ICLab Collateral Censorship

Jesse Brizzi
jbrizzi@cs.stonybrook.edu

Konstantin Dmitriev
kdmitriev@cs.stonybrook.edu

Yingtao Tian
yittian@cs.stonybrook.edu

***Abstract*—In this project we are proposing a survey of neighboring sovereign nations to modern day Russia to investigate any possible collateral censorship. Given the socioeconomic state of some of these countries there may be limited infrastructure for Internet access, which requires their traffic to be routed through Russian territory. Russia actively censors various websites and Internet sources based on various reasons. We intend to use this to fulfill the experiment portion of project option 1 in the class forking the IClab software to complete our experiment. As part of option 1 we will also create a Web interface to run our experiment on IClab and a website presenting our final results.**

Keywords*—*Collateral Censorship, Russia, Block, DPI, DNS, IP.

I. Motivation

In the summer of 2008, when Russia's mass media and telecom watchdog Roskomnadzor [1] was re-established, the Russian Internet, or RuNet, changed significantly. This Federal Service is regulated and put into motion by two laws, - "On Protecting Children from Information Harmful to Their Health and Development"[2] and "On Information, Information Technology and Information Protection"[3]. Both of them give judges a free hand in decision-making. As a result, a number of websites have been blocked quite chaotically, starting with opposition websites and articles, to Bitcoin communities and GitHub.

Sometimes such censorship systems can case collateral censorship, or damage. They block access to sites from users beyond those intended to protect[1]. This projects goal is to examine the effect of such possible collateral censorship to the requests that are originating from outside of Russia, with the possible extension to other countries that maintain the censoring services. The result of this project can be used to create a detailed analysis of collateral damage caused by different types of censoring techniques, and to potentially discover the paths at fault.

II. Censorship tools

The Russian Internet Service Providers (ISPs) and government use a number of different censorship techniques to block access to "unwanted" websites. Fig. 1 shows a chart of the most popular ones by the number of providers that maintain a particular method.

[1]Federal Service for Supervision of Communications, Information Technology and Mass Media (Russian:)

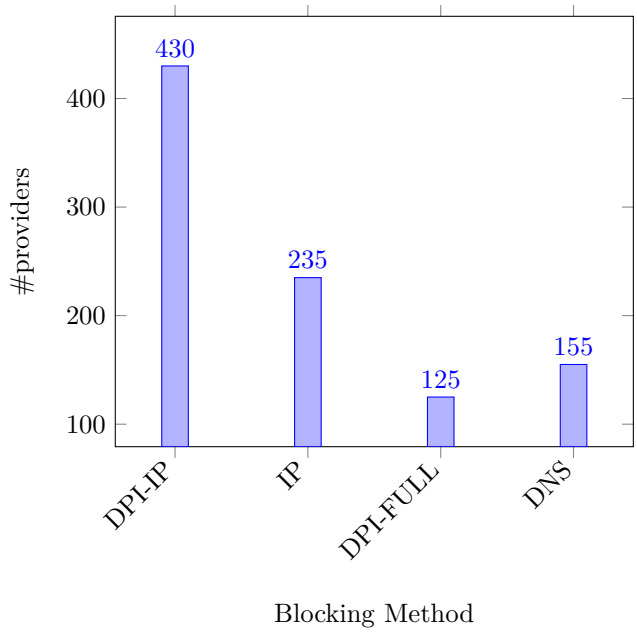

Figure 1: Number of providers that maintain a particular blocking method (DPI-IP - blocking using Deep Packet Inspection (DPI), that checks URL only at a specific IPs and port:80; DPI-FULL - blocking using DPI at every IP and ports; IP - blocking by IP address; DNS - DNS injection)

III. Resources

As a main reference for blacklisted URLs, domain names, and IPs in Russia, we plan to use the service http://antizapret.info which maintains and persistently updates its catalog. In addition, it also provides an API for external access.

Listing 1: An example of the possible output from requesting http://api.antizapret.info/all.php?type=json

```
"id":"16971",
"rsoc_id":"91191193",
"includeTime":"2015-02-13 11:55:47",
"rsocDate":"2015-02-04",
"org":"",
"org_act":"2/1/11-32425",
"url":http://chetkiibro.com/,
"domain":"http://chetkiibro.com/,
"ip":"104.28.16.89,104.28.17.89",
"country":"",
"proof":"http://antizapret.info/site.php?id=16971
    "
```

As a reference of the potential victims of the collateral censorship, we are going to use telegraphy maps (Fig. 2), and the map of the supported countries for one of the largest Russian backbone service provider (Fig. 3), concentrating on the bordering countries.

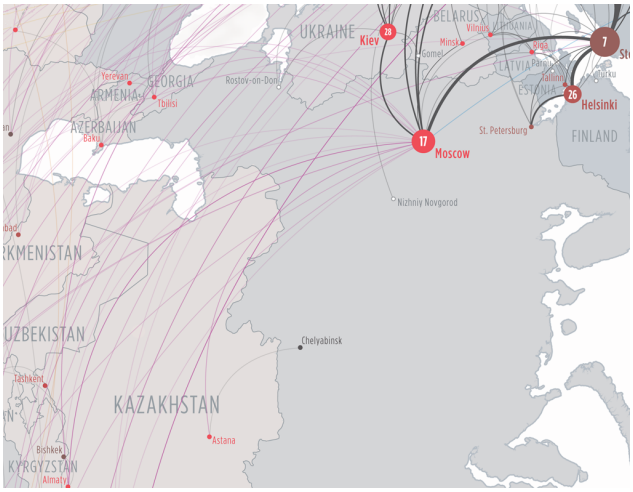

Figure 2: Telegeography Map of the Region

Figure 3: RETN's backbone map

IV. Research Plan

A. Ultimate Plan(?)

Our ultimate aim is to write an experiment for the ICLab project [4] in the form of Python scripts that will probe websites censored in Russia from computers of registered ICLab users. This experiment will not only be able to compare the received web-pages with the blocked ones, but also return the type of the applied censorship technique in case of detected similarity between the received and the blocked web-pages. To collect the source code of blocked web-pages we plan to use our groups own private computer in Russia or a VPN service

In order to create this experiment, we plan to use the following modules:

1) **urllib** - for network resource access;
2) **socket** - to get an access to the BSD socket interface;
3) **ssl** - to get an access to Transport Layer Security encryption and peer authentication facilities for network socket;
4) **dnspython** - to get an access to high and low levels of DNS.

The coarse description of the experiment is the following:

1) Collect a list of URLs and IPs of the censored web-pages from http://antizapret.info;
2) For each item in the list:
   a) Request the web-page and compare its source code with the code of actually blocked web-page;
   b) Test DNS access;
   c) Test HTTP access.

B. Contingency Plan

Given the possibility where no censorship leakage is found, we will restructure the experiment to try and prove our results are accurate, i.e. that there is little to no collateral censorship resulting from the Russian government. This will be done by repeating the experiment multiple times at different times of the day, along with expanding our list of candidates for possible collateral censorship to other countries in close proximity geographically and in terms of Internet topology.

V. Web User Interface

To display the results of our tests we will create a Web UI, that will consists of a table with the outcomes of the particular experiment, including URL addresses, URL categories, statuses and explanations. That Web UI will also have an option that will give the user a visual summary for the all conducted experiments.

VI. Timeline

Estimation of progress by week.

2/16 - 2/22	Setup and design
2/23 - 3/01	Design Interface Website/Experiment
3/02 - 3/08	Code Interface Website/Experiment
3/09 - 3/15	Code Interface Website/Experiment
3/16 - 3/22	Spring Break/Coding/Debugging
3/23 - 3/29	Run Experiment
3/30 - 4/05	Run Experiment/Analysis Data
4/06 - 4/12	Midterm project Report due
4/13 - 4/19	Expand Experiment if needed
4/20 - 4/26	Create Website for Results
4/27 - 5/03	Buffer Week
5/04 - 5/10	Final Project Report Due

References

[1] Anonymous, *The Collateral Damage of Internet Censorship by DNS Injection*. SIGCOMM Comput. Commun. Rev., July 2012.

[2] *"Law on Protecting Children from Negative and Harmful Information."* President of Russia. N.p., n.d. Web. 14 Feb. 2015.

[3] *Russian Federation: Federal Law No. 149-FZ* of July 24, 2006, on Information, Information Technology and Information Protection (as Amended up to Federal Law No. 398-FZ of December 28, 2013). N.p., n.d. Web. 14 Feb. 2015.

[4] *ICLab*. GitHub. N.p., n.d. Web. 15 Feb. 2015. https://github.com/iclab.