Understanding and Circumventing The Great Firewall of China

Lisa Fan

Mentor: Ming Chow

12/12/15

Abstract

The “Great Firewall of China” is nowadays almost as famous as the country’s original Great Wall. However, not many people know exactly how the government blocks and monitors foreign content and user access. In this paper, I will discuss both the methods taken by the government to censor content, as well as current methods for circumventing the firewall. I will start with a brief history of internet censorship in China, then examine the current state of the firewall. Specifically, I will look out how the firewall is set up, and how the government monitors its citizens’ internet access. Then, I will discuss the current techniques being used to circumvent the firewall, including VPNs, proxy servers, and popular applications. Finally, the paper will consider the implications of internet censorships, including the morality, citizen response, and future outlook, as well as comparisons against internet censorship in other countries.

To the Community

The Great Firewall of China affects the everyday lives of over a billion people. Understanding the various ways to circumvent it is not only useful for us American students who may one day travel to China, but also from a moralistic perspective, in realizing the extent to which Chinese citizens must go to gain freedom to information. By studying how the Firewall is implemented, we can also become more vigilant of potential censorship happening in the United States. For example, the rejected SOPA bill of 2013 would have opened the door to deep packet inspection and DNS poisoning, both utilized in China[1]. This paper will also shed light on some common attacks and tools used on the various layers of the internet.

I. Introduction

The internet in the People's Republic of China has been censored almost since it first became publicly accessible. What started as the censoring of major groups of political opposition, such as Voice of America and human rights groups, now spans major foreign websites such as Google and Facebook[2]. The Great Firewall of China (GFW) in recent years has been used not only as a method of blocking information within the country, but a means to attack foreign sites, as was in the case of the DDoS attack on GitHub in 2015[3]. While both companies and individuals have been developing ways to circumvent the GFW, the government is simultaneously working to shut down these loopholes.

II. History

The first systematic blocking of web content in China occurred in 1996, when several Chinese dissident sites and Western news sites were banned using a filtering system. This happened a year and a half after the internet was made publicly accessible in China in January of 1995. Since then, major sources of information, like Google and YouTube, and social media sites such as Facebook and Twitter have also been banned by the National Information Security Management System, colloquially known as the Great Firewall[2]. In addition to lack of access to these sites, communications between users on messaging boards and messaging applications have been known to be surveilled and censored.

III. Current Status

The current GFW blocks information using three main methods: DNS Poisoning, IP Address blocking, and filtering URLs and TCP packets for sensitive keywords via deep packet inspection. In addition, the newly created "Great Cannon" utilizes foreign traffic to conduct DDoS Attacks on foreign websites.

A. DNS Poisoning

One of the ways by which China censors its internet is a technique called DNS Poisoning[4]. When a user types the URL of a site they'd like to visit in their browser, it first

contacts a Domain Name System server to resolve the human-readable URL into a numerical IP address, which the computer then accesses. Recent resolutions are cached both on your local computer as well as in the Internet Service Provider's DNS server. Therefore, if a cached address is modified to point to an incorrect IP address, the user will unintentionally be directed to that wrong IP Address in the future. If the modification happens on a DNS server at the ISP level, that "poisoned" address may spread when other DNS servers and local computers request that address. Internet Service Providers in China intentionally caches incorrect addresses in their DNS servers for target websites such as Twitter and Facebook, thereby making it impossible for users within the country to access these websites through their URL.

B. IP Address Blocking

One way to circumvent China's DNS Poisoning is by accessing the IP address of a website directly if it is known, therefore bypassing the DNS lookup. However, China also blocks certain IP addresses directly. This is done by dropping packets going to and coming from the blocked IP address, again at the ISP level[4]. The destination and origin IP address of a packet can easily be found in its header. This relies on the list of blocked IP addresses to be up to date and relevant, and users can access a website that moves to or acquires a new IP address through that new address until that address is also blocked.

C. URL/Packet Filtering

The Chinese Firewall also blocks content by filtering URLs and TCP packet payloads[4]. If a user requests a URL with a banned keyword, or requests a webpage that contains a keyword, the packets are dropped and do not reach the user. This means that while access to non-sensitive portions of that site may be still reachable (ex. searching for "flowers" in a search engine), other specific searches may fail (ex. searching "democracy"). In addition, the GFW will send TCP reset packets to both the client and the server, thus closing the connection between the two points. However, some sites circumvent the monitoring of keywords by using HTTPS, which encrypts the payload and thus makes the keyword unreadable in the packet, or by escaping the URL so that the keywords are not readable in plain text. The Firewall has countered this circumvention by banning sites such as Wikipedia completely using the aforementioned IP address blocking, thus even blocking harmless material.

D. DDoS Attack

More recently, the Golden Shield Project has evolved not only to block foreign content from coming into the country, but also to attack foreign websites. In 2015, a new system dubbed The Great Cannon was used to perform a Distributed Denial of Service Attack on anti-censorship website GreatFire.org and the American Git repository website Github.com[3]. In a DDoS attack, an attacker infects multiple systems to act as "zombies" that in turn send traffic to the actual target system in order to flood the target system's network. The Cannon works as an in-path barrier, which means all traffic between the outer world and China must flow through the Cannon. With the 2015 attacks, the Great Cannon returned a malicious script to a small percentage of out-of-country users trying to access a server of Baidu, a large Chinese website. Thus, the user unwittingly becomes a zombie in the DDoS attack.

IV. Circumvention

Despite the methods identified in the section above, Chinese internet users have been known to use VPNs, proxies, and the software Tor to circumvent the Firewall. In addition to individual users, large companies such as Wikipedia and Google have also taken steps to evade the Firewall.

A. VPNs

The most common way users get around the Firewall is by using paid Virtual Private Networks. The user connects his or her computer to the network, and that network encrypts the user's requests and sends them to a foreign server, which processes the actual request. The request is able to bypass the Firewall because it is encrypted. Although VPNs are relatively inexpensive to purchase access for, and are used widely both by organized companies and individuals, the Chinese government is beginning to shut them down. Currently being targeted is the Point-to-Point Tunneling Protocol and the Layer 2 Tunneling Protocol, which are two common implementations of a VPN. Researchers believe that machine learning is being used to analyze and identify encrypted packets as those encrypted via these tunneling protocols[5]. However, a complete ban on all VPNs seems unlikely in the foreseeable future, since it is believed that all major companies in China utilize VPNs to conduct business[6].

B. Web Proxies and P2P Methods

Web proxies are also very widely used. Unlike a VPN, a proxy server operates through the browser, connecting a Chinese user's machine with a server located outside the country, and masks that user's IP address with the server's IP address. Although the use of a web proxy is typically free, and one proxy server can host a large number of users (whereas every individual using a VPN has their own private channel), the caveat is that using a web proxy slow down processes immensely, since the requests must first be transmitted to the foreign proxy server[7].

Internet users also make use of peer-to-peer (P2P) methods for jumping the Great Firewall. Two specific tools are Freegate and VPN gate. Freegate accesses DynaWeb, a network of P2P proxy servers. DynaWeb evades the Firewall through its constant changes: "It has hundreds of mirror sites at anytime, and each with a varying IP and DNS domain name, to defeat IP blocking and DNS hijacking. On the backstage, DynaWeb also has mechanisms to proactively monitor the blocking status of each of its mirror sites, and as soon as blocking is detected, it will change the IP and DNS domain name instantly."[8] DynaWeb also has features that easily alert a user of any updates to their system. On the other hand, like the name suggests, VPN gate is more similar to the VPNs mentioned in the above section in its implementation. VPN gate consists of a network of VPNs that are hosted by volunteering peers rather than servers[9].

C. Tor

A once common method of circumvention was using the free software Tor. The software encrypts and relays a user's connection in order to anonymize and secure data. The Firewall has countered this by inspecting packets for the "unique sequence of code" that identifies the handshaking protocol of connecting to the Tor network, and blocking further communication between those two endpoints if identified. While Tor has been blocked by the Firewall since 2012, the software is still used for circumvention with the help of tools that fragment packets to break up the unique code sequence, or tools like Obfsproxy, which mask the sequence[10].

D. Company Resistance

Steps to evade China's Firewall are not only being taken by individuals, but also by large corporations. One such website is Wikipedia, whose founder Jimmy Wales conducted an interview with anti-censorship site GreatFire.org. Wikipedia defaulted to using only HTTPS in

order to avoid the aforementioned keyword filtering. This has resulted in the entire site being blocked completely. Wikipedia's stance is that it prefers to be blocked entirely than to compromise to censorship[11]. Another company that has a more complex history with China's censorship is Google. After a directed cyber attack in 2010, Google ended its policy of self-censoring Google.cn, the Chinese version of the site, and moved their servers to neighboring Hong Kong[12]. In addition, Google created a new feature which warned users querying a sensitive keyword and suggested alternate queries that would not be blocked[13]. However, since last year, Google has also been completely blocked in China.

V. Implications and Observations

A. Chinese citizens' response

The reaction that Chinese citizens have towards the Great Firewall has been mixed. There are certainly users who detest the censorship, who have gone as far as to create a site like GreatFire.org, which directly protests the Firewall. On the other hand, several studies have found that a large number of the population only views the censorship as a minor nuisance: "Instead of Google, there's Baidu. If we can't get on Twitter, we can use Weibo. There are plenty of domestic platforms to share personal photos and videos."[14] Furthermore, a study in 2014 found that 76% of their Chinese poll takers believed they were "free from government surveillance" on the internet, and that 45% believed they could freely express their opinions online[15]. I believe that this lack of awareness of the censorship could be attributed to the fact that the Chinese internet has been censored nearly since its inception, thus, citizens are unaware of any difference to "free" internet. The Chinese Firewall also does not explicitly inform users that information is being censored, blocked content merely shows up as an error message.

B. Comparison to other country-wide censorship

China is not the only country with internet censorship. Reporters Without Borders, a freedom of speech organization, identified 19 countries that censor their internet in the 2014 edition of their yearly "enemies of the internet" report, with the majority of the countries located in Asia and the Middle East[16]. However, also on the list was the US, with the organization citing the Snowden leaks of NSA surveillance as an abuse of government power. Two years ago, when the US proposed the Stop Online Piracy Act, citizens were alarmed by the bill's potential to be

used for censorship. While the bill was directed towards sites that distributed copyrighted media, the technologies that would have been necessary to support the bill would have been very similar to the ones used in creating the Great Firewall of China[1].

Application

For my supporting material, I created a poster that summarizes the main points brought up in this paper, in particular the various methods for implementing and circumventing the Great Firewall of China. My hope is that the information will be general enough that non-technical readers will be able to understand the high-level concepts, and detailed enough that technical readers will have a better understanding of the technologies behind the Firewall. I also hope that through a summary of the comparison to US internet censorship, readers will begin to think about the Chinese censorship issue as more than just an foreign problem that doesn't concern us here in the US.

Conclusion

The Great Firewall of China has been around almost since the release of the public internet in 1995, and improvements are made frequently to make the blocking of information more precise and thorough. In this paper, we discussed methods of both implementing and circumventing the GFW. The Firewall works by DNS poisoning its own servers so that blocked website URLs are not directed to the corresponding IP address. The Firewall also blocks IP addresses flat out by identifying destination addresses during deep packet inspection. Deep packet inspection is also used to identify sensitive keywords in destination URLs and packet payloads. Recently, the GFW has gone on the offensive with "the Great Cannon," which forces foreign users to act as zombies in DDoS attacks. Chinese internet users evade the Firewall by using paid VPNs, which establish a private network for each user, or by using web proxies, which connects a user to a foreign server through the web browser. Other methods discussed were peer-to-peer methods, which rely on foreign volunteers, and using the software Tor, with some tools and bridges to make it usable in China. Also discussed were how major companies are resisting the policy, whether through subtle actions or bold statements. As an American student, it is important to study the topic of internet censorship in China not only to understand the technologies being implemented around the world, but also to consider the morality of the issue, and to be aware of how these same technologies may affect us in the US in the near future.

Citations

[1] McCullagh, Declan. "Vint Cerf: SOPA means' unprecedented censorship'of the Web." *CBNET News* (2011).

[2] "The Art of Concealment." The Economist. The Economist Newspaper, 06 Apr. 2013. Web. 13 Dec. 2015.

[3] Marczak, Bill, et al. "China's Great Cannon." *Citizen Lab, University of Toronto, Technical Report* (2015).

[4] Clayton, Richard, Steven J. Murdoch, and Robert NM Watson. "Ignoring the great firewall of china." *Privacy Enhancing Technologies*. Springer Berlin Heidelberg, 2006.

[5] Grey One. "The Best VPN For China (Updated December 2015)." GreyCoder. N.p., 4 Oct. 2015. Web. 13 Dec. 2015.

[6] Fallows, James. "The connection has been reset." *Atlantic Monthly* 301.2 (2008): 19.

[7] "How to Use Proxies in China to Bypass Blocks and Filters." GhostProxies Blog. N.p., 30 Sept. 2015. Web. 13 Dec. 2015.

[8] http://www.dit-inc.us/dynaweb.html

[9] http://www.vpngate.net/en/about_overview.aspx

[10] Winter, Philipp, and Stefan Lindskog. "How the great firewall of china is blocking tor." *Free and Open Communications on the Internet* (2012).

[11] Charlie. "GreatFire Q&A with Jimmy Wales on China Censorship."GreatFire.org. N.p., 4 Sept. 2015. Web. 13 Dec. 2015.

[12] Helft, Miguel, and David Barboza. "Google shuts China site in dispute over censorship." *NY TIMES, Mar* 22 (2010).

[13] Worstall, Tim. "Google's Very Clever Reaction to Chinese Censorship."Forbes. Forbes Magazine, 1 June 2012. Web. 13 Dec. 2015.

[14] Xuecun, Murong. "Scaling China's Great Firewall." The New York Times. The New York Times, 18 Aug. 2015. Web. 13 Dec. 2015.

[15] Keck, Zachary. "Chinese Don't Believe They're Being Watched and Censored." The Diplomat. N.p., 3 Apr. 2014. Web. 13 Dec. 2015.

[16] http://12mars.rsf.org/2014-en/