Cyber Kung-Fu: The Great Firewall Art of DNS Poisoning

February 23, 2015

February 23, 2015

Adam Kozy Research & Threat Intel

Wing Chun (咏春拳), the first Chinese martial art learned by the legendary Bruce Lee, is often best known for its principles of simultaneous attack and defense. This experience later inspired him to create his own style of “gong-fu” in the U.S., Jeet Kune Do (截拳道) – literally, “Way of the Intercepting Fist”. It appears that this philosophy of interception and redirected attacks has come back to roost in China in cyber form. China has been using DNS poisoning to redirect users attempting to access censored sites to legitimate sites it wants to take down via Distributed Denial of Service (DDoS) attacks.

Recently observed activity shows that the infamous censorship apparatus the Great Firewall of China (GFW – 中国防火长城) changed its method of redirecting users from sites deemed dangerous by the Chinese Communist Party (CCP). Previous to early January 2015, users within China trying to access restricted sites such as Facebook, Google, and Twitter were simply redirected to a block of IP addresses, many of which were nonexistent. After a short while, users would receive a timeout message or an error message saying the website was unavailable.

This form of DNS poisoning was fairly easy to route around, since the GFW used a small subset of IPs to redirect traffic; users quickly developed anti-poisoning tools[1] that recognized the few fake IP addresses and automatically circumvented the block. However, the new upgrade has adopted a new strategy: redirecting users to random **real** IP addresses. This makes it much more difficult for anti-censorship supporters to develop anti-poisoning tools, since the IPs are random and there are no discernable patterns. Around the same time, several of the most popular VPN services in China (which hundreds of thousands of business owners and academics use everyday to access sites like YouTube and Google) became unavailable as the Cyberspace Administration of China (CAC) appeared to tighten its grip on normal workarounds.[2]

Possibly more disturbing than the idea of China once again suppressing its masses with remarkable efficiency is what China has been doing with its newfound method of censorship. Early January 2015 reporting indicates that after the GFW was believed to have been upgraded, thousands of Chinese Internet users attempted to visit censored sites and were instead directed to a variety of sites.[3] In one case, the destination was a German pornographic site, something that would normally be outlawed in China as pornography is illegal.

Other “random” candidates included a government site in South Korea, an American firewall and security company, and a French digital freedom association, among countless others. It was confirmed on all victims except the South Korean government site that the traffic caused a DDoS attack as servers not normally prepared to handle that kind of traffic were suddenly pummeled with traffic redirected from China. Since hosting with DDoS protection like Cloudflare and Arbor Networks is often not yet affordable to many of these smaller sites, most of these system admins were left to deal with the massive problem on their own. [4] [5]

The sites mentioned above are particularly interesting as they each hold some interesting possibilities for what this DNS poisoning and DDoS combination can do. The South Korean government site shows the ability for China to potentially knock foreign government sites offline by simply redirecting traffic for a brief period and claiming a “glitch” caused the attack. This carries serious implications, especially if the DDoS attack is directed at an election site, which was a tactic CrowdStrike observed several times in 2014 and that had an impact on democratic elections. The DDoS attack on the American firewall company was also interesting as it shows the ability to gauge a security company’s response to attacks, possibly in advance of further cyber action against the security firm’s customers.

The most disturbing by far, however, is the attack against the French digital freedom site, as it shows the potential for China to not only censor its own citizens, but then also use them to censor other sites that advocate digital freedom[6] with DDoS attacks, in essence becoming a self-perpetuating censorship machine. With more than 632 million Chinese Internet users[7] and a censorship juggernaut capable of censoring the majority of that population, China has effectively turned the GFW into the largest botnet in the world. And like all good botnets, its host of “zombie users” are most likely blissfully unaware of their involvement in the attacks. This was reiterated as several of the DDoS victim sites voiced their feelings of frustration and helplessness in public blogs, only to have Chinese netizens respond by saying they felt “ashamed” that the attacks were connected to the GFW.

All of this comes on the heels of what appears to be a giant consolidation of power by the CAC and new head LU Wei (鲁炜).[8] This has manifested over the past several months with a December 2014 CAC takeover of the China Internet Network Information Center (CNNIC), which is a designated certificate authority. There were also several Man-In-The-Middle (MITM) attacks against mail users from Yahoo, Google, and Apple during late 2014, before another attack was carried out against Microsoft Outlook in January 2015 with some fairly damning evidence pointing the finger at the CAC provided by anti-censorship site GreatFire.org.[9] Finally, the crackdown on popular VPN services in late January 2015 indicates that this is a coordinated campaign to suppress and censor not just domestically, but overseas as well. China is no longer harnessing only an attractive, rapidly growing tech market as leverage over foreign countries and companies hoping to do business in China, but now also its own citizens.

The fact that the GFW sprang out of something called the “S219/Golden Shield Project” makes it clear this notion of simultaneous attack and defense suits China well, and that it will likely continue to use its existing strengths of a large population and the world’s most restrictive censorship apparatus to its advantage.

Turns out using a shield as a weapon isn’t just for Captain America anymore.

[1] https://github.com/ihacku/gfw_dns_resolver/blob/master/gfw_dns_resolver.c
[2] http://cn.nytimes.com/china/20150130/c30chinainternet/
[3] https://en.greatfire.org/blog/2015/jan/gfw-upgrade-fail-visitors-blocked-sites-redirected-porn
[4] http://blog.sucuri.net/2015/01/ddos-from-china-facebook-wordpress-and-twitter-users-receiving-sucuri-error-pages.html
[5] http://furbo.org/2015/01/28/grass-mud-horse/
[6] https://benjamin.sonntag.fr/DDOS-on-La-Quadrature-du-Net-analysis
[7] CNNIC June 2014 estimate
[8] http://www.washingtonpost.com/blogs/worldviews/wp/2015/02/02/why-internet-users-all-around-the-world-should-be-worried-about-chinas-great-firewall/
[9] https://en.greatfire.org/blog/2015/jan/open-letter-lu-wei-and-cyberspace-administration-china

Related Content

Who is EMBER BEAR?

A Tale of Two Cookies: How to Pwn2Own the Cisco RV340 Router

PROPHET SPIDER Exploits Citrix ShareFile Remote Code Execution Vulnerability CVE-2021-22941 to Deliver Webshell