A Study on Exploitable DRDoS Amplifiers in Europe

Emre Murat Ercan[1], Ali Aydın Selçuk[2]

[1]Barikat Cyber Security, Ankara, Turkey
[2]Department of Computer Engineering, TOBB University of Economics and Technology, Ankara, Turkey
Corresponding Author: aliaydinselcuk@gmail.com

Research Paper Received: 04.03.2021 Revised: 17.04.2021 Accepted: 13.05.2021

Abstract—One of the best-known cyber attacks, distributed denial of service (DDoS), is evolving. It has become much more malefic and effective with the use of amplification power of reflected messages. This attack is known as the distributed reflected denial of service (DRDoS) or the amplification attack. Attackers abuse UDP-based protocols' connectionless property for this attack and achieve an attack volume of hundreds of Gbps. The attack occurs by botnets' spoofing a victim's IP address and demanding some service from unhardened servers. Attackers generally prefer protocols that have high a "amplification factor" such as NTP and Memcached, or protocols where it is hard to differentiate legal requests from malicious ones, such as DNS. At this point, an important defensive strategy against these attacks is to harden servers not to play a role as amplifiers. In this paper, we carried out a detailed research of servers in 41 European countries and focused on three UDP-based protocols most commonly abused by attackers: DNS, NTP, and Memcached. We searched these servers by automatic regional scans and analyzed whether they have been hardened against DRDoS attacks.

Keywords—Denial of service, DRDoS attacks, DNS, NTP, Memcached

1. Introduction

Denial of service (DoS) attack, one of the oldest type of cyber attacks, is still in use for stopping or slowing down internet services. DoS has been one of the favorite tactics for attackers due to its ease of implementation and effectiveness. Any online service can be targeted, such as political sites, e-commerce sites, universities, health care sites, etc. DoS attacks have evolved over time to distributed DoS (DDoS) attacks, where attackers use botnets to achieve their goal. Attackers have deployed different techniques, like flooding attacks, to exhaust a victim's resources such as CPU, memory, or bandwidth [1].

Distributed reflected DoS (DRDoS) has become one of the most popular types of DDoS attacks in recent years [2]. It is similar to classical DDoS in its use of botnets, but is much more effective with amplification power of reflectors. Generally UDP-based protocols are preferred, which are open to IP spoofing as they are connectionless [3]. In these UDP-based attacks, the attacker uses bots to

A preliminary version of this paper with a limited set of results was presented at the International Conference on Cyber Security and Computer Science (ICONCS'18).

send request packets to servers with the victim's IP address written as the source, and vulnerable servers send their response packets to the victim. This is known as reflection. Typically request messages with large responses are preferred, hence the exploited servers are used as "amplifiers". TCP-based protocols can be used for DRDoS too [4], [5], but they are not as effective and are not used much in practice The DRDoS attack methodology is demonstrated Figure 1.

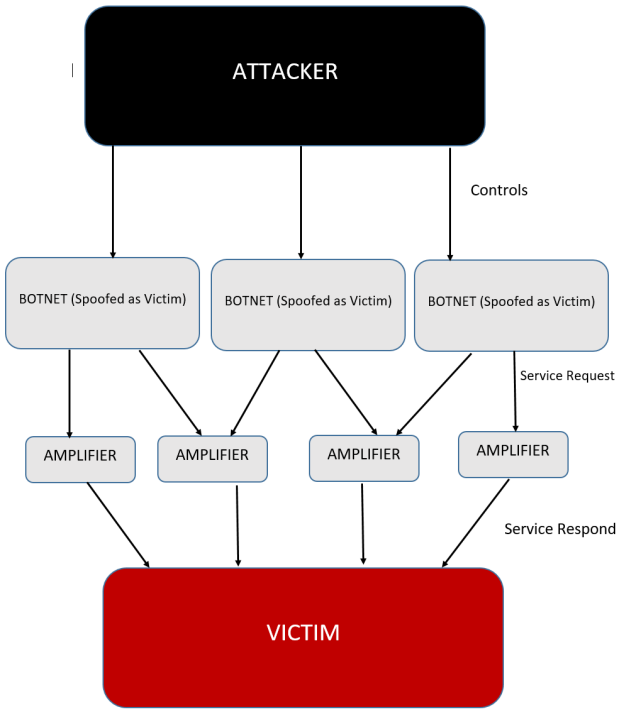

Fig. 1. DRDoS attack methodology.

Reflection is the crucial component of DRDoS attacks. Another essential element for the effectiveness of an attack is the amplification factor. Amplification factor can be defined as the byte amplification factor (BAF) or the packet amplification factor (PAF). The more significant one is BAF, which is defined as the ratio of the response bytes to the request bytes. An attack generally takes its power from BAF [2]. It has been observed that some protocols, such as Memcached, may have a BAF of 50000x or more [6].

$$BAF = \frac{\text{Byte size of response}}{\text{Byte size of request}}$$

PAF is the ratio of the response packet count to the request packet count. It can be as high as 10x or more for some protocols. While PAF is significant too, in most studies the amplification factor has been identified with BAF.

$$PAF = \frac{\text{Number of response packets}}{\text{Number of request packets}}$$

Rossow et al. [2] studied the amplification factors of several UDP-based protocols which were already identified as dangerous for DRDoS, such as NTP, SNMPv2, DNS, NetBios, SSDP, CharGen, QOUTD. Some legacy services such as file sharing networks and game servers were also examined as potential amplifiers. According to this study, NTP has one of the largest amplification factors where BAF can be as high as 4670x. Besides NTP, they also showed how unhardened DNS servers could be dangerous for service providers. According to this study, DNS servers can amplify requests by 76x. More recently, the Memcached protocol has been used for reflection attacks and one of the largest DRDoS attacks ever was carried out using unhardened Memcached servers in February 2018, where BAF was as high as 50000x [24].

In this study, we concentrated on three services most exploited by DRDoS attackers: DNS, NTP, and Memcached. DNS is normally used to map domain names to IP addresses. This service runs over TCP or UDP, on port 53 by default. NTP, the second service we analyzed, is used for time synchronization between a server and a client, or between two servers. NTP runs on UDP port 123 by default. Memcached, the third service we

studied, was designed for speeding up dynamic web applications by mitigating database load. Memcached services may run either over TCP and UDP, on port 11211 by default.[1]

In this paper, we explored the state of these three services in Europe and checked whether the available servers can be used as amplifiers in DRDoS attacks. We focused on 41 European countries: Albania, Armenia, Austria, Belarus, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Czechia, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuanian, Luxembourg, Macedonia, Malta, Moldova, Montenegro, Netherlands, Norway, Poland, Portugal, Romania, Russia, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey, Ukraine, and United Kingdom.

The rest of the paper is organized as follows: We begin with a survey of the literature and some of the most significant DRDoS attacks in recent history in Section 2. In Section 3, we give the details of the methodology we used the to discover the vulnerable servers. In Section 4, we present our findings on exploitable DNS, NTP, and Memcached reflectors in Europe. We discuss our results in Section 5, and conclude the paper with recommendations to avoid future attacks.

2. Survey of the DRDoS Landscape

The possibility of a DoS attack with spoofed IP source addresses was first discussed by Bellovin in 1989 [3]. Heberlein and Bishop [7] analyzed the concept in further detail. Webb [8] demonstrated the attack for the first time during the DEFCON 1997 conference, and one year later the first DDoS attack was observed in the wild. Since then, neither DDoS attacks nor studies analyzing them have ever stopped. Much havoc has been caused by botnets. One of the earliest well known DDoS attack was carried out in 2000. “Mafiaboy”, who was 15 years old at the time, took down several major websites such as CNN, eBay, E-Trade, Dell, and Yahoo! with the help of compromised university networks. Another well-known DDoS attack directly targeted Estonia in 2007, where virtually the whole country felt the impact of the attack and many services were disabled [13]. Many surveys and taxonomy studies have been conducted analyzing and classifying the DDoS attacks [1], [10], [11], [12].

Although the idea was well-known, amplifiers were not encountered in DDoS attacks in a significant way before 2013. After 2013, both attackers and researchers began to concentrate on DRDoS reflection attacks with large amplification factors. DRDoS attacks became popular after a number of high-profile attacks in 2013: The first well-known DRDoS attack was used to take down real-time financial exchange platforms, which achieved a traffic volume of 167 Gbps using DNS reflection [15]. After that, there were three other large-scale attacks in 2013 with a volume of 100 Gbps or more. Attackers used DNS reflection for two of these attacks and NTP reflection for the third [15]. An attack in August 2013 targeted the GreenNet company, and is believed to be politically motivated: Zimbabwe would have an election in those days, and GreenNet was providing hosting services for the Zimbabweans Human Rights Forum [16]. Another DRDoS attack in 2013 targeted the Spamhaus systems. Servers of the Spamhaus Project, which publishes real-time intelligence about spam, was hit with a combination of SYN flooding and DNS amplification attacks. The volume of the attack reached 300 Gbps and most of Spamhaus’

1. https://memcached.org/

servers were down [17], [18]. Another notable attack in 2013 used NTP servers as amplifiers. The attack reached approximately 100 Gbps, and game servers such as Dota2 and League of Legends played by tens of thousands of people were put out of service [19].

UDP is used in many services to reduce overhead and enhance performance. Due to its efficiency, services running on UDP are increasing constantly. As a natural result of this increase, the number of amplifiers available for DRDoS attacks are also increasing. Not just the number of attacks but also the volume of attacks have seen a surge in recent years: While DRDoS attacks in 2013 had volumes up to several 100 Gbps, since 2020 attacks with volumes up to 2.3 Tbps have been observed [14].

Several key studies have been published on DRDoS attacks: Rossow [2] published a detailed analysis of UDP-based amplification attacks and discussed methods to harden servers against these attack. This paper defined some of the key DRDoS concepts. Kuhrer et al. [4] studied additional issues on DRDoS attacks such as exploitation of NTP servers and attacks that may use TCP-based protocols. Another paper from the same group [5] analyzed TCP-based amplification attacks and countermeasures, where they showed that TCP-based amplification can also be harmful. Ryba et al. [9] provided a comprehensive survey of DRDoS attacks up until 2016.

2.1. Common Amplifiers

An amplifier type most commonly exploited by attackers is DNS servers. DNS has several desirable features for attackers: First of all, DNS is a widely-used protocol across the internet and there are so many DNS servers available (10,846,037 servers in total according to Shodan[2]). Second, DNS has a very large amplification factor, and hardening DNS servers is not as straightforward as just updating them, and certain procedures must be followed carefully to harden these servers [20]. There are two different calculation methods for DNS amplification factors; one regarding open resolvers and the other regarding authoritative resolvers. For open resolvers, the average packet amplification rate is 1.32x, while the BAF is 64.1x for the highest 10% of the servers and 61.2x for the highest 50%. For authoritative resolvers, the average packet amplifier rate is 2.08x, while the BAF is 98.3x for the highest 10% of the servers and 76.7x for the highest 50%. These factors can be achieved with the “ANY” query, which returns all data available about the queried domain. This information, combined with recursive queries, creates a situation that is useful for attackers [2].

Although DNS hardening methods have been known for decades, there are still many vulnerable servers across the internet. Many attacks have been carried out exploiting these vulnerable servers causing great damage on victim domains.

Many significant DRDoS attacks have occurred over the past few years that exploited DNS servers. A major attack in 2015 targeted Turkey, which has been known as the “nic.tr attack”. According to the official nic.tr statement [21], the attack traffic at one point exceeded 200 Gbps. The attack resulted in slowing down the country’s internet access in general without any specific target.

Another major DNS-based DRDoS attack occurred a year later in October 2016 which came to be known as the“Dyn attack”. The attack

2. https://www.shodan.io/search?query=port%3A53

targeted Dyn, Inc. which provides DNS services for major companies such as Twitter, Spotify, SoundCloud, Boston Globe, New York Times, Vox Media, Reddit, Box, Github, Airbnb, Freshbooks, and Heroku. Many of these services, including Twitter, became unreachable during the attack [22]. An interesting point about the Dyn attack was that the attack was executed from "internet of things" (IoT) devices infected by the Mirai malware. Through malicious requests from tens of millions of IoT devices, the attack reached a record volume of 1.2 Tbps, which highlighted the potential of IoT devices for the future of DDoS attacks.

Another service that attackers frequently use as an amplifier is the NTP protocol, which is used for consistent time synchronization over the internet. The main reason for using NTP servers as amplifiers is the protocol's potentially very high packet and byte amplification factor: The packet amplification factor is 10.61x byte on average, 4670x for the highest 10% of the servers and 1083x for the highest 50% [2]. These high amplification factors are related to the "monlist" query, which returns information on recently connected devices to that server, and is normally used for administrative purposes. The response message contains information on the last 600 devices that connected to the server and includes detailed information such as the IP addresses, how many times each client connected, and the version number. If there is no hardening on the server, it will respond to any query made by anyone.

Many attacks exploiting the NTP protocol have occured in recent years. One of the most significant attacks was conducted in February 2014. Cloudflare announced that one of its costumers was attacked with a traffic of 400 Gbps [23]. Attackers exploited 4,529 NTP servers from 1,298 different networks, where each server sent a traffic of up to 87 Mbps to the victim.

Memcached is a protocol designed for speeding up dynamic web applications by mitigating database load. This protocol was not seen in DRDoS attacks until recently, when an attack in February 2018 targeted GitHub servers with a traffic that peaked at 1.3 Tbps using the Memcached protocol, which was the largest attack volume ever seen until that day [24]. The main source for the power of this attack was the large amplification factor of the Memcached protocol, which may can be as high as 50000x.

3. Methodology

In this study we focused on 41 European countries. We used Ivan Erben's semi-live database[3] to obtain country IP addresses. His automated script scans all countries' IP CIDRs daily, and the results are published freely.[4]

To discover all DNS, NTP and Memcached servers in these IP blocks, we used the "ZMap" tool [25], developed by Durumeric et al. for internet-wide network scans. According to its developers, this tool can scan the entire public IPv4 address domain under 45 minutes with a gigabit connection.[5]

We started our study by scanning UDP port 53 over the IP address domains for DNS servers. We scanned all these countries with two different probes available in ZMap: "dns_53_queryAwww.google.com.pkt" and "dns_53_queryAwww.google.it.pkt". We also scanned all these IPs without probes, directly

3. http://www.iwik.org/ipcountry/

4. http://blog.erben.sk/2014/01/28/generating-country-ip-ranges-lists/

5. https://zmap.io/

with a UDP scan. After the scans were finished we ran a script to see whether the discovered servers were amplifiers. We used the "nslookup" command in this script and sent an "ANY" request to these discovered servers, as it is favored by attackers. As we explained in Section 2.1, the highest amplification factor for DNS is obtained by an ANY lookup. The response to this request returns all records the server has regarding the queried domain. This vulnerability of the DNS protocol is identified as CVE-2006-0987 [26] and CVE-2006-0988 [27]

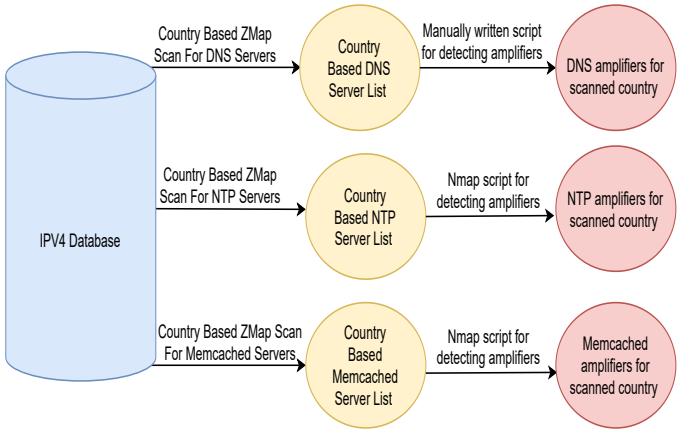

Fig. 2. Country-based scanning process for three protocols.

After DNS we studied the NTP servers. We used a ZMap probe which was written specifically to discover NTP servers in the IPv4 domain. We used ZMap output results as the input list for Nmap[6], which is a well-known tool for scanning services and vulnerabilities. Nmap has the script "ntp-monlist" for gathering responses to monlist queries, and we used it to gather the monlist responses. The monlist DRDoS vulnerability of NTP servers is identified as CVE-2013-5211 [28].

For the Memcached study, we used a method similar to that used for NTP, combining ZMap with Nmap. The Memcached protocol runs on port 11211 over both TCP and UDP. If the UDP port is open, it leads to the amplification vulnerability as identified by CVE-2018-1000115 [29]. If the server is hardened, it should be running only on TCP. We first identified the available Memcached servers by scanning the TCP port 11211 with ZMap. After this scan was completed, we used the Nmap script "memcached-info" written for gathering Memcached servers' information and identified the vulnerable ones with UDP port 11211 open.

The scanning process for these three protocols is illustrated in Figure 2.

We summarized the commands and scripts that we used to identify vulnerable servers in the Appendix section.

4. Results

In this section, we summarize the results of our automated scan of exploitable amplifier servers in European countries for DNS, NTP, and Memcached. We rank the countries according to the awareness we observed as a result of this analysis.

4.1. DNS Results

In our scan of UDP port 53 for DNS servers, we discovered 4,709,277 servers in 41 countries. Among them, 3,107,409 were not directly reachable, and 1,279,787 were successfully hardened. The remaining 322,081 were usable for DRDoS attacks in one way or the other, as we explain below.

If a DNS server is correctly hardened against DRDoS reflection attacks, it should respond by "REFUSED" to a request of type "ANY". The

6. https://nmap.org

response sent to the querying party by such a hardened server is shown in Figure 3.

```
root@ubuntu:/home/mercan# nslookup -timeout=4 -retry=1 -q
=ANY www.etu.edu.tr 1  .1  .9 .1
Server:         1  .1  .9 .1
Address:        1  .1  .9 .1 #53

** server can't find www.etu.edu.tr: REFUSED
```

Fig. 3. Response of a correctly hardened DNS server.

A DNS server can be exploitable for DRDoS reflection in several ways: It can be completely unhardened, responding to an "ANY" query with the full data available for that domain, which causes a large amplification factor. The response of such an unhardened server is demonstrated in Figure 4. In our survey, we identified 35,395 unhardened servers in 41 countries.

```
root@ubuntu:/home/mercan# nslookup -timeout=4 -retry=1 -q
=ANY www.etu.edu.tr 1  .1  .3 .4
Server:         109.1  .3 .4
Address:        109.1  .3 .4 #53

Non-authoritative answer:
Name:   www.etu.edu.tr
Address: 2001:a98:100:1b:10:1:11:140
Name:   www.etu.edu.tr
Address: 193.140.108.140

Authoritative answers can be found from:
etu.edu.tr      nameserver = ns1.etu.edu.tr.
etu.edu.tr      nameserver = ns2.etu.edu.tr.
etu.edu.tr      nameserver = ns.ulak.net.tr.
ns1.etu.edu.tr  internet address = 1  .1  .1  .2
ns2.etu.edu.tr  internet address = 1  .1  .1  .1
```

Fig. 4. Response of an unhardened DNS server.

A second kind of exploitable DNS servers are "partially hardened", responding with only the IP information of the queried domain. The amplification caused by such servers is not as bad as unhardened servers, but still exploitable for DRDoS attacks. The response of such a server queried for the www.etu.edu.tr domain is shown in Figure 5. In our survey, we identified 239,133 partially hardened servers in 41 countries.

```
root@ubuntu:/home/mercan# nslookup -timeout=4 -retry=1 -q
=ANY www.etu.edu.tr 109.106.136.212
Server:         1  .1  .1  .2
Address:        1  .1  .1  .2  #53

Non-authoritative answer:
Name:   www.etu.edu.tr
Address: 2001:a98:100:1b:10:1:11:140
Name:   www.etu.edu.tr
Address: 193.140.108.140

Authoritative answers can be found from:
```

Fig. 5. Response of a partially hardened DNS server.

A third kind of DNS amplification vulnerability is caused by servers that return a list of other servers to be contacted as a response. This is different from an unhardened server, but is potentially more dangerous with a higher amplification factor. The response of such a DNS server is demonstrated in Figure 6. We categorized the DNS servers with this condition separately and labeled them as "misconfigured", in the sense that these servers are misconfigured for the purpose of a DRDoS defense. In our survey, we identified 72,524 misconfigured servers in 41 countries with this vulnerability.

The DNS amplifier distribution results according to countries are summarized in Table 1. In the "Port 53 Open" column, the total number of servers discovered via the ZMap scan is given. The "Part.Hardened" column shows the number of servers that return only IP records about the requested domain. The "Unhardened" column shows the number of servers that return all the available data for the queried domain. The "Misconfigured" column shows the number of servers that return the information of other servers to be queried. The "Ratio" column shows the proportion of exploitable DNS servers in that country. Countries are ranked from the best (i.e., the lowest) to the worst (i.e., the highest) in terms

TABLE 1
Country-based DNS vulnerability results, in increasing order (i.e., from best to worst).

Country	Port 53	Part.Hardened	Unhardened	Misconfigured	Total	Ratio
Spain	990684	4636	415	2116	7167	0.00723
Croatia	75877	280	69	362	711	0.00937
Belgium	82171	838	139	354	1331	0.01620
Malta	9413	147	6	74	227	0.02412
Finland	53993	1242	101	203	1546	0.02863
Netherlands	209751	5342	404	3422	9168	0.04371
France	438344	12682	2967	3673	19322	0.04408
Germany	406282	13188	839	6096	20123	0.04953
Norway	46200	1724	260	381	2365	0.05119
Estonia	10437	410	96	147	653	0.06257
Lithuania	20143	620	324	413	1357	0.06737
Luxembourg	2917	128	28	56	212	0.07268
Romania	153822	8635	814	2003	11452	0.07445
Bosnia	6948	248	162	171	581	0.08362
Czechia	70802	3558	1228	1421	6207	0.08767
Armenia	8467	284	246	225	755	0.08917
Russia	573916	32909	8436	11786	53131	0.09258
Iceland	2376	131	32	67	230	0.09680
Latvia	18698	685	485	648	1818	0.09723
Ireland	13426	926	67	360	1353	0.10077
Portugal	27289	2012	275	559	2846	0.10429
Poland	140181	9125	2049	3909	15083	0.10760
Sweden	109745	9144	1257	1458	11859	0.10806
Slovenia	7009	333	85	355	773	0.11029
Switzerland	31275	2422	422	769	3613	0.11552
Italy	238688	23412	1786	2737	27935	0.11704
Austria	19651	1367	382	585	2334	0.11877
Denmark	14336	822	560	344	1726	0.12040
Hungary	28301	1564	925	980	3469	0.12258
Greece	15320	1121	440	355	1916	0.12507
UK	325067	34384	1839	6563	42786	0.13162
Bulgaria	130017	14837	854	1953	17644	0.13571
N. Macedonia	2587	159	133	113	405	0.15655
Slovakia	15138	1042	723	660	2425	0.16019
Turkey	234003	28244	1495	10571	40310	0.17226
Ukraine	133452	16143	1981	4879	23003	0.17237
Moldova	11697	1740	257	210	2207	0.18868
Belarus	4944	591	151	297	1039	0.21015
Serbia	21683	1266	2470	924	4660	0.21491
Albania	3410	326	168	291	785	0.23021
Montenegro	817	466	25	34	525	0.64259
Total	4709277	239133	35395	72524	347052	

of the exploitable server ratios. Spain has the best mitigation performance according to these results, whereas Montenegro has the worst. While about 7 out of every 1000 DNS servers discovered in Spain are available as reflectors, this number is 645 in Montenegro.

```
root@ubuntu:/home/mercan# nslookup -timeout=4 -retry=1 -q
=ANY www.etu.edu.tr 1  .2  .1  .13
Server:         1  .2  .1  .1
Address:        1  .2  .1  .1 #53

Non-authoritative answer:
*** Can't find www.etu.edu.tr: No answer

Authoritative answers can be found from:
.       nameserver = m.root-servers.net.
.       nameserver = h.root-servers.net.
.       nameserver = a.root-servers.net.
.       nameserver = i.root-servers.net.
.       nameserver = b.root-servers.net.
.       nameserver = l.root-servers.net.
.       nameserver = g.root-servers.net.
.       nameserver = f.root-servers.net.
.       nameserver = c.root-servers.net.
.       nameserver = e.root-servers.net.
.       nameserver = j.root-servers.net.
.       nameserver = d.root-servers.net.
.       nameserver = k.root-servers.net.
m.root-servers.net      internet address = 202.12.27.33
h.root-servers.net      internet address = 128.63.2.53
a.root-servers.net      internet address = 198.41.0.4
i.root-servers.net      internet address = 192.36.148.17
b.root-servers.net      internet address = 128.9.0.107
l.root-servers.net      internet address = 198.32.64.12
g.root-servers.net      internet address = 192.112.36.4
f.root-servers.net      internet address = 192.5.5.241
c.root-servers.net      internet address = 192.33.4.12
e.root-servers.net      internet address = 192.203.230.10
j.root-servers.net      internet address = 192.58.128.30
d.root-servers.net      internet address = 128.8.10.90
k.root-servers.net      internet address = 193.0.14.129
```

Fig. 6. Response of a misconfigured DNS server.

4.2. NTP Results

As we explained in Section 2, the monlist query in NTP is used for administrative purposes. It returns a list of recently connected devices to that server with some additional information. If a server has many recently connected clients, a monlist query may result in a very large amplification factor.

Through our ZMap scan of UDP port 123, we discovered 3,302,943 NTP servers in 41 European countries. Although the NTP hardening requirements were specified in 2013, we discovered 5,132 NTP servers are still exploitable for DRDoS attacks.

Similar to DNS, an NTP server can be exploitable for DRDoS reflection in several different ways: It can be completely unhardened, returning all relevant information of the connected clients, or it can be partially hardened, returning just the IP addresses. The latter can be very risky as an amplifier as well, depending on the number of recently connected clients. With a high number of recent clients, a partially hardened server will have a much higher BAF than unhardened servers with few clients, as we discuss below.

The response we get from a partially hardened NTP server, which returns only the IP address information, is given below. The server in this example has just one client connection. Even though such a partially hardened server can be used for an attack, it will provide little amplification as long as it has just a few clients:

```
ntp-monlist:
Target is synchronised with 1xx.1xx.1xx.xx0
Public Clients (1)
1xx.1xx.1xx.2xx
```

The response of a completely unhardened server will be only slightly larger, if it also has just a few client connections. Such an example is given below. Although it is somewhat more effective as an amplifier than the partially hardened NTP server above, it still has a relatively small BAF due to the small number of recent client connections:

```
ntp-monlist:
Target is synchronised with 1xx.1xx.1xx.xx0
Alternative Target Interfaces:
1xx.1xx.1xx.1xx
Public Clients (1)
1xx.1xx.2xx.1xx
Other Associations (1)
1xx.1xx.1xx.xx2 (You?) seen 3 times.
last tx was unicast v2 mode 7
```

A more dangerous case arises when the server has many recent client connections. In this case, even if the server is partially hardened, the monlist response message will be quite large. Such an example is given in Figure 7 where the server has 588 recent connections, and it is much more risky as an amplifier than the completely unhardened server with just a few client connections.

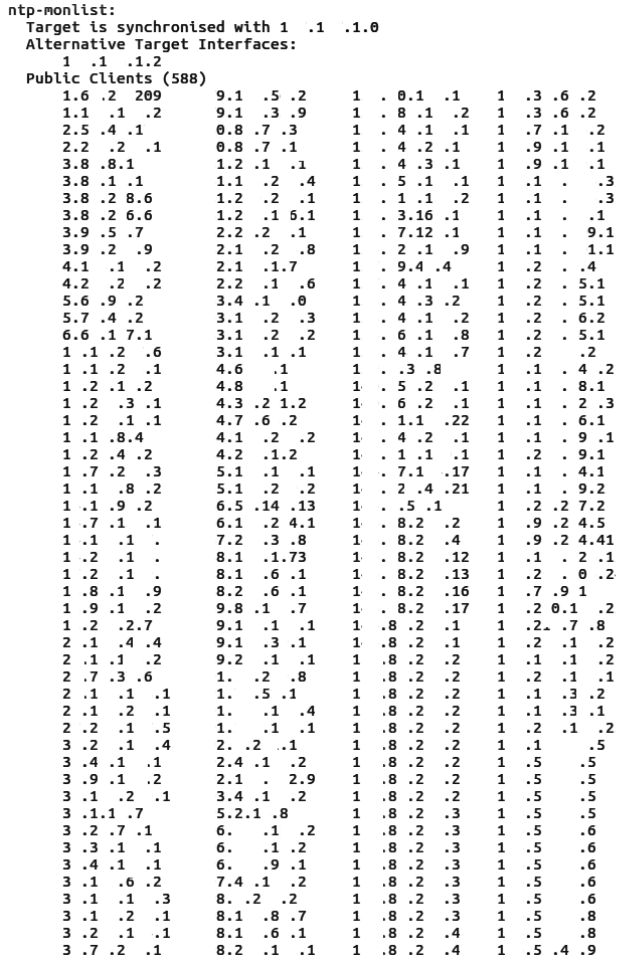

Fig. 7. Response of a partially hardened NTP server with many clients. Only the first screen (204 clients in this case) is shown here due to space limitations.

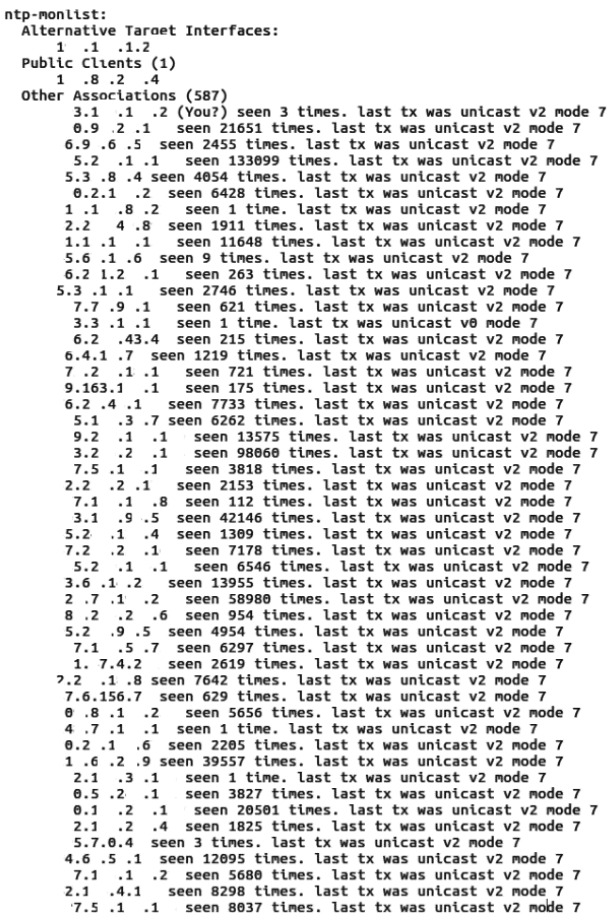

Fig. 8. Response of an unhardened NTP server with many clients. Only the first screen (50 clients in this case) is shown here due to space limitations.

Figure 8 shows an example of an NTP server that is not hardened and has many clients recently connected to it. This is the riskiest combination for an NTP reflection attack.

The results of the NTP monlist scans we made over the 41 countries are shown in Table 2. The "Port 123 Open" column shows the total number of NTP servers discovered in a country. The "Only IP" column shows the number of partially hardened servers, such as those in Figure 7, whose monlist responses are limited to the clients' IP addresses. In the "Full" column, the number of servers responding with the full answer format, such as those in Figure 8, is given. The "Ratio" column shows the proportion of exploitable NTP servers in a country. Again, countries are ranked from the best to the worst in terms of exploitable server ratios.

In this analysis, Luxembourg and Montenegro stand out as countries with no exploitable NTP amplifiers. Estonia and Switzerland are also re-

TABLE 2
Country-based NTP vulnerability results, in increasing order (i.e., from best to worst).

Country	Port 123	Only IP	Full	Total	Ratio
Luxembourg	3267	0	0	0	0
Montenegro	1048	0	0	0	0
Estonia	6792	1	0	1	0.00015
Switzerland	112763	17	1	18	0.00016
Denmark	38090	8	1	9	0.00024
Germany	409388	85	21	106	0.00026
Romania	95904	19	7	26	0.00027
Russia	525551	153	27	180	0.00034
Slovakia	26604	8	2	10	0.00038
Belarus	15907	4	2	6	0.00038
Serbia	16017	7	0	7	0.00044
Croatia	8836	4	0	4	0.00045
Slovenia	8387	4	0	4	0.00048
Italy	605936	262	45	307	0.00051
N. Macedonia	8519	5	0	5	0.00059
Moldova	10041	5	1	6	0.00060
UK	286877	148	31	179	0.00062
Ukraine	60783	27	12	39	0.00064
Iceland	5905	3	1	4	0.00068
Ireland	10313	5	2	7	0.00068
Sweden	90982	50	12	62	0.00068
Albania	5775	2	2	4	0.00069
Malta	2863	2	0	2	0.00070
Belgium	37806	24	6	30	0.00079
Netherlands	135962	90	23	113	0.00083
Czechia	65614	43	14	57	0.00087
Bulgaria	36811	28	4	32	0.00087
Bosnia	3308	3	0	3	0.00091
Poland	70118	95	22	117	0.00167
Portugal	45223	64	14	78	0.00172
Finland	21640	34	4	38	0.00176
Austria	34875	64	5	69	0.00198
France	266694	558	46	604	0.00226
Norway	42988	114	12	126	0.00293
Armenia	2306	5	2	7	0.00304
Greece	24983	67	9	76	0.00304
Lithuania	3584	11	2	13	0.00363
Hungary	6096	29	2	31	0.00509
Spain	70602	739	115	854	0.01210
Turkey	77436	1865	16	1881	0.02429
Latvia	349	12	5	17	0.04871
Total	3302943	4664	468	5132	

markable for their small numbers. The countries with the highest vulnerability ratios are Latvia, Turkey, and Spain where approximately 48, 24, and 12 servers, respectively, out of every 1000 are vulnerable.

It should also be noted that the ratios of

vulnerable servers for NTP are much smaller than those for the other two protocols we studied, DNS and Memcached. Remarkably, 28 out of the 41 surveyed countries have a vulnerability ratio that is below 1/1000 for NTP.

4.3. Memcached Results

As we explained earlier, Memcached is used by web servers to mitigate database load. It can run either on TCP or UDP, on port 11211. After the 2018 DRDoS attack on GitHub, Memcached servers have been recommended to disable running on UDP as a hardening measure [29].

Through our ZMap scan of Memcached servers, we discovered 742,267 servers broadcasting over TCP port 11211 in 41 countries, where United Kingdom with 146,667 Memcached servers had the highest number. Through our Nmap scan for UDP, we identified 4,238 servers with UDP port 11211 open and hence can be abused as amplifiers. The results are summarized in Table 3. The "Port 11211" column shows the total number of Memcached servers in a country discovered via the ZMap scan. The "UDP" column indicates the number of servers that respond to a UDP Memcached request. The "Ratio" column shows the proportion of exploitable servers in that country. Countries are ranked from the best to the worst in terms of the exploitable server ratios.

We found Russia to be the country with the highest number of amplifiers, but in terms of the vulnerability ratio Lithuania came first. Russia, Turkey, Germany, the United Kingdom, the Netherlands, and France together make up about 64% of the entire exploitable Memcached server population in Europe.

5. Conclusion and Recommendations

Reflection attacks are the dominant technique used by DDoS attackers today, and they will remain significant in the future of DDoS attacks. Adversaries are already abusing UDP-based services to achieve attack volumes of hundreds of gigabits. They can abuse many different protocols to obtain these volumes. In this paper, we concentrated on three of the most significant ones: DNS, NTP, and Memcached. We found that although there are well-defined methods for fixing these services' vulnerabilities, plenty of vulnerable servers remain as available amplifiers for attackers.

Hardening of NTP and Memcached servers is quite straightforward and can be achieved by a software update, whereas hardening of DNS servers is slightly more complex. DNS servers have two main restrictions to be applied to make them unusable as amplifiers: Disabling recursive searches is the first one [20], and restricting "ANY" queries is the second [30].

Hardening of NTP servers is achieved by restricting or disabling monlist requests. These restrictions can be implemented manually or by automatic updates. Besides command-line interface programming, system administrators can make their NTP servers immune to exploitation by upgrading their systems to ntpd version 4.2.7 or later [31], [32].

Memcached servers have two main issues regarding hardening. First, it must be decided whether the server needs be open to the internet. The official recommendation for Memcached servers [33] states that servers should not be open to the internet unless they have to. Second, if a server has to be on the internet, UDP port 11211 must be disabled. Like NTP servers, Memcached servers can be hardened either manually [34] or

TABLE 3
Country-based Memcached vulnerability results, in increasing order (i.e., from best to worst).

Country	Port 11211	UDP	Ratio
Bosnia	39	0	0
Malta	40	0	0
Croatia	64871	6	0.00009
Denmark	8703	1	0.00011
Finland	32500	4	0.00012
Austria	3932	1	0.00025
Belgium	13962	6	0.00043
Estonia	4313	3	0.00070
Iceland	693	1	0.00144
Norway	9216	14	0.00152
France	129797	347	0.00267
UK	146677	401	0.00273
Romania	26864	78	0.00290
Spain	8907	32	0.00359
Latvia	8212	30	0.00365
Poland	25031	96	0.00384
Slovenia	960	4	0.00417
Italy	27901	163	0.00584
Greece	698	5	0.00716
Czechia	5290	41	0.00775
Sweden	6557	71	0.01083
Germany	42658	580	0.01360
Switzerland	2060	29	0.01408
Luxembourg	110	2	0.01818
Netherlands	19431	385	0.01981
Armenia	47	1	0.02128
N. Macedonia	46	1	0.02174
Albania	35	1	0.02857
Slovakia	242	8	0.03306
Hungary	770	34	0.04416
Turkey	11719	595	0.05077
Bulgaria	513	28	0.05458
Portugal	226	15	0.06637
Ukraine	1284	89	0.06931
Russia	9863	786	0.07969
Serbia	115	10	0.08696
Montenegro	11	1	0.09091
Belarus	43	4	0.09302
Moldova	70	7	0.10000
Ireland	185	20	0.10811
Lithuania	430	338	0.78605
Total	742267	4238	

by an automatic update: A few days after the GitHub attack, a new version (1.5.6) was released to fix that vulnerability [35].

In our study, we noticed that some countries have shown a good performance on all three protocols, such as Estonia and Croatia, and, to a

lesser degree, Malta. Some other countries such as Denmark did well on NTP and Memcached, which can be hardened by a software update, but did poorly on DNS. Still some other countries, such as Armenia, Albania, Hungary, and Turkey, showed a relatively bad performance in most, if not all, protocols.

With performance pressures constantly high, there will be many UDP-based services in use on the internet in the foreseeable future and we will see many servers being exploited as amplifiers. This will lead to higher traffic volumes in DRDoS attacks with more damaging effects. Constant vigilance and regular maintenance will always be necessary to keep the internet running without being crippled by DRDoS attacks.

Appendix
Discovering Vulnerable Servers

In this appendix, we list the commands and scripts that we used to discover vulnerable DNS, NTP, and Memcahced servers. After discovering the IP addresses of the servers within a given country via ZMap, as described in Section 3, we ran the following commands to find out the vulnerable ones. For each protocol, [zmap output file] denotes the file containing the list of server IP addresses returned by ZMap.

To discover the vulnerable DNS servers that allow an "ANY" request, the following script is used:

```
#!/bin/sh
for LINE in ‘cat [zmap output file]‘
do
echo ”-------------------------” >> [output file]
echo ”IP = $LINE\n” >> [output file]
nslookup -q=ANY etu.edu.tr $LINE >> [output file]
done
```

The results returned by this script are analyzed according to four possible criteria: If the response says "REFUSED", this shows the DNS server has been properly hardened. Otherwise, it may return the full DNS record of the queried domain, or its IP information, or a list of root servers to be contacted, as illustrated in Figures 4, 5, and 6, respectively. As explained in Section 4.1, these cases are classified as unhardened, partially hardened, and misconfigured DNS servers, respectively.

To discover the vulnerable NTP servers that respond to a monlist query, the following command is used which utilizes Nmap's ready "ntp-monlist" script:

```
nmap -sU -n -p 123 -Pn --script=ntp-monlist -iL
[zmap output file] -oN [nmap output file]
```

The results returned by this command are analyzed according to three possible criteria: If the result only says that the port is open and gives no further information, this indicates a properly hardened server. Otherwise, the response may either contain the IP addresses of recently connected clients or their detailed information, as shown in Figures 7 and 8. These cases are classified as partially hardened and unhardened NTP servers, respectively, as described in Section 4.2.

Finally, to discover the vulnerable Memcached servers that respond to a UDP Memcached query, the following command is used which utilizes Nmap's ready "memcached-info" script:

```
nmap -p 11211 --script memcached-info -iL
[zmap output file] -oN [nmap output file]
```

The vulnerable servers are indicated by the status information in the output file: A status with UDP PORT 0 indicates a properly hardened server, whereas a status with UDP PORT 11211

indicates a vulnerable server.

Acknowledgments

We would like to thank Bahtiyar Bircan, Evren Pazoğlu, Kamil Seyhan, and Sertaç Katal for their suggestions on our discovery methods and for their comments on the paper.

References

[1] Specht SM, Lee RB. Distributed denial of service: taxonomies of attacks, tools, and countermeasures. In: International Conference on Parallel and Distributed Computing Systems (ISCA PDCS), San Francisco, CA, USA, 2004.

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

[3] Bellovin SM. Security problems in the TCP/IP protocol suite. ACM SIGCOMM Computer Communication Review 1989, 19 (2): 32–48.

[4] Kührer M, Hupperich T, Rossow C, Holz T. Exit from hell? Reducing the impact of amplification DDoS attacks. In: 23rd USENIX Security Symposium, San Diego, CA, USA, 2014.

[5] Kührer M, Hupperich T, Rossow C, Holz T. Hell of a handshake: Abusing TCP for reflective amplification DDoS attacks. In: 8th USENIX Workshop on Offensive Technologies (WOOT'14), San Diego, CA, USA, 2014.

[6] CERT. UDP-based amplification attacks. CERT Advisory, revised 2019. https://www.us-cert.gov/ncas/alerts/TA14-017A. Accessed: March 4, 2021.

[7] Heberlein LT, Bishop M. Attack class: address spoofing. In: 19th National Information Systems Security Conference, 1996.

[8] Webb A. How have DDoS weapons evolved in recent years? International Security Journal 2019. https://internationalsecurityjournal.com/how-have-ddos-weapons-evolved/. Accessed: March 4, 2021.

[9] Ryba FJ, Orlinski M, Wahlisch M, Rossow C, Schmidt TC. Amplification and DRDoS attack defense - a survey and new perspectives. arXiv:1505.07892v3, 2016.

[10] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review 2004, 34 (2): 39–53.

[11] Asosheh A, Ramezani N. A comprehensive taxonomy of DDOS attacks and defense mechanism applying in a smart classification. WSEAS Transactions on Computers 2008, 7 (4): 281–290.

[12] Osterweil E, Stavrou A, Zhangi L. 20 Years of DDoS: A call to action. arXiv:1904.02739, 2019.

[13] Cloudflare. Famous DDoS attacks: The largest DDoS attacks of all time. Cloudflare Learning Center, 2020. https://www.cloudflare.com/learning/ddos/famous-ddos-attacks/. Accessed: March 4, 2021.

[14] Amazon Web Services. Threat Landscape Report – Q1 2020. AWS Shield, 29 May 2020. https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf. Accessed: March 4, 2021.

[15] Prolexic Technologies. Prolexic stops largest-ever DNS reflection DDoS attack. Prolexic Quarterly Global DDoS Attack Report Q2 2013.

[16] Weinberg F. NGO Forum website launched before crucial presidential elections in Zimbabwe. HURIDOCS, 30 July 2013.

[17] Prince M. The DDoS that almost broke the Internet. The Cloudflare Blog, 27 March 2013.

[18] Prince M. The DDoS that knocked Spamhaus offline (and how we mitigated it). The Cloudflare Blog, 20 March 2013.

[19] Takashi D. Hackers attack Dota 2 and League of Legends servers in quest for one game livestreamer. GamesBeat, 30 December 2013.

[20] US CERT. Alert TA13-088A: DNS Amplification Attacks. CERT Alerts, 2013. https://us-cert.cisa.gov/ncas/alerts/TA13-088A. Accessed: March 4, 2021.

[21] Nic.TR. 14/12/2015 Tarihinde Başlayan DDoS Saldırısı. Nic.TR Kamuoyu Duyurusu. 21 December 2015 (in Turkish).

[22] Chacos B. DDoS attack on Dyn DNS knocks Spotify, Twitter, Github, PayPal, and more offline. PCWorld, 21 October 2016.

[23] Prince M. Technical details behind a 400Gbps NTP amplification DDoS attack. The Cloudflare Blog, 13 February 2014.

[24] Kottler S. February 28th DDoS incident report. The GitHub Blog, 1 March 2018. https://github.blog/2018-03-01-ddos-incident-report/. Accessed: March 4, 2021.

[25] Z. Durumeric Z, Wustrow E, Halderman JA. ZMap: fast Internet-wide scanning and its security applications. In: 22nd USENIX Security Symposium, Washington, DC, USA, 2013.

[26] MITRE. CVE-2006-0987 detail. National Vulnerability Database, 2006. https://nvd.nist.gov/vuln/detail/CVE-2006-0987. Accessed: March 4, 2021.

[27] MITRE. CVE-2006-0988 detail. National Vulnerability Database, 2006. https://nvd.nist.gov/vuln/detail/CVE-2006-0988. Accessed: March 4, 2021.

[28] MITRE. VE-2013-5211 detail. National Vulnerability Database, 2013. https://nvd.nist.gov/vuln/detail/CVE-2013-5211. Accessed: March 4, 2021.

[29] MITRE. CVE-2018-1000115 detail. National Vulnerability Database, 2018. https://nvd.nist.gov/vuln/detail/CVE-2018-1000115. Accessed: March 4, 2021.
[30] Microsoft. Use DNS policy for applying filters on DNS queries. Microsoft Documentation, 2020.
[31] Team Cymru. Secure NTP template. Team Cymru Community Services, 2019. https://www.team-cymru.com/secure-ntp-template.html. Accessed: March 4, 2021.
[32] Graham-Cumming J. Understanding and mitigating NTP-based DDoS attacks. The Cloudflare Blog, 9 January 2014.
[33] Dormando. Disable UDP port by default. https://github.com/memcached/memcached/commit/dbb7a8af90054bf4ef51f5814ef7ceb17d83d974. 27 February 2018. Accessed: March 4, 2021.
[34] Alibaba Cloud. Harden Memcached service security. Alibaba Cloud Security Advisories, 8 May 2018.
[35] Dormando. Memcached 1.5.6 release notes. https://github.com/Memcached/Memcached/wiki/ReleaseNotes156. 27 February 2018. Accessed: March 4, 2021.