DNS infrastructure of .RU

(stability & security)

p.khramtsov@msk-ix.ru
.RU & DNS anycast cloud

Nodes in Russia:
1. Moscow
2. St Petersburg
3. Ekaterinburg
4. Novosibirsk
5. Kazan
6. Samara
7. Vladivostok
8. Rostov-Don
9. Stavropol

Nodes overseas:
1. New York
2. Los Angeles
3. São Paulo
4. Hong Kong
5. Prague
6. Amsterdam
7. Frankfurt
8. Astana
9. Singapore
10. Kharkov

Name servers have IPv4/IPv6 addresses in the following ASs: 42385, 43832.
DNS anycast cloud statistics

Number of DNS requests (06.02.2016)

Russia    USA    Mexico    Ukr    India    China    Germany    Turkey    Indonesia    Tai

18.02.16  APTLD-2016
DNS anycast cloud statistics

Number of DNS requests (06.02.2016)
DNS infrastructure problems

1. DDOS attacks on the anycast cloud
2. DDOS attacks on the servers supporting second-level domains in .RU and resolvers
3. DDOS attacks on the Registry Services (Whois for example)
4. Misconfiguration of DNS servers supported second level domains
5. Misconfiguration of DNS resolvers that request .RU authoritative servers
DNS anycast cloud (typical attacks)

26.10.2015 – flood
27.11.2015 – icmp+udp flood

Our nodes are under **DDoS Attack Protection** and **Mitigation** (Service of PCCW, Vodafon, Tata)
Dns.ix.ru open resolver statistics (a lot of ANY requests)
Wrong DNS requests

Number of DNS requests (06.02.2016)
Rank of active Whois users
(Top-20, 01.01.2016)
Conclusions and Recommendations

• Geographically distributed anycast cloud balances traffic and allows a quick response to an attack.
• Geographically distributed anycast cloud allows us comparing versions of the zone file received from different locations worldwide
• Squatters and Registrars are the main threat to registry services :)
• Misconfiguration of DNS servers produces a lot of wrong queries to the System
Questions?

p.khramtsov@msk-ix.ru