International Conference on Cyber Security and Computer Science (ICONCS'18),
Oct 18-20, 2018 Safranbolu, Turkey

An Analysis DRDoS Amplifiers in Europe

Emre Murat ERCAN[1] and Ali Aydın SELÇUK[1]

[1] TOBB University of Economics and Technology, Ankara/Turkey, emremuratercan@yandex.com
TOBB University of Economics and Technology, Ankara/Turkey, aliaydinselcuk@ gmail.com

Abstract - DRDoS is the new method of choice for denial of service attacks: Certain services running over UDP is chosen for the attack. Servers across the Internet are contacted by bots with the spoofed IP address of the victim host. In response, huge amounts of response data created by the servers are sent to the victim, temporarily disabling it. The most commonly exploited protocols are those that yield the highest "amplification factor", including NTP, DNS, and Memcached.

Mitigation of these attacks can be done simply by hardening servers against known vulnerabilities. However, in practice, there are many servers that lag behind. In this study, we carried out a regional analysis of NTP, DNS, and Memcached servers in Europe, and assessed their readiness against being used as amplifiers in DRDoS attacks.

***Keywords* – DDoS, DRDoS, Amplification Attack, NTP, DNS, Memcached.**

I. INTRODUCTION

Distributed denial-of-service attack (DDoS), one of the oldest attack types on the Internet, is still an effective tool for stopping services. It is one of the most favorite attack approaches of attackers. In a DDoS attack, the adversary exhausts the bandwidth or some other resource, such as CPU or memory, of the target host. All these attacking factors can stop or slow down the target's services [7].

Usage of reflection with DDoS attacks which named as Distributed reflective denial-of-service (DRDoS) attack is newly used technique with the same logic of DDoS attack. The attack is also known as amplification attack. This attack takes its power from the amplification factor which mostly occurs in UDP protocols [3]. Attack may also take place with TCP based protocols but this idea is out of scope in this study. Usage of amplifiers has become popular after 2012, but it is known from years. Adversaries directly aim targets' bandwidth with his slave botnets in DRDoS attacks. There is no handshake in UDP protocol that make UDP connectionless is one of the most important reason of reflection. The responses to all the requests made by the attacker's slaves in the name of target will be returned to the target. Additionally, attackers choose some special services whose responses could be as high as 50000 times the request size [6].

DRDoS attacks make trouble because of byte amplification factor (BAF) and packet amplification factor (PAF). BAF is a rate of response byte to rate of request byte. PAF is a rate of response packet number to request packet number. As an attack's amplification factor, BAF is more dangerous than PAF. While BAF can be as high as 4670x, PAF can barely reach 10.61x.

There are many known vulnerabilities in UDP-based protocols including network services such as NTP, SNMP, SSDP, NetBIOS, or legacy services such as CharGen, QOTD, P2P filesharing networks such as BitTorrent, Kad, or game servers such as Quake 3 and Steam, as we have seen in the early studies [2]. These studies and real world observations showed us NTP and DNS could easily destroy target services. Amplification factor can be change according to service version, hardening methods and protocol itself. Even TCP based services could be usable as an amplifier. Early studies showed us TCP-based protocols may have 79x amplification factor [13]. One of the most crucial service is DNS. This protocol averagely responses 28.7x more than a request for open resolvers with "any" lookup. Also open resolvers send back 64.1x more than a request in worst cases. NTP has more demolish amplification factor as 556x. This factor can up to 4670x in some worst case scenarios [2]. Beyond all these studies in 28.02.2018 GitHub attack showed us there is a new cruel vulnerability in memcached servers [17]. Memcached, the newest one, has the most terrifying amplification factor as 50000x [6].

In this study we focused on DNS, NTP, and memcached servers in 25 European countries. These countries as fallows; Armenia, Belarus, Bulgaria, Cyprus, Czechia, Denmark, Estonia, Germany, Georgia, Greece, Hungary, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Moldova, Poland, Romania, San Marino, Sweden, Switzerland Slovakia, Slovenia and Ukraine. DNS protocol is responsible for translating domain names to IP addresses. This protocol generally uses TCP port 53 for zone transfers and UDP port 53 for relation between domain names and IP addresses. NTP is a protocol that helps time synchronization between server to server or server to client. This protocol uses UDP port 123. Memcached is a system that is designed for use distributed memory object caching [10]. This protocol uses both TCP and UDP port 11211. In this study, we explored the servers for these three services in the IPv4 domain and requested the vulnerable services. We analyzed the responses to see whether they are usable in attacks.

Organization of this paper as follows: In Section 2, we survey the literature on known DRDoS attacks with DNS, memcached, and NTP protocols. We explain our server discovery methodology in Section 3. In Section 4, we present the results of our analysis on vulnerable NTP, DNS, and memcached servers. In Section 5, we conclude the paper with our recommendations.

II. Related Work

While foresight papers about Denial of Service attacks with a spoofed IP source were first published in 1989 [1], detailed analyses started in 1996 [4]. After these studies, there have been many papers published about detecting, filtering, or tracing the attacker [11]. In 2014 Rossow et al. published a study on discovering UDP-based amplification attacks and hardening methods for service providers. That paper also has many defines about DRDoS terms [2]. After that, they published a second paper with some additional points such as tackling NTP servers and warnings about TCP protocols [5]. Kuhrer et al. worked on TCP amplification factor and countermeasures [13]. That paper indicates TCP based amplification attacks could be also harmful for service providers. Furthermore, we have already observed effective attacks with DNS, NTP, and memcached protocols [17,20,21]. These studies were the starting point for this paper. We also performed a similar research for Turkey [22].

DRDoS attacks are becoming more harmful than the past with the increased usage of UDP-based protocols. Before 2012 there were no significant DDoS attacks with amplifiers. In 2012 DRDoS attacks became popular with the gigantic amount of traffic with amplification factors. First well-known DDoS attack with amplification factor was performed in 2012. That attack targeted real-time financial exchange platforms and it achieved 167 Gb/s [8]. Others followed this attack in 2013. In 2013 there were four large-scale attacks that reached at least 100 Gb/s. These attacks targeted MIT, Zimbabwe Human Rights Forum, Spamhaus, and streaming sites. Attackers used SNMP, DNS, and NTP servers for these attacks [11].

DNS has many advantages for attackers. First of all, there are too many DNS servers on the Internet. Secondly, DNS has a tremendous amplification factor and could not be closed for use. This protocol works both TCP and UDP port 53. The most immense amplification factor occurs with ANY lookup in DNS [9]. As a response of this request, the server returns all records about the queried domain. Misconfiguration of DNS servers for DRDoS attacks have been identified as vulnerabilities CVE-2006-0987 [24] and CVE-2006-0988 [25]. It is easy to harden, but somehow there are still too many misconfigured DNS servers in the wild. Many DRDoS attacks have been observed using DNS servers. One of them targeted Turkey in 2015, which became known as the "nic.tr attack" [20]. According to nic.tr officials, in some phase of the attack, the traffic volume was exceeded 200 Gb/s and slowed down most of the country's Internet without any specialized target. One year later in October 2016 another well-known DNS-based attack occurred. This attack targeted Dyn, a company that services Twitter, SoundCloud, Spotify, Shopify, Box, Boston Globe, New York Times, Github, Airbnb, Reddit, Freshbooks, Heroku and Vox Media properties etc. Because of this attack, many of these services were unreachable on the day of the attack including Twitter [21]. This attack was also significant because, according to Dyn officials, the attack originated from Mirai-based botnets, which highlights importance of "Internet of things" (IOT) devices in the future of DDoS attacks.

The NTP protocol has been used for proper time synchronization for online devices. NTP servers can be contacted by clients or servers to make time stable. These connections use the NTP protocol at UDP port 123. Nowadays this protocol is also significant for security management. Security information and event management (SIEM) software, one of the most important security products today, needs proper time synchronization for discovering incidents. On the other hand, NTP is also meaningful for DRDoS attackers. It has a 4670x factor as a BAF in the worst cases. On average it has 556x amplification factor [2]. Those results are making adversaries ambitious to use NTP servers. The worst case happens when attackers are able to use the "monlist" request [10]. This request was designed for server administration, but somehow it can also be used from anywhere without hardening. As a response of monlist, server sends back the last 600 clients' IP addresses and more detailed information such as their NTP version, how many times they have been seen, etc. This vulnerability of NTP servers, which is a target of DRDoS attacker, has been identified as CVE-2013-5211 [10]. Many attacks with NTP servers have been observed in the last few years. One of the most significant NTP-based DRDoS attack was conducted in 2014. According to Cloudflare, one of their costumers was attacked with 400 Gb/s in February 2014. In this attack, adversaries used 4,529 NTP servers from 1,298 different networks and each of these servers sent 87 Mb/s to the victim [14].

Memcached was designed for high-performance, distributed memory object caching systems for speeding up dynamic web applications [15]. It is the newest trend in DRDoS attacks. This protocol uses both TCP and UDP port 11211. The protocol was not considered for DRDoS attacks until February 2018. That attack targeted to GitHub servers and peaked at 1.3 Tb/s which has the largest volume ever seen in a DDoS attack [17]. The main reason of this attack power is the large amplification factor. According to common vulnerabilities and exposures, memcached protocol's amplification factor is 50000x. The memcached vulnerability for DRDoS attacks has been identified as CVE-2018-1000115 [26].

III. Methodology

We focused on three UDP-based protocols in this study: DNS, NTP, and memcached. We limited our scans with 25 European countries. As the first step of the study, we concentrated on figuring out which country-based IP database would be the most effective to use. There are different IPv4 databases available on the Internet but we decided to use Ivan Erben's database [12] which is updated daily by an automated script. The studied countries are given alphabetically in Table 1. The dates in the table show the date of the database used for that study. For Armenia, for instance, the DNS studies were done with the database of July 27, the NTP studies were done with the database of August 3, and the memcached studies were done with the database of August 5.

After choosing which database to use, we focused on finding all DNS, NTP, and memcached servers for these 25 countries. For this purpose, we scanned all these countries with "zmap", an open source tool for fast Internet scanning, developed by Durumeric et al, [18]

Table 1: Date of Used Database.

Country	DNS	NTP	Memcached
Armenia	27 July	3 August	5 August
Belarus	22 July	4 August	5 August
Bulgaria	13 July	4 August	5 August
Czechia	16 July	3 August	6 August
Cyprus	31 July	4 August	6 August
Denmark	17 July	4 August	6 August
Estonia	13 July	3 August	5 August
Georgia	15 July	3 August	5 August
Germany	13 July	4 August	6 August
Greece	28 July	3 August	7 August
Hungary	31 July	4 August	6 August
Ireland	23 July	4 August	6 August
Italy	15 July	3 August	5 August
Liechtenstein	31 July	4 August	5 August
Luxembourg	21 July	4 August	5 August
Malta	31 July	3 August	6 August
Moldova	18 July	4 August	6 August
Poland	19 July	3 August	5 August
Romania	27 July	4 August	5 August
San Marino	31 July	6 August	6 August
Slovakia	23 July	4 August	6 August
Slovenia	23 July	4 August	6 August
Sweden	19 July	4 August	6 August
Switzerland	19 July	4 August	6 August
Ukraine	23 July	4 August	6 August

As a starting point we focused on DNS servers because of time issues. First we discovered severs which open at port 53 for these 25 countries by an aggressive search. We only restricted scans to the target port number. After discovery phases we executed our script for that country. The script tries to get a response to see whether a DNS server allows the recursive search for "ANY" query. In our script we used "nslookup" to obtain records.

Our second target was detecting NTP servers in those countries. Again, we used zmap for scanning. While we were scanning we used zmap module which is specialized for NTP scans. We used zmap scan outputs as nmap script inputs. This script was specialized for gathering all monlist information about the given input.

As the last part of the scans, we made a search for memcached servers using zmap again for discovering available services at port 11211 with a memcached probe. After discovering the open ports, we started the nmap tool with the output of the zmap probe.

In our study we did not cover some of the largest European countries such as Spain, Great Britain, France. The main reason of that is a time management problem for DNS servers. For instance, according to our scan results, there were more than 300,000 DNS servers in Spain. Our script can scan approximately 9,000 DNS servers in a day. Therefore, we had to choose between covering some countries only partially or skipping those countries altogether. We opted for the latter.

IV. Results

We discovered more than 654,000 DNS servers in this study. Most of them are not amplifiers but more than 56,000 servers are still available for attackers. More than 45,000 these servers were already hardened to some degree, but according to our research they are still usable as an amplifier, albeit with a smaller factor. They return only IPv6 address of the requested IP. Unfortunately, we discovered 10,433 servers to be harmful as much as possible. They do not have any secure configuration against DRDoS attacks. The results of the study on DNS servers are summarized in Table 2. We showed all available servers that run at port 53 in "Port 53 Open" column. This column shows our zmap results. "Only IPv6 Information" column indicates the number of amplifiers that respond only with the IPv6 information of the requested host. These servers' administrators have already made some hardening and they have a smaller amplification factor, but we can still describe them as amplifiers. In the last column "All DNS Records", we gave the number of DNS servers that respond with all DNS records about requested host, which is the worst case for DNS servers. According to our results, Estonia has the best and Armenia has the worst ratio of hardened DNS servers among the countries studied. The number of DNS servers open to amplification is taken as the sum of the last two columns.

In the second phase of the study we discovered 2,003,021 servers that respond to queries at UDP port 123. Compared to the DNS study, the results are more promising: We discovered that only 1,601 of them are amplifier. While 1,364 of them respond with only client IP addresses, 228 of them still respond with much more information about clients. This scenario is the worst case where we can expect a 1260x amplification factor. Table 3 shows the results of our study on NTP servers. The "Port 123 Open" column gives the results of our zmap scan, which returns the number servers that run on port 123. The "Only IP Information" column gives the number of amplifiers that return only client IPs. These servers' administrators have already made some hardening. They are returning only the IP addresses of their clients. They have a smaller amplification factor compared to the servers that respond with all monlist information. The last column "All Monlist Information" shows the number of servers that return all information in response to a monlist request as the worst case for NTP servers. According to our research, Ireland has the worst ratio for hardened NTP servers. According to our results, San Marino, Liechtenstein, and Estonia have the best and Ireland has the worst ratio of hardened NTP servers among the countries studied. The number of NTP servers open to amplification is taken as the sum of the last two columns.

Table 2: County-based DNS information. The results are given in decreasing ratio (i.e., from worst to best) of unhardened servers.

Country	Port 53 Open	Only IPv6 Info	All DNS Records
Armenia	3603	905	397
Belarus	4015	623	167
Liechtenstein	61	6	6
Ukraine	81535	11859	2834
Greece	5300	604	293
Slovakia	2225	211	95
Georgia	2628	317	36
Switzerland	22058	2413	405
Hungary	23278	2444	389
Denmark	10148	739	370
Poland	51205	4118	1004
Czechia	29914	2453	522
Ireland	13833	1208	68
San Marino	88	1	7
Italy	105959	6607	1354
Slovenia	4774	304	47
Moldova	5557	276	116
Sweden	72154	3749	1064
Cyprus	5246	179	155
Romania	77438	3508	476
Malta	9209	429	42
Luxembourg	1928	77	9
Bulgaria	41888	1381	271
Germany	69680	1716	254
Estonia	10296	209	52

Table 3: County-based NTP information. The results are given in decreasing ratio (i.e., from worst to best) of unhardened servers.

Country	Port 123 Open	Only IP Information	All Monlist Information
Ireland	11193	57	5
Armenia	2530	10	0
Greece	22560	67	9
Denmark	39224	77	5
Czechia	65294	127	8
Hungary	32048	46	13
Poland	77207	113	22
Bulgaria	37390	43	5
Ukraine	67125	44	18
Germany	419529	323	34
Cyprus	8919	6	1
Slovakia	27653	16	5
Sweden	90332	51	16
Moldova	9032	5	1
Belarus	15907	6	4
Georgia	7181	0	0
Romania	101214	41	13
Switzerland	222514	86	12
Italy	724083	245	57
Malta	2922	0	0
Slovenia	8782	0	0
Luxembourg	4101	0	0
Estonia	5592	1	0
Liechtenstein	528	0	0
San Marino	161	0	0

Lastly, we examined the memcached servers, which has become a hot topic after the 28 February 2018 attacks. In our research we discovered 178,359 memcached servers. It is not possible to know for sure whether these memcached servers are necessarily available on the Internet. But we are sure these servers should not respond at UDP port 11211 with a proper hardening. We discovered 1,801 memcached servers still available at UDP port 11211. In Table 4 we gave our results for memcached servers. After the country name in "Port 11211 Open" column we gave the number of discovered memcached servers. On the third column "UDP Response", we gave the number of amplifiers that are still available for UDP communication. According to our research, Armenia has the worst ratio for hardened memcached servers. On the other hand, we could not find any memcached servers in San Marino, nor any memcached amplifiers in Liechtenstein. Except these two countries Denmark has the best ratio for hardening memcached servers.

Table 4: County-based memcached information. The results are given in decreasing ratio (i.e., from worst to best) of unhardened servers.

Country	Port 11211 Open	UDP Response
Armenia	16	5
Cyprus	53	14
Ireland	122	23
Ukraine	888	163
Moldova	51	8
Belarus	36	5
Poland	1204	152
Luxembourg	74	8
Georgia	37	3
Hungary	771	49
Bulgaria	1907	78
Slovakia	271	7
Switzerland	2260	52
Malta	45	1
Italy	12490	200
Czechia	3565	47
Germany	57102	655
Sweden	11206	99
Estonia	577	5
Greece	709	5
Romania	59478	218
Slovenia	916	1
Denmark	4328	3
Liechtenstein	3	0
San Marino	0	0

V. Conclusion and Recommendations

DRDoS attacks that exploit large amplification factors in certain UDP-based protocols are the new trend for DDoS attacks. Although ways of fixing vulnerable servers are well-known, many servers on the Internet remain unfixed, waiting to be used as launching pads in new attacks. In this paper, we studied the situation of servers in several European countries running three of the most vulnerable protocols, DNS, NTP, and memcached, and analyzed their readiness.

All these three protocols could be made harmless for service providers with proper hardening. DNS servers can be hardened

by applying some restrictions. Two main points to make DNS servers secure against being a part of a DRDoS attacks are, first, disabling recursive search [9], and second, restricting the query type of "ANY" [16]. NTP servers which can amplify with an 1260x factor can be hardened by disabling monlist requests. It is easy to relatively straightforward to harden NTP servers [10]. It is also strongly recommended to update the NTP servers. All ntpd versions before 4.2.7 are vulnerable by default [19,23] and must be updated. Memcached servers can be hardened by observing two main points: First, if a server does not need to serve the Internet, then it should be made only locally available. Second, after the GitHub attack memcached has a new version 1.5.6 published where UDP port 11211 is disabled by default. Administrators should update their servers accordingly.

ACKNOWLEDGMENT

We would like to thank Bahtiyar Bircan, Kamil Seyhan, and Sertaç Katal from Barikat Internet Security, for their help with improving our scanning methods and defining the security needs.

REFERENCES

[1] S. M. Bellovin, "Security Problems in the TCP/IP Protocol Suite," ACM SIGCOMM Comput. Commun. Rev., vol. 19, no. 2, pp. 32–48, Apr. 1989

[2] C. Rossow. Amplification Hell: Revisiting Network Protocols for DDoS Abuse. In Symposium on Network and Distributed System Security (NDSS) (2014).

[3] CERT Advisory, "UDP-Based Amplification Attacks" https://www.us-cert.gov/ncas/alerts/TA14-017A

[4] L. T. Heberlein and M. Bishop, "Attack Class: Address Spoofing," in Proc. of the 19th National Information Systems Security Conference, 1996, pp. 371–377.

[5] M. Kührer, T. Hupperich, C. Rossow, and T. Holz. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks Proceedings of the 23rd USENIX Security Symposium, San Diego, USA, August 2014

[6] Memcached Reflection Attacks Akamai https://www.akamai.com/uk/en/multimedia/documents/brochure/memcached-reflection-attacks-launch-a-new-era-for-ddos-brochure.pdf

[7] S. M. Specht, R. B. Lee. Distributed Denial of Service: Taxonomies of Attacks, Tools, and Countermeasures. In Proceedings of the International Conference on Parallel and Distributed Computing (and Communications) Systems (ISCA PDCS), San Francisco, CA, September 2004.

[8] [2] Prolexic Quarterly Global DDoS Attack Report Q2 2013, "Prolexic Stops Largest-Ever DNS Reflection DDoS Attack," May 2013. [Online]. https://sm.asisonline.org/ASIS%20SM%20Documents/Prolexic%20Quarterly%20Global%20DDoS%20Attack%20Report.pdf.

[9] CERT Advisory, "DNS Amplification Attacks" https://www.us-cert.gov/ncas/alerts/TA13-088A

[10] CERT Advisory, "NTP Amplification Attacks Using CVE-2013-5211" https://www.us-cert.gov/ncas/alerts/TA14-013A

[11] F. J. Ryba, M. Orlinski, M W¨ahlisch, C. Rossow, T. C. Schmidt. "Amplification and DRDoS Attack Defense – A Survey and New Perspectives". arXiv:1505.07892v3 [cs.NI] 17 May 2016

[12] I. Erben. http://www.iwik.org/ipcountry/

[13] M. Kuhrer, T. Hupperich, C. Rossow, T. Holz. Hell of a Handshake: Abusing TCP for Reflective Amplification DdoS Attacks. . In Proceedings of the 8th USENIX Workshop on Offensive Technologies, San Diego, CA, August 2014

[14] M. Prince. Technical Details Behind a 400 Gbps NTP Amplification DDoS Attack. https://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack/ , February 2014

[15] What is Memcached? https://memcached.org/

[16] Use DNS Policy for Applying Filters on DNS Queries. https://docs.microsoft.com/en-us/windows-server/networking/dns/deploy/apply-filters-on-dns-queries, March 2018

[17] S. Kottle, February 28th DDoS Incident Report, https://githubengineering.com/ddos-incident-report/ , March 2018

[18] Z. Durumeric, E. Wustrow, and J. A. Halderman. ZMap: Fast Internet-wide Scanning and Its Security Applications. In Proceedings of the 22nd USENIX Security Symposium, Washington, D.C., USA, August 2013.

[19] J. Graham-Cumming. Understanding and Mitigating NTP-Based DdoS Attacks. https://blog.cloudflare.com/understanding-and-mitigating-ntp-based-ddos-attacks/

[20] 14/12/2015 Tarihinde Başlayan DDoS Saldırısı Kamuoyu Duyurusu. https://www.nic.tr/2015-12-DDoS-Saldirisi-Kamuoyu-Duyurusu-20151221.pdf . 21 Dec 2015

[21] S. Hilton. Dyn Analysis Summary Of Friday October 21 Attack https://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/. 26 Oct 2016

[22] E. M. Ercan, A.A. Selcuk. A Nationwide Study of DRDoS Amplifiers. Submitted paper to ISC Turkey 2018, Ankara, TURKEY, October 2018.

[23] Team Cymru. Secure NTP Template. https://www.team-cymru.com/secure-ntp-template.html

[24] National Vulnerability Database, "CVE-2006-0987 Detail " https://nvd.nist.gov/vuln/detail/CVE-2006-0987#vulnCurrentDescriptionTitle

[25] National Vulnerability Database, "CVE-2006-0988 Detail " https://nvd.nist.gov/vuln/detail/CVE-2006-0988

[26] National Vulnerability Database, "CVE- 2018-1000115 Detail " https://nvd.nist.gov/vuln/detail/CVE-2018-1000115