Handling DNS Abuse and Securing DNS

SANOG36

Champika Wijayatunga
January 2021
DNS Security: Understanding Threats and Abuses

- Large attack surface due to the complexity of the DNS ecosystem
- Query/Response data integrity
  - As originally defined in the protocol, no protection against data corruption
- Query/Response confidentiality
  - As originally defined in the protocol, all data is in clear text (Attacker can see connection meta data)
- Namespace risks
  - Homoglyphs e.g. example.com vs examplé.com (xn--exampl-gva.com)
  - Typosquatting e.g. example.com vs exmaple.com
DNS Security: Understanding Threats and Abuses

- Redirection
  - Change domain’s name servers to point to attacker-controlled authoritative servers

- Resolver Hijacking
  - Cause DNS queries to be answered by attacker-controlled resolver

- Denial of Service
  - Overload victim traffic and services

- Impact of Hierarchical name space
  - Compromise of higher layers means potential compromise of that layer and all lower layers
DNS Security: Understanding Threats and Abuses

- Registrant Compromise
  - Allow attacker to pose as registrant and change domain data

- Registrar Compromise
  - Attacker breaks into registrar system and change customer data

- Registry Compromise
  - Attacker can modify any domain data administered by the registry

- DNS Software vulnerabilities
ICANN DNS Abuse Handling Initiatives
The Domain Abuse Activity Reporting System

What is it?
• A system for reporting on domain name registration and abuse data across TLD registries and registrars

How does DAAR differ from other reporting systems?
• Studies all gTLD registries and registrars for which we can collect zone and registration data
• Employs a large set of reputation feeds (e.g., blocklists)
• Accommodates historical studies
• Studies multiple threats: phishing, botnet, malware, spam
• Takes a scientific approach: transparent, reproducible

https://www.icann.org/octo-ssr/daar
Figure 6: Total number of domains identified as security threats over time

Figure 7: Breakdown of domains identified as security threats across all DAAR threat types

Figure 14: Average percentage of abuse in gTLDs across different threat types over time
Individual Security Threats Oct 2017 to Sep 2020
ITHI, or Identifier Technologies Health Indicators is an ICANN initiative to “measure” the “health” of the “identifier system” that “ICANN helps coordinate”.

The goal is to produce a set of indicators that will be measured and tracked over time that will help determine if the system of identifiers is overall doing better or worse.

ISPs; universities and other operators running DNS recursive resolvers can participate).

https://ithi.research.icann.org
## Some ITHI Results

<table>
<thead>
<tr>
<th>Indicator</th>
<th>July 2020</th>
<th>Past 3 months</th>
<th>Historic Low</th>
<th>Historic High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Server DGA</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of DGA queries seen by root servers</td>
<td>44%</td>
<td>40%</td>
<td>35%</td>
<td>49%</td>
</tr>
<tr>
<td>DNSSEC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% of resolvers that perform DNSSEC validation</td>
<td>32%</td>
<td>32%</td>
<td>23%</td>
<td>34%</td>
</tr>
<tr>
<td>Resolver Concentration</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Number of resolvers seeing 50% of first queries</td>
<td>212</td>
<td>217</td>
<td>206</td>
<td>240</td>
</tr>
<tr>
<td>Number of resolvers seeing 90% of first queries</td>
<td>2149</td>
<td>2133</td>
<td>2036</td>
<td>2231</td>
</tr>
<tr>
<td>Name collision</td>
<td>.LOCAL</td>
<td>4.4%</td>
<td>4.6%</td>
<td>2.4%</td>
</tr>
<tr>
<td>%requests to top 3 names at the root</td>
<td>.HOME</td>
<td>3.0%</td>
<td>3.1%</td>
<td>2.5%</td>
</tr>
<tr>
<td>%requests to top 3 names at resolvers</td>
<td>.LAN</td>
<td>1.0%</td>
<td>1.2%</td>
<td>0.5%</td>
</tr>
<tr>
<td>%requests to top 3 names at resolvers</td>
<td>.LOCALDOMAIN</td>
<td>0.2%</td>
<td>0.0%</td>
<td>0.00%</td>
</tr>
<tr>
<td>%requests to top 3 names at resolvers</td>
<td>.LOCAL</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
<tr>
<td>%requests to top 3 names at resolvers</td>
<td>.WORKGROUP</td>
<td>0.0%</td>
<td>0.0%</td>
<td>0.0%</td>
</tr>
</tbody>
</table>
ICANN Community Work

- Domain Name Security Facilitation Initiative (DSFI) technical study group
- Outside ICANN the contracted parties (Registries & Registrars) have their project on the DNS Abuse Framework:
  - [http://dnsabuseframework.org/](http://dnsabuseframework.org/)
DNS Abuse during Covid-19
Methodology to Identifying Suspect Domains

- Searching for zone files (gTLD and some ccTLD) of keywords related to the Covid-19 pandemic.

  - Jan-Nov 2020: 248,718 domains Identified (blue line)
  - May-Nov 2020: 9,194 of 147,529 found to have some evidence of misuse (red line)
  - Of those, 2,573 had "high confidence" reports
60% of domains related to 4 keywords
Top 4 keywords: **covid**, **mask**, **corona** and **virus**
Consider deploying DNSSEC!
All TLDs vs. ccTLDs

All TLDs 02 Sep 2020

- DS Record: 90.93%
- No DNSSEC: 8.278%
- 12 Signatures: 0.7947%
- All: 100.0%

All ccTLDs 02 Sep 2020

- DS Record: 56.17%
- No DNSSEC: 40.26%
- 11 Signatures: 3.571%
- All: 100.0%
All ccTLDs vs. Asia Pacific ccTLDs

All ccTLDs
02 Sep 2020

ccTLD AP region
02 Sep 2020

No DNSSEC

DS Record

173 DS Record 56.17%
124 No DNSSEC 40.26%
11 Signatures 3.571%
308 All 100.0%

69 DS Record 58.47%
42 No DNSSEC 35.59%
7 Signatures 5.932%
118 All 100.0%
Visit us at icann.org  
Email: champika.wijayatunga@icann.org

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann
linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann