DNS content blocking
Through the years

APTLD Members Meeting
Tashkent, September 2018
Good old days

Content blocking by domain name. How was it:

1. Domain market players stay away from the content

2. All expertise lays on law enforcements

3. Website could be blocked only upon the court order
How registries and registrars deal with the malicious domains

1. Registries and registrars typically are not cybersecurity experts

2. All expertise lays on third part contractors

3. Registrars (and sometimes registries) could block domain names relaying on external requests
How we do it today

Competent organizations
Special right to seize domain names
How we will do it tomorrow

Cyberdefense based on deep analysis and predictions

1. To understand more about domain usage patterns

2. To predict how domain will be used (even before the registration)

3. Sharing the information with registrars, registries and third part contractors
Dealing with the large botnets

1. Analysis of malware shows the number of embedded domain names (not even registered yet)

2. Cyberexperts define the DGA

3. Registry sinkholes the domain names and prevent it further registrations

4. Botnet could not receive external commands
Who does it:

Project Partners

[Logos of various companies and organizations]
Who does it:

Canadian “Think tank” SDF (Secure Domain Foundation)

1. Collects the digital fingerprints of registrants (e-mail, IP, preferable name servers, browser fingerprints)

2. Stores the WHOIS history for many years

3. Makes prognoses of how domain names will be used

4. Attracts the attention of domain industry players to the name
ICANN Domain Abuse Activity Reporting

1. Collects and processes large amount of data from different TLDs

2. Defines domain misusage patterns

3. Shares the information with TLDs and registrars for high-level analysis
Conclusions:

1. The main idea is not fight but to prevent malicious activity

2. The only way is to collect the information from different sources (that means we will have to share it)

3. We need to further develop analytical tools to make the prognoses more reliable (prevent false positives, false negatives etc.)
Thank You!

Mikhail Anisimov
m.anisimov@cctld.ru