **Time-release + IP address of requesting user**
 - Mailing list
 - **Email auto response**
- Arms race

Other Bridge Issues

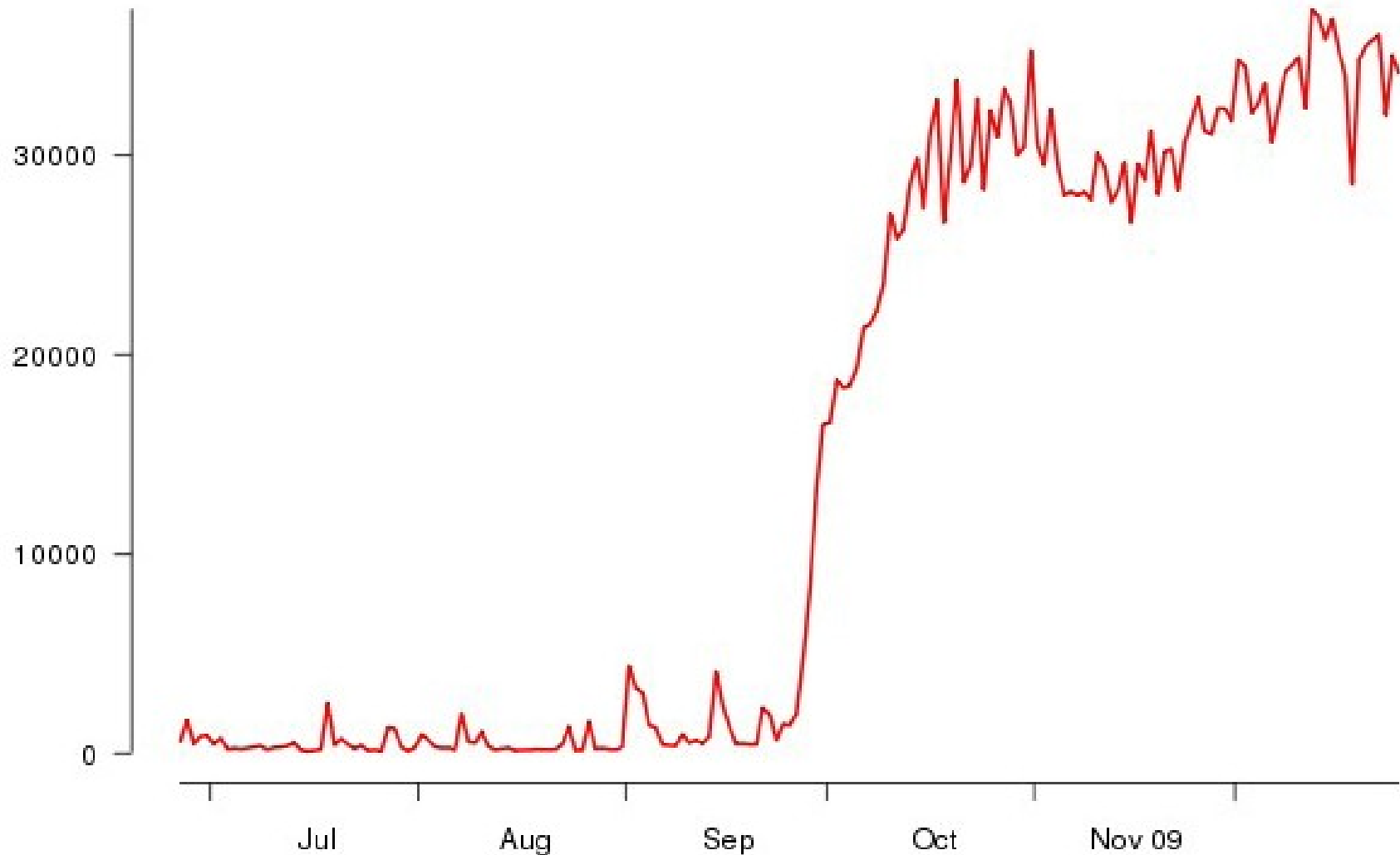
- Is a bridge blocked?
- Is a bridge real?
- Anonymity impact of running a bridge?
- Scanning resistance
- Cable/DSL IP addresses don't usually run websites

Hiding Tor's Network Fingerprint

- Avoid plaintext HTTP connection to directory caches.
 - Now obtained over same TLS connection.
- Made Tor's TLS handshake look like Firefox + Apache
- Arms race

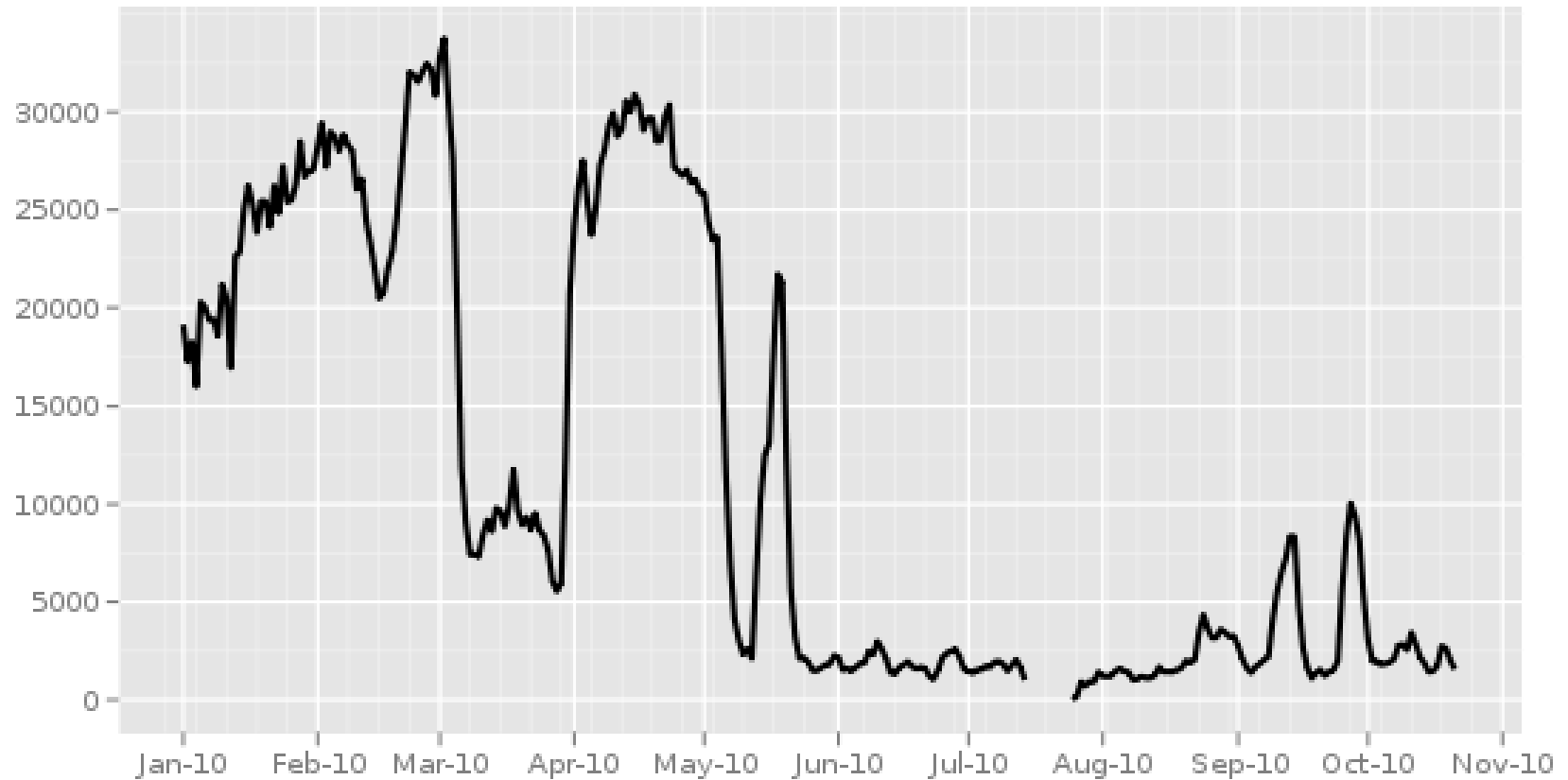
July-December 2009

Chinese Tor users via bridges



2010

Chinese users via bridges



The Tor Project - <https://metrics.torproject.org/>

May 2010

- <https://blog.torproject.org/blog/may-2010-progress-report>
 - On May 4, China's Great Firewall began blocking connections to the public Tor relays. They also updated their blocking to include bridge relays published via email and https websites. Further research into the blocking mechanisms from inside China show they are simply blocking IP Address and TCP port combinations. Bridge relays that have been seeded into various social networks in China continue to work well.

August 2010

- <https://blog.torproject.org/blog/august-2010-progress-report>
 - Continuing research into China's Great Firewall shows **bridges are surviving for 1-2 weeks before being blocked**. We're working to improve the bridge database such that it only gives out bridges that work in a requested country. Right now, we hand out a random selection of 3 bridges regardless of potential country of usage. In China, bridges and relays are still blocked by IP address and TCP port combinations.

September 2010

- <https://blog.torproject.org/blog/september-2010-progress-report>
 - **Steven submitted a proposal to automatically promote nodes to bridges.** This proposal describes how Tor clients could determine when they have sufficient bandwidth capacity and are sufficiently reliable to become either bridges or Tor relays. When they meet this criteria, they will automatically promote themselves, based on user preferences.

References

- “Tor and circumvention: Lessons learned”
 - <https://blog.torproject.org/blog/tor-and-censorship-lessons-learned>
- “Design of a blocking-resistant anonymity system.”
 - Tor Project technical report, Nov 2006.
 - Roger Dingledine, Nick Mathewson
 - <https://svn.torproject.org/svn/projects/design-paper/blocking.pdf>