Government as DDoS Facilitator

Dmitry Kohmanyuk

Budva, SEE 6 2017.06.12

Background

- Some governments insist on blocking of certain web content by operators.
- Some people propose to impose sanctions on governments which block Internet (Afrinic).
- "At the 2016, eight countries banned Facebook, 12 banned WhatsApp messenger, Telegram was banned in four countries.

  The most severe restrictions exist in China, Syria, Iran, Ethiopia, Uzbekistan, Cuba, Saudi Arabia, Bahrain." *)

*) http://uacrisis.org/56242-ukraine-blocks-russian-sm

Implementation

- “Black list” registry.
- DNS blocks.
- IP blocks.
- DPI devices.
- AS path filtering.

Case 1, Russia

- Blocking law exists since 2012, black list managed by Roskomnadzor agency
- Examples: narcotics, suicide, child pornography, copyright violations, calls to protest rallies...
- Hosting servers with multiple HTTPS hosts get blocked, Cloudflare gets blocked, etc.
- ISPs use DNS lookups to find out IP addresses to block (without verification of where they point to.)
- "Rublacklist.net activists suppose that more than 100,000 pages have been blocked accidentally."
- https://meduza.io/en/feature/2015/08/13/this-is-how-russian-internet-censorship-works

Russia, attack

- 2017.06.05 Disgruntled domain owner (dymoff.space) add some A records to their domain..
- Results: Root DNS servers, VKontakte/OK/Facebook networks, Telegram messenger gets blocked.
- More results: 2017.06.09 some 3D Secure bank authentication servers gets blocked.
- Reaction: government publishes “white lists” for DNS, including “*.google.*”
- Further reaction: government asks ISPs to stop resolving blocked domains in DNS.

Case 2, Ukraine

- President issues decree 2017.05.16 with sanctions towards many Russian companies.
- Blocked: Russia-owned social networks (VK, OK), Mail.RU and Yandex.
- Mobile providers and major ISPs rush to implement it.
- Results: Domain and mail hosting on Yandex gets blocked (this includes 15 government sites..)

Ukraine, continued…

- Yandex goes to Cloudflare for help...
- BGP route leaks from Dataline.UA with Cloudflare /32 addresses…
- they get aggregated a bit to… 104.16.0.0/12… Oops!
- * (thanks to Alexander Asimov of Qrator Labs for research material.)

Further reading

- Internet Society Perspectives on Internet Content Blocking: An Overview
- https://www.internetsociety.org/doc/internet-content-blocking

DON’T LET YOUR GOVERNMENT BLOCK THE INTERNET