The Great Firewall

and

The Great Cannon

Chee Yeong Lim (4933643)

Faculty of Engineering & Information Sciences

University of Wollongong

NSW, Australia

cyl851@uowmail.edu.au

Table of Contents

1. Objectives

I. Figure out why China Government need The Great Firewall and The Great Cannon.
II. Understand how The Great Firewall and The Great Cannon works.
III. Determine the way of bypassing and/or stopping The Great Firewall and The Great Cannon.

2. Abstract

Purpose - To understand how The Great Firewall and The Great Cannon worked.

Design/Methodology/Approach - From the recent affairs, depth analysis and explore about the firewall and redirect attack technique used by the China Government to create The Great Firewall and The Great Cannon.

Findings - The result of this research is to figure out how The Great Firewall and The Great Cannon works and the solution of it.

Originality/Value - This report provided opportunity for the author and the readers to understand The Great Firewall and The Great Cannon easily.

Keywords - Firewall, DDoS, Censorship, Internet, Javascript, TLS/SSL

Paper Type - Research Report

3. Introduction

In this paper, the author will show you the internet censorship system built by the China Government, differentiate between those systems and how those system worked. Beside that, the author will also discuss about the methods and solutions to bypass or prevent user from facing the issues.

3.1. Story about Google

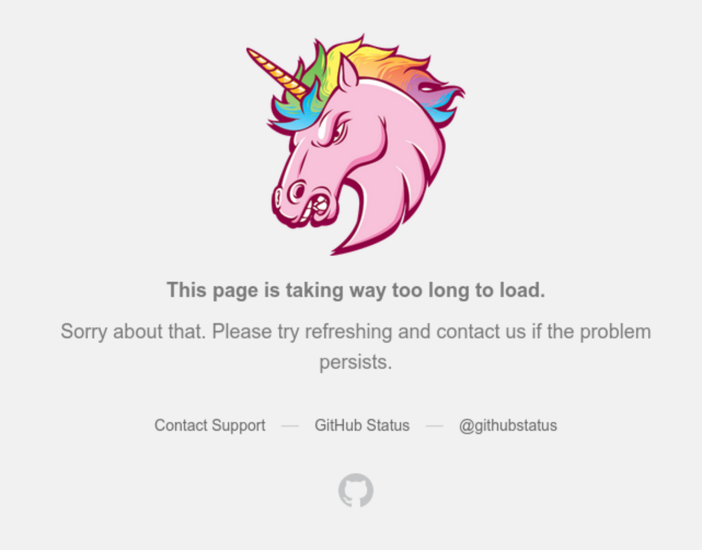
In year 2010, Google released a statement about the company new approach in China. Google had detected a highly sophisticated and targeted attack regular basis on Google corporate infrastructure originating from China. Google stated that they would no longer censor the search results on Google.cn (Jin J., 2012), which might lead to shutdown the services and the office in China.

Figure 1: People of China express sadness because of Google leaving China.

Currently, most products from Google is inaccessible in China, The China Government use their firewall (widely known as The Great Firewall) to blacklist Google products. More information about the blacklist is available at Google Transparency Report (Google Inc., 2015).

3.2. Story about GitHub

GitHub is a web based Git repository hosting service. It offered version control and source code management features to developers. Beside that, GitHub also provide certain features beyond the Git standard services, which is bug tracker, access control, documentation of repository and also private pages for each project.


This page is taking way too long to load.

Sorry about that. Please try refreshing and contact us if the problem persists.

Figure 2: GitHub is unable to access from March 26th to March 31th, 2015.

A few months ago, GitHub faced Distributed Denial of Service attack (GitHub Inc, 2015) for whole week. The attacker targeted certain Github project which is used to bypass the censorship of China. A report stated that the malicious Javascript returned by Baidu servers as the source of the attack. Several previous technical reports (NETRESEC, 2015) suggested that The Great Firewall of China (Great Firewall) orchestrated these attacks by injecting malicious Javascript into Baidu connections as they transited China’s network border.

3.3. Overview of The Great Firewall and The Great Cannon

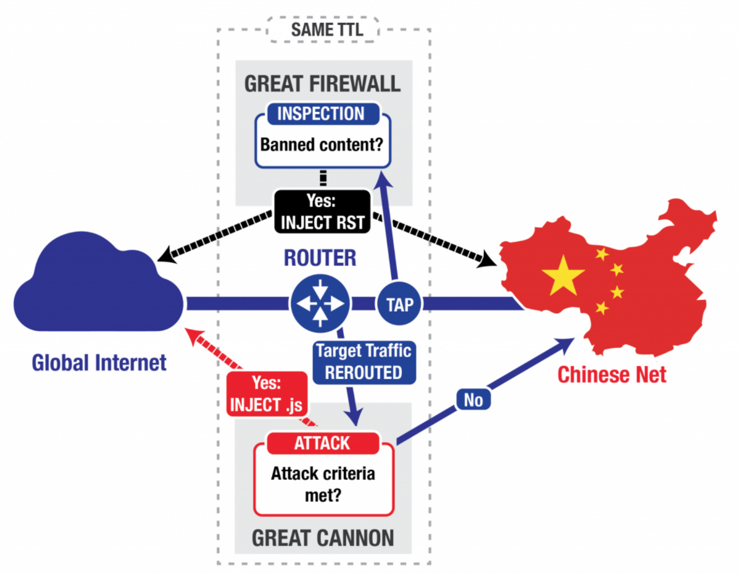


Figure 3: A simplified logical topology of the Great Cannon and Great Firewall

Recent research by Marczak B. & Weaver N. (2015) showed that the Great Firewall and the Great Cannon is two different system which share same codebase in certain part.

In general, firewall should be used as in-path barrier between networks, but the Great Firewall is an on-path system which eavesdrops the traffic between China and the world, terminates requests for banned content by injecting a series of forged TCP Reset(RST) packets that tell both the requester and the destination to stop communicating regardless of the actual destination server. The Great Firewall also keeps track of connections and reassembles their packets to determine if it should be blocked.

The Great Cannon is an in-path system, it is not only able to inject traffic, it can be suppressing traffic as well which able to act as man-in-the-middle(MITM) for targeted traffic.

4. The Great Firewall

The Great Firewall of China is a blanket term with ironic connotations thought to have been coined in an article in Wired magazine (Geremie R., 1997) and used by international to refer to legislation and projects initiated by the China government that attempt to regulate the internet in Mainland China. It is the main instrument to achieve Internet censorship in China. These regulations include criminalizing certain online speech and activities, blocking from view selected websites, and filtering keywords out of searches initiated from computers located in Mainland China.

4.1. How Great Firewall Works

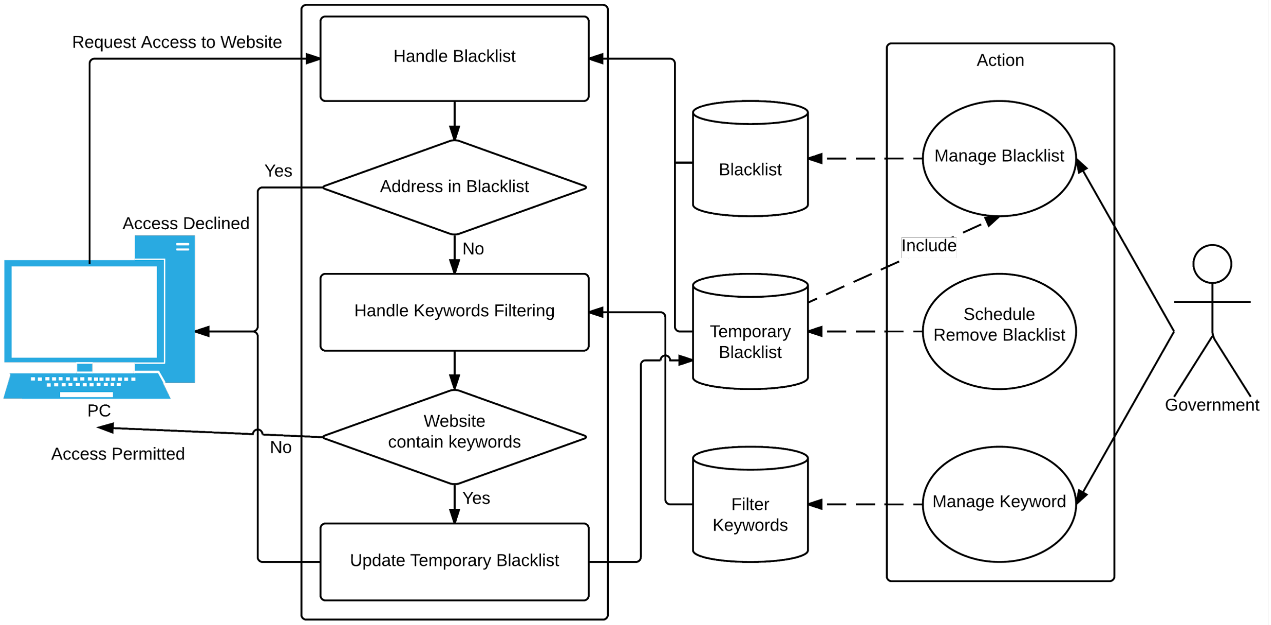


Figure 4: Mechanism of The Great Firewall (unofficial)

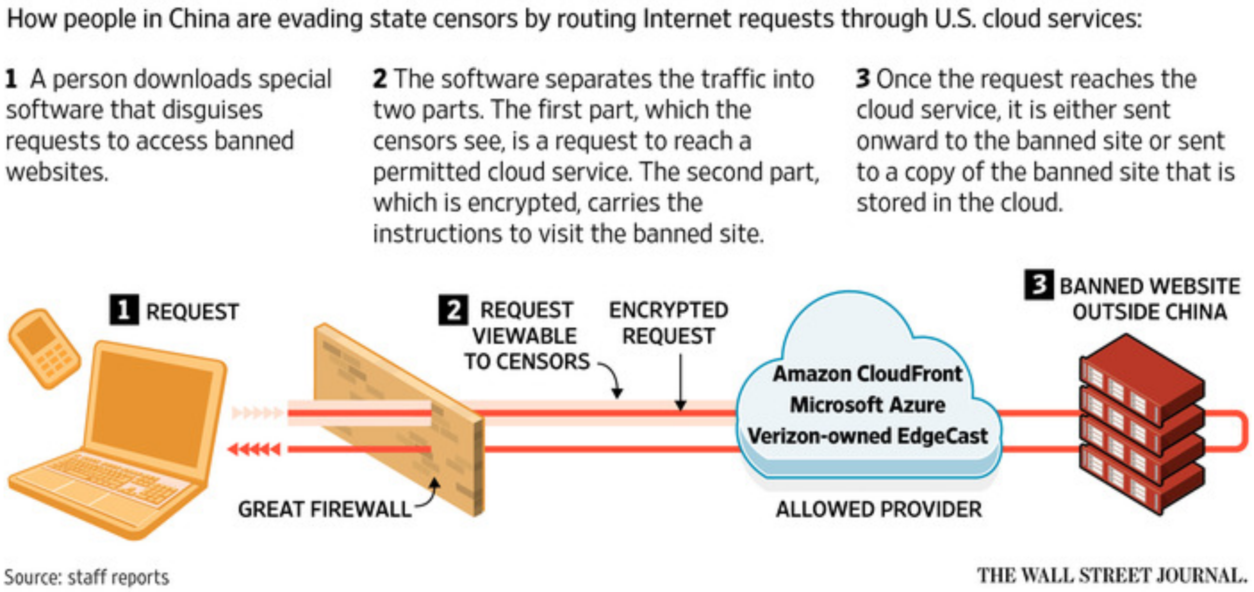
In general, The Great Firewall consists of a few type of functionality for censorship purposes (Feng G.C., 2012). Basically, the author can separate them into two categories, which is blacklist and keywords filter.

When a user from China request access to a website, the firewall will check it against the blacklist in the system, if the website is not blacklisted, the system will examine the packet from the website to determine whether it contains certain keywords which is filtered by the government for censorship purposes. If the website do contain certain keywords, the system will be temporary blacklist the website and send TCP Reset(RST) packet to both user and server in order to terminate the connection. In otherwise, the connection will have established.

4.2. Bypass methods

Although the Great Firewall is an advance technology which is able to grow over time, but the government can't simply block all the services from overseas due to certain services are quite useful and China does not have a local version of those services, which lead to the holes of the firewall system.

Popular cloud hosting services like Amazon Web Server, Microsoft Azure and Google Cloud Platform is used by a lot of international companies as well as China companies. If the government blocked either one of the website used above hosting, it might lead to unstable and unable to connect to other website using similar hosting.



How people in China are evading state censors by routing Internet requests through U.S. cloud services:

1 A person downloads special software that disguises requests to access banned websites.

2 The software separates the traffic into two parts. The first part, which the censors see, is a request to reach a permitted cloud service. The second part, which is encrypted, carries the instructions to visit the banned site.

3 Once the request reaches the cloud service, it is either sent onward to the banned site or sent to a copy of the banned site that is stored in the cloud.

Source: staff reports

THE WALL STREET JOURNAL.

Figure 5: How to bypass The Great Firewall

Below are a few methods of bypassing the author is going to discuss about,

4.2.1. Proxy Server

proxy server is a server that acts as an intermediary for requests from clients seeking resources from other servers. A client connects to the proxy server, requesting services from a different server which facilitating access to content on the World Wide Web and providing anonymity.

GoAgent using the Google App Engine to browse blocked information, each instances we created in Google App Engine do provide 1GB bandwidth daily, if the user creates a few instance, which should be enough for the user to browse censored websites for whole day.

4.2.2. Tor Network

Tor directs Internet traffic through a free, worldwide, volunteer network consisting of more than six thousand relays to conceal a user's location and usage from anyone conducting network surveillance or traffic analysis and protect the personal privacy of users, as well as their freedom and ability to conduct confidential communication by keeping their Internet activities from being monitored.

There is no evidence of Tor anonymity network is able to circumvention the Great Firewall, because Tor is relay on its global public lists of IPs, the firewall can simply download the list and blacklist all of them (Ensafi R., 2015).

4.2.3. Virtual Private Network (VPN)

Virtual Private Network is a network that is constructed by using the Internet to connect to a private network, such as a company's internal network. There are a number of systems that enable you to create networks using the Internet as the medium for transporting data. Mostly, people often use VPN as the tools to achieve anonymity and access to the blocked websites, for example the author can access to Netflix by using VPN to fake my location to the United States.

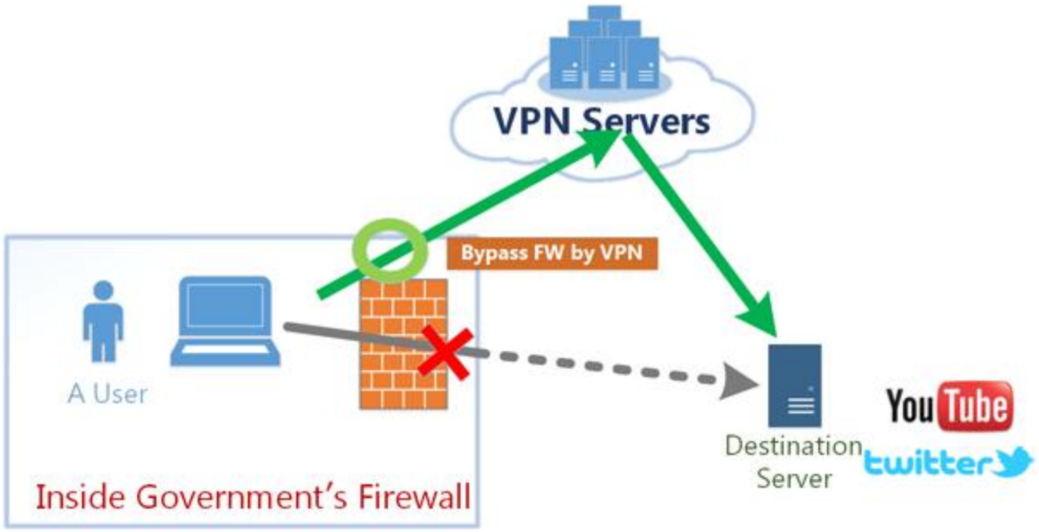


Figure 6: Using VPN to bypass firewall

Beside that, VPN can be used to bypass the Great Firewall, most multi-national company in China is using VPN to connect with other branches outside of China, which lead to the government can't block the port for VPN.

VPN is not the best solution to bypass the Great Firewall due to the Great Firewall can detect and analysis the traffic going to particular VPN server and temporary blacklist the VPN for the system administrator to check whether the IP address should be whitelisted or permanent blacklisted (Arthur C. 2012).

5. The Great Cannon

The Great Cannon is an attack tool that is used to launch distributed denial-of-service attacks on websites by intercepting massive amounts of web traffic and redirecting them to targeted websites. While it is co-located with the Great Firewall, the Great Cannon is "a separate offensive system, with different capabilities and design." The Great Cannon hijacks foreign web traffic intended for Chinese websites and re-purposes them to flood targeted web servers with enormous amounts of traffic in an attempt to disrupt their operations (Marczak B. & Weaver N. 2015).

The Great Cannon is also capable of monitoring web traffic and distributing malware in targeted attacks in ways that are similar to the Quantum Insert system used by the U.S. National Security Agency (Lorenzo F. B., 2015).

5.1. How Great Cannon works

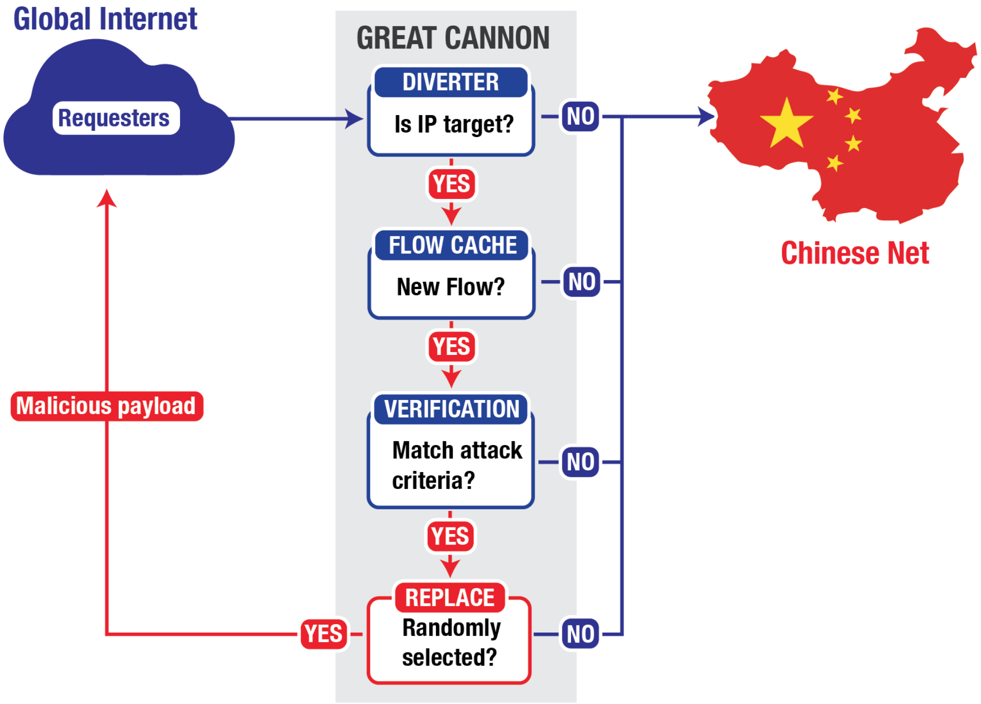


Figure 7: Mechanism of The Great Cannon

The Great Cannon examines individual packets in determining whether to take action, avoiding the computational costs of TCP byte stream reassembly. The Great Cannon also maintains a flow cache of connections that it uses to ignore recent connections it has deemed no longer requiring examination.

Similar to the Great Firewall, the Great Cannon also uses a multi-process design, with different source IP addresses handled by distinct processes. The packets injected by the Great Cannon have the same peculiar TTL side-channel as those injected by the Great Firewall, suggesting that both the Great Firewall and the Great Cannon likely share some common code.

In the attack on GitHub, the Great Cannon intercepted traffic sent to Baidu infrastructure servers that host commonly used analytics, social, or advertising scripts. If the Great Cannon saw a request for certain JavaScript files on one of these servers, it appeared to probabilistically take one of two actions: it either passed the request on to Baidu's servers, or it dropped the request before it reached Baidu and instead sent a malicious script back to the requesting user. The malicious script enlisted the requesting user as an unwitting participant in the DDoS attack against GitHub.

5.2. Way of Prevention

The attack used by The Great Cannon is JavaScript Distributed Denial of Service attack, which inject malicious JavaScript to clients computer when certain criteria is met(Google Inc., 2015).

Which is able to be prevent by using technique stated below,

5.2.1. User

The Great Cannon is an attack tools created by China government to protect the censorship in the country. As an user, you can choose not to use any services that is related to China, which might be able to prevent the JavaScript injection occurred in the user computer, but this technique is almost impossible to perform, as if you can eliminate the injection from China does not mean you can eliminate the same injection performed by other countries.

Although user can also turn off JavaScript in their browser, so that the injection script would not be able to run, but nowadays, most websites are built with JavaScript, if user turn off the JavaScript, which mean the user have to sacrifice his user experiences in modern web.

Besides that, the user can also remove the certificate of malicious sites when there is news about this attacks. There is no permanent solutions for user to get rid of the code injection for now.

5.2.2. Server

The Great Cannon is able to inject malicious JavaScript to the server is because of the server is not encrypt their JavaScript code. Encryption for JavaScript code is not the normal practices for current web development, but it is still achievable by using some tools like jQuery encryption - jqCrypt.

Beside that, if the web server is run in HTTPS-only, which mean that the web server is run in TLS/SSL, which encrypts the transmission of JavaScript files from the server to the client. It can be free to run the whole websites in TLS/SSL mode by using CloudFlare Content Delivery Network (Sullivan N., 2015).

6. Conclusion

The author encourages that currently available websites and newly developed website to upgrade their protocols to use HTTP Strict Transport Security(HSTS) which force user to use the HTTPS connection to the server in order to prevent session hijacking and malicious JavaScript code injection as what the Great Cannon did in above example.

According to the two stories (available at Appendices), the author understand that the Internet censorship has profound social and technological implications in China. In China, there is a lot of homegrown websites which have the similarity features as those which are famous worldwide but inaccessible in the country. For example: Google - Baidu, Facebook - RenRen, Twitter - WeiBo and YouTube - Youku. Those companies had already monopolized the market in their respective field in China.

If there are more services in China is able to replace the service offered worldwide, the government might blacklist those worldwide services as it can significantly decrease the way of bypassing the Great Firewall, especially if those services are cloud hosting.

7. References

I. Jin J. (2012). Ethics, strategy and user relevance: The case of Google.cn (Response to: Google vs. China's "Great Firewall": Ethical Implications for Free Speech and Sovereignty). Elsevier, vol. 34, no. 2, pp. 182-184.

II. Google Inc (2015). Google Transparency Report - Recent and ongoing disruptions of traffic to Google products. [Online] Available at: http://www.google.com/transparencyreport/traffic/?hl=en#expand=CN (Accessed: October 21st, 2015).

III. GitHub Inc (2015). GitHub Status. [Online] Available at: https://status.github.com/messages/2015-03-31 (Accessed: October 21st, 2015).

IV. NETRESEC (2015). China's Man-on-the-Side Attack on GitHub. [Online] Available at: http://www.netresec.com/?month=2015-03&page=blog&post=china%27s-man-on-the-side-attack-on-github (Accessed: October 21st, 2015).

V. Marczak B. & Weaver N. (2015). An Analysis of China's "Great Cannon". [Online] Available at: https://citizenlab.org/2015/04/chinas-great-cannon/ (Accessed: October 21st, 2015).

VI. Geremie R. (1997). The Great Firewall of China. Wired Magazine, [Online] (Issue 5.06). Available at: http://archive.wired.com/wired/archive/5.06/china.html (Accessed: October 21st, 2015).

VII. Feng G. C. (2012). Tracing the route of China's Internet censorship: An empirical study. Elsevier, vol. 30, no. 4, pp. 335-345.

VIII. Ensafi R. (2015). Examining How the Great Firewall Discovers Hidden Circumvention Servers. [Online] Available at: https://www.cs.princeton.edu/~pwinter/pdf/ensafi2015b.pdf (Accessed: October 21st, 2015).

IX. Lorenzo F.B. (2015). The 'Great Cannon' Is China's Powerful New Hacking. [Online] Available at: http://motherboard.vice.com/read/the-great-cannon-is-chinas-powerful-new-hacking-weapon (Accessed: October 21st, 2015).

X. Arthur C. (2012). China tightens 'Great Firewall' internet control with new technology. [Online] Available at : http://www.theguardian.com/technology/2012/dec/14/china-tightens-great-firewall-internet-control (Accessed: October 21st, 2015).

XI. Crotty J. M. (2015). How The Great Firewall Prevents China From Becoming A World Education Power. [Online] Avalaible at: http://www.forbes.com/sites/jamesmarshallcrotty/2015/04/15/how-the-great-firewall-prevents-china-from-becoming-a-world-education-power/ (Accessed: October 21st, 2015).

XII. Google Inc. (2015). Google Online Security Blog. [Online] Available at: https://googleonlinesecurity.blogspot.com.au/2015/04/a-javascript-based-ddos-attack-as-seen.html (Accessed: October 21st, 2015)

XIII. Sullivan N. (2015). An introduction to JavaScript-based DDoS [Online] Available at: https://blog.cloudflare.com/an-introduction-to-javascript-based-ddos/ (Accessed: October 21st, 2015)

8. Appendices

8.1. Article I - Google Quit China

On January 12, we announced on this blog that Google and more than twenty other U.S. companies had been the victims of a sophisticated cyber attack originating from China, and that during our investigation into these attacks we had uncovered evidence to suggest that the Gmail accounts of dozens of human rights activists connected with China were being routinely accessed by third parties, most likely via phishing scams or malware placed on their computers. We also made clear that these attacks and the surveillance they uncovered—combined with attempts over the last year to further limit free speech on the web in China including the persistent blocking of websites such as Facebook, Twitter, YouTube, Google Docs and Blogger—had led us to conclude that we could no longer continue censoring our results on Google.cn.

So earlier today we stopped censoring our search services—Google Search, Google News, and Google Images—on Google.cn. Users visiting Google.cn are now being redirected to Google.com.hk, where we are offering uncensored search in simplified Chinese, specifically designed for users in mainland China and delivered via our servers in Hong Kong. Users in Hong Kong will continue to receive their existing uncensored, traditional Chinese service, also from Google.com.hk. Due to the increased load on our Hong Kong servers and the complicated nature of these changes, users may see some slowdown in service or find some products temporarily inaccessible as we switch everything over.

Figuring out how to make good on our promise to stop censoring search on Google.cn has been hard. We want as many people in the world as possible to have access to our services, including users in mainland China, yet the Chinese government has been crystal clear throughout our discussions that self-censorship is a non-negotiable legal requirement. We believe this new approach of providing uncensored search in simplified Chinese from Google.com.hk is a sensible solution to the challenges we've faced—it's entirely legal and will meaningfully increase access to information for people in China. We very much hope that the Chinese government respects our decision, though we are well aware that it could at any time block access to our services. We will therefore be carefully monitoring access issues, and have created this new web page, which we will update regularly each day, so that everyone can see which Google services are available in China.

In terms of Google's wider business operations, we intend to continue R&D work in China and also to maintain a sales presence there, though the size of the sales team will obviously be partially dependent on the ability of mainland Chinese users to access Google.com.hk. Finally, we would like to make clear that all these decisions have been driven and implemented by our executives in the United States, and that none of our employees in China can, or should, be held responsible for them. Despite all the uncertainty and difficulties they have faced since we made our announcement in January, they have continued to focus on serving our Chinese users and customers. We are immensely proud of them.

(link: https://googleblog.blogspot.com.au/2010/03/new-approach-to-china-update.html)

8.2. Article II - GitHub Faced DDoS Attack

We are currently experiencing the largest DDoS (distributed denial of service) attack in GitHub.com's history. The attack began around 2AM UTC on Thursday, March 26, and involves a wide combination of attack vectors. These include every vector we've seen in previous attacks as well as some sophisticated new techniques that use the web browsers of unsuspecting, uninvolved people to flood GitHub.com with high levels of traffic. Based on reports we've received, we believe the intent of this attack is to convince us to remove a specific class of content.

We are completely focused on mitigating this attack. Our top priority is making sure GitHub.com is available to all our users while deflecting malicious traffic. Please watch our status site or follow @githubstatus on Twitter for real-time updates.

(link: https://github.com/blog/1981-large-scale-ddos-attack-on-github-com)