The Collateral Damage of Internet Censorship by DNS Injection

Anonymous <zion.vlab@gmail.com>

presented by Philip Levis
Basic Summary

- Great Firewall of China injects DNS responses to restrict access to domain names
- This affects traffic originating outside China
  - 26.4% of open resolvers affected
  - .de is the most affected TLD (70% of open resolvers in kr)
- Explain how, where, and why this happens
- Present several possible solutions
This talk assumes that the Great Firewall of China is not designed to restrict Internet access to computers outside of China.

“Collateral damage” means restricting access to computers outside China.
DNS Overview

- root
- top level domain (TLD): .com, .edu, .cn, .de
- domain (authoritative): stanford.edu, baidu.cn
- resolver
- client
- www.stanford.edu?
DNS Overview

- root .
- top level domain (TLD) .com, .edu, .cn, .de
- domain (authoritative) stanford.edu, baidu.cn
- resolver
- client

Internet

www.stanford.edu?
DNS Overview

root.

top level domain (TLD)
.com, .edu, .cn, .de

domain (authoritative)
stanford.edu, baidu.cn

Internet

resolver

client

www.stanford.edu?
DNS Overview

root .

top level domain (TLD) .com, .edu, .cn, .de

domain (authoritative) stanford.edu, baidu.cn

Internet

resolver

client

www.stanford.edu?
DNS Overview

Internet

root
.

resolver

client

top level domain (TLD)
.com, .edu, .cn, .de

domain (authoritative)
stanford.edu, baidu.cn

www.stanford.edu?
DNS Overview

root .

Internet

 resolver

client

www.stanford.edu?

top level domain (TLD)
.com, .edu, .cn, .de

domain (authoritative)
stanford.edu, baidu.cn
DNS Overview

root .

top level domain (TLD)
.com, .edu, .cn, .de

domain (authoritative)
stanford.edu, baidu.cn

Internet

resolver

client

www.stanford.edu?
DNS Overview

- **Root**
  - .

- **Top Level Domain (TLD)**
  - .com, .edu, .cn, .de

- **Domain (Authoritative)**
  - stanford.edu, baidu.cn

- **Internet**

- **Resolver**

- **Client**

**Example**: www.stanford.edu?
DNS Overview

root .

top level domain (TLD) .com, .edu, .cn, .de

domain (authoritative) stanford.edu, baidu.cn

Internet

resolver

client

www.stanford.edu?

171.53.10.4
DNS Injection

DNS server

Censoring AS

resolver

client

www.youtube.com?
DNS Injection

DNS server

DNS injector

Censoring AS

resolver

client

www.youtube.com?
DNS Injection

- DNS server
- DNS injector
- resolver
- client
- Censoring AS
- lemon IP
DNS Injection

DNS server

Censoring AS

DNS injector
Typically affects both inbound and outbound queries

lemon IP

resolver

client
DNS Injection

DNS server

Censoring AS

DNS injector
Typically affects both inbound and outbound queries.

lemon IP
Typically does not suppress “correct” response, just wins race to respond.

 resolver

 client
Methodology

• *HoneyQueries* to detect autonomous systems paths to whom see DNS injection

• *TraceQueries* to identify location of injectors on affected paths

• *StepNXQueries* to measure collateral damage of DNS injection
HoneyQuery

• HoneyQuery: DNS query to sensitive domains, sent to unresponsive IP
  ‣ Assumption: all observed DNS responses are from DNS injectors

• Send from a single vantage point (AS 40676)
  ‣ 14 million IPs that cover all /24 subnets
  ‣ Paths spread to discover all injecting autonomous systems

• Record IPs in responses: lemon IPs
# Probed Domain Names

<table>
<thead>
<tr>
<th>Domain</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>Search Engine</td>
</tr>
<tr>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
<td>Social Network</td>
</tr>
<tr>
<td><a href="http://www.twitter.com">www.twitter.com</a></td>
<td>Social Network</td>
</tr>
<tr>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>Streaming Media</td>
</tr>
<tr>
<td><a href="http://www.yahoo.com">www.yahoo.com</a></td>
<td>Portal</td>
</tr>
<tr>
<td><a href="http://www.appspot.com">www.appspot.com</a></td>
<td>Web Hosting</td>
</tr>
<tr>
<td><a href="http://www.xxx.com">www.xxx.com</a></td>
<td>Pornography</td>
</tr>
<tr>
<td><a href="http://www.urltrends.com">www.urltrends.com</a></td>
<td>Site Ranking</td>
</tr>
<tr>
<td><a href="http://www.live.com">www.live.com</a></td>
<td>Portal</td>
</tr>
<tr>
<td><a href="http://www.wikipedia.com">www.wikipedia.com</a></td>
<td>Reference</td>
</tr>
</tbody>
</table>
## Blacklisted Domains

<table>
<thead>
<tr>
<th>Domain</th>
<th>Category</th>
</tr>
</thead>
<tbody>
<tr>
<td><a href="http://www.google.com">www.google.com</a></td>
<td>Search Engine</td>
</tr>
<tr>
<td><a href="http://www.facebook.com">www.facebook.com</a></td>
<td>Social Network</td>
</tr>
<tr>
<td><a href="http://www.twitter.com">www.twitter.com</a></td>
<td>Social Network</td>
</tr>
<tr>
<td><a href="http://www.youtube.com">www.youtube.com</a></td>
<td>Streaming Media</td>
</tr>
<tr>
<td><a href="http://www.yahoo.com">www.yahoo.com</a></td>
<td>Portal</td>
</tr>
<tr>
<td><a href="http://www.appspot.com">www.appspot.com</a></td>
<td>Web Hosting</td>
</tr>
<tr>
<td><a href="http://www.xxx.com">www.xxx.com</a></td>
<td>Pornography</td>
</tr>
<tr>
<td><a href="http://www.urltrends.com">www.urltrends.com</a></td>
<td>Site Ranking</td>
</tr>
<tr>
<td><a href="http://www.live.com">www.live.com</a></td>
<td>Portal</td>
</tr>
<tr>
<td><a href="http://www.wikipedia.com">www.wikipedia.com</a></td>
<td>Reference</td>
</tr>
</tbody>
</table>
HoneyQuery Results

• 28 lemon IPs found
  ‣ Use later to detect injected responses

• 388,988 (2.7%) of HoneyQueries responded
  ‣ Use to generate poisoned path list

<table>
<thead>
<tr>
<th>Destination</th>
<th>Count</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>CN</td>
<td>388,206</td>
<td>99.80%</td>
</tr>
<tr>
<td>CA</td>
<td>363</td>
<td>0.09%</td>
</tr>
<tr>
<td>US</td>
<td>127</td>
<td>0.03%</td>
</tr>
<tr>
<td>HK</td>
<td>111</td>
<td>0.03%</td>
</tr>
<tr>
<td>IN</td>
<td>94</td>
<td>0.02%</td>
</tr>
</tbody>
</table>

Top 5 of 16 regions

• Why are paths to IP addresses outside of China experiencing DNS injection?
TraceQuery

- For each IP address in the poisoned path list, send a DNS query to a blacklisted domain with increasing TTL
  - Queries which reach an injector will trigger a response
- Mark IP address and autonomous system of router for TTL that triggers response
  - Sometimes queries trigger multiple responses, from multiple injectors
Example

www.facebook.com?
Example

www.facebook.com?
Example

lemon IP
Example

l lemon IP

AS1

AS2

AS3

AS4
Example

lemon IP, lemon IP

AS1

AS2

AS3

AS4
Example

lemon IP, lemon IP,
good IP

AS1

AS2

AS3

AS4
Example

l<red>emon IP, lemon IP, good IP</red>
TraceQuery Results

• Found 3,120 router IP addresses associated with DNS injection
• All 3,120 IP addresses belong to 39 Chinese autonomous systems

<table>
<thead>
<tr>
<th>AS Name</th>
<th>AS Number</th>
<th>IPs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chinanet</td>
<td>4134</td>
<td>1952</td>
</tr>
<tr>
<td>CNCGroup China169 Backbone</td>
<td>4837</td>
<td>489</td>
</tr>
<tr>
<td>China Telecom (Group)</td>
<td>4812</td>
<td>289</td>
</tr>
<tr>
<td>CHINA RAILWAY Internet (CRNEt)</td>
<td>9394</td>
<td>78</td>
</tr>
<tr>
<td>China Netcom Corp.</td>
<td>9929</td>
<td>67</td>
</tr>
</tbody>
</table>

Top 5 ASes by router IP count

• How much does this affect the Internet?
Methodology

• Tested 43,842 open DNS resolvers in 173 countries outside of China
  ‣ List from probing DNS servers of Alexa 1M top websites
  ‣ Supplemented by lists from researchers

• Query for blacklisted domain from vantage point, check if response is lemon IP
  ‣ Test blacklisted name for all 312 TLDs
  ‣ Also, check against TCP-based DNS queries (injectors do not target DNS queries over TCP)
StepNX Query

- To identify where injection occurs, inject random strings into domain name
  - Injectors use very liberal pattern matching
  - Generate invalid names, expect NXDOMAIN response
  - www.facebook.com.{INVALID}: path to root server
  - www.facebook.com.{INVALID}.com: path to TLD server
  - Repeat 200 times to try different servers/paths

<table>
<thead>
<tr>
<th>DNS Level</th>
<th>Affected Resolvers</th>
<th>Affected Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>1</td>
<td>0.002%</td>
</tr>
<tr>
<td>TLD</td>
<td>11573</td>
<td>26.4%</td>
</tr>
<tr>
<td>Authoritative</td>
<td>99</td>
<td>0.23%</td>
</tr>
</tbody>
</table>

Which resolution step sees injection
StepNX Query

• To identify where injection occurs, inject random strings into domain name
  ‣ Injectors use very liberal pattern matching
  ‣ Generate invalid names, expect NXDOMAIN response
  ‣ www.facebook.com.{INVALID}: path to root server
  ‣ www.facebook.com.{INVALID}.com: path to TLD server
  ‣ Repeat 200 times to try different servers/paths

<table>
<thead>
<tr>
<th>DNS Level</th>
<th>Affected Resolvers</th>
<th>Affected Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root</td>
<td>1</td>
<td>0.002%</td>
</tr>
<tr>
<td>TLD</td>
<td>11573</td>
<td>26.4%</td>
</tr>
<tr>
<td>Authoritative</td>
<td>99</td>
<td>0.23%</td>
</tr>
</tbody>
</table>

Which resolution step sees injection
Who’s Affected?

- **3 TLDs affected almost completely (99.53%)**
  - cn, xn--fiqs8s, xn--fiqz9s
  - Expected: domains from within Great Firewall of China

- **11,573 (26.4%) of resolvers affected for one or more of 16 unexpected TLDs**

<table>
<thead>
<tr>
<th>TLD</th>
<th>Affected Resolvers</th>
</tr>
</thead>
<tbody>
<tr>
<td>de</td>
<td>8192</td>
</tr>
<tr>
<td>xn--3e0b707e</td>
<td>5641</td>
</tr>
<tr>
<td>kr</td>
<td>4842</td>
</tr>
<tr>
<td>kp</td>
<td>384</td>
</tr>
<tr>
<td>co</td>
<td>90</td>
</tr>
<tr>
<td>travel</td>
<td>90</td>
</tr>
<tr>
<td>pl</td>
<td>90</td>
</tr>
<tr>
<td>no</td>
<td>90</td>
</tr>
<tr>
<td>iq</td>
<td>90</td>
</tr>
<tr>
<td>hk</td>
<td>90</td>
</tr>
<tr>
<td>fi</td>
<td>90</td>
</tr>
<tr>
<td>uk</td>
<td>90</td>
</tr>
<tr>
<td>xn--j6w193g</td>
<td>90</td>
</tr>
<tr>
<td>jp</td>
<td>90</td>
</tr>
<tr>
<td>nz</td>
<td>90</td>
</tr>
<tr>
<td>ca</td>
<td>90</td>
</tr>
</tbody>
</table>

16 unexpected TLDs affected by DNS injection on path from an open resolver
Whose Resolvers?

Open resolvers in 109 regions affected

<table>
<thead>
<tr>
<th>Region</th>
<th>Affected Resolvers</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Iran</td>
<td>157</td>
<td>88%</td>
</tr>
<tr>
<td>Myanmar</td>
<td>163</td>
<td>85%</td>
</tr>
<tr>
<td>Korea</td>
<td>198</td>
<td>79%</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>403</td>
<td>75%</td>
</tr>
<tr>
<td>Taiwan</td>
<td>1146</td>
<td>66%</td>
</tr>
<tr>
<td>India</td>
<td>250</td>
<td>60%</td>
</tr>
</tbody>
</table>

Top 6 regions by affected open resolver percentage
Details: .de

<table>
<thead>
<tr>
<th>Region</th>
<th>Resolvers Affected</th>
</tr>
</thead>
<tbody>
<tr>
<td>kr</td>
<td>76%</td>
</tr>
<tr>
<td>my</td>
<td>66%</td>
</tr>
<tr>
<td>hk</td>
<td>54%</td>
</tr>
<tr>
<td>ar</td>
<td>44%</td>
</tr>
<tr>
<td>il</td>
<td>42%</td>
</tr>
<tr>
<td>ir</td>
<td>36%</td>
</tr>
<tr>
<td>tw</td>
<td>36%</td>
</tr>
<tr>
<td>bg</td>
<td>31%</td>
</tr>
<tr>
<td>jp</td>
<td>28%</td>
</tr>
<tr>
<td>ro</td>
<td>25%</td>
</tr>
</tbody>
</table>

10 regions whose open resolvers are most greatly affected for .de queries
Example .de Injection
Example .de Injection
Damage for 70% of the experimental resolvers from KR's claim that the operator of I-Root server, Netnod, "with-paths to TLD servers. Our result partly confirms Mauricio shows that the primary damage arises from censored transit its experimental resolvers suing 109 regions. The most a TLDs and the top 82 domain names. 26.41% of the exper-suing the huge number of domain names in the whole Internet. the over-zealous pattern matching adopt by censorship and this may only represent the tip of the iceberg, considering potentially trigger censorship on 30–90 resolvers, as shown in resolvers to authoritative name servers for several domains.

Twitter.com.abssdfds.ibm.com

Except (AS 12008) hosts some authority servers for all these TLDs name servers and find that it is not a coincidence: UltraDNS.f.ling with the same name infrastructure with the second one, UltraDNS.f.ling from collateral damage because of paths to root, similar to probing TLD servers, we finally constructed querying from collateral damage. Unlike the worries presented by Mauricio [8], Table 6 shows that the primary damage arises from censored transit its experimental resolvers suing the most a...
Solutions

• DNS injectors could filter out transit queries
• Autonomous systems could avoid transit through injecting neighbors
  ‣ Particularly, TLD operators could monitor peering paths
• Security extensions for DNS (DNSSEC) prevent injection
  ‣ DNSSEC has signed responses
  ‣ Resolvers would reject injected responses, accept slower ones from authoritative servers
  ‣ .de and .kr both support DNSSEC
Conclusion

- Great Firewall of China’s DNS injection is affecting lookups originating outside China
  - Caused by queries traversing Chinese ASes
  - Effect is greatest at routes between resolvers and TLDs
- Suggestions on preventing collateral damage
- Some recent changes...
Questions

please contact
Anonymous <zion.vlab@gmail.com>