TLS: portrait of your TLD

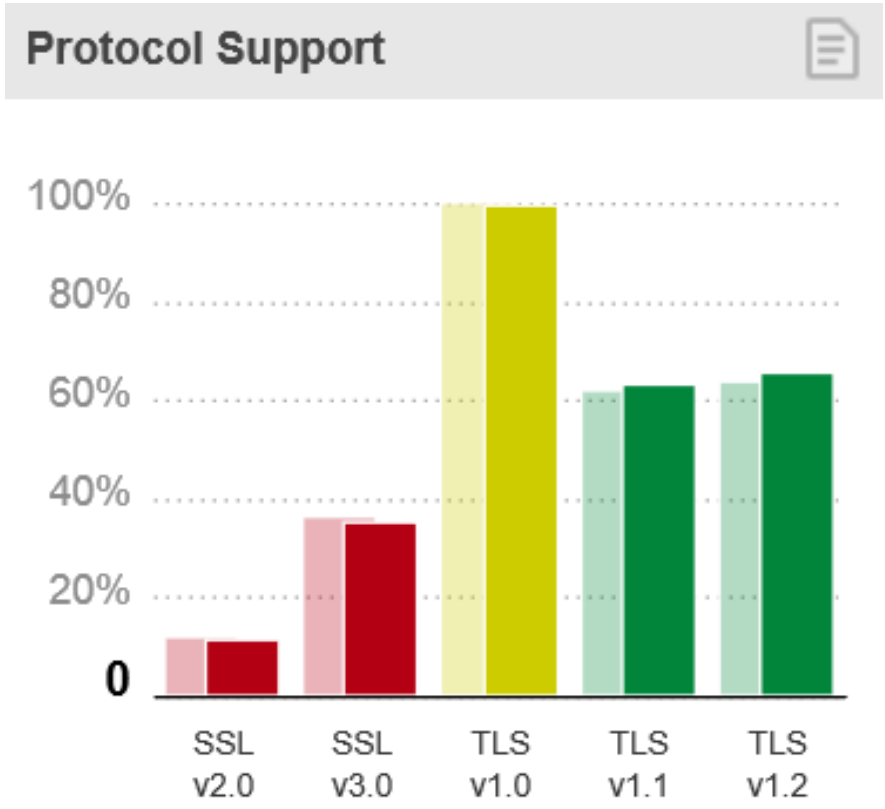
Dmitry Belyavskiy, TCI

TLDCON
September 9-10, 2015
Yerevan

Technical Centre of Internet

TLS: history

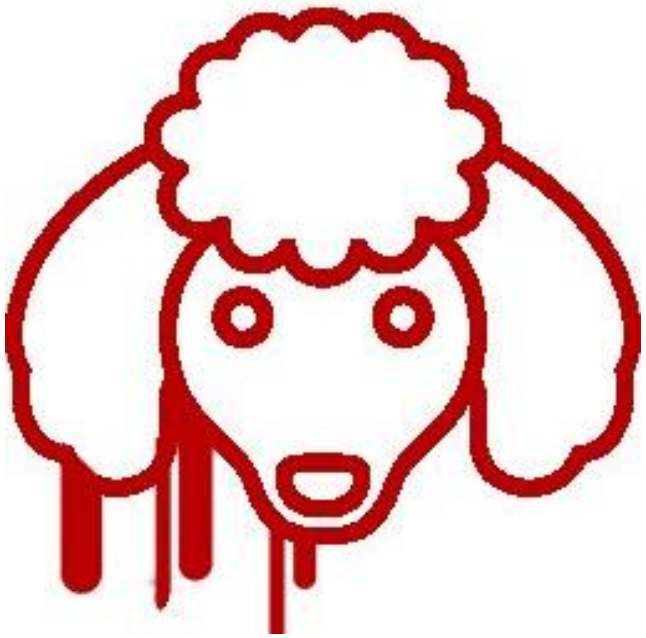
- SSLv2 deprecated (RFC 6176)
- SSLv3 deprecated (RFC 7568)
- TLS 1.0 – RFC 2246 (1999)
- TLS 1.1 – RFC 4346 (2006)
- TLS 1.2 – RFC 5246 (2008)



Source: https://www.trustworthyinternet.org/ssl-pulse/

Vulnerabilities 2014-2015

- Heartbleed
- POODLE
- FREAK
- LogJam



To be continued…

Old algorithms

- SHA1 is deprecating
- 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

TldStat

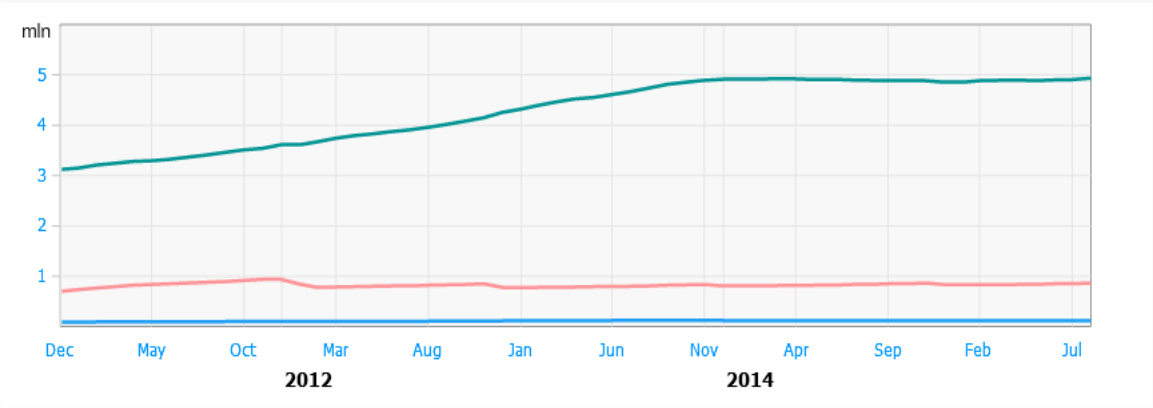
02 September 2015 (yesterday)

.RU
4 930 412 ▼ - 0,05 %
New domains in the current month: **12 070**

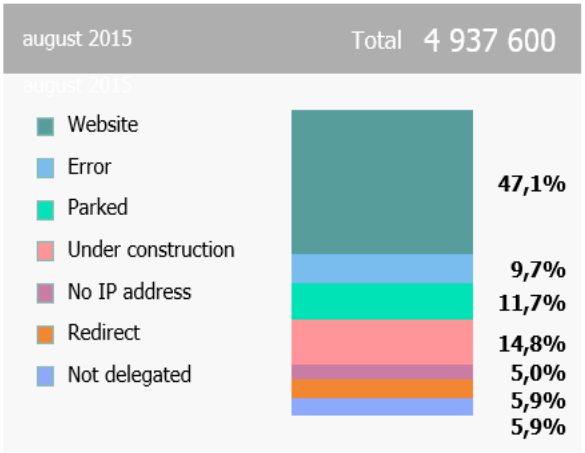
.РФ
863 492 ▲ + 0,06 %
New domains in the current month: **1 549**

.SU
118 316 ● 0 %
New domains in the current month: **177**

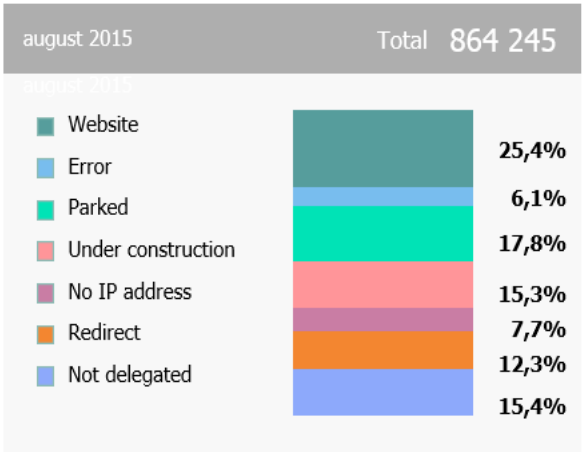
.RU/.РФ growth



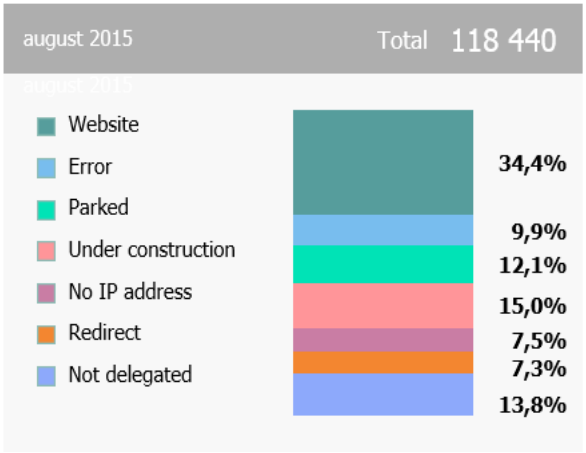
.RU domain names usage



.РФ domain names usage



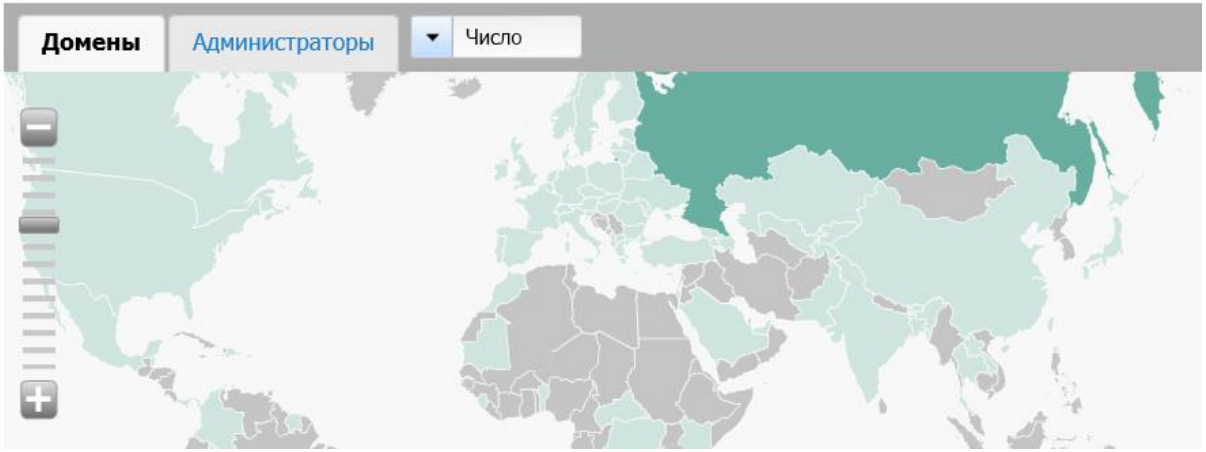
.SU domain names usage

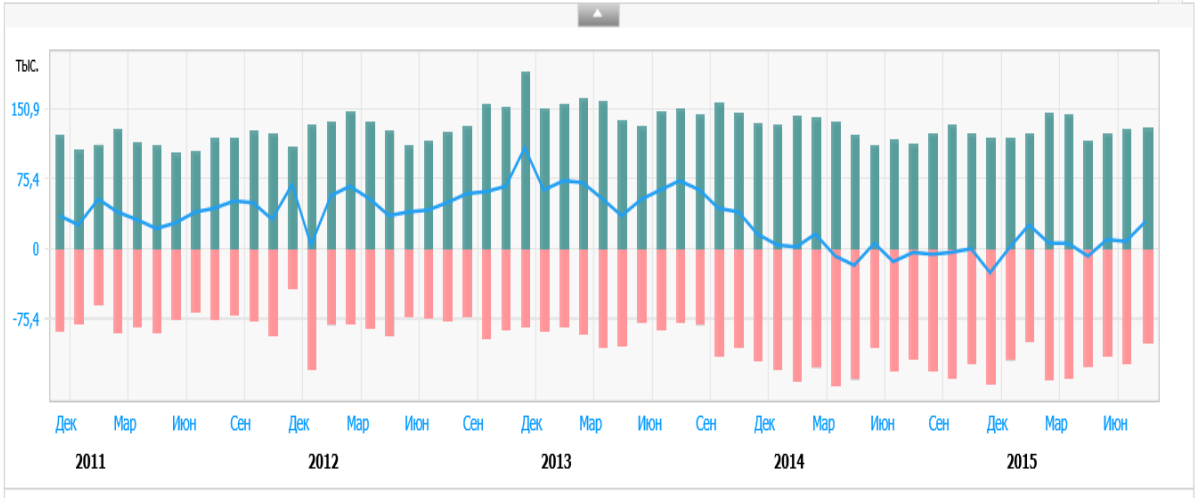


Source: http://statdom.ru/

TldStat

География





Source: http://statdom.ru/

За 01 сентября 2015 (вчера)

.RU
4 933 073 - 0,09 %
Новых с начала месяца: **5 458**

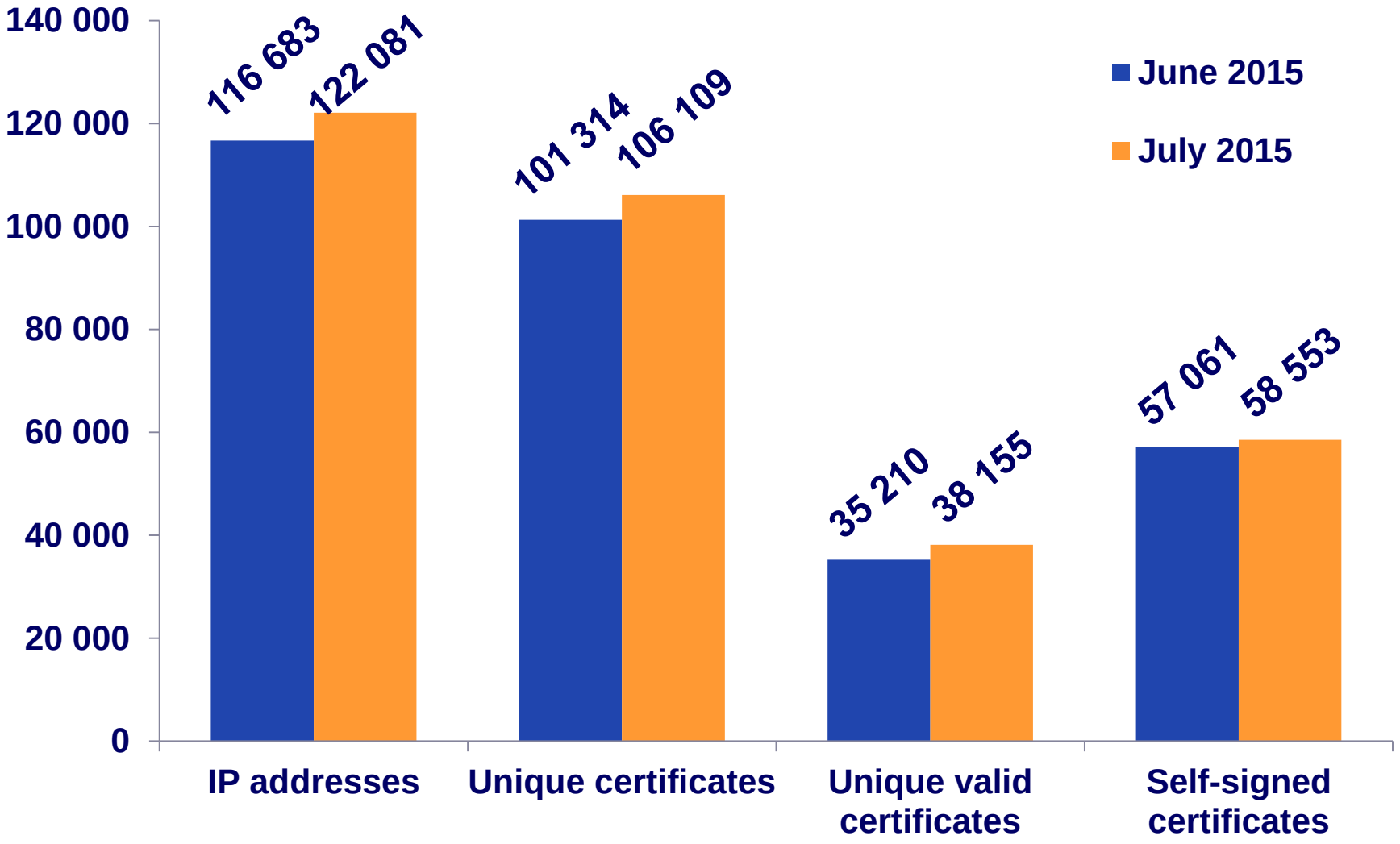
.РФ
862 997 - 0,14 %
Новых с начала месяца: **798**

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

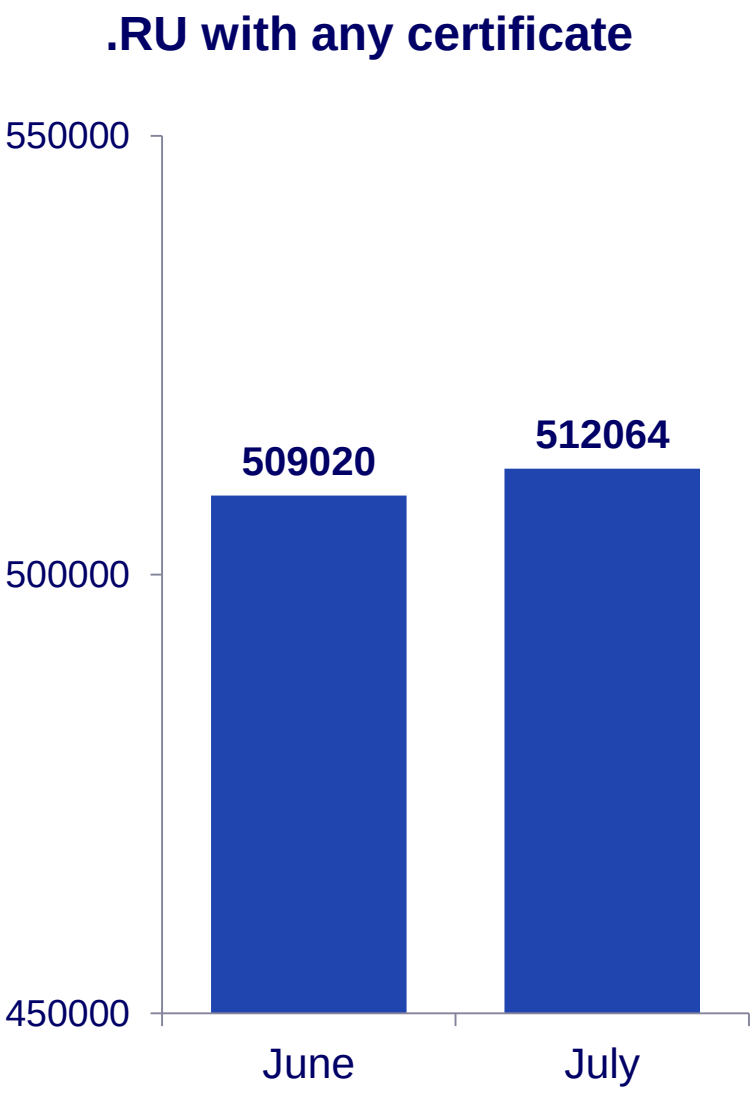
Использование доменов .RU

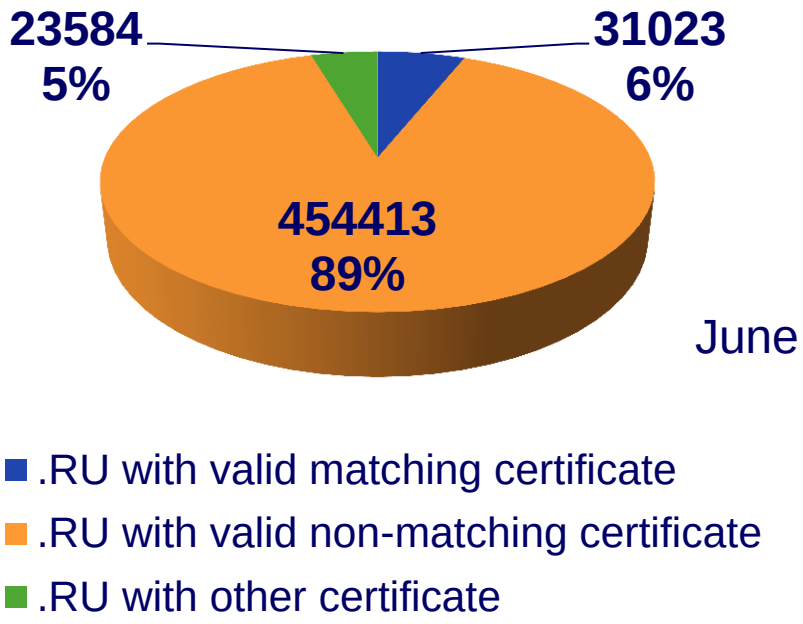
Требующие про	Продлённые, число	Продлённые, доля
353 294	**244 597**	**69,23 %**
113 118	49 552	43,81 %
55 215	37 221	67,41 %
40 611	31 694	78,04 %
32 937	26 529	80,54 %
28 876	24 799	85,88 %

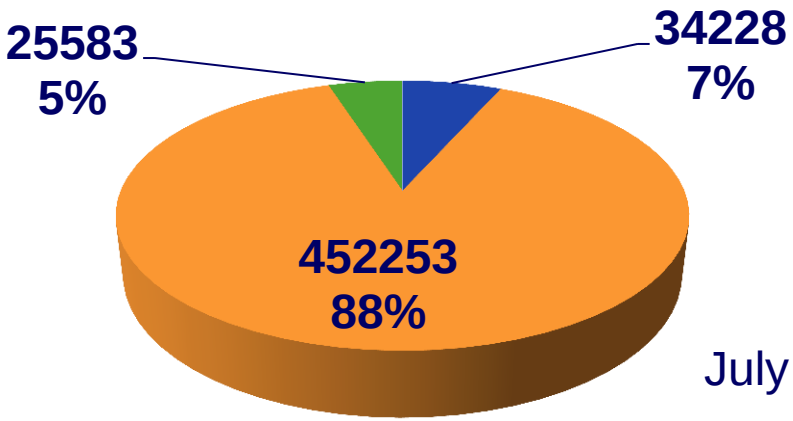
Overall statistics



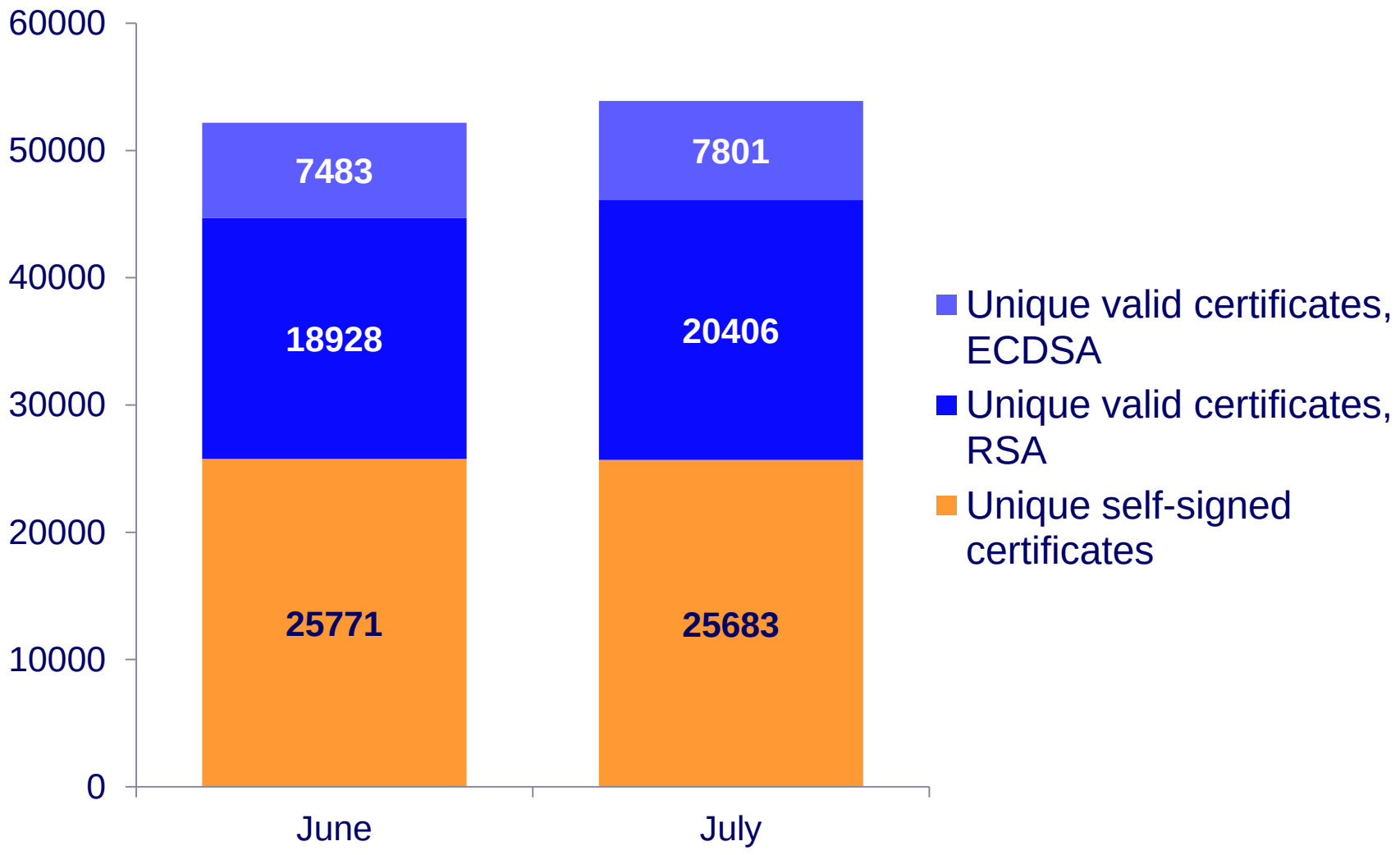
.RU statistics







.RU statistics



Some details

- 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 has 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