TLS: portrait of your TLD

Dmitry Belyavskiy, TCI
10th CENTR Security workshop
October 26, 2015
Oxford, United Kingdom
• SSLv2 deprecated (RFC 6176)
• SSLv3 deprecated (RFC 7568)
• TLS 1.0 – RFC 2246 (1999)
• TLS 1.1 – RFC 4346 (2006)
• TLS 1.2 – RFC 5246 (2008)

Source: https://www.trustworthyinternet.org/ssl-pulse/
Vulnerabilities 2014-2015

- Heartbleed
- POODLE
- FREAK
- LogJam

To be continued…
Old algorithms

- SHA1 is deprecating
  - Freestart collision
- RC4 is deprecated

1024-bit RSA is not enough!
New solutions

- Elliptic curves
- Edwards curves
- Perfect Forward Secrecy
- ChaCha20
- Poly1305
- Certificate transparency
Encrypt everything!

- Share of encrypted traffic grows
- New protocols require encryption
- Hosting provides TLS by default *(Universal SSL)*
- DNS is the last unencrypted protocol  
  *RFC 7626*
02 September 2015 (yesterday)

**.RU**
- Total: 4,930,412
  - Change: -0.05%
  - New domains in the current month: 12,070

**.РФ**
- Total: 863,492
  - Change: +0.06%
  - New domains in the current month: 1,549

**.SU**
- Total: 118,316
  - Change: 0%
  - New domains in the current month: 177

---

### .RU domain names usage

<table>
<thead>
<tr>
<th>Category</th>
<th>Total</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>4,930,374</td>
<td>47.1%</td>
</tr>
<tr>
<td>Error</td>
<td>47,015</td>
<td>0.97%</td>
</tr>
<tr>
<td>Redirect</td>
<td>55,000</td>
<td>1.17%</td>
</tr>
<tr>
<td>Under construction</td>
<td>254,000</td>
<td>5.14%</td>
</tr>
<tr>
<td>No IP address</td>
<td>535,000</td>
<td>10.87%</td>
</tr>
<tr>
<td>Not delegated</td>
<td>155,500</td>
<td>3.16%</td>
</tr>
</tbody>
</table>

---

### .РФ domain names usage

<table>
<thead>
<tr>
<th>Category</th>
<th>Total</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>863,015</td>
<td>25.4%</td>
</tr>
<tr>
<td>Error</td>
<td>54,000</td>
<td>6.1%</td>
</tr>
<tr>
<td>Redirect</td>
<td>133,000</td>
<td>17.8%</td>
</tr>
<tr>
<td>Under construction</td>
<td>529,000</td>
<td>15.3%</td>
</tr>
<tr>
<td>No IP address</td>
<td>64,000</td>
<td>7.7%</td>
</tr>
<tr>
<td>Not delegated</td>
<td>168,000</td>
<td>12.3%</td>
</tr>
</tbody>
</table>

---

### .SU domain names usage

<table>
<thead>
<tr>
<th>Category</th>
<th>Total</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Website</td>
<td>118,000</td>
<td>34.4%</td>
</tr>
<tr>
<td>Error</td>
<td>1,000</td>
<td>9.9%</td>
</tr>
<tr>
<td>Redirect</td>
<td>1,000</td>
<td>12.1%</td>
</tr>
<tr>
<td>Under construction</td>
<td>1,000</td>
<td>15.0%</td>
</tr>
<tr>
<td>No IP address</td>
<td>1,000</td>
<td>7.5%</td>
</tr>
<tr>
<td>Not delegated</td>
<td>1,000</td>
<td>7.3%</td>
</tr>
</tbody>
</table>

---

**Source:** [http://statdom.ru/](http://statdom.ru/)
География

За 01 сентября 2015 (вчера)

.РУ — 4 933 073 ▼ - 0,09 %
Новых с начала месяца: 5 458

.РФ — 862 997 ▼ - 0,14 %
Новых с начала месяца: 798

.SU — 118 311 ▼ - 0,11 %
Новых с начала месяца: 110

Использование доменов .RU

<table>
<thead>
<tr>
<th>Требуемые прок</th>
<th>Проданные, число</th>
<th>Проданные, доля</th>
</tr>
</thead>
<tbody>
<tr>
<td>число</td>
<td>числа</td>
<td>числа</td>
</tr>
<tr>
<td>353 294</td>
<td>244 597</td>
<td>69,23 %</td>
</tr>
<tr>
<td>113 118</td>
<td>49 552</td>
<td>43,81 %</td>
</tr>
<tr>
<td>55 215</td>
<td>37 221</td>
<td>67,41 %</td>
</tr>
<tr>
<td>40 611</td>
<td>31 694</td>
<td>78,04 %</td>
</tr>
<tr>
<td>32 937</td>
<td>26 529</td>
<td>80,54 %</td>
</tr>
<tr>
<td>28 876</td>
<td>24 799</td>
<td>85,88 %</td>
</tr>
</tbody>
</table>

Source: http://statdom.ru/
Collecting Data

- Resolve the names
- Collect mapping IP => hosts
- 443 port
- Do handshake
- Validate against Mozilla trusted roots
All EC certificates are from Cloudflare

~50% of certs are free or bundle

~400 EV certificates at 2nd level, more at 3rd level

>90% RSA certs 2048 bits

<10 have 1024 bits
Conclusions

- Practice in Russia matches recommendations
- We will improve the statistics
  - MX, ciphersuites,…
- We can analyze our zones for threats
Questions?

Email:

beldmit@tcinet.ru