The Collateral Damage of Internet Censorship by DNS Injection

Brad Karp
UCL Computer Science

CS 3035/GZ01
11th December 2014
Internet Censorship: Background

- Some nations’ governments block their citizens’ access to Internet content deemed politically sensitive or “indecent”

- Widely known example: Great Firewall of China (GFC)

  - Blocks access to sites such as twitter.com, facebook.com

- Major implementation approach: prevent DNS queries for these domain names from returning correct IP addresses for sites
Today’s Topic:
Collateral Damage in Censorship

The Collateral Damage of Internet Censorship by DNS Injection

- GFC sends forged DNS responses with incorrect IP addresses to queries for domain names it wishes to censor

- Anonymous paper presented at SIGCOMM 2012 offered experimental finding: GFC causes collateral damage to Internet access by users outside China—it often censors content for Internet users outside China
Censorship Mechanism: DNS Injection

- Install injector on ISP’s link that sees all DNS query packets that traverse that link

- Note that DNS queries always contain full domain name queried for, regardless of server to which query addressed

- Injector configured with domain names for which to block correct resolution
  - For these domain names, injector replies to query with incorrect (“lemon”) IP address
  - Injector doesn’t prevent DNS query from reaching real target DNS server; but injector’s reply reaches querier first
DNS Injection
Works at All Query Stages

- Queries to root, TLD server, authoritative server all liable to injection if Internet path incorporates DNS injector
Questions

• How does collateral damage occur?

• Which ISPs practice DNS injection?

• Which domain names and resolvers (resolver locations) are affected by collateral damage?
Causes of Collateral Damage

• Iterative queries create multiple opportunities for collateral damage:
  • Caching name server to root DNS server
  • Caching name server to TLD DNS server
  • Caching name server to authoritative DNS server

• Censored transit: DNS injector may target all DNS queries on link; caching name server’s route to target server may transit censored AS!

• Redundant, anycasted DNS servers
  • 13 anycasted root servers, 13 anycasted global TLD servers
  • Path to any of these 26 IPs may pass through censored network
Experiment:
Finding Paths Affected by Injection

• Randomly select one IP address in each /24 of IP address space; verify doesn’t respond to DNS queries

• Probe the resulting 14 million IP addresses with a DNS query for a likely censored DNS name (e.g., facebook.com, twitter.com, youtube.com, etc.)

• Launch probes from server in AS 40676 in US

• If response received, must be from injector: record domain name as blacklisted; record target IP address as poisoned; remember IP address in response ("lemon IP")
Many Paths Affected by DNS Injection

- 388,988 IP addresses poisoned in 16 regions (CN, CA, US, HK, IN, AP, KR, JP, TW, DE, PK, AU, SG, ZA, SE, FI)
- 28 distinct IPs in list of lemon IPs
Experiment: Locating Injecting ISPs

• Generate DNS query for blacklisted name sent to known poisoned target IP

• Send queries with successively increasing IP header TTL field values
  • Observe IP addresses in “ICMP time exceeded” replies to learn locations of routers on path
  • Observe DNS replies—they are from injectors

• Result: learn ASes where injectors located
Injector Locations

- 3120 router IPs associated with DNS injectors
- All these IPs in 39 ASes in China
- Implication: poisoned IP addresses not in China caused by **DNS queries transiting China** (or by errors in geolocating those IP addresses)
Experiment: Assessing Effect of Injection on Real Resolvers

• Send queries for blacklisted names to 43,842 non-censored open recursive resolvers in 173 countries

• If reply gives a lemon IP address, conclude queries handled by that open resolver censored

• Injectors tend to censor queries in which any part of domain name string is blacklisted

• So can force tests of path from open resolver to root and TLD servers with queries like:
  
  • www.facebook.com.{random string}

  • www.facebook.{random string}.com
Incidence of Collateral Damage Censorship

- DNS queries to root almost never censored; implication: DNS queries to root seldom transit ASes in China

- TLDs suffer substantial collateral damage; among all 312 TLDs:
  - 99.53% of resolvers (43,322) censored for TLDs in China
  - 26.4% of resolvers (11,573) censored for one or more of 16 other TLDs
TLD Servers on Censored Paths from Open Resolvers

![Bar Chart]

- Number of Resolvers
- Top Level Domain

- de
- kr
- kp
- co
- travel
- pl
- no
- it
- uk
- fi
- jp
- zn
- ca

- xn--3e0b707e
- xn-j6w193g
TLD .de in Detail

- Left: number of censored resolvers in various countries when looking up names in .de

- Right: percentage of censored resolvers in various countries when looking up names in .de
Summary

• Evidence of collateral damage of censorship: even when resolver and target nameserver outside censored network, users can be censored

• DNS injectors in 39 ASes located in China

• 26.41% of open recursive resolvers around the world could be affected by collateral censorship damage

• Primary mechanism of collateral damage: paths between resolvers and TLD servers