Trends in Abuse: New and Legacy gTLDs

Maciej Korczyński, TU Delft, Grenoble INP
Maarten Wullink, SIDN Labs
Brian Aitchison, ICANN
Drew Bagley, Secure Domain Foundation

Thursday, September 5, 2017
Toronto, Canada
Attendees Reminders:

What occurs in a M³AAWG meeting cannot be shared outside the membership

- Attendees can blog, tweet and post on either your personal or business social media account about the **selected, pre-approved sessions where we show a slide indicating that social media posting is allowed.** Please reference @maawg or #m3aawg41 where we are also tweeting.

- In all cases, respect M³AAWG anonymity: No publishing people or company names, except as cited on the official M³AAWG channels: @maawg, facebook.com/maawg, plus.google.com/+MAAWG

- No use of Wireshark or similar products on the M³AAWG network

- No photography - No video - No audio recording

- Any exception requires written permission from the Executive Director and may require permission from the session members

- All meeting attendees must wear and have their M³AAWG badge visible at all times during the meeting

- Please silence all electronic devices; be courteous to those listening to the presentations

- **DO NOT LEAVE YOUR BELONGINGS UNATTENDED.** Be aware and cautious at all times

**Treat all attendees respectfully in and out of sessions. No less will be tolerated. Please review our meeting Conduct Policy at [https://www.m3aawg.org/conduct-policy](https://www.m3aawg.org/conduct-policy)**

For questions, please contact Jerry Upton at: jerry.upton@m3aawg.org
Reminders for Our Worldwide Friends

All meeting content is confidential: No photos, no video, no recording.
See staff with questions.

L’ensemble du contenu de la réunion est confidentiel : les photos, vidéos et enregistrements sont interdits. Pour toute question, demandez conseil au personnel.

Todo el contenido de la reunión es confidencial: No está permitido sacar fotografías ni grabar vídeo o audio. Consulte con el personal si tiene alguna pregunta.

Der gesamte Inhalt des Meetings ist vertraulich: Keine Fotos, kein Video, keine Tonaufzeichnung. Bei Fragen wenden Sie sich an die Mitarbeiter.

会议的内容是全部保密的。禁止拍照、录影、录音。如有疑问，请咨询职员。

 всё ведущее содержание конфиденциальное: запрещены фотографии, видеозапись, аудиозапись. Вопросы обращайтесь к персоналу.
Social Media Posting Allowed

Tweeter, Facebook, LinkedIn, other social media posts are welcomed in this session if you:

- Only post comments made by the speakers or panelists
- Do not post comments or questions from the audience (but you can share the speakers’ responses to questions)
- Do not post the name, position or company of other meeting attendees
- Do not post conversations with attendees
- M³AAWG is not a deliverability conference; we are:
  - An industry working group meeting
  - An anti-abuse conference, or
  - A gathering of security experts
- All of the M³AAWG Membership, Trademarks and Logo guidelines apply
  (https://www.m3aawg.org/members/how-promote-m3aawg#TrademarkGuidelines)
- Appreciate a shout out to @maawg and #m3aawg41
Code of Conduct

M3AAWG is dedicated to making our meetings and business open to all members and guests and to making it a safe place for all. We do not tolerate harassment of any kind.

We insist that all participants, attendees and meeting staff adhere to a civil demeanor at all times. This includes refraining from inappropriate language, comments and behavior, in person or by electronic communications and/or public or semi-public social media. In accordance with applicable law, M3AAWG prohibits sexual harassment and harassment because of race, color, gender, age, religion, disability, sexual orientation or any other basis protected by federal, state or local law.

Participants, attendees and meeting staff who are being harassed, intimidated, or are dealing with otherwise improper behavior are encouraged to report it immediately to the Executive Director or a Board member without fear of repercussion.

Alternate methods of reporting issues include: contacts listed on the back of your badge, email to the Executive Director, jerry.upton@m3aawg.org, or if needed, calling the local police department.

Anyone who is found to be in violation of this policy may be handled in any one or more of these methods, depending on the offense: Warning, Expulsion, Contacting of employer, or Contacting the police or other legal authorities. Actions stronger than a warning will be taken at the discretion of the M3AAWG Board of Directors.

M3AAWG reserves the right to remove any participant or attendee at any time for any reason.

The policy also extends outside of the meeting rooms to include all areas of the meeting hotel and social gatherings sponsored by M3AAWG or M3AAWG member organizations.

Note: You can download this file at https://www.m3aawg.org/conduct-policy
Session Feedback

Please share your comments on this session with M³AAWG – good, could-be-better or new ideas – to help improve our meetings.

Click on the session title in SCHED then use the Feedback Survey button above the description.

Thanks! Your comments are appreciated.
Agenda

- Introduction from the ICANN organization: Background of Study
- Presentation from SIDN and Delft University of Technology
- Q & A
## 2009: Mitigating Malicious Conduct: New gTLD Program Explanatory Memorandum

<table>
<thead>
<tr>
<th>Question</th>
<th>Recommendation(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1) How do we ensure that bad actors do not run registries?</td>
<td>1. Vet registry operators</td>
</tr>
<tr>
<td>3) How do we ensure more focused efforts on combating identified abuse?</td>
<td>5. Require “Thick” WHOIS records&lt;br&gt;6. Centralize Zone File access&lt;br&gt;7. Document registry- and registrar-level abuse contacts and policies&lt;br&gt;8. Provide an expedited registry security request process</td>
</tr>
<tr>
<td>4) How do we provide an enhanced control framework for TLDs with intrinsic potential for malicious conduct?</td>
<td>9. Create a draft framework for a high security zone verification program</td>
</tr>
</tbody>
</table>
2016: New gTLD Program Safeguards Against DNS Abuse: Revised Report

Research aid to Competition, Consumer Trust, and Consumer Choice Review Team

How to measure effectiveness of safeguards?

**Base Research Model**

**Explanatory Variable:**
DNS Expansion

**Potential proxy metrics:**
- Number of domain names
- Legacy TLDs
- New TLDs
- Entire DNS

**Intervening Variable(s)**
Safeguards to Mitigate DNS Abuse

What about...
- Pricing?
- Operational policies and/or practices?
- Systemic policies and/or practices?
- Cybercriminal preferences and practices?

**Response Variable:**
DNS Abuse Rate

**Potential proxy metrics:**
- Spam rate
- Phishing rate
- Malware rate
- Others as relevant to the “effectiveness” objectives of the safeguards
Study Background (cont’d)

2016-2017: Competition, Consumer Trust, and Consumer Choice Review Team

- Affirmation of Commitments (AoC) specified that “malicious abuse issues” be addressed in expansion of top-level domain space
- CCT-RT mandated by AoC to examine “effectiveness of…safeguards put in place to mitigate issues involved in…the expansion [of the top-level domain space]”
- Required comprehensive descriptive statistics as **baseline measure** of abuse rates in new compared to legacy gTLDs in order to gauge safeguard effectiveness
- Also serves as proxy for “Trust”, i.e. changes in abuse rate \(\rightarrow\) changes in trust
- CCT-RT Draft Report recommends ongoing DNS abuse measurement
Study

Statistical Analysis of DNS Abuse in gTLDs (SADAG)

Consortium: SIDN and TU Delft

Requested by: Competition, Consumer Trust, and Consumer Choice Review Team
Goal

- Comprehensive statistical comparison of rates of DNS abuse in new and legacy gTLDs
  - Spam
  - Phishing
  - Malware
- Statistical analysis of potential abuse drivers
Motivation

- New Generic Top-Level Domain (gTLD) Program enabled hundreds of new generic top-level domains
Data

Blacklists

- **Anti Phishing Working Group**
  - Phishing URLs

- **StopBadware**
  - Malware URLs

- **SURBL (4 blacklists)**
  - Phishing domains
  - Spam domains
  - Malware domains
Blacklists

- Spamhaus
  - Spam domains

- CleanMX (3 feeds)
  - Phishing URLs
  - Malware URLs
  - Defaced URLs

- Secure Domain Foundation
  - Phishing URLs
  - Malware URLs
Data

WHOIS data

- WHOIS XML API
  - All new gTLDs
  - Subset of legacy gTLDs

- DomainTools
  - Providing missing domains

Domain data

- Zone files
  - Per gTLD
  - Per day
  - 3-year period
Active Web & DNS Scan

- Scanned
  - All new gTLDs
  - Sample of legacy gTLDs

Registry (ICANN)

- Sunrise periods
- Registry operators (parent companies of registry operators)
Distribution of malicious content: *

- Number of unique domains
  E.g. malicious.com

* "Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs", Maciej Korczyński, Samaneh Tajalizadehkhoob, Arman Noroozian, Maarten Wullink, Cristian Hesselman, and Michel van Eeten, in the IEEE European Symposium on Security and Privacy (Euro S&P)
Security Metrics

- Distribution of malicious content:
  - Number of unique domains
    E.g. malicious.com
  - Number of FQDNs
    E.g. connect.secure.wellsfargo.malicious.com, bankofamerica.com.malicious.com, (…)

* "Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs", Maciej Korczyński, Samaneh Tajalizadeh khoob, Arman Noroozian, Maarten Wullink, Cristian Hesselman, and Michel van Eeten, in the IEEE European Symposium on Security and Privacy (Euro S&P)
Security Metrics

Distribution of malicious content:

- Number of unique domains
  E.g. malicious.com

- Number of FQDNs
  E.g. connect.secure.wellsfargo.malicious.com,
  bankofamerica.com.malicious.com, (…)

- Number of URLs
  E.g. malicious.com/wp-content/file.php,
  malicious.com/wp-content/gate.php, (…)

* "Reputation Metrics Design to Improve Intermediary Incentives for Security of TLDs", Maciej Korczyński, Samaneh Tajalizadehkhooob, Arman Noroozian, Maarten Wullink, Cristian Hesselman, and Michel van Eeten, in the IEEE European Symposium on Security and Privacy (Euro S&P)
Security Metrics for gTLDs

Phishing domains, FQDNs, and URLs (APWG) per legacy gTLDs
Security Metrics for gTLDs

Phishing domains, FQDNs, and URLs (APWG) per legacy gTLDs

Three measures reflect attackers’ profit-maximizing behavior. They abuse free legitimate services and affect the reputations of such associated services.
Security Metrics for gTLDs

Phishing domains (APWG) per new and legacy gTLDs
Security Metrics for gTLDs

Phishing domains (CleanMX ph) per new and legacy gTLDs
Security Metrics for gTLDs

Phishing domains (SURBL ph) per new and legacy gTLDs
Security Metrics for gTLDs

Malware domains (SURBL mw) per new and legacy gTLDs

Statistical Analysis of DNS Abuse in gTLDs
While the number of abused domains remains approximately constant in legacy gTLDs, we observe a clear upward trend in the absolute number of phishing and malware domains in new gTLDs.
Security Metrics for gTLDs

Spam domains (Spamhaus) per new and legacy gTLDs
Security Metrics for gTLDs

Spam domains (SURBL ws) per new and legacy gTLDs

The **absolute** number of spam domains in new gTLDs higher than in legacy gTLDs at the end of 2016

Statistical Analysis of DNS Abuse in gTLDs
Phishing domains (APWG) per new and legacy gTLDs

Size matters!
- Size estimate: Number of domains in each gTLD zone file
Size

- Size estimate: Number of domains in each gTLD zone file

- Rates: \( \frac{\text{#blacklisted domains}}{\text{#all domains}} \times 10,000 \)
Abuse Rates

- Time series of abuse rates of phishing domains in legacy gTLDs and new gTLDs based on the APWG feed.
Abuse Rates

- Time series of abuse rates of **phishing** domains in legacy gTLDs and new gTLDs based on the APWG feed
Abuse Rates

- Time series of abuse rates of phishing domains in legacy gTLDs and new gTLDs based on the APWG feed.

![Graph showing abuse rates over time for new and legacy gTLDs]

- .com (82.5%), .net, .org, .info, and .biz legacy gTLDs.
Abuse Rates

- Time series of abuse rates of **phishing** domains in legacy gTLDs and new gTLDs based on the APWG feed.

```
new gTLDs
legacy gTLDs
```

- .com (82.5%), .net, .org, .info, and .biz legacy gTLDs
Abuse Rates

- Time series of abuse rates of **phishing** domains in legacy gTLDs and new gTLDs based on the APWG feed

![Graph showing abuse rates for new and legacy gTLDs]

Top 5 most abused new gTLDs collectively owned 58.7% of all blacklisted domains in all new gTLDs

**.com (82.5%), .net, .org, .info, and .biz legacy gTLDs**
Abuse Rates

- Time series of abuse rates of malware domains in legacy gTLDs and new gTLDs based on the StopBadware feed
Abuse Rates

- Time series of abuse rates of spam domains in legacy gTLDs and new gTLDs based on the Spamhaus feed
Abuse Rates

- Top 10 new gTLDs with the highest relative concentrations of blacklisted domains for SURBL and Spamhaus datasets (4Q 2016)

<table>
<thead>
<tr>
<th>TLD</th>
<th># Domains</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCIENCE</td>
<td>117,782</td>
<td>5,154</td>
</tr>
<tr>
<td>STREAM</td>
<td>18,543</td>
<td>4,756</td>
</tr>
<tr>
<td>STUDY</td>
<td>1,118</td>
<td>3,343</td>
</tr>
<tr>
<td>DOWNLOAD</td>
<td>16,399</td>
<td>2,016</td>
</tr>
<tr>
<td>CLICK</td>
<td>20,713</td>
<td>1,814</td>
</tr>
<tr>
<td>TOP</td>
<td>736,339</td>
<td>1,705</td>
</tr>
<tr>
<td>GDN</td>
<td>45,547</td>
<td>1,602</td>
</tr>
<tr>
<td>TRADE</td>
<td>23,581</td>
<td>1,521</td>
</tr>
<tr>
<td>REVIEW</td>
<td>9,415</td>
<td>1,318</td>
</tr>
<tr>
<td>ACCOUNTANT</td>
<td>6,722</td>
<td>1,279</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TLD</th>
<th># Domains</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>RACING</td>
<td>51,443</td>
<td>3,812</td>
</tr>
<tr>
<td>DOWNLOAD</td>
<td>21,515</td>
<td>2,645</td>
</tr>
<tr>
<td>ACCOUNTANT</td>
<td>10,543</td>
<td>2,007</td>
</tr>
<tr>
<td>REVIEW</td>
<td>12,615</td>
<td>1,766</td>
</tr>
<tr>
<td>GDN</td>
<td>49,427</td>
<td>1,739</td>
</tr>
<tr>
<td>FAITH</td>
<td>5,540</td>
<td>1,301</td>
</tr>
<tr>
<td>TRADE</td>
<td>19,330</td>
<td>1,247</td>
</tr>
<tr>
<td>CLICK</td>
<td>13,270</td>
<td>1,162</td>
</tr>
<tr>
<td>STREAM</td>
<td>4,406</td>
<td>1,130</td>
</tr>
<tr>
<td>DATE</td>
<td>1,385</td>
<td>999</td>
</tr>
</tbody>
</table>

- Rates: (#blacklisted domains / #all domains) * 10,000

Statistical Analysis of DNS Abuse in gTLDs
Abuse Rates

– Does the problem affect all new gTLDs?
Abuse Rates

- Does the problem affect all new gTLDs?
- No
Abuse Rates

- Does the problem affect all new gTLDs?
- **No**

- Spamhaus and SURBL blacklists reveal that 32% and 36% of all new gTLDs available for registration did not experience a single incident in 4Q 2016.

- Spamhaus blacklisted at least 10% of all registered domains in as many as 15 new gTLDs in 4Q 2016.
Compromised and Maliciously Registered Domains

- Distinguishing between compromised and maliciously registered domains is critical because they require different mitigation actions by different intermediaries.

- Three heuristics:
  - if a given domain name contains a string of a brand name, or
  - if its misspelled version, or
  - if it’s involved in malicious activity within three months after creation.
Compromised and Maliciously Registered Domains

- Distinguishing between compromised and maliciously registered domains is critical because they require different mitigation actions by different intermediaries.
Compromised Domains

Rates of malware domains per new and legacy gTLDs

- New gTLDs
- Legacy gTLDs

Rates of compromised malware domains per new and legacy gTLDs, SBW

- New gTLDs
- Legacy gTLDs

Statistical Analysis of DNS Abuse in gTLDs
Rates of abused domains in legacy gTLDs (StopBadware URL blacklists) are driven by compromised domains.
Maliciously Registered Domains

- Rates of abused domains in new gTLDs (StopBadware URL blacklist) are driven by maliciously registered domains.
Maliciously Registered Domains

Rates of malware domains per new and legacy gTLDs

- Rates of abused domains in new gTLDs (StopBadware URL blacklist) are driven by maliciously registered domains

...and can be driven by single campaigns (domains registered in bulk, common patterns in domain names)
Inferential Analysis of Abuse in New gTLDs

<table>
<thead>
<tr>
<th>Driver</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>New gTLD size</td>
<td>Larger TLDs have a larger “attack surface” (compromised domains)</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Hypothesis: proxy for security efforts, however, miscreants could be interested in deploying DNSSEC and signing their maliciously registered domains</td>
</tr>
<tr>
<td>Parked</td>
<td>Domains serving content are exposed to certain types of vulnerabilities and can be hacked. However, parked domains may be used to scam users or to distribute malware</td>
</tr>
<tr>
<td>No DNS, HTTP error</td>
<td>Domains serving content are exposed to certain types of vulnerabilities and can be hacked</td>
</tr>
<tr>
<td>Type</td>
<td>Proxy for strict registration policies (registration “levels” to new gTLDs, from the least to most restricted groups: 1 generic, 2 geographic, 3 community, and 4 brand)</td>
</tr>
<tr>
<td>Registry operator (parent companies of registry operators)</td>
<td>Proxy for registration practices (e.g. pricing, registration in bulk, payment methods)</td>
</tr>
</tbody>
</table>
“No DNS” domains account for 24.2% of all domains, whereas domains for which the websites serve an HTTP error account for another 12.2%.
### Inferential Analysis of Abuse in New gTLDs

<table>
<thead>
<tr>
<th>Driver</th>
<th>Correlation with abuse counts</th>
</tr>
</thead>
<tbody>
<tr>
<td>New gTLD size</td>
<td>Very weak positive</td>
</tr>
<tr>
<td>DNSSEC</td>
<td>Very weak positive</td>
</tr>
<tr>
<td>Parked</td>
<td>Very weak positive</td>
</tr>
<tr>
<td>No DNS</td>
<td>Very weak negative</td>
</tr>
<tr>
<td>HTTP Error</td>
<td>Very weak negative</td>
</tr>
<tr>
<td>Type</td>
<td>Negative (statistically significant results for phishing)</td>
</tr>
<tr>
<td>Registry operator</td>
<td>No statistically significant results</td>
</tr>
</tbody>
</table>
Privacy or Proxy Services

• Why use Privacy and Proxy services
  – Protecting your personal data
  – Blocking Spam
  – Stopping unwanted solicitations

• Analyzing use of Privacy and Proxy
  – Extract list of registrants
  – Keyword search using “privacy”, “proxy”, “protect” etc.
  – Manual inspection

• How many?
  – We found 570
Privacy or Proxy Services

Unprotected

yourdomain.com

- Your Real Name
- Your Business Name
- 123 Real Home Address, Apt 213
- Your Hometown, VA 22201
- Phone: (703) 555-5555
- Email: yourname@yourdomain.com

Protected

domain.example

- Whois Agent
- Whois Privacy Protection Service, Inc.
- PO Box 639
- Kirkland, WA 98083
- +1 425.274.0657
- domain@protecteddomainservices.com

Image source: https://www.name.com/whois-privacy
Privacy or Proxy Services

Usage for Newly Created Domains

Statistical Analysis of DNS Abuse in gTLDs
Privacy or Proxy Services

Usage for Abusive Newly Registered Domains

Statistical Analysis of DNS Abuse in gTLDs
Privacy or Proxy Services

- The usage of Privacy or Proxy Services by itself is not a reliable indicator of abuse.
- Usage of Privacy or Proxy Services remains higher for legacy gTLDs.
Geographical Location

- Using domain registrar location from WHOIS
  - Registrant details not reliable

- Method
  - Extract unique "registrar name" from WHOIS data.
  - Combine the registrar name with the country information for ICANN-Accredited Registrars.
  - Match remaining name variants
  - Manually lookup the country information for missing registrars

- Result
  - 5,985 registrars
  - 99.99% of domains
## Geographical Location

### Registrar Distribution

<table>
<thead>
<tr>
<th>Country</th>
<th>#Registrars</th>
<th>share</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>2,682</td>
<td>53.88</td>
</tr>
<tr>
<td>China</td>
<td>281</td>
<td>5.64</td>
</tr>
<tr>
<td>Germany</td>
<td>201</td>
<td>4.04</td>
</tr>
<tr>
<td>Canada</td>
<td>177</td>
<td>3.56</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>160</td>
<td>3.21</td>
</tr>
<tr>
<td>India</td>
<td>144</td>
<td>2.89</td>
</tr>
<tr>
<td>France</td>
<td>116</td>
<td>2.33</td>
</tr>
<tr>
<td>Australia</td>
<td>111</td>
<td>2.23</td>
</tr>
<tr>
<td>Spain</td>
<td>105</td>
<td>2.11</td>
</tr>
<tr>
<td>Japan</td>
<td>95</td>
<td>1.91</td>
</tr>
</tbody>
</table>
## Geographical Location

### Domain Distribution

<table>
<thead>
<tr>
<th>New</th>
<th>New #Domains</th>
<th>New Share</th>
<th>Legacy</th>
<th>Legacy #Domains</th>
<th>Legacy Share</th>
</tr>
</thead>
<tbody>
<tr>
<td>China</td>
<td>8,076,776</td>
<td>27.92</td>
<td>US</td>
<td>152,527,872</td>
<td>56.72</td>
</tr>
<tr>
<td>US</td>
<td>6,283,269</td>
<td>21.72</td>
<td>China</td>
<td>24,098,150</td>
<td>8.96</td>
</tr>
<tr>
<td>Gibraltar</td>
<td>3,028,035</td>
<td>10.47</td>
<td>Germany</td>
<td>18,044,735</td>
<td>6.71</td>
</tr>
<tr>
<td>Cayman Is.</td>
<td>2,069,919</td>
<td>7.16</td>
<td>Canada</td>
<td>16,704,693</td>
<td>6.21</td>
</tr>
<tr>
<td>Singapore</td>
<td>1,870,886</td>
<td>6.47</td>
<td>India</td>
<td>11,135,408</td>
<td>4.14</td>
</tr>
<tr>
<td>Japan</td>
<td>1,741,228</td>
<td>6.02</td>
<td>Japan</td>
<td>7,935,585</td>
<td>2.95</td>
</tr>
<tr>
<td>India</td>
<td>1,323,117</td>
<td>4.57</td>
<td>Australia</td>
<td>6,425,896</td>
<td>2.39</td>
</tr>
<tr>
<td>Germany</td>
<td>1,105,708</td>
<td>3.82</td>
<td>France</td>
<td>4,988,581</td>
<td>1.86</td>
</tr>
<tr>
<td>Hong Kong</td>
<td>836,069</td>
<td>2.89</td>
<td>UK</td>
<td>4,511,714</td>
<td>1.68</td>
</tr>
<tr>
<td>France</td>
<td>450,371</td>
<td>1.56</td>
<td>Turkey</td>
<td>2,418,232</td>
<td>0.90</td>
</tr>
</tbody>
</table>
# Geographical Location

## SURBL Distribution

<table>
<thead>
<tr>
<th>New gTLD Country</th>
<th>#Incidents</th>
<th>Percentage</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gibraltar</td>
<td>751,748</td>
<td>49.44</td>
<td>2482.63</td>
</tr>
<tr>
<td>Japan</td>
<td>295,647</td>
<td>19.44</td>
<td>976.37</td>
</tr>
<tr>
<td>China</td>
<td>214,332</td>
<td>14.1</td>
<td>707.83</td>
</tr>
<tr>
<td>United States</td>
<td>109,989</td>
<td>7.23</td>
<td>363.24</td>
</tr>
<tr>
<td>India</td>
<td>54,782</td>
<td>3.6</td>
<td>180.92</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>24,955</td>
<td>1.64</td>
<td>82.41</td>
</tr>
<tr>
<td>France</td>
<td>20,121</td>
<td>1.32</td>
<td>66.45</td>
</tr>
<tr>
<td>United Arab Emirates</td>
<td>11,793</td>
<td>0.78</td>
<td>38.95</td>
</tr>
<tr>
<td>Cayman Islands</td>
<td>8,912</td>
<td>0.59</td>
<td>29.43</td>
</tr>
<tr>
<td>Canada</td>
<td>6,494</td>
<td>0.43</td>
<td>21.45</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legacy gTLD Country</th>
<th>#Incidents</th>
<th>Percentage</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>1,985,574</td>
<td>47.06</td>
<td>130.18</td>
</tr>
<tr>
<td>Japan</td>
<td>1,190,409</td>
<td>28.21</td>
<td>78.05</td>
</tr>
<tr>
<td>China</td>
<td>319,546</td>
<td>7.57</td>
<td>20.95</td>
</tr>
<tr>
<td>India</td>
<td>268,812</td>
<td>6.37</td>
<td>17.62</td>
</tr>
<tr>
<td>Germany</td>
<td>73,185</td>
<td>1.73</td>
<td>4.8</td>
</tr>
<tr>
<td>Ireland</td>
<td>58,292</td>
<td>1.38</td>
<td>3.82</td>
</tr>
<tr>
<td>Canada</td>
<td>40,355</td>
<td>0.96</td>
<td>2.65</td>
</tr>
<tr>
<td>Australia</td>
<td>33,080</td>
<td>0.78</td>
<td>2.17</td>
</tr>
<tr>
<td>Turkey</td>
<td>32,266</td>
<td>0.76</td>
<td>2.12</td>
</tr>
<tr>
<td>Bahamas</td>
<td>28,918</td>
<td>0.69</td>
<td>1.9</td>
</tr>
</tbody>
</table>

*Statistical Analysis of DNS Abuse in gTLDs*
Reginistrar Reputation

• Method
  – Filter out registrars designed for sinkholing domains.
  – Count number of incidents per registrar.
  – Calculate percentage of total abuse linked to registrar.
## Registrar Reputation

### SURBL Distribution

<table>
<thead>
<tr>
<th>new gTLD registrar</th>
<th>#Domains</th>
<th>#Incidents</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nanjing Imperiosus Technology</td>
<td>38,025</td>
<td>35,502</td>
<td>93.36</td>
</tr>
<tr>
<td>Intracom Middle East FZE</td>
<td>20,640</td>
<td>11,255</td>
<td>54.53</td>
</tr>
<tr>
<td>Dot Holding Inc.</td>
<td>153</td>
<td>76</td>
<td>49.67</td>
</tr>
<tr>
<td>Alpnames Limited</td>
<td>3,028,011</td>
<td>751,748</td>
<td>24.83</td>
</tr>
<tr>
<td>Todaynic.com, Inc.</td>
<td>329,399</td>
<td>69,404</td>
<td>21.07</td>
</tr>
<tr>
<td>Web Werks India Pvt. Ltd</td>
<td>785</td>
<td>146</td>
<td>18.6</td>
</tr>
<tr>
<td>GMO Internet, Inc. d/b/a Onamae.com</td>
<td>1,734,775</td>
<td>295,641</td>
<td>17.04</td>
</tr>
<tr>
<td>TLD Registrar Solutions Ltd.</td>
<td>163,988</td>
<td>24,700</td>
<td>15.06</td>
</tr>
<tr>
<td>Xiamen Nawang Technology Co., Ltd</td>
<td>282,925</td>
<td>42,089</td>
<td>14.88</td>
</tr>
<tr>
<td>Instra Corporation Pty Ltd.</td>
<td>77,642</td>
<td>6,200</td>
<td>7.99</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Legacy gTLD registrar</th>
<th>#Domains</th>
<th>#Incidents</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOAPDI INC.</td>
<td>141</td>
<td>126</td>
<td>89.36</td>
</tr>
<tr>
<td>asia registry r2-asia (700000)</td>
<td>1,379</td>
<td>598</td>
<td>43.36</td>
</tr>
<tr>
<td>Nanjing Imperiosus Technology</td>
<td>35,309</td>
<td>10,834</td>
<td>30.68</td>
</tr>
<tr>
<td>Paknic (Private) Limited</td>
<td>10,525</td>
<td>3,083</td>
<td>29.29</td>
</tr>
<tr>
<td>OwnRegistrar, Inc.</td>
<td>22,188</td>
<td>5,238</td>
<td>23.61</td>
</tr>
<tr>
<td>Eranet International Limited</td>
<td>6,109</td>
<td>1,339</td>
<td>21.92</td>
</tr>
<tr>
<td>BR domain Inc. dba namegear.co</td>
<td>847</td>
<td>158</td>
<td>18.65</td>
</tr>
<tr>
<td>Netlynx Inc.</td>
<td>17,612</td>
<td>3,030</td>
<td>17.2</td>
</tr>
<tr>
<td>AFRIREGISTER S.A.</td>
<td>1,551</td>
<td>266</td>
<td>17.15</td>
</tr>
<tr>
<td>GMO Internet, Inc. d/b/a Onamae.com</td>
<td>7,306,312</td>
<td>1,177,886</td>
<td>16.12</td>
</tr>
</tbody>
</table>
Registrator Reputation

Nanjing Imperiosusus Technology Co. Ltd.

Statistical Analysis of DNS Abuse in gTLDs
Registrar Reputation

Alpnames Ltd.

- SURBL
- SpamHaus

![Graph showing the Registrar Reputation of Alpnames Ltd. from Apr 2014 to Apr 2017. The graph compares the total number of abuse records for SURBL and SpamHaus over time.]

Statistical Analysis of DNS Abuse in gTLDs
Questions?
Contact information

Maciej Korczyński
Grenoble INP - Grenoble Alps University
maciej.korczynski@univ-grenoble-alpes.fr

Maarten Wullink, SIDN Labs
maarten.wullink@sidn.nl
Acknowledgements

This study was commissioned by the Competition, Consumer Trust, and Consumer Choice Review Team with the support of ICANN.

We would like to thank ICANN, Domain-Tools, Whois XML API, Spamhaus, SURBL, StopBadware, CleanMX, Secure Domain Foundation, Anti-Phishing Working Group for providing access to their data.

Authors also thank Roland van Rijswijk for his help in obtaining additional domain data.