On the Effects of Large-Scale DNS Poisoning

Antonio Barili
Dept. of Industrial and Information Engineering
University of Pavia
Pavia, Italy
antonio.barili@unipv.it

Dario Lanterna
Dept. of Industrial and Information Engineering
University of Pavia
Pavia, Italy
dario.lanterna@unipv.it

***Abstract*—The Great Firewall of China (GFW) has recently put in place an internet filtering scheme based on DNS injection and poisoning that may have far reaching effects on DNS servers outside China borders and that may cause DDoS-like traffic on unknowing and apparently randomly selected sites. We provide an analysis of the traffic collected during such a DDoS-like attack and of the effects of large-scale DNS Poisoning.**

***Index Terms*—DNS poisoning, DDoS traffic analysis.**

I. Introduction

Internet filtering is a widespread practice and is implemented by almost all ISP, as well as companies, schools, and governments themselves. It is quite difficult to draw a line between acceptable filtering (e.g. to stop criminal activities), trade abuse and freedom-of-speech restrictions [1,2]. While we are not going to deal with the ethical or legal problems connected to the practice, nonetheless we believe that some Internet filtering practices put in place by the Great Firewall may cause global effects on the Internet and on the DNS system itself that deserve deeper investigation [3].

II. Short Report

Starting March 6, 2015 the site under analysis was flooded by HTTP and HTTPS requests for nonexistent pages coming from some 300K+ different IP addresses, a clear symptom of an ongoing Distributed Denial-of-Service (DDoS) attack. [4,5,6,7]

After a short investigation the Web Portal was relocated to a new IP address and an honeypot was setup at the original IP address to catch and log all DDoS traffic.

The honeypot was kept online for about 2 months. At the end of the observation period we had collected about 50 GB of traffic log data.

From incident reports published online we also discovered that DDoS traffic much like the one we were experiencing had been reported by several sites [8,9,10,11] some of which had also related the traffic to the DNS poisoning feature of the so called Great Firewall of China (GFW). [12,13]

III. Honeypot Setup

The honeypot ran in a virtual machine and was configured as a standard Linux / Apache (v. 2.2.22) web server. It collected traffic data on ports 80 (HTTP) and 443 (HTTPS). *Iptables* filters dropped all network traffic directed to other ports. Kernel parameters were tuned to avoid overflows in kernel memory due to the huge amount of incoming connections.

All reported findings are based on data collected while the honeypot was in its final configuration. Traffic was mainly logged by the Apache server itself, but we also ran sample packet captures via *tcpdump* for short periods.

While all DDoS page requests packets were well formed, all of them were originally directed to servers other than ours, as flagged by the *http-host* field.

A scripted query on open Chinese DNS servers for some selected hostnames revealed that all those servers returned wrong translations.

We also collected evidence that even Google's DNS servers (8.8.4.4) had been indirectly poisoned, likely by trying to translate a request for some Chinese domain (e.g. *.yy45.com, 59d2b.545u.com).

Note that this kind of indirect poisoning may add a degree of complexity to DDoS mitigation procedures, since requests resolved by Google's DNS servers usually come from geographical zones different from China and the Far East and cannot be filtered by origin.

IV. Traffic Analysis

The DDoS flood started on March 6, 2015 and ended on May 1, 2015, a few days after we shut down the honeypot leaving its IP address unassigned. All figures provided (unless otherwise stated) are referred to the observation period going from March 31, 2015 to April 15th, 2015.

Traffic volume was stable in the range 1.5-3.0 Mb/s, far lower that the capacity of the network link of the Data Center (1 Gb/s). The overall data received averaged to 22 GB/day.

The honeypot logged more than one million HTTP and HTTPS requests per day, from about 300,000 different IP addresses, with an average number of 4.7 requests per single source IP address. The maximum number of daily requests from a single source IP address was 5,865.

Although we did not traced traffic back to its sources, we are fairly confident that IP addresses were not spoofed (IP address geolocation was performed against the *maxmind* databases at dev.maxmind.com). About 97% of all requests

came from IP addresses located in China, followed by US and Japan.

All HTTP and HTTPS requests were well-formed, but the *http-host* field did not pointed at our hostname (i.e. traffic were originally directed to another host). All requests from the sample we analyzed were meaningful if decoded in the context of the intended destination host. Possible bad registration with DNS servers were ruled out by querying authoritative servers for the intended hosts.

Requests were originally directed to 12,000+ different hosts belonging to 2,000+ different domains, per day.

V. DNS Poisoning Effects

Querying open Chinese DNS servers for misdirected hostnames, we received different answers each time, even within a minute or less.

A detailed analysis of traffic logs revealed that the Google Spider (the process that indexes sites on behalf of the Google search engine) had visited our honeypot while trying to index a site named *oyffy.aghg0088comdaili.com*.

Since the Google Spider is supposed to use Google's DNS servers (8.8.8.8 and 8.8.4.4) we hypothesized that those DNS servers had been indirectly poisoned, too.

While Chinese policies to filter some sites when accessed from China is well known , the indirect poisoning of Google DNSs shows that such policies spread their effects even outside China borders.

Additionally we found that if anyone, anywhere, tries to visit sites registered in China but apparently falling under their filtering policies (e.g. tevf.aghg0088comdaili.com), Chinese DNS servers will return a poisoned response that may eventually be cached outside China, thus adding to the poisoning spread.

VI. Conclusions

Although Chinese Internet filtering policies have been in place for a long time, the large scale DNS poisoning recently deployed can spread its effects far over GFW and China borders.

First, unknowing sites may suddenly become target of the DDoS-like traffic generated by the poisoning. It is not clear how these targets are selected, even if some author reported that traffic was directed to sites that may be perceived as hostile to the Chinese government; while some of the targets we discovered may indeed be involved in activities that may be perceived as such, the large majority of them is apparently selected at random.

Second, even if the traffic per site is not that large, some sites – especially those running application servers - may experience severe application DoS effects.

Third, the volume of traffic is so large that it may easily exhaust the monthly volume available to smaller sites in a few days, thus creating an economic DoS (EDoS) effect.

Fourth, and worse than all, DNS poisoning spreads its effects outside China borders: all open DNS servers within China and some servers that should be authoritative for Chinese domains return poisoned answers even to foreign queries, thus possibly poisoning DNS servers outside China, as shown by our Google's DNS server poisoning evidence.

On the other side, poisoned traffic could be easily spotted by checking the *http-host* field of each page request: although we could not yet get definitive evidence of that, apparently dropping misdirected traffic without answering is an effective way to get the GFW forget the target IP. Unfortunately, this mitigation procedure may only be put in place by the target server, especially on HTTPS connections, and may require significant resources.

Note

All traffic data collected is available to the research community upon request. Signature of a privacy compliance agreement is required.

References

[1] Wu, Tim. "World Trade Law of Censorship and Internet Filtering, The." Chi. J. Int'l L. 7, 2006.

[2] J. Zittrain and B. Edelman, "Internet filtering in China," IEEE Internet Comput., vol. 7, no. 2, pp. 70–75, 2003.

[3] Anonymous, "The collateral damage of internet censorship by DNS injection," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 42, no. 3, p. 21, 2012.

[4] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2. p. 39, 2004.

[5] D. Garg, "DDOS Mitigation Techniques-A Survey," *Int. Conf. Adv. Comput. Commun. Networks*, pp. 319–326, 2011.

[6] H. Kumawat, G. Meena, "Characterization, Detection and Mitigation of Low-Rate DoS attack", Proceeding ICTCS '14, Article No. 69

[7] B. Saini, G. Somani, "Index Page Based EDoS Attacks in Infrastructure Cloud", Communications in Computer and Information Science Volume 420, 2014, pp 382-395

[8] //insight-labs.org/?p=1682

[9] //blog.crowdstrike.com/cyber-kung-fu-great-firewall-art-dns-poisoning/

[10] //blog.sucuri.net/2015/01/ddos-from-china-facebook-wordpress-and-twitter-users-receiving-sucuri-error-pages.html

[11] //benjamin.sonntag.fr/DDOS-on-La-Quadrature-du-Net-analysis

[12] Lowe, Graham, Patrick Winters, and Michael L. Marcus. "The great DNS wall of china." MS, New York University, 2007

[13] Winter, Philipp, and Jedidiah R. Crandall. "The Great Firewall of China.", 2012.