Available online at www.sciencedirect.com

SciVerse ScienceDirect

Procedia Computer Science 10 (2012) 466 – 473

Procedia Computer Science

The 3rd International Conference on Ambient Systems, Networks and Technologies (ANT)

The Role of DNS TTL Values in Potential DDoS Attacks: What Do the Major Banks Know About It?

N. Vlajic, M. Andrade, U. T. Nguyen

Department of Computer Science and Engineering
York University, Toronto, Canada
vlajic@cse.yorku.ca, cse01009@cse.yorku.ca, utn@cse.yorku.ca

Abstract

In this paper, we examine the impact of DNS TTL values on the overall user experience in accessing a web site. We demonstrate that a web-site that utilizes inappropriate DNS TTL values could experience damaging and costly consequences, especially if falling victim to a DDoS attack. Subsequently, we represent the results of our survey that has looked into the DNS TTL values of the major US and EU banks. The results of this survey show that in the world of financial institutions, the level of assets and public exposure is highly correlated with the level of sophistication in DNS (Record) management. Specifically, we show that a number of (often smaller-scale) banks choose inappropriately long DNS TTL values, creating a vulnerability that could be easily exploited by an adversary.

1. Introduction

Distributed Denial of Service (DDoS) attacks are recognized as one of the most serious threats to today's Internet due to the relative simplicity of their execution and their ability to severely degrade the quality at which Web-based services are offered to the end users [1]. Based on a recent study by VeriSign, unskilled cyber criminals can now rent a swarm of infected PC's capable of tremendous online destruction for less than $9 an hour [2]. Although the motives and targets of DDoS attacks can greatly vary, the commonality of all DDoS attacks is that they involve concerted efforts to saturate the victim machine (often a web-server) with a large volume of traffic, leaving the server unable to respond to legitimate user requests. The most effective way of executing a DDoS involves the use of a system of compromised machines, the so-called botnet (see Fig. 1). Most botnets discovered so far operate in a centralized manner, with the master machine (owned and operated by the actual cybercriminal) remotely controlling a large number of infected third-party computers, also known as zombies. The execution of a DDoS is accomplished with the master instructing the zombies to send large amounts of attack traffic to the victim machine, either directly or through some form of route reflection.

doi:10.1016/j.procs.2012.06.060

Given potentially detrimental effects of DDoS attacks on web-based services, the implementation of anti-DDoS solutions is a high priority for the majority of web-based business. The most commonly implemented anti-DDoS techniques include: 1) adequate use of firewalls and intrusion-detection systems, 2) over-provisioning of bandwidth, 3) deployment of multiple physically and logically separated web-server replicas. Unfortunately, all of these techniques focus solely on DDoS mitigation on the server end of the network, and way too often the client-side (i.e., end-user side) of the DDoS problem remains overlooked. Namely, not many organizations seem to be aware of the critical role that the DNS system may play in a DDoS attack – in particular, the role of DNS Records and the way they impact the operation and/or user experience of their respective web-client population.

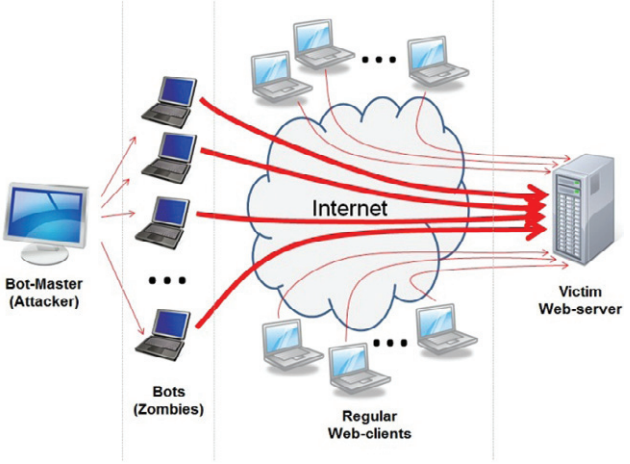

Fig. 1. A botnet executing a DDoS

In the following section, we first briefly summarize the significance of DNS Records in the process of web-page download. Subsequently, we discuss how inadequately chosen DNS TTL values can, in fact, help a cybercriminal in amplifying both short- and long- term effects of a DDoS against a web-site.

2. Impact of DNS TTL Values on Web-User Experience

As illustrated in Fig. 2, the key steps involved in the process of a web-page download include:

(1) The end-user provides the user program (typically a web-browser) with the web-page's URL comprising a symbolic name of the host server.
(2) The browser sends the server's symbolic name to the local (client OS's) DNS-resolver. The resolver looks up the local DNS-cache for a match. If a match is found, the corresponding IP address is immediately sent back to the user program. Otherwise, the resolver sends a query to the local DNS server.
(3) The local DNS server looks up its own DNS-cache for a match, and if no match is found, the query is forwarded to a higher-level DNS server. The process of query forwarding is continued until a result (i.e., a DNS Record containing a valid 'symbolic-name to IP address' mapping) is returned to the user program.
(4) Once the user program fetches the desired DNS Record, the program moves onto establishing an HTTP connection with the obtained IP address (i.e., respective server machine) and downloading the actual web-page content.

Now, an important component of each DNS Record is the so-called time-to-live (TTL) value. This value is controlled by the original (authoritative) DNS server, and represents the length of time that other DNS servers and applications are allowed to store the given DNS Record before they must discard it and, if

needed, request its new copy. In practical terms, the TTL value determines the validity period of the provided 'symbolic-name to IP-address' mapping. The choice of the TTL is typically dictated by the following:

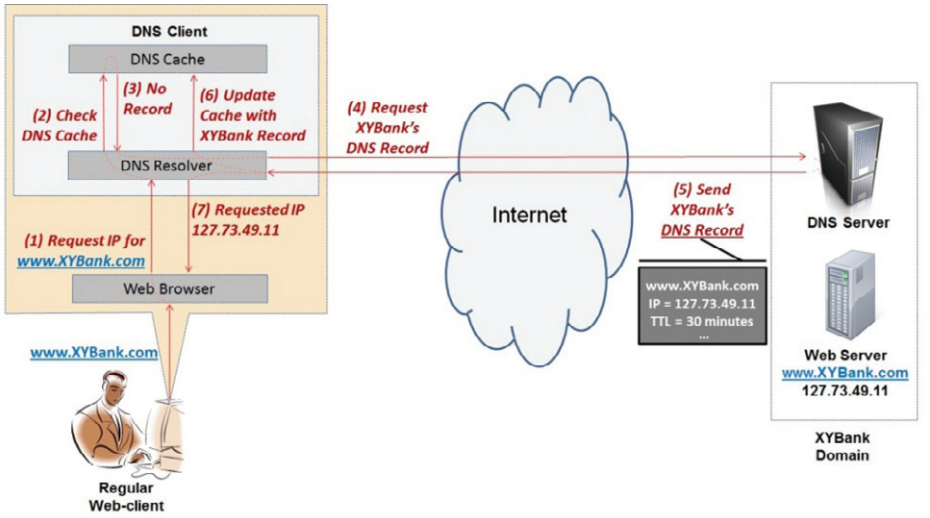

Fig. 2. Steps involved in a web-page download[a]

a) ***Frequency of updates in the web-site's content and/or the location of the host-server.*** Web-sites with static content and/or static IP mappings tend to choose long TTL values, since long TTLs are likely to result in faster web-page download for the end user. Namely, with long TTLs the DNS requests are likely to be served directly from the client's Cache or the Cache of the local DNS-server, thus avoiding the latency involved in contacting a higher-level DNS server. On the other hand, web-sites with frequently changing content and/or dynamic IP mappings tend to choose short TTL values, in order to force frequent refreshing of their DNS records and thereby achieve timely and accurate delivery of information.
b) ***Efforts to control the number of DNS lookups***. Increased load on the DNS servers – in particular the authoritative DNS servers – is an inherent consequence of short DNS TTL times. Namely, with short TTLs, DNS Records expire sooner from the clients' DNS Caches, hence a larger number of DNS requests end up being forwarded to the higher-level DNS servers. For this reason, many web-sites opt to use long TTL times as a mechanism of DNS-load balancing.

For most web-sites operating under normal conditions TTL values of 15 to 30 min (or higher) are consider optimal [3]. Nevertheless, there are situations where TTLs of this duration may have very damaging and costly consequences for an organization, such as in the case of a DDoS attack against the organization's web-site. To understand how a poorly chosen DNS TTL value can contribute to the success of a DDoS attack against a web-site, let us look at the example illustrated in Fig. 3. In the given example, we assume that a client (i.e., web user) accesses a web-site of interest (i.e., respective web-server currently running on IP_Address_1) shortly before the onset of a DDoS attack. The intensity of the DDoS is such that it cripples the server, hence after some Δt [sec] the server migrates to another location (IP_Address_2). Unfortunately, at the time of the initial access, the client's DNS resolver Caches IP_Address_1 as the server's valid IP address with the validity interval of TTL seconds. Consequently, all the client's requests generated within the next TTL seconds get forwarded to the old, currently blocked/disabled IP address (IP_Address_1). We will refer to this situation as *Faulty DNS-Cache Lock*.

[a] Communication with intermediate, higher-level DNS servers is omitted from the picture for the purposes of clarity.

The only way to resolve the *Faulty DNS-Cache Lock* is by flushing the client's DNS Cache, which can be accomplished by typing ipconfig /flushdns in the Windows console - a command likely unknown to the average web-user.[b] It is worth pointing that other actions more likely to be performed by the average user, such as: a) web-page reload, b) opening of a new tab or opening of a new browser window, c) switching to a completely different browser (e.g. from Internet Explorer to Firefox), are shown to be generally ineffective when dealing with the *Faulty DNS-Cache Lock* (see Section 5).

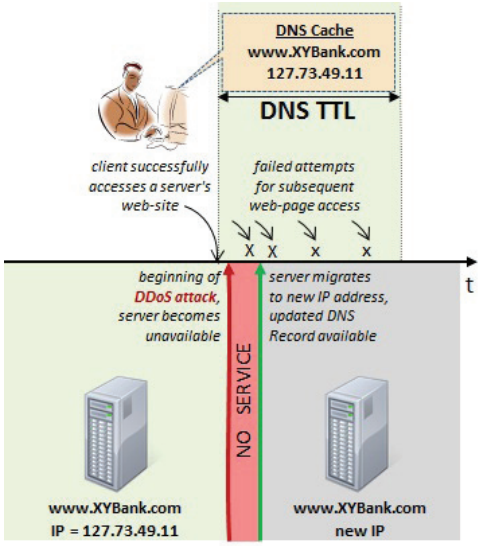

Fig. 3. Client's DNS-Cache Lock in case of DDoS attack

Fig. 3 also aims to illustrate that a long *Faulty DNS-Cache Lock* (caused by a long TTL) is likely to result in a number of repeated failed access attempts and, therefore, higher dissatisfaction and/or frustration level for the end user. A recent study [5] has shown that 37% to 49% of users who experience performance issues when completing a transaction will abandon the site and/or ultimately switch to a competitor. Similarly, a joint study by Google and Bing researchers [6] has shown that 57% of online consumers abandon a site after waiting 3 seconds for a page to load. 8 out of 10 people do not return to a site after a disappointing experience. A 2010 study by Forrester Consulting [7] has looked specifically at bank consumers and their expectations for web-site performance. The results of this study show that 75% of online consumers of financial services expect 99% or higher web-site availability, and they rank web-site performance second on a list of user expectations, right after security.

From the preceding discussion, we can draw the following conclusion: DDoS attacks on web-sites (i.e., web servers) whose DNS Records carry inappropriate long TTL values are likely to be more successful (i.e., be more detrimental to the attacked site), from both short- and long- term perspective. Namely,

a) Short-term, long DNS TTL times are statistically more likely to put a larger number of client machines into *Faulty DNS-Cache Lock* and result in a larger number of reload attempts (see Fig. 2). For a web-site under a DDoS attack, a flood of reload attempts by legitimate users will only aggravate the bandwidth

[b] Our study looks primarily at users with Windows OS, as they constitute nearly 90% of the entire Internet user population [4].

congestion and/or processing load on the server, thereby assisting the attacker in achieving his objective(s).
b) As indicated by [5], [6], and [7], long *Faulty DNS-Cache Locks* (caused by an interplay of a long DNS TTL for a web-site undergoing a DDoS), as shown in Fig. 2, are likely to have negative long-term consequences for the site (i.e., organization) in question, since user experiencing a poor web-site performance are likely to abandon the given site, switch to a competitor and/or share their negative experience with others.

3. Choosing Optimal DNS Record / TTL Strategy

The discussion of Section 2 has illustrated the complexity behind choosing an appropriate DNS Record strategy (i.e. choosing an appropriate value of DNS TTL parameter). To reiterate:

- Users accessing a web-site would generally benefit from a small TTL value in the site's DNS Record, as it would imply frequent updates of the clients' DNS Caches and good resilience in case of the site failure (possibly caused by a DDoS).
- However, with a small TTL, the number of requests, and accordingly the overall load, on the local and authoritative DNS servers could be significant. Also, studies have shown that a small TTL increases the risks of a successfully conducted DNS Poisoning Attack [8].

Now, for companies whose business critically depends on the performance of their web-sites, it is not uncommon to see the values of DNS TTLs set as low as 0 [sec]. However, such extreme lowering of TTL values is generally not recommended, since under normal operating conditions - which constitute vast majority of operating time - TTL = 0 [sec] unnecessarily increases the processing and traffic load both on the involved clients and DNS servers [9].

A more appropriate strategy of ensuring good resilience to potential web-server failure and successful dealing with the situations of *Faulty DNS-Cache Lock* (see Fig. 2) is the utilization of multiple concurrently running web-server replicas – with each replica running on a unique IP address and in a different physical location. In other words, this solution assumes that multiple IP addresses are associated with the same symbolic name, and all of the employed IP addresses are simultaneously included in the site's DNS Record. Hence, if one of the IP addresses falls victim to a DDoS attacks, the clients will have other alternative IP addresses readily available in their local (OS's) DNS Cache. This solution is very much utilized by Content Distribution Networks (CDN), and is at the heart of their strategy of achieving load-balancing and fault-tolerance for hosted web-sites [10].

4. Survey of DNS Record / TTL Strategies in Major US and EU Banks

4.1 Experimental Setup

As part of our research on the *Faulty DNS-Cache Lock* phenomenon, we have conducted a survey looking into the DNS TTL values employed in the DNS Records of some major US and EU banks. Specifically, we have surveyed the following three groups of banks:
Group A: 15 best performing US banks according to Forbes.com [11];
Group B: 15 largest US banks, in terms of their total assets, again according to Forbes.com [11];
Group C: 15 top EU banks and banking groups, according to BanksDaily.com [12].

In order to collect the above mentioned DNS TTL values as accurately as possible, we have pursued three different strategies of obtaining the respective DNS Records:
1) By conducting multiple independent downloads of the front (index) web-pages of the 45 banks in question, with Wireshark [13] running in the background and capturing the passing DNS traffic (i.e., the passing DNS Records).

2) By using nslookup utility, and acquiring the DNS Records of the 45 banks in questions from three different public DNS servers, located in three different countries/continents: resolver1.opendns.com (in USA), wew.stejau.de (in Germany), altair.usb.ve (in Venezuela).
3) By acquiring the DNS Records of the 45 banks in question using http://just-dnslookup.com/index.php. This on-line tool retrieves DNS Records of any given/requested web domain by relying on 63 monitoring servers located in various cities all over the world. A summary of the 63 obtained records is, subsequently, presented to the user.

4.2 Collected Results

A detailed list of our findings (i.e., the exact values of the retrieved DNS TTLs) are presented in Tables 1, 2 and 3. The obtained findings can be summarized as follows:

- In Group A, 8 out of 15 banks are observed employing DNS TTL values of 60 min or longer. Furthermore, all 15 banks are observed using a single 'symbolic-name to IP address' mapping in their DNS Records, which suggests that neither of the banks in this group has any provisions for web-server redundancy and/or automated web-server migration. Such findings are rather alarming, and are a likely indicator that the IT staff of the given banks are unaware of the potential dangers associated with the use of excessively long TTL values and of the risks of utilizing a single web-server. We should keep in mind, however, that most of the banks in this category are 'smaller-scale' in terms of their assets and exposure, and probably have not yet been in the position to deal with the consequences of serious DDoS attacks.
- On the other hand, in Group B, only 2 out of 15 banks are observed using DNS TTL values of 60 min and longer, while 10 out of 15 are observed using DNS TTLs of under 1 min. 6 of these banks are also observed using multiple 'symbolic-name to IP address' mappings in their DNS Records, which suggests the utilization of multiple web servers and/or provisions for server migration. Furthermore, one bank in this category is observed deploying the web-hosting service of Akamai CDN – a rather costly solution, but with the best resilience against potential DDoS attacks or accidental server failure. Clearly, when contrasted against Group A, these findings show that in the world of financial institutions, greater assets and public exposure also imply greater sophistication in terms of DNS and web-server management.
- In Group C, 5 out of 15 banks are observed using DNS TTLs of over 60 min, 4 are observed using TTLs of under 1 min, while the remaining 6 banks had TTLs ranging between 5 and 30 minutes. 3 banks in this group are observed employing multiple 'symbolic-name to IP address' mappings, while one bank relies on the web-hosting services of Akamai CDN.

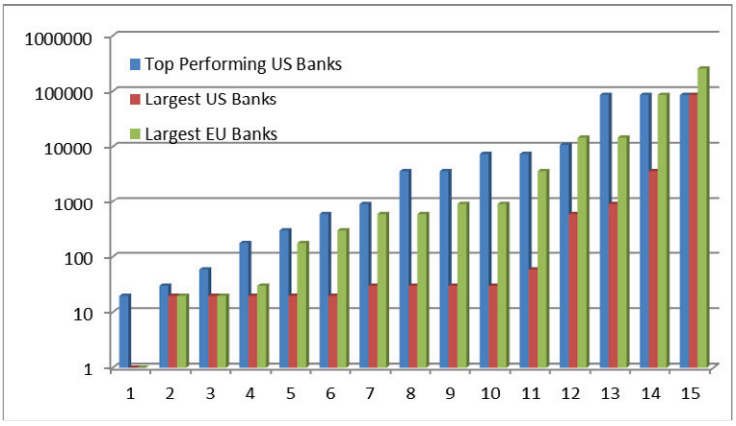

Fig. 4. DNS TTL times in seconds (log scale) of 3 groups of banks

5. Ongoing Work

Some of the issues related to the *Faulty DNS-Cache Lock* phenomenon that are currently under investigation by our research group include:

1) The term *local (client) DNS Cache* is generally used to refer to the DNS Cache of the client's OS system. It should not be forgotten, however, that on the same client machine - in addition to the OS's DNS Cache - there also exist DNS Caches of individual browsers. To date, there has been very little research on mutual interaction among different types of browser DNS caches and the impact each of them could have in situations involving *Faulty DNS-Cache Lock*.

2) The task of determining the most optimal value of DNS TTL parameter for a particular web-site is far from trivial. Namely, what constitutes the optimal TTL will depend on a number of factors, including: a) actual behavior of the users visiting the given site and their physical/geographic distribution relative to the location of the site's authoritative DNS server; b) whether or not the site utilizes multiple 'symbolic-name to IP address' mappings; c) probability that the site becomes the target of a DDoS attack, etc. According to our knowledge, there has been no previous work looking in the interplay of all these factors, and providing an analytical model for calculation of optimal DNS TTL values.

References

[1] J. Mirkovic, P. Reiher, "*A Taxonomy of DDoS Attack and DDoS Defence Mechanisms*", ACM SIGCOMM Computer Communications Review, Vol. 34, No. 2, pp. 39 – 54, April 2004.
[2] Techspot, "VeriSign: Botnets rented for a few bucks an hour", May 25, 2010
http://www.techspot.com/news/39066-verisign-botnets-rented-for-a-few-bucks-an-hour.html
[3] S. N. Bhatti, R. Atkinson, "Reducing DNS Caching", 31st IEEE INFOCOM 2011, Changhai, China, April, 2011.
[4] Techspot, "*Windows XP Usage*", Aug 1, 2011.
http://www.techspot.com/news/44902-windows-xp-usage-finally-falls-below-50-mark.html
[5] S. Power, "*Metrics 101: What to Measure on Your Website*", Velocity - Web Performance and Operations Conference, Santa Clara, USA, June 2010.
[6] E. Schurman, J. Brutlag, "*The User and Business Impact of Server Delays, Additional Bytes, and HTTP Chunking in Web Search*", Velocity - Web Performance and Operations Conference, San Jose, USA, June 2009.
[7] Forrester Consulting, "*The Impact of Poor Web Site Performance in Financial Services*", January 2010.
http://www.banktech.com/business-intelligence/222500093
[8] R. Aitchison, "Pro DNS and BIND 10", Apress, 2011.
[9] Microsoft Technet, "DNS Reference Information", 2011.
http://technet.microsoft.com/en-us/library/dd197499%28WS.10%29.aspx
[10] J. Dilley, B. Maggs, J. Parlkh, H. Prokop, R. Sitaraman, B. Weihl, "Globally Distributed Content Delivery", IEEE Internet Computing Magazine, Vol. 6, No. 5, pp. 50 -58, Sep./Oct. 2002.
[11] http://www.forbes.com/2010/01/06/bofa-hawaii-umb-business-wallstreet-best-worst-banks-chart.html
[12] http://www.banksdaily.com/topbanks/europe/2011.html
[13] http://www.wireshark.org/

Appendix A. An example appendix

Table 1. Number of utilized IP addresses and TTL values in DNS records of 15 best performing US banks

Rank	Bank	Number of Advertised / Utilized IP-Addresses / Servers	Advertised DNS TTL
1	Prosperity Bancshares	1	7200 sec = 2 h
2	Bank of Hawaii	1	900 sec = 15 min
3	First Republic Bank	1	600 = 10 min
4	Community Bank System	1	60 = 1 min
5	Signature Bank	1	20 sec
6	East West Bancorp	1	86400 sec = 24 h

7	Commerce Bancshares	1	86400 sec = 24 h
8	SVB Financial	1	3600 sec = 1 h
9	First Citizens BancShares	1	300 sec = 15 min
10	Cullen/Frost Bankers	1	180 sec = 3 min
11	CVB Financial	1	86400 sec = 24 h
12	Westamerica Bancorp	1	7200 sec = 2 h
13	BankUnited	1	10800 sec = 3 h
14	State Street	1	30 sec
15	National Penn Bancshares	1	3600 sec = 1 h

Table 2. Number of utilized IP addresses and TTL values in DNS records of 15 largest US banks

Rank	Bank	Number of Advertised / Utilized IP-Addresses / Servers	Advertised DNS TTL
1	JPMorgan Chase	2 in separate DNS records	20 sec
2	Bank of America	3 in separate DNS records	30 sec
3	Citigroup	2 in separate DNS records	3600 sec = 1 h
4	Wells Fargo	2 in same DNS record	900 sec = 15 min
5	U.S. Bancorp	1	600 sec = 10 min
6	Bank of New York Mellon	1	30 sec
7	Capital One Financial	1	30 sec
8	HSBC North America Holdings Inc.	1	20 sec
9	PNC Financial Services Group Inc.	1	0 sec
10	State Street Corp.	1	20 sec
11	TD Bank US Holding Co.	2 in separate DNS records	20 sec
12	SunTrust Banks Inc.	1	600 sec = 10 min
13	BB&T Corp.	1	86400 sec = 24 h
14	American Express Co.	Akamai	20 sec
15	Citizen Financial Group Inc.	2 in separate DNS records	30 sec

Table 2. Number of utilized IP addresses and TTL values in DNS records of 15 largest US banks

Rank	Bank	Number of Advertised / Utilized IP-Addresses / Servers	Advertised DNS TTL
1	HSBC Holding, UK	1	20 sec
2	BNP Paribas, France	1	14400 sec = 4 h
3	Sberbank, Russia	1	180 sec = 3 min
4	Deutsche Bank, Germany	1	900 sec = 15 min
5	Santander Group, Spain	Akamai	20 sec
6	ING Group, Netherlands	1	900 sec = 15 min
7	UBS, Switzerland	1	30 sec
8	BBVA, Spain	1	259200 sec = 3 days
9	Commerzbank, Germany	1	3600 sec = 1 h
10	Barclays, UK	2 in same DNS record	600 sec = 10 min
11	Crédit Agricole S.A., France	1	86400 sec = 24 h
12	Groupe BPCE, France	2 in same DNS record	0 sec
13	Société Générale, France	1	600 sec = 10 min
14	KBC Group, Italy	1	14400 sec = 4 h
15	UniCredit, Italy	2 in separate DNS records	300 sec = 5 min