Identifier Technology Health Indicators (ITHI)

https://ithi.research.icann.org

Alain Durand

October 2019
ITHI: an ICANN Initiative

- **ITHI**, or **I**dentifier **T**echnologies **H**ealth **I**ndicators 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.

- This is a long term project, expected to run for a number of years.
ITHI Phases

○ Phase 1: Analysis (2015-2016)
  ○ Strategic choice to define problem areas first
  ○ Many discussions with the larger community
  ○ Split of project ICANN / RIR

○ Phase 2: Development (2017-2018)
  ○ Building platform
  ○ Finding partners
  ○ Getting data

○ Phase 3: Sustaining (2019-…)

We are here now
### Simplified Indicator Dashboard

**ITHI by ICANN**

<table>
<thead>
<tr>
<th>Indicator Description</th>
<th>As of Jan 2019</th>
</tr>
</thead>
<tbody>
<tr>
<td>% No Such Domain queries seen by root servers</td>
<td>70.63%</td>
</tr>
<tr>
<td>% of resolvers that perform DNSSEC validation</td>
<td>28.10%</td>
</tr>
<tr>
<td>%requests to top name at the root</td>
<td>.HOME</td>
</tr>
<tr>
<td>%requests to top name at resolvers</td>
<td>.MAIL</td>
</tr>
<tr>
<td>Number of resolvers accounting for 50% of eyeballs</td>
<td>Coming soon</td>
</tr>
<tr>
<td>Phishing Domains per 10,000 registered names</td>
<td>2.51</td>
</tr>
</tbody>
</table>

*The home page at ithi.research.icann.org provides a quick view of chosen indicators.*
# Complete Dashboard

## ITHI by ICANN

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
<th>As of Jan 2019</th>
<th>Past 3 months</th>
<th>Historic Low</th>
<th>Historic High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root Server Health</td>
<td>% No Such Domain queries seen by root servers</td>
<td>70.63%</td>
<td>68.39%</td>
<td>62.95%</td>
<td>69.40%</td>
</tr>
<tr>
<td>DNSSEC Deployment</td>
<td>% of resolvers that perform DNSSEC validation</td>
<td>27.67%</td>
<td>24.72%</td>
<td>23.43%</td>
<td>27.29%</td>
</tr>
<tr>
<td>Name collision</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>% requests to top 3 names at the root</td>
<td>.HOME</td>
<td>3.09%</td>
<td>3.15%</td>
<td>2.90%</td>
<td>3.67%</td>
</tr>
<tr>
<td></td>
<td>LOCAL</td>
<td>2.82%</td>
<td>3.70%</td>
<td>2.52%</td>
<td>4.47%</td>
</tr>
<tr>
<td></td>
<td>.P</td>
<td>0.82%</td>
<td>0.84%</td>
<td>0.64%</td>
<td>0.92%</td>
</tr>
<tr>
<td></td>
<td>.MAIL</td>
<td>2.00%</td>
<td>0.99%</td>
<td>0.60%</td>
<td>2.55%</td>
</tr>
<tr>
<td></td>
<td>.UNIFI</td>
<td>0.07%</td>
<td>0.05%</td>
<td>0.63%</td>
<td>0.07%</td>
</tr>
<tr>
<td></td>
<td>.LOCAL</td>
<td>0.03%</td>
<td>0.04%</td>
<td>0.60%</td>
<td>0.06%</td>
</tr>
<tr>
<td>Resolver Concentration</td>
<td>Number of resolvers accounting for 50% of eyeballs</td>
<td>Coming soon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Number of resolvers accounting for 90% of eyeballs</td>
<td>Coming soon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Dns Abuse (as of Nov 2018, measured on 1210 GTLD and 2280 registrars)</td>
<td>Abuse Domains per 10,000 registered names</td>
<td>Phishing</td>
<td>2.51</td>
<td>2.57</td>
<td>2.31</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malware</td>
<td>1.62</td>
<td>1.67</td>
<td>1.10</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Botnets C&amp;C</td>
<td>0.15</td>
<td>0.16</td>
<td>0.11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spam</td>
<td>42.03</td>
<td>41.15</td>
<td>40.47</td>
</tr>
<tr>
<td></td>
<td>Number of GTLD to account for 50% of abuses</td>
<td>Phishing</td>
<td>1</td>
<td>1.00</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malware</td>
<td>2</td>
<td>2.33</td>
<td>1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Botnets C&amp;C</td>
<td>1</td>
<td>2.00</td>
<td>2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spam</td>
<td>4</td>
<td>4.00</td>
<td>3</td>
</tr>
<tr>
<td></td>
<td>Number of GTLD to account for 90% of abuses</td>
<td>Phishing</td>
<td>13</td>
<td>16.00</td>
<td>11</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Malware</td>
<td>10</td>
<td>10.33</td>
<td>7</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Botnets C&amp;C</td>
<td>5</td>
<td>5.00</td>
<td>4</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Spam</td>
<td>25</td>
<td>24.33</td>
<td>18</td>
</tr>
<tr>
<td>Metric</td>
<td>Name</td>
<td>Data Source</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>-------------------------------------------</td>
<td>-------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M1:</td>
<td>Inaccuracy of Whois Data</td>
<td>ICANN compliance dept.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M2:</td>
<td>Domain Name Abuse</td>
<td>ICANN’s DAAR Project <a href="https://www.icann.org/octo-ssr/daar">https://www.icann.org/octo-ssr/daar</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M3:</td>
<td>DNS Root Traffic Analysis</td>
<td>Samples of DNS root traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M4:</td>
<td>DNS Recursive Server Analysis</td>
<td>Summaries of recursive resolvers traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M5:</td>
<td>DNS Resolver Behavior</td>
<td>APNIC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M6:</td>
<td>IANA registries for DNS parameters</td>
<td>Scan of recursive resolvers traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M7:</td>
<td>DNSSEC Deployment</td>
<td>Snapshots of DNS root zone</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>M8:</td>
<td>DNS TLD Traffic Analysis</td>
<td>Summaries of TLD traffic</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
ITHI: From Problem Areas to Measurements

- Technical focus

- **Problem areas → Metrics → Measurement**

- Current value and trend over time
  - Automated process to collect & analyze data

- Measurement, not interpretation
ITHI Data: ICANN + Partners + Contracts

- **ICANN (Internal Data)**
  - Compliance department (M1)
  - DAAR (M2)
  - L-Root data (M3)
  - Root zone (M7)

- **White box measurements with partners**
  - Measurements at recursive & authoritative servers
  - M4, M6, M8

- **Black box measurements**
  - APNIC/Google Ads platform
  - Eyeball view of resolvers M5
ITHI Data: ICANN + Partners + Contracts

- **ICANN (Internal Data)**
  - Compliance department (M1)
  - DAAR (M2)
  - L-Root data (M3)
  - Root zone (M7)

- **White box measurements with partners**
  - Measurements at recursive & authoritative servers
  - M4, M6, M8

- **Black box measurements**
  - APNIC/Google Ads platform
  - Eyeball view of resolvers M5

*This is where we need your help!*
White Box Measurements: ITHI Software

- **DNSCAP Plug-in (running at partner’s site)**
  - Leverage existing code
  - Extract information from DNS transactions
  - Processes at line rate, create small summaries

- **Summarization tools (running at ICANN)**
  - Summarize the summaries, compute metrics
  - From metrics, prepare data for web pages

- **Designed for speed (C++), reliability, privacy**
  - Open source (github.com/private-octopus/ithitools)
  - Code: 23 KLOC, tests: 7 KLOC
  - Code reviewed performed by NLLab
Partner’s Role

- **Partners are in control of their data**
  - They run the tools on their machines
  - They upload data on the staging server
  - We provide assurance about tool quality, privacy
  - We also provide “local view” of the statistics

- **Early Warning System**
  - Partners can decide to share their data with others in exchange for reciprocity
  - Comparing results can serve as an early warning system
  - If a collection point observes a divergence from its baseline but others point don't, it might be an indicator that an attack is under way.
No PII, only statistics, are sent to ICANN org

No “naming and shaming”
ITHI Operation at Partners

- **Agree** to work with us (outreach effort)
- **Install** tools
- **Get account** on staging server (SSH)
- **Set up captures:**
  - At least 4 times a week
  - Typically 1 million transactions per session
- **Set up upload scripts**
- **Verify behavior** with “partners only” pages on web server
Current Partners

- **Active partners:**
  - National University of La Plata (UNLP), Argentina,
  - University of Cape Coast, Ghana,
  - DNS Nawala, Indonesia,
  - Kaznic, Kazakhstan (.KZ)
  - TWNIC, Taiwan
Thank You and Questions
Visit us at icann.org
Email: email

@icann
facebook.com/icannorg
youtube.com/icannnews
flickr.com/icann

linkedin/company/icann
slideshare/icannpresentations
soundcloud/icann
instagram.com/icannorg