Aalborg Universitet

AALBORG UNIVERSITY
DENMARK

Large-scale empirical evaluation of DNS and SSDP amplification attacks

Anagnostopoulos, Marios; Lagos, Stavros; Kambourakis, Georgios

Published in:
Journal of Information Security and Applications

DOI (link to publication from Publisher):
10.1016/j.jisa.2022.103168

Creative Commons License
CC BY 4.0

Publication date:
2022

Document Version
Publisher's PDF, also known as Version of record

Link to publication from Aalborg University

Citation for published version (APA):
Anagnostopoulos, M., Lagos, S., & Kambourakis, G. (2022). Large-scale empirical evaluation of DNS and SSDP amplification attacks. *Journal of Information Security and Applications*, *66*, Article 103168. https://doi.org/10.1016/j.jisa.2022.103168

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal -

Take down policy
If you believe that this document breaches copyright please contact us at vbn@aub.aau.dk providing details, and we will remove access to the work immediately and investigate your claim.

Downloaded from vbn.aau.dk on: April 17, 2024

Journal of Information Security and Applications 66 (2022) 103168

Contents lists available at ScienceDirect

Journal of Information Security and Applications

journal homepage: www.elsevier.com/locate/jisa

Large-scale empirical evaluation of DNS and SSDP amplification attacks

Marios Anagnostopoulos [a], Stavros Lagos [b], Georgios Kambourakis [c,*]

[a] Department of Electronic Systems Aalborg University, Denmark
[b] Department of Information and Communication Systems Engineering, University of the Aegean, 83200 Samos, Greece
[c] European Commission, Joint Research Centre (JRC), 21027 Ispra, Italy

ARTICLE INFO

Keywords:
DDoS
DNS
SSDP
Network security
Internet measurement
Amplification attacks
Reflection attacks

ABSTRACT

Reflection-based volumetric distributed denial-of-service (DDoS) attacks take advantage of the available to all (open) services to flood and possibly overpower a victim's server or network with an amplified amount of traffic. This work concentrates on two key protocols in the assailants' quiver regarding DoS attacks, namely domain name system (DNS) and simple service discovery protocol (SSDP). Our contribution spans three axes: (a) We perform countrywide IP address scans (probes) across three countries in two continents to locate devices that run open DNS or SSDP services, and thus can be effectively exploited in the context of amplification attacks, (b) we fingerprint the discovered devices to derive information about their type and operating system, and (c) we estimate the amplification factor of the discovered reflectors through a dozen of diverse, suitably crafted DNS queries and a couple of SSDP ones depending on the case. The conducted scans span fifteen months, therefore comparative conclusions regarding the evolution of the reflectors population over time, as well as indirect ones regarding the security measures in this field, can be deduced. For instance, for DNS, it was calculated that the third quartile of the amplification factor distribution remains more than 30 for customarily exploited queries across all the examined countries, while in the worst case this figure can reach up to 70. The same figures for SSDP range between roughly 41 and 73 for a specific type of query. To our knowledge, this work offers the first full-fledged mapping and assessment of DNS and SSDP amplifiers, and it is therefore anticipated to serve as a basis for further research in this ever-changing and high-stakes network security field.

1. Introduction

Nowadays, denial of service (DoS) attacks constitute a major threat against the resilience and stability of Internet's infrastructure. Indeed, according to a March 2020 report, it is estimated that the number and magnitude of distributed DoS (DDoS) assaults will constantly increase globally each year [1]. To fulfil their goals, DDoS attackers typically exploit protocols that rely on the user datagram protocol (UDP) transport protocol. That is, the connectionless nature of UDP facilitates the spoofing of the sending requests' source IP address, thus accomplishing the reflection of the attack traffic. Naturally, among others, this situation lingers due to the still insufficient adoption rate of BCP 38 [2]. On the other hand, there exist specific types of protocols requests that trigger hefty responses, hence significantly amplifying the attack traffic towards the victim device or network. In fact, the latest trend from the side of the assailants is to launch multi-protocol volumetric attacks, namely they utilize a variety of protocols, each one with high amplification capabilities to inflict the maximum possible impact on the victim [3].

More specifically, based on the 2021 "Threat Report FHY 2021 Distributed Denial of Service (DDoS)" by NexusGuard [4], DNS and SSDP amplification attacks account for about half of the total attacks of this kind, with the other half assigned to Connection-less Lightweight Directory Access Protocol (CLDAP) and Network Time Protocol (NTP) protocols, which also run over UDP. In addition, the proliferation of DDoS-capable IoT malware with complex, multi-vector attack repertoire [5–7], simply confirms this tendency and urges a closer scrutiny of the precipitating, perpetuating, or mitigating factors.

Contributing to this field, the present work offers a contemporary, multi countrywide, and full-fledged Internet measurement study on the potential of the domain name system (DNS), and particularly the domain name system security extensions (DNSSEC), as well as the simple service discovery protocol (SSDP) UDP-based protocols as catalysts in the context of overwhelming DDoS assaults. Particularly, the highlights of the current work can be summarized as follows:

- After probing the IP address ranges of three countries, namely Greece, Portugal, and Singapore, we identify devices that run DNS

* Corresponding author.
E-mail addresses: mariosa@es.aau.dk (M. Anagnostopoulos), icsdd20011@icsd.aegean.gr (S. Lagos), gkamb@aegean.gr, georgios.kampourakis@ec.europa.eu (G. Kambourakis).

https://doi.org/10.1016/j.jisa.2022.103168

Available online 3 April 2022
2214-2126/© 2022 The Author(s). Published by Elsevier Ltd. This is an open access article under the CC BY license (http://creativecommons.org/licenses/by/4.0/).

or SSDP services and potentially yield a high amplification factor. Such devices can be abused as DDoS reflectors in amplification attacks. Especially for DNS, the probing process embraces a variety of queries, i.e., protocol-specific fingerprinting, thus enabling a meticulous assessment of the discovered device's amplification ability.

- To obtain a clearer view, we fingerprint such devices, namely we extract information about the device type, the hardware, and the OS running on it, and loosely compare the volume of the results against those obtained by the well-known *Shodan* search engine. For DNS, the analysis is done separately for forwarders and resolvers, while for SSDP a particular focus is given to ephemeral source ports from which SSDP responses stem from. No less important, it is demonstrated that SSDP can be of great aid to remote opponents trying to fingerprint the internal network.
- To capture the general trend as well as the adoption rate of possible security countermeasures in this field, the experiments were done in a fifteen months time frame; the first during mid-March 2020 and the second in mid-June 2021.

As detailed in Section 6, vis-à-vis similar studies, which are scarce and anymore partly outdated, we examine and quantify the subject from three novel angles. First and foremost along with the identification of the DNS and SSDP reflectors, for the first time in the literature, we assess their amplification capabilities in a painstaking way, namely by means of diverse, properly crafted queries. Second, focusing on the DNS services per se, we differentiate between open DNS resolvers and forwarders, given that the reflection threat is mainly due to the latter. Namely, the population of forwarders is far much higher than that of resolvers, and the former are incorrectly configured to operate as such and typically left unattended for long periods, revealing an install and forget mentality. This contribution was made possible by meticulously fingerprinting the amplifiers, which in turn point at proper mitigations depending on the device type. In regard to SSDP, we examine two types of queries utilized for the advertising of offered services by the respective servers, and we investigate the peculiar use of ephemeral source ports in servers' responses.

The rest of the paper is split up into sections as follows. The next section delivers an introduction to volumetric DoS attacks exploiting UDP-based protocols. Section 3 provides preliminaries on DNS and SSDP protocols as enablers in the context of amplification attacks. Our methodology is presented in Section 4, while Section 5 presents the results. The related work is discussed in Section 6, and the paper is concluded in Section 7.

2. Preliminaries

The goal of volumetric DoS attacks is to abruptly exhaust the bandwidth of the victim with numerous and large in size packets. To this direction, the majority of DoS attacks take advantage of UDP-based protocols. This is due to the IP source address spoofing capability, which can be exploited for reflecting the attack traffic towards the victim. Furthermore, such UDP-based attacks capitalize on the amplification characteristics of network protocols, where specific types of request provide a much larger response. Overall, the amplification/reflection type of a DoS attack aims to flood the victim with traffic produced as a response to small but legitimate requests initiated by the attacker and redirected towards the victim via a reflector service [8].

Specifically, for accomplishing reflection, the assailant spoofs the source IP address of the requests, making them appear as they originate from the victim. Spoofing is straightforward for UDP-based protocols since they are connectionless in nature, and thus they do not establish a handshake with the initiator as in the case of TCP protocol. This way, the involved server reflects unwittingly its large responses towards the victim. Usually, the attackers favour on network protocols and services that support specific types of requests generating much larger responses compared with the triggering request. Typical examples of abused protocols are the DNS protocol, and especially DNSSEC [9], the network time protocol (NTP) [10], the Simple Service Discovery Protocol (SSDP) [11], and others. Typically, the perpetrators utilize servers of the protocols that operate "openly", meaning that these servers accept and respond to requests from anyone on the Internet and do not limit their services to their intranets.

The attack's efficiency is evaluated by its amplification factor (AF). In short, the greater the AF, the more voluminous the attack traffic and the quicker the bandwidth and resource saturation at the victim's side. Two ways for measuring the amplified traffic are reported in the literature [10]. The packet amplification factor (PAF) (Eq. (1)) expresses the number of – probably fragmented – IP packets the amplifier sends as a response to the request.

$$\text{PAF} = \frac{\text{response's number of packets}}{\text{request's number of packets}} \tag{1}$$

On the other hand, the bandwidth amplification factor (BAF) (Eq. (2)) [10,12] corresponds to the bandwidth multiplication in terms of the number of bytes that the amplifier sends, as a response to the request, divided by the number of bytes of the request. As it is a common practice in the related literature [10,13], this work considers only the application-layer messages (UDP payload), meaning that the length of the UDP packet headers are excluded from the aforementioned calculations.

$$\text{BAF} = \frac{\text{length(response)}}{\text{length(request)}} \tag{2}$$

Until now, a great number of amplification attack incidents with enormous AF have been reported. The most severe case was that of the *Memcached* attack, where perpetrators exploited a vulnerability of memchached servers. These attacks achieved a BAF of 51,200 [14]. Other typical examples are that of NTP protocol where the *monlist* request can yield a maximum BAF of 4670 [10], and the DNS protocol where the *ANY* request for DNSSEC-related records can provide a BAF of up to 230 [15]. A representative example of a protocol with high packet amplification is the SSDP, which accomplishes a low BAF of 20, but a high PAF of 7, meaning that for each request, a SSDP server can reply with up to 7 responses [11].

3. Evaluated protocols

As already pointed out, this work assesses the contribution of DNS and SSDP protocols as facilitators in amplification/reflection DoS attacks. Precisely, the current section details on how these protocols operate, the way they are exploited for launching an amplification/reflection attack, and which type of queries (requests) are commonly abused to amplify the response.

3.1. Domain name system

The DNS service is used mainly to provide the mapping of a domain name to the corresponding IP address. It is based on the client–server architecture, where the server side of the service constitutes a distributed database organized in a hierarchical structure of domain zones. For each zone, there is a DNS authoritative nameserver (ANS) responsible to provide answers regarding the network resources of the zone. At the client side of the architecture, there are the DNS recursive resolvers, which undertake on the behalf of the end-users to traverse the DNS hierarchy and locate the final response for a domain name. For performance reasons, the DNS resolvers have caching capabilities, namely they store in their cache memory the received DNS resource records (RRs) for immediately fulfilling subsequent similar requests. There is another type of DNS client, called DNS forwarder, which accepts DNS queries and forwards them to a DNS resolver. In turn, the DNS resolver finds the answer and returns it to the forwarder. Usually, a forwarder possesses caching features as well. In numerous occasions, there exist

network devices, such as asymmetric digital subscriber line (ADSL) routers and network printers, that operate as open DNS forwarders due to a misconfiguration or inadequate and improper employment of security policies.

Typically, a recursive resolver belongs to an Internet service provider (ISP) or an internal network and serves solely the end-users connected to this specific network. However, there are DNS resolvers and forwarders that operate openly and provide their DNS services to the open Internet, meaning that clients from any network are able to send DNS requests to these open services and receive the resolutions. DNS uses both UDP and TCP port 53, with UDP being the default. Fallback to TCP typically happens when the packet size is too large to fit in a single UDP packet.

A DNS amplification attack [9] utilizes open DNS recursive resolvers or DNS forwarders as reflectors to send the DNS traffic towards the victim. Specifically, the attacker spoofs the source IP address of the packet to be that of the victim, and forwards these DNS requests towards the reflector. This way, the responses are directed to the victim instead of the initiator of the request. For amplifying the impact of the attack, the assailants use special type of queries that force the resolver to include multiple and sizeable records on its response. Before the DNSSEC extension, the attackers usually took advantage of DNS RR types that carry a volume of data, such as TXT records. However, with the increased adoption of DNSSEC, the aggressors' task become easier as the DNSSEC-related RRs are much more sizeable [12,16]. Furthermore, there exist a special type of meta-query called "ANY", which essentially returns all the available RRs about the queried domain name. There is no specification about what types and how many RRs the response will contain, but commonly a resolver responds with whatever RRs related to the queried domain name has in its cache memory. Recently, there is an increasing effort to deprecate the ANY query as it has no practical application, but rather it is abused heavily with the purpose of mounting DNS amplification attacks [17].

3.2. Simple service discovery protocol

With the proliferation of the computer equipment and networking devices dedicated for small office home office (SOHO) environments, the need for a simple and user hassle-free way of advertising and discovering network services over a network was emerged. To this direction, the SSDP protocol, as part of universal plug and play (UPnP) protocol, was proposed [18]. Specifically, SSDP offers a mechanism where devices with zero knowledge of the network can discover other network devices and services. This way, a network client can issue an *M-SEARCH* command. Then, all SSDP supporting devices will respond with the details of the service they provide. Note that for each different service offered, a separate response will be issued by the device. On top of everything else, this mechanism provides multicast discovery support as well as server-based notification and discovery routing. A device in SSDP is either a control point (client) or root (server) that offers one or more SSDP services. The protocol does not check if the control point that sent the multicast or unicast search request resides in the same network as the active UPnP root device. Therefore, every such IP packet with unicast addresses as source or destination could be routed through the Internet.

SSDP utilizes the hypertext transfer protocol over UDP (HTTPU) to send a message either to the multicast specific reserved address 239.255.255.250 or to the unicast address of the root device on port 1900. Besides the queries for specific kinds of devices, there are two generic query types:

- *upnp:rootdevice*, which seeks for all root devices.
- *ssdp:all*, which searches for all UPnP-supporting devices and services.

In the context of this work, both of these generic queries were probed for evaluating the magnitude (and difference) of the produced AFs. Throughout our experiments, a SSDP request was measured to have a payload between 90–100 bytes, while a SSDP response packet had a size around 100 bytes. Nevertheless, the fact that a UPnP-supporting device generates one response per distinct service, certifies that SSDP can straightforwardly facilitate amplifications attacks.

4. Methodology

The objective of our research work is to scan the IP ranges of three different countries, namely Greece and Portugal from the European continent and Singapore from South-East Asia. Our purpose is to detect and identify exploitable, possibly unattended, devices running DNS and SSDP services. As already mentioned, these devices can be exploited as reflectors in potential UDP-based amplification attacks. The choice of these specific three countries was made with the reasoning that all of them have more or less similar allocation of IP addresses, but they may differ significantly in regard to the level of security awareness. To obtain the blocks of the IP addresses for the considered countries, we used the ip2location.com[1] database.

For the "probing" and identification process, we issue a properly formatted request for each of the evaluated protocols to every IPv4 address contained in the country's IP range and monitor the triggered responses. Whenever a response is received from a specific IP address, it means that in this address a device operates the service openly, and therefore a potential reflector is found. Afterwards, the evaluation of each identified device is conducted in terms of amplification capabilities, namely we calculate both the BAF and PAF provided by the response of the device. That is, the incoming and outgoing traffic is assessed in terms of packet length in bytes for the case of DNS and packet length and multitude of packets received for the case of SSDP. Thus, Eq. (2) is applicable for the first case, while both Eqs. (2) and (1) are applied to the latter one.

4.1. DNS

The discovery process of either the DNS recursive resolvers or forwarders are akin to that given in [19]. First, a legitimate DNS request is issued to each candidate IP address. The domain name of the request is specifically crafted in such way so as if the receiving machine operates as DNS open resolver or forwarder will directly or indirectly consult the DNS ANS under our control. That is, the queried domain name is related with a domain zone that we have purchased and is under our control. In addition, the first (leftmost) label of this domain name contains in integer format the device's IP address that the query is headed to. Such queries are resolved with the help of wildcard DNS records. Finally, with the aid of a network sniffer, we capture all the incoming DNS packets in our ANS and process them to infer which devices are operating as either open DNS resolvers or forwarders. No less important, to avoid miscalculating devices with peculiar behaviour, that is, those which do resolve DNS requests, but do not return the responses to the initial requestor [20], we also capture the incoming traffic in the prober and filter out the unresponsive devices. The matching criteria used in this process is the IP address of the responder, the source port, and the transaction ID (TXID).

The experimental setup comprises a prober machine that generates and dispatches the DNS queries towards the pool of IP addresses per country. This machine is hosted in the network of our university campus. Moreover, we operate a DNS authoritative server hosted in the cloud, enabling us to monitor the ingress DNS traffic originating from the probed devices. For facilitating the experiment and not interfering

[1] IP2Location LITE IP-COUNTRY Database: https://lite.ip2location.com/database/ip-country.

with possible legitimate traffic, we utilize as source port of every DNS request the UDP ports 10,000 to 65,000 in a circular order.

In details, when a device receives our DNS request and does operate as open DNS resolver, it will try to resolve the queried domain name. For this purpose, it will traverse the DNS hierarchy and contact directly our ANS. In such case, the source IP address of the request reaching the ANS will be identical with the information contained in the first label of the domain name. This allows us to infer that in the investigated IP address does operate an open DNS resolver. On the other hand, if the receiving device functions as an open DNS forwarder, it will forward the request to a DNS resolver, which in turn will traverse the DNS hierarchy and reach our ANS. In that case, the source IP address of the request, that we will observe in the ANS, will be different from that contained in the first label of the queried domain name. In most of the cases, as verified by our experiments given in Section 5.2.1, the devices operating as open forwarders are related with the network's customer-premises equipment, and therefore we assume that they rely on the ISP's recursive resolver to forward the queries.

The identified devices, either open resolvers or forwarders, that actually resolve the DNS queries and return back to the initiator a DNS response, can be exploited as reflectors to steer DNS traffic towards a victim. However, further assessment to measure their amplification capabilities is conducted. As detailed in the next subsection, this is accomplished by means of different types of DNS queries, which allow us to measure the BAF produced by the devices for various scenarios.

4.1.1. Assessment of amplification capabilities

Depending on the queried domain name, the type of the requested RRs, the advertised buffer size, and whether the respondent supports DNSSEC, a DNS query triggers a various set of RRs to be included in the response. Essentially, a response of diverse length, possibly composed of several fragmented packets, results in a different BAF.

In the context of our experiments, the hosts identified as open DNS resolvers or forwarders were examined via eleven DNS queries, each one with a diverse set of characteristics. This way, we aim to estimate more accurately the BAF a host produces and evaluate its amplification potential. These queries are given below and explained in detail in Section 5.2.3.

- Q1: si. or fi., type 'A'
- Q2: si. or fi., type 'ANY'
- Q3: isc.org, type 'ANY', (DNSSEC), buffer size 8192
- Q4: isc.org, type 'DNSKEY', (DNSSEC), buffer size 8192
- Q5: isc.org type 'A', (DNSSEC), buffer size 8192
- Q6: si. or fi., type 'A', (DNSSEC), buffer size 8192
- Q7: tm. or lk., type 'A', (DNSSEC), buffer size 8192
- Q8: si. or fi., type 'DNSKEY', (DNSSEC), buffer size 8192
- Q9: tm. or lk., type 'DNSKEY', (DNSSEC), buffer size 8192
- Q10: si. or fi., type 'ANY', (DNSSEC), buffer size 8192
- Q11: tm. or lk., type 'ANY', (DNSSEC), buffer size 8192

The rationale behind the choice of the specific queries is as follows. Generally, the inclusion of DNSSEC-related RRs in a response increases excessively the BAF vis-à-vis the case where the base DNS protocol is involved [16]. Therefore, this fact will be evident when comparing the results of Q1, Q2 vis-à-vis those of the rest of the queries. Additionally, this juxtaposition will reveal whether the identified hosts support DNSSEC, and consequently they include in their responses DNSSEC-related RRs. Furthermore, it has been reported in the literature that the use of Top-level domain (TLD) instead of fully qualified domain name (FQDN) as the queried name provides a noticeably augmented BAF [15]. This assertion will be confirmed after collating Q3 to Q5 with the remaining queries. Historically, the specific domain name was involved in DNS amplification attack incidents, as an "ANY" query for this domain produced a BAF of more than 60 [21]. Fortunately, however, nowadays, the DNS response is much lower.

Finally, we query about various types of RRs, namely "A", "DNSKEY", and "ANY", which are expected to yield a different response size. Specifically, an "A" query type contains only the resolved IPv4 address of a domain, while a "DNSKEY" one provides the DNS public key(s) of the zone. According to RFC 6781 [22], it is recommended the usage of RSA public keys with a key length of at least 1024 bits, and further, each zone usually possesses two pairs of keys, i.e., the key signing key (KSK) and the zone signing key (ZSK). Lastly, the "ANY" query type forces the receiving server to return all the available RRs about the queried domain name. With this latter case, we aspire to investigate if the discovered open resolvers, or the resolvers that the discovered open forwarders consult, do apply the latest recommendations for minimizing the effects of the "ANY" query type [17]. It is worthy to note that, according to the results of our previous work [15], the considered TLDs provide a high BAF for the "ANY" query type, and they support DNSSEC.

4.2. SSDP

For SSDP protocol, a more direct approach is followed. Specifically, a properly formatted SSDP query is crafted and directed towards each IP address in the examined IP ranges. The query contains a header with configurable parameters. The interesting ones in the context of our experiment are those for the host (HOST) and the search target (ST). Precisely, the parameter for host can be configured with the IP address that the query is addressed to or the multicast address *239.255.255.250*, followed by a colon and the standard SSDP port number, which is 1900. The ST determines the type of service required. In this work, as already explained in Section 3.2, both the generic query types, i.e., ssdp:all and upnp:rootdevice are investigated.

Since a SSDP response does not provide any indication related to the search target of the query, namely what was the query type in the request, to differentiate between the responses, we issue each query type to a different group of UDP port ranges. That is, the "ssdp:all" requests are headed towards UDP port range 10,000 to 35,000, while the others towards UDP port range 40,000 to 65,000. This choice made the filtering and analysis of the ingress SSDP traffic straightforward.

4.3. Probing considerations

A number of important considerations were taken into account for the effective design of the probing process and to lower the network noise of the experiment. First off, as anticipated, the majority of the vulnerable and potentially exploitable devices in the context of an amplification assault are assigned dynamic IP addresses. This means that they are network appliances associated to ADSL connections, and thus they migrate to different IP address at random time period depending on the ISP's policy. Therefore, it is of utmost importance to fingerprint and further analyse the device shortly after its discovery. Hence, this process is immediately started to ensure that the device will be assessed before it migrates to another IP address.

Secondly, it is expected that the probing process will induce noticeable network noise. To cope with this issue, special care has been taken to minimize the burden imposed by our experiments and avoid raising alarms on the examined ISPs. That is, we probed the IP addresses in a random way, ensuring that we evaluate sequentially IP addresses belonging to different network/subnetworks. We also made sure that every IP is probed only once.

4.4. Device fingerprinting

For extracting more details about the discovered devices, we employ the well-known *Nmap* tool. The purpose is to deduce information about the device type, the hardware, and the OS running on it. Overall, Nmap fingerprinting derives numerous details regarding the examined IP address, including DNS pointer (PTR) record, i.e., reverse DNS lookup,

Table 1
Demographics per examined country.

Country	E1 (5/2020)			E2 (5/2021)		
	IPs	ASs	ISP	IPs	ASs	ISP
Greece	5,716,737	219	7	5,736,704	226	7
Portugal	6,715,581	135	7	6,822,400	135	7
Singapore	12,435,739	560	6	13,420,544	603	6
Total	**24,868,057**	**914**	**19**	**25,979,648**	**964**	**19**

device, hardware, and software type, OS, and others. The meticulous fingerprinting of amplifiers aids in understanding the core root of the amplification threat and provides directions in identifying and applying the necessary measures for its mitigation. That is, the devices identified as "general purpose" most likely correspond to dedicated computer systems intentionally running the service in question, however being accessible from the open Internet due to negligence or lack of proper security policies. In this case, the most straightforward action is to restrict access to the service to only the intended clients; this can simply be enforced by the system administrator. On the other hand, the devices identified as "specific purpose" are probably misconfigured by default, so the vendors should fix them through firmware update.

4.5. Shodan.io

Shodan[2] is a search engine that allows to locate a variety of devices connected to the Internet with potential vulnerabilities. This is achieved by maintaining a database with discovered devices, including their type and available services. Shodan is used by cybersecurity professionals, as well as by cybercrooks for acquiring details of vulnerable devices and services. Therefore, the results of Shodan can be used to indirectly cross verify the outcomes of the work at hand. However, there are some differences in the methodology followed by Shodan compared to ours. Mainly, the Shodan database does not make any distinction between the open DNS resolvers and open DNS forwarders, but characterizes both types as "servers with recursive capabilities". In addition, they include some results that we did not, for example authoritative NSs with no external recursion support. Therefore, Shodan's results were tapped into as a roughly estimated value intended to crosscheck our results in a rather loosly way.

5. Results

5.1. IP demographics

Recall that this work examines three countries, namely Greece, Portugal and Singapore, which have a similar amount of IP addresses that does not exceed 13.5M, but are expected to vary on the level of cybersecurity awareness. Our experiments were conducted twice, roughly fifteen months apart in time. This way, we intend to capture the evolution and adoption rate of possible security countermeasures, and thus the differences on the security posture of the probed networks. The first run were executed in mid-March 2020, while the second in mid-June 2021. In the following, the first run is referred to as *E1*, while the latter as *E2*. The allocation of IP addresses per examined country for both runs are given in Table 1.[3]

As noticed in Table 1, at the time of E1, the Greek pool of IP addresses were ≈5.7M. These addresses belong to 220 different Autonomous System (AS), while there are seven major ISPs for providing Internet access to home and small office customers. Portugal's IP pool included ≈6.7M IP addresses, which belong to 136 AS, while they operate seven major ISPs. Singapore's IP pool comprises ≈12.4M IP addresses belonging to 566 AS, while six major ISPs operate in this country. In the second run of our experiment, we observed a slight increase on the IP address range for Greece and Portugal, but a notable increase for Singapore. Altogether, Singapore's IP address pool increased by 1M, reaching a total of 13.4M. This last remark coincides with the 43 additional ASs observed for Singapore.

5.2. Results on DNS

As presented in Table 2, during E1, ≈7.5k and 82 unique IPs were identified to operate in Greece as open forwarders and recursive resolvers, respectively, that is, a total of 7616 IP addresses. On the other hand, for the same country, Shodan reports ≈6.7k IP addresses that seem to support DNS recursion. Accordingly, for Portugal ≈4.5k and 165 unique IPs were discovered as open forwarders and recursive resolvers, respectively, while Shodan reported a ≈6.4k recursion-enabled IPs. For Singapore, our experiments yielded ≈4.1K and 489 unique IP addresses as open forwarders and recursive resolvers, respectively. On the other hand, Shodan reported ≈6.4k IPs with recursive capabilities for the same country. On the second run (E2), we observe a slight increase of the order of 16% of the population of open forwarders in Portugal, a moderate increase of 40% of that in Greece, but the number of forwarders in Singapore was practically tripled (210%). The population of resolvers for all countries remained almost constant.

Despite the country's smaller IP pool, especially compared to that of Singapore, for E1, Greece accounts for almost double the number of forwarders and double and quadruple in terms of percentage than Portugal and Singapore, respectively. This divergence decreased during E2, due to the unexpected raise of the forwarders' population in Singapore. Still, Greece holds the lead with the percentage to be almost or more than double to that of the other two countries. This is an initial but strong indication that Greece significantly lacks on adaptation for security measures regarding DNS open recursion capabilities. For open resolvers, which in any case are quite scanty, Singapore clearly leads in both runs in terms of percentages, followed by Portugal and Greece in that order.

5.2.1. Analysis of forwarders

Based on the results of Nmap, we categorize the detected devices (IP addresses) according to their PTR record, AS number, and device's OS type. As reflected in Table 2 for both experiments, PTR records were considered for grouping the devices into two categories, namely known and unknown PTR. Specifically, the PTR record indicating the domain names corresponding to the discovered IPs can aid in identifying dynamically assigned IP addresses, as these domain names follow a distinctive naming pattern that ISPs use for their clients. Indeed, an inspection of the PTR records demonstrate that the majority of the PTR records follows such pattern, and therefore it is confirmed that the known PTR category mainly comprises SOHO devices.

Furthermore, we categorize the open forwarders according to their administrative organization (see Table 3). Recall from Table 1 that there are seven major ISPs in Greece, each one owning more than one AS. We realized that this seven-piece group is also responsible for the majority of the identified hosts. It is deduced that the identified forwarders from the Greek IP address pool reside within the major ISPs in a percentage of 88% for both runs, while the rest belong to the remaining organizations. In fact, a single Greek provider is responsible for approximately 45% of the total forwarders in the country for the case of E2. Even worst, that number was almost 65% on the previous year (E1) for the same ISP. The second-ranked ISP hosts 20% compared to the 2% of E1, the third 11% compared to the 5% of E1, while the fourth and fifth have around 8.7% (12.7%) and 1.6 (2.9%) of the total amount of open forwarders, respectively. For Portugal, the forwarders belonging to major ISPs are around 70% (75% for E1) of the overall number detected. In addition, the two first-ranked of the major ISPs in this country share the 62% (70% for E1) of the forwarders. For

[2] Search Engine for the Internet of Everything: www.shodan.io.
[3] The data for demographics were retrieved from ipinfo.io.

Table 2
Demographics of DNS reflectors per country. Percentage values, rounded to 3 decimal places, are given in parenthesis.

Hosts	Greece		Portugal		Singapore	
	5,716,737 (E1)	5,736,704 (E2)	6,715,581 (E1)	6,822,400 (E2)	12,435,739 (E1)	13,420,544 (E2)
Forwarders	7534 (.132)	10,682 (.186)	4501 (.067)	5234 (.076)	4131 (.033)	12,822 (.096)
Resolvers	82 (.001)	111 (.002)	165 (.003)	168 (.003)	489 (.004)	551 (.004)
Total	7616 (.133)	10,793 (.188)	4666 (.07)	5402 (.079)	4620 (.037)	13,373 (.1)
Known PTR	4994 (.087)	7294 (.130)	1303 (.019)	3129 (.050)	1189 (.010)	10,001 (.070)
Unknown PTR	2622 (.046)	3499 (.060)	3363 (.050)	2273 (.030)	3431 (.028)	3372 (.030)
Shodan	6747 (.118)	10,348 (.181)	6412 (.096)	14,578 (.214)	6444 (.004)	54,894 (.409)

Table 3
DNS forwarders by organization. Percentage values, rounded to 2 decimal places, are given in parenthesis.

Greece			Portugal			Singapore		
ISP	E1	E2	ISP	E1	E2	ISP	E1	E2
Forthnet	7051 (64.36)	4853 (45.43)	MEO	1814 (30.18)	1717 (32.80)	Google	1346 (25.84)	4214 (32.87)
HOL	225 (2.25)	2156 (20.18)	NOS COMUNIC.	2397 (39.88)	1515 (28.95)	SingTel	2107 (40.46)	4192 (32.69)
OTE	547 (4.99)	1201 (11.24)	GOOGLE	921 (15.32)	1348 (25.75)	Microsoft	0 (–)	373 (2.91)
GOOGLE	979 (8.94)	1160 (10.86)	VODAFONE	262 (4.36)	309 (5.90)	Amazon	0 (–)	181 (1.41)
Panafonet	1385 (12.64)	933 (8.73)	ALMOUROLTEC	7 (0.12)	22 (0.42)	Alibaba	2 (0.04)	144 (1.12)
Wind	316 (2.88)	171 (1.60)	NOS MADEIRA	12 (0.20)	10 (0.19)	M1	842 (16.17)	106 (0.83)
GRNET	57 (0.52)	38 (0.36)	FORTINET	13 (0.22)	4 (0.08)	Starhub	81 (1.56)	50 (0.39)
Lancom	1 (0.01)	2 (0.02)	OpenDNS	121 (2.01)	0 (–)	Viewqwest	0 (–)	33 (0.26)
OpenDNS	145 (1.32)	0 (–)	Contabo	2 (0.03)	0 (–)	MyRepublic	45 (0.86)	27 (0.21)
FORTINET	3 (0.03)	0 (–)				Tencent	0 (–)	22 (0.17)
						OVH	0 (–)	14 (0.11)
						Digital Ocean	2 (0.04)	9 (0.07)
						UpCloud	0 (–)	8 (0.06)
Other	247 (2.25)	168 (1.57)	Other	462 (7.69)	309 (5.90)	Other	783 (15.04)	3449 (26.90)
Total	10,955 (100)	10,682 (100)		6011 (100)	5234 (100)		5208 (100)	12,822 (100)

Singapore, around 60% of the forwarders for both runs belong to major ISPs. Lastly, around 32% of the forwarders seem to be owned by a single ISP, when for the same ISP the percentage was around 40% with reference to E1.

Finally, Nmap has the capacity to possibly identify the OS running on a device, thus indirectly revealing its type. According to Nmap documentation, there exist 26 specialized OS categories corresponding to specific type of devices. As seen from Table 4, the identified devices are grouped to the specific specialized types and a generic "unknown" category consisting of hosts, for which Nmap was unable to identify the OS type. According to the figures, for all the three countries, we can observe that the discovered devices are related with networking, telecommunication, printers, storage units, and IP-based IoT devices, which usually are deployed in SOHO environments. Lastly, Table 5 details on the open forwarder's OS of the general purpose category, where it is evident that the majority of the general purpose devices run a Linux distribution.

Table 4
DNS forwarders by OS type. The "Specialized" type designates all other categories not defined explicitly.

Device type	Greece		Portugal		Singapore	
	E1	E2	E1	E2	E1	E2
Bridge	1	0	0	0	0	0
Broadband router	541	422	1025	596	1993	1,375
Firewall	271	250	225	134	242	325
General purpose	545	242	794	520	1144	4,579
Load balancer	0	2	5	0	4	0
Media device	10	0	7	0	8	1
Phone	19	9	52	27	93	222
Printer	3	2	12	8	5	1
Proxy server	4	0	1	0	49	0
Remote management	58	0	2	0	1	0
Router	123	171	114	54	57	58
Specialized	54	4	246	19	45	386
Storage-misc	2	2	0	0	151	3
Switch	730	275	308	137	160	352
Terminal	0	0	1	0	2	9
VoIP adapter	4	10	39	5	8	7
VoIP phone	12	0	6	1	2	1
Wireless Access Point	856	1,246	1995	1388	551	601
Webcam	2	0	22	0	0	0
Unknown	7,720	8,047	1175	2345	693	4,902
Total	10,955	10,682	6011	5234	5208	12,822

5.2.2. Analysis of resolvers

Usually, organizations and companies, including ISPs, hosting providers, cloud providers, IT firms, research institutions, or universities, deploy their own local DNS resolver to serve their internal clients. Although sound security practices recommend restricting access to such services to the internal users only, there are numerous occasions where this service is available to the open Internet as well. Commonly, this is due to misconfiguration or security negligence. Of course, there are companies that do provide DNS recursive services to the public, but in this case, the administrators typically implement specific security countermeasures, such as DNS Response Rate Limiting (RRL) [23] to curtail the respective devices' involvement in reflection/amplifications attacks.

For our experiments, we investigated the discovered hosts that operate as open DNS resolvers. Furthermore, the corresponding AS were analysed for grouping the number of hosts per organization. From Table 6, one can notice that there exist specific organizations contributing considerably to the amount of open resolvers. However, the nature of the concerned organization varies throughout the three countries. In Greece, the prominent places are possessed by ISPs and university networks, while in Portugal by only ISPs. Lastly, for Singapore, we can deduce that many of the resolvers are hosted in the cloud, as the respective ASs are owned by cloud computing provider companies.

Regarding the analysed OS of the devices operating as open DNS resolvers, the results are summarized in Table 7. As observed, the majority of the identified OSs belong to the general purpose type, and thus it can be safely argued that these hosts correspond to general (dedicated) computer systems purposely operating as DNS resolvers. However, we cannot make any further conclusion on whether this

Table 5
Detailed view of general purpose forwarders' OS type.

Operating system	Greece		Portugal		Singapore	
	E1	E2	E1	E2	E1	E2
FreeBSD 4	0	0	0	2	3	0
FreeBSD 6	1	0	0	0	0	0
FreeBSD 7	1	0	0	0	0	3
FreeBSD 8	26	0	35	2	1	0
FreeBSD 9	0	0	5	0	2	0
Linux 2	384	183	443	418	562	1285
Linux 3	30	23	107	52	117	285
MS Windows 7	2	0	8	2	9	1
MS Windows Vista	7	0	7	1	5	8
MS Windows XP	23	17	13	7	18	11
MS Windows Server 2000	0	0	1	0	0	0
MS Windows Server 2003	5	0	3	1	4	2
MS Windows Server 2008	35	5	55	3	37	19
MS Windows Server 2012	26	1	80	10	330	2876
Minix	0	0	5	0	2	0
OpenBSD 4	0	2	5	1	3	0
OpenBSD 5	0	0	1	0	0	3
Sun Solaris 8	0	3	4	3	0	1
Sun Solaris 9	3	8	20	18	51	85
Sun Solaris 10	1	0	2	0	0	0
NetBSD	1	0	0	0	0	0
Total	545	242	794	520	1144	4579

service is deliberately intended to the internal users or the public. The remaining types are networking devices, including routers and firewalls, which presumably are misconfigured to run open DNS recursive services.

To obtain a clearer view of the general purpose category's demographics, we summarize the identified OS families in Table 8. As it can be observed, most of the OS families are server-related distributions, including, Linux, MS Windows Server, and Sun Solaris. Specifically, the majority of the discovered devices run MS Windows Server 2012, which was first released on Sept. 2012. The second most popular category is Linux v2.6.32, which was firstly introduced on Dec. 2009. In the list of the identified OSs, there are as well several popular but old versions of MS Windows, like 7, XP, Server 2003, and Server 2008. Also, there are some instances of Sun Solaris 9 and 10 released back in 2003 and 2005, respectively. Lastly, a special Linux distribution for firewalls, named IPCop 2.0 was also detected; The latest stable IPCop 2.0 version was released back on Feb. 2012.

Based on the aforementioned findings, a straightforward observation is that the distributions of the identified OS families can be considered as outdated in the vast majority of the cases. We can only assume that they belong to enterprises' "install and forget" recursive resolvers, therefore never upgraded or updated. In addition, the discovered OS type list in Table 7 includes devices for which their specifications are inconsistent with their actual role. Namely, firewalls, IP phones, terminals, and VoIP adapters are types of devices evidently incompatible with the typical role of a DNS resolver. Perhaps, some of them correspond to honeypot setups by ISPs to detect attacks at the ISP level [24].

5.2.3. DNS query results

We further scrutinize the discovered hosts for their amplification capabilities. Recall that every device found to operate as an open DNS resolver or forwarder can be unwillingly involved in DDoS attacks. To assess such devices' value to an aspiring perpetrator, we measure their amplification capabilities by sending specific types of queries, which are frequently exploited in DDoS incidents, and noticing the size of the responses.

The provided BAF depends mainly on the examined device's support of the exploitable query type, e.g., "ANY" query type, and DNSSEC extension. For this purpose, as detailed in Section 4.1.1, we devised 11 diverse DNS queries, each one with a diverse set of characteristics. This way, we intend to trigger a different set of RRs to be included in the response, and therefore it is expected their length to vary significantly. These queries were sent to all the identified hosts and the responses were captured at the prober side for further analysis. We grouped the queries according to their corresponding size into three groups, namely, Q1 to Q2, Q3 to Q5, and Q6 to Q11, with 20, 36, and 31 bytes query size, respectively.

We summarize the results according to the produced BAF and payload size in Tables 9–12 for E1 and E2, correspondingly. Each column represents the results for the queries per country. Specifically, for each country, we calculated the BAF for both the minimum and maximum response length received as well as for the first and third quartile of the BAF distribution. That is, by grouping the hosts by their amplification effect, we can perceive a more precise view of their amplification potential as a group of possible attack actors. This is because the first and third quartiles offer in a concise format the information regarding the range of the BAF pertaining to the exploitable hosts. In all the tables, the highest score(s) is indicated with an asterisk, while in boldface is shown the highest score per quartile across the 11 queries.

With a quick glance on the figures contained in Table 11 regarding E2, the largest response is observed for a Greek IP address as a response to Q2 which yielded a UDP payload length of 1449 bytes, thus achieving an BAF of 72.45. For E1 (Table 9), the largest response stemmed from a Singaporean IP triggered by Q2, producing a response of 1429 bytes or a BAF of 71.45. On the bright side, during both runs (E1 & E2), the minimum response length is the base response to all queries. Precisely, such a response could be empty or contain a single RR, and its size fluctuates between 12 and 25 bytes. We notice that there exists a constant number of devices that provide the minimum response, rendering them bootless for the purposes of DDoS attackers.

In more detail, the following observations can be made per query type. For the sake of brevity, the focus is mostly on the results of the latest run (E2), namely Tables 11 and 12.

–Q1: It is the simplest query, requesting only the IPv4 address of a domain name. It is used to determine the baseline of the responses. As anticipated, the lower 75% of the provided BAF for all the three countries ranges between 0.6 (12 bytes) and 4 (80 bytes). The maximum response is recorded for Portugal and Greece generating a BAF of 25.6 triggered by a response of 520 bytes. Same are the outcomes for E1, where the majority of the devices produce a low BAF.

–Q2: It intends to examine whether the enquired devices support the "ANY" query type, and thus they include multiple RRs in their responses. The results exhibit a similar behaviour for all the three countries, demonstrating an BAF ranging from 0.6 to 18.5 or a length of 12 bytes to 370 bytes for the lower 75% of the IP addresses. However, the upper quartile amplifies the responses up to ≈70 times. The worst case was recorded for a Greek IP address yielding a BAF 72.45 or 1449 bytes. This was also the largest BAF observed across E2. For E1, the results were similar, with the only difference that the maximum BAF for Greece and Portugal was capped at 67 and 42, respectively. This query also produced the largest BAF throughout E1 for the case of a Singaporean IP address with a value of 71.45.

–Q3: Q3 involves the DNSSEC extension as well. It is a type of query that is typically exploited in DNS amplification attacks [8]. For this probe, we observe that the upper quartile provides a considerable BAF. Specifically, the top 25% produced a BAF between 6.39 (230 bytes) and 40.89 (1472 bytes). All the maximum responses from the three countries produced a BAF of around 41 or a payload of 1472 bytes, which was actually one of the largest observed throughout E2. Similarly, this query produced one of the largest responses observed throughout E1 for the case of a Singaporean IP with a BAF of 40.89.

–Q4: This query examines the support of DNSKEY, and therefore the size of the response depends on the length of the corresponding key. The upper quartile for the three countries generates a BAF of at least 11.17 or 402 bytes with a maximum of 27.19 or 979 bytes. For E1, the maximum amplification capabilities of the IP addresses in Greece and

Table 6
DNS resolvers by organization. Percentage values, rounded to 2 decimal places, are given in parenthesis.

Greece			Portugal			Singapore		
ISP	E1	E2	ISP	E1	E2	ISP	E1	E2
GR-NET	17 (19.77)	30 (27.03)	MEO	66 (39.29)	5 (29.41)	SingTel	8 (1.60)	73 (13.25)
OTE	9 (10.47)	28 (25.23)	Vodafone	27 (16.07)	6 (35.29)	Digital Ocean	62 (12.40)	69 (12.52)
Forthnet	10 (11.63)	10 (9.01)	NOS COMUNIC.	20 (1.90)	4 (23.53)	OVH	46 (9.20)	51 (9.26)
HOL	12 (13.95)	6 (5.41)	Claranet	15 (8.93)	2 (11.76)	Microsoft	38 (7.60)	38 (6.90)
NTUA	3 (3.49)	2 (1.80)	ONI	12 (7.14)	0 (–)	Amazon	29 (5.80)	29 (5.26)
DuthNet	0 (0)	2 (1.80)	Artelecompt	5 (2.98)	0 (–)	M1	18 (3.60)	25 (4.54)
Panafonet	3 (3.49)	2 (1.80)	Almouroltec	5 (2.98)	0 (–)	Google	10 (2.00)	10 (1.81)
HOU	3 (3.49)	2 (1.80)				My Republic	8 (1.60)	9 (1.63)
Wind	5 (5.81)	2 (1.80)				StarHub	5 (1.00)	7 (1.27)
UCNet	0 (–)	1 (0.90)				Alibaba	6 (1.20)	6 (1.09)
						Leaseweb	5 (1.00)	6 (1.09)
						UpCloud	5 (1.00)	5 (0.91)
						Viewqwest	4 (0.80)	4 (0.73)
						Netpluz	2 (0.40)	2 (0.36)
						Tencent	2 (0.40)	2 (0.36)
Other	24 (27.91)	26 (23.42)	Other	18 (10.71)	0 (–)	Other	252 (50.40)	215 (39.02)
Total	86	111		168	17		500	551

Table 7
DNS resolvers by OS type.

Device type	Greece		Portugal		Singapore	
	E1	E2	E1	E2	E1	E2
Broadband router	4	6	6	1	0	1
Firewall	1	3	8	1	1	11
General purpose	28	23	50	4	45	199
Phone	0	3	4	1	3	19
Specialized	3	0	3	0	1	3
Terminal	0	0	0	0	1	0
VoIP adapter	0	1	2	0	0	1
WAP	0	2	3	1	0	3
Switch	0	0	0	0	0	1
Storage-misc	0	0	0	0	0	1
Unknown	50	73	92	9	449	312
Totals	86	111	168	17	500	551

Table 8
Detailed view of general purpose resolvers' OS type.

Operating system	Greece		Portugal		Singapore	
	E1	E2	E1	E2	E1	E2
FreeBSD 9.0 - 10.1	0	0	0	0	0	2
IPCop 2.0 (Linux 2.6.32)	0	2	3	0	1	3
Linux 2.6.18	0	0	0	0	0	2
Linux 2.6.18 - 2.6.22	1	4	0	0	1	0
Linux 2.6.25 (openSUSE 11.0)	0	2	0	0	0	0
Linux 2.6.32	4	4	11	0	13	95
Linux 2.6.32 or 3.10	0	0	1	0	3	12
Linux 2.6.9 - 2.6.18	2	2	0	0	2	3
Linux 2.6.9 - 2.6.27	0	0	1	0	0	1
Linux 3.1 - 3.2	0	0	0	0	0	16
Linux 3.10	0	0	0	0	0	2
Linux 3.11 - 4.1	0	1	3	0	1	7
Linux 3.12	0	0	0	0	0	2
Linux 3.2 - 3.8	1	0	0	0	0	0
MS Windows 2000 SP4	0	0	1	0	0	0
MS Windows Server 2003 SP1	0	0	1	0	0	0
MS Windows Server 2003 SP1 or SP2	1	1	2	0	0	0
MS Windows Server 2008 or 2008 Beta	0	0	3	0	0	0
MS Windows Server 2008 R2	2	0	3	0	2	1
MS Windows Server 2008 R2 SP1	0	0	1	0	0	1
MS Windows Server 2012	13	0	16	3	1	42
MS Windows Server 2012 R2	1	0	0	0	16	0
MS Windows 7 SP1	1	0	0	0	0	0
MS Windows Vista Pro	0	0	0	0	0	1
MS Windows XP SP3	0	2	0	0	3	2
Sun Solaris 10	0	0	1	0	1	0
Sun Solaris 9	2	5	3	1	1	7
Total	28	23	50	4	45	199

Singapore are significantly lower, as they do not exceed a BAF of 16.78 or a size of 604 bytes.

–Q5: It examines the support of the DNSSEC extension, but for a more commonly used record type, i.e., "A" type. The lower 75% of the provided BAF for all the three countries ranges between 0.33 (12 bytes) and 7.15 (258 bytes), but with a maximum BAF of 34 (1224 bytes). Similarly, for E1 the lower 75% ranges between 0.33 (12 bytes) and 7.06 (254 bytes), with a maximum of 34 (1224 bytes).

–Q6: With Q6 and the remaining queries, we focused on TLDs as queried domain names. It is reported in the literature that this kind of requests have a minimal size, and hence they provide a somehow higher BAF [15]. On the latest run (E2) we observe that the low 75% of the Greek IPs produce a much lower response with sizes in the range of 20 to 295 bytes, or a BAF of 0.65 to 9.52. The relevant IPs of the two other countries provided even smaller responses with a size between 12 and 86 bytes, i.e., a BAF between 0.39 to 2.77 for Portugal and 0.42 to 2.42 for Singapore. For E1, the distribution of the BAF is equivalent for all the three countries, with the maximum BAF of 25.94 (804 bytes) recorded for a Singaporean IP address.

–Q7: This query is similar to Q6, but for a different set of TLDs. This way, we aim to collect comparative results for our hypothesis. For E2, the responses of Greece and Portugal are in a similar range, as the middle 50% of the IPs provide a BAF of 1.0 to 14.35 or a response of 31 and 445 bytes. The average responses from Singapore are in a generally lower range, i.e., a BAF of 1.0 to 4.13 translated to a response size of 31 and 128 bytes. The maximum BAF of 17.71 (549 bytes) stems from a Singaporean IP address. The results are similar for E1.

–Q8: It requests the DNSKEY record of a TLD. As observed from the Table 11, this query appears the most effective way to exploit the reflectors residing in the Greek IP address pool. Specifically, the upper 75% of the responses originating from Greek IP addresses yielded a BAF of 16.52 (512 bytes) to 47.48 (1472 bytes). For the two other countries, only the upper 25% can be considered beneficial for an attacker, as the corresponding IP addresses for this quartile deliver a BAF between 27.35 (848 bytes) and 47.23 (1464 bytes). For E1, the outcomes were somehow reversed, as the majority of the Portuguese produced a larger BAF than that of the Greek IPs. Specifically, the upper 75% of the responses originating from Portugal's IP addresses yielded a BAF of 16.52 (512 bytes) to 47.23 (1464 bytes). On the contrary, the corresponding BAF for Greek IP addresses fluctuated within a considerably lower range of 9.55 (296 bytes) to 46.55 (1443 bytes). Lastly for Singapore, only the upper 25% produced a BAF of 28.16 (873 bytes) to 45.32 (1405 bytes), while the first quartile contributed a very low BAF with a value of 1.00.

Table 9
BAF per country (E1).

Greece	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	1.00	1.00	0.69	1.00	1.00	0.65	0.65	0.65	0.65	0.65	0.65
25%	1.00	1.00	6.67	5.44	4.19	1.00	1.00	9.55	**14.68**	1.00	1.00
75%	4.00	17.55	22.64	11.17	5.22	4.44	13.71	28.16	**29.26**	11.99	14.29
Max	20.35	**66.70**	37.14	16.78	31.97	24.48	16.52	46.55	40.00	24.55	16.39
Portugal	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	1.00	1.00	0.33	0.33	0.33	0.39	0.39	0.39	0.39	0.39	0.39
25%	1.00	1.00	1.00	5.44	4.19	2.87	1.00	**16.52**	14.74	1.00	1.00
75%	4.00	16.75	18.75	11.17	6.74	4.13	14.29	28.16	**29.32**	14.10	15.61
Max	22.70	42.15	40.22	16.61	34.00	24.55	16.52	**47.23**	40.00	**47.23**	**47.23**
Singapore	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	1.00	1.00	0.69	0.69	0.69	0.65	0.65	0.65	0.65	0.65	0.65
25%	3.75	1.00	1.00	**5.14**	1.14	1.42	1.00	1.00	1.74	1.00	1.00
75%	4.00	18.50	13.69	11.17	7.06	4.26	14.94	28.16	**29.32**	14.48	16.52
Max	25.60	**71.45***	40.89	16.89	34.00	25.94	17.71	45.32	39.94	47.48	47.35

Table 10
Response length in bytes per country (E1).

Greece	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	20	20	25	36	36	20	20	20	20	20	20
25%	20	20	240	196	151	31	31	296	**455**	31	31
75%	80	351	815	402	188	138	425	873	**907**	372	443
Max	407	1334	1337	604	1151	759	512	**1443**	1240	761	508
Portugal	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	20	20	12	12	12	12	12	12	12	12	12
25%	20	20	36	196	151	89	31	**512**	457	31	31
75%	80	335	675	402	243	128	443	873	**909**	437	484
Max	454	843	1448	598	1224	761	512	**1464**	1240	**1464**	**1464**
Singapore	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	20	20	25	25	25	20	20	20	20	20	20
25%	75	20	36	**185**	41	44	31	31	54	31	31
75%	80	370	493	402	254	132	463	873	**909**	449	512
Max	512	1429	**1472***	608	1224	804	549	1405	1238	**1472***	1468

Table 11
BAF per country (E2).

Greece	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	1.00	1.00	0.56	0.69	0.56	0.65	0.65	0.65	0.65	0.65	0.65
25%	1.00	3.75	1.00	7.67	3.67	0.65	1.00	**16.52**	14.68	1.00	1.00
75%	4.00	18.25	14.22	11.17	7.15	9.52	14.35	**43.97**	29.26	18.58	22.87
Max	25.60	**72.45***	40.89	27.19	34.00	24.48	16.52	47.48	40.00	47.48	47.48
Portugal	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	0.60	0.60	0.33	0.33	0.33	0.39	0.39	0.39	0.39	0.39	0.39
25%	1.00	1.00	1.14	5.14	1.14	0.65	1.00	1.00	**14.39**	1.00	1.00
75%	4.00	18.10	13.78	11.17	4.31	2.77	14.29	**38.55**	27.39	12.29	16.16
Max	25.60	**71.10**	40.36	16.78	31.75	24.55	16.52	47.23	38.45	47.29	47.23
Singapore	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	1.00	1.00	0.36	0.69	0.36	0.42	0.65	0.42	0.65	0.42	0.65
25%	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00	1.00
75%	4.00	18.50	6.39	11.17	4.31	2.42	4.13	27.35	**29.26**	11.68	11.32
Max	21.95	**70.10**	40.86	27.19	34.00	25.94	17.71	47.06	39.94	47.29	47.35

–Q9: This query is identical to Q8, but for a different set of TLDs. The findings are comparable with that of Q8, but with the notable exception of the Portuguese IPs, where the upper 75% of the responses generate a BAF between 14.39 (446 bytes) and 38.45 (1192 bytes); this is in contrast to the Q8 where only the upper 25% produced a beneficial BAF. In E1, the responses from the identified IP addresses exhibit a similar distribution to that of E2, where again the upper 75% of the responses generated for Greece and Portugal and only the 25% for Singapore supplied a high BAF. The largest response for Q9 stemmed from a Portuguese and Greek IP address exhibiting a payload of 1240 bytes, translated to a hefty BAF of 40.00.

–Q10: It investigates the performance of the "ANY" query for DNSSEC-enabled TLD zones. For E2, the distribution is similar across the three countries, where the top 25% ranges from 11.68 (362 bytes) to 47.48 (1472 bytes). On the contrary, E1 results exhibit that this query was less beneficial from an attacker's viewpoint when involving the Greek IP addresses. Specifically, the top quartile of the responses ranged between 11.99 (372) and 24.55 (761). The largest BAF for Q9 is recorded for a Greek IP address with a BAF of 47.48 and payload of 1472 bytes.

–Q11: Comparable to Q10 are the results for this query, as once again the top quartile for the three countries fluctuates between 11.32 (351 bytes) to 47.48 (1472 bytes). For E1, it was observed that the maximum response originated from the Greek IP addresses was 508 bytes and produce a BAF of 16.39. Meaning that the upper 75% responses contribute a low BAF in the range of 1.00 (31 bytes) to 16.39 (508 bytes). On the other hand, Portugal and Singapore demonstrated

Table 12
Response length in bytes per country (E2).

Greece	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	20	20	20	25	20	20	20	20	20	20	20
25%	20	75	36	276	132	20	31	**512**	455	31	31
75%	80	365	512	402	258	295	445	**1363**	907	576	709
Max	512	1449	**1472***	979	1224	759	512	**1472***	1240	**1472***	**1472***
Portugal	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	12	12	12	12	12	12	12	12	12	12	12
25%	20	20	41	185	41	20	31	31	**446**	31	31
75%	80	362	496	402	155	86	443	**1195**	849	381	501
Max	512	1453	1453	604	1143	761	512	1464	1192	**1466**	1464
Singapore	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10	Q11
Min	20	20	13	25	13	13	20	13	20	13	20
25%	20	20	**36**	**36**	**36**	31	31	31	31	31	31
75%	80	370	230	402	155	75	128	848	**907**	362	351
Max	439	1402	**1471**	979	1224	804	549	1459	1238	1466	1468

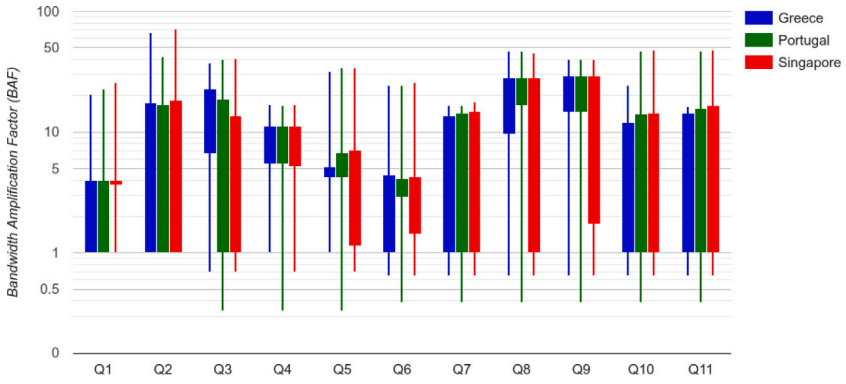

Fig. 1. BAF per DNS query per country (E1).

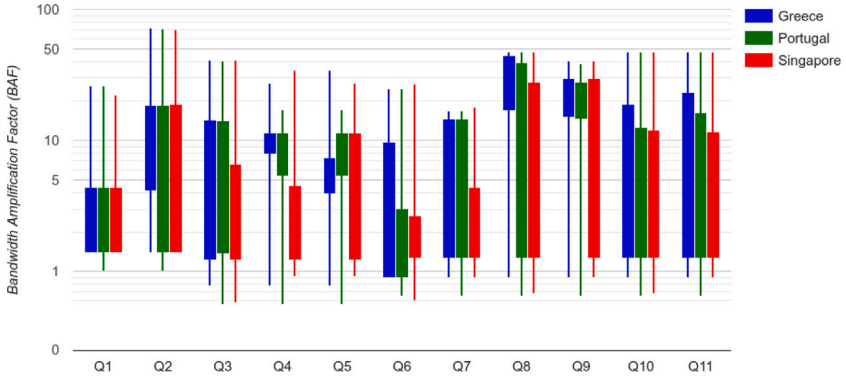

Fig. 2. BAF per DNS query per country (E2).

a considerable packet size for Q11 as the top 25% of responses produce a BAF between 15.61 (484 bytes) and 47.35 (1468 bytes).

To facilitate the reader to easily grasp the value range of the quartiles, we also present the BAF results in a box-and-whisker format in Figs. 1 and 2 for E1 and E2, respectively. A straightforward remark, verifying the aforesaid observations, is that the identified exploitable hosts residing in the Greek IP addresses pool are beneficial for potential attackers when they issue queries similar to Q8 and Q9, namely regarding requests for DNSKEY RRs for DNSSEC enabled zones. As Table 11 demonstrates, the highest BAF, among all the quartiles obtained for this country, is achieved for these two queries. Specifically, an attacker would attain the highest amplification rate if using queries similar to Q8 or Q9, as the BAF is the highest in the lowest point (first quartile) but also the topmost of the maximum responses, setting a very high rate for ≈75% of all the exploitable hosts. Finally, the comparison of the findings between Q8, Q9 and Q10, Q11 demonstrates that it is more beneficial for the attackers to exploit the DNSKEY RR than the "ANY" query type, which is typically harnessed in DNS amplification attacks so far. The highest BAF for this country is achieved with Q2 with a value of 72.45, which is also the highest throughout our experiments. However, the observations from the rest quartiles demonstrate that only the 25% of the identified devices would be of value to a perpetrator. A similar picture applies to E1 where the most beneficial queries for the Greek IP addresses were also Q8 and Q9. The achieved BAF is equivalent to the highest BAF of the E2 findings obtained for this country.

Regarding Portugal, we observe likewise that the most profitable query is Q9 for E2. Particularly, as shown in Fig. 2, the highest BAF for the first quartile was perceived for this query. That means that the upper 75% percent of the discovered hosts could contribute a high BAF of at least 14, considering that the BAF for the lowest point (first quartile) is the highest of all, and the maximum BAF is among the highest observed. Q8 has the topmost third quartile as well, however,

Table 13
Demographics of SSDP reflectors per country.

Country	Exper	ssdp:all		upnp:rootdevice	Total	Shodan.io
Greece	E1	93	6523	2126	8472	17,239
	E2	112	1471	27	1610	4,180
Portugal	E1	5	107	2	114	3,427
	E2	10	100	4	114	868
Singapore	E1	103	24	39	166	1,420
	E2	11	147	2	160	664

with a low first quartile, which makes valuable for an attacker only the top 25% of the available devices. The highest BAF for this country was achieved for Q2 and had a value of 71.10. Regarding E1, we noted that the highest BAF stemming from a Portuguese IP was triggered for Q8, Q10 and Q11. Each of these queries produced a hefty BAF of 47.23 with a payload size of 1464 bytes. Overall, for E1, the most beneficial queries exploiting Portuguese IPs were Q8 and Q9. A similarly high BAF was recorded for Q10 and Q11, however with lower first and third quartile.

With reference to Singapore, we can deduce that despite the steep increase of the Singaporean IP addresses that operate as reflectors in E2, these devices cannot be considered valuable from an attacker's viewpoint. For all the queries, the first quartile does not exceed a BAF of 1, while the third quartile produces a BAF of up to 18.50, with the exception of Q8 and Q9. Put it differently, the 75% of the reflectors provide a relatively negligible BAF for the 9 out of the 11 investigated queries. The only exception is that of the "DNSKEY" RR type of DNSSEC enabled zones, where the upper quartile produces at least a BAF of 27. These results show that the "DNSKEY" RR type of DNSSEC enabled zones is more appropriate for the case of the Singaporean IP addresses. The highest BAF for E2 was recorded for Q2 and had a value of 70.10. However, as the corresponding first and third quartile values are significantly low, this result seems rather random and cannot be considered beneficial from an attacker's perspective. Regarding E1, the highest BAF of 71.45 was also recorded for Q2. Moreover, even though the maximum BAF for Q10 and Q11 is high, the 75% of the remaining responses has a very low factor, thus making these queries inefficient for an attack. Q8 and Q9 on the other hand showed the best results for the top 25% of the hosts. These results, combined with the second highest BAF of the maximum response size, render Q8 as the optimal query type to utilize in a DNS amplification attack. Q9 follows in the line of the most prolific queries for this country. Lastly, Q10 and Q11 indicate that the devices within the Singaporean IP ranges do not support or interpret the "ANY" query type, but rather the "DNSKEY" RR type is more profitable for amplification purposes.

Overall, it is pinpointed that contrary to the expectations, the "ANY" query type is not anymore the most beneficial query type for DNS amplification attacks, but rather the "DNSKEY" RR type is more favourable. With reference to Tables 9 and 11 and specifically to columns for Q3, Q10 and Q11, we can infer that the first quartile is the lowest and the third quartile is among the lowest across all countries. These findings demonstrate that the identified reflectors do not support or interpret the "ANY" query type. This observation holds also true for the case of E1. From the previous, it can be safely argued that there is an augmenting number of DNS resolvers, that the investigated forwarders rely on, which have adopted the latest security recommendations regarding the support of the "ANY" query type [17].

5.3. Results on SSDP

Recall from Section 3.2, that regarding the discovery of SSDP services, we utilize a prober that sends both the examined types of SSDP queries. In turn, the prober captures the ingress SSDP traffic in pcap files. In the course of the analysis of the incoming network traffic and as detailed in Section 5.3.4, we realized that the matching responses were originating from random non-standard UDP source ports instead of the anticipated and predefined for the SSDP protocol port 1900, where we dispatched the request. This behaviour is related with the broad use of the open source library *libupnp* [25] in customer-premises equipment (CPE) type of devices [26]. This fact also makes the mitigation of amplification attacks exploiting the SSDP protocol more challenging, as filtering the traffic based on the source port is ineffective, but instead inspection of the packet content is required.

5.3.1. Analysis of SSDP servers

Table 13 summarizes the findings for both runs of our experiment (E1 & E2). For each country, the third and fifth columns represent the number of devices that respond solely to the ssdp:all and upnp:rootdevice query respectively, while the middle column shows the intersection of these two sets, namely the number of devices that responded to both query types. The last column gives the number of SSDP devices reported by Shodan at the time of our probes.

As illustrated in the Table 13 for E1, the Greek pool of IP addresses contained approximately 8.5K hosts that responded to either one or both of the SSDP queries. On the other hand, both the IP address pools of Portugal and Singapore yielded a couple of hundreds of potentially exploitable hosts. In addition, one can note that there is a considerable percentage of Greek IP addresses that responded exclusively to the upnp:rootdevice query and of Singaporean IP addresses to the ssdp:all one. Actually, for the latter case, the number of the devices is greater than the remaining groups. For E2 and for all the three countries, the majority of the devices responded to both ssdp:all and upnp:rootdevice query types, still there is a number of devices that responded only to the first and a small portion to the latter query.

Surprisingly enough, the number of SSDP supporting devices residing within the Greek IP pool decreased drastically during E2; almost 7K devices ceased to provide (open) SSDP services. For instance, a prominent Greek ISP which was responsible for 2428 devices during E1, it accounts for 1088 devices in E2, a reduction of 50%. It can be quite safely assumed that a key change in the ISPs' security policy or an improvement in their network configuration significantly contributed to the reduction of the attack surface and the enhancement of the Greek's cyberspace security posture against amplification assaults. On the downside, still the figures for this country are too high vis-à-vis the Portuguese and Singaporean ones.

5.3.2. Device fingerprinting

A fingerprinting analysis of the discovered devices with reference to the corresponding PTR record and OS type were also conducted, similarly to the DNS evaluation. We observed that the hosts with a known PTR record follow the naming patterns adapted by ISPs for their dynamically assigned clients. This result once again supports the conclusion that the majority of the available SSDP services are attributed to SOHO devices, given that these types of devices are usually connected to dynamically assigned IP addresses.

In detail, the categorization of the results by device's type is summarized in Tables 14 and 15 for E1, and in Tables 16 and 17 for E2. As observed, although Nmap was unable to identify the type for a significant portion of the SSDP responding devices, especially for the devices within the Greek IP address pool, the outcomes are indicative of the situation. For Portugal and Singapore, about the half of the identified devices are of the general purpose type, and thus it can be deduced that they correspond to general computer systems providing some kind

Table 14
Fingerprinting results by OS type per country (E1). We kept Nmap's categorization where "power-device" refers to miscellaneous power devices, like Uninterruptible Power Supply (UPS), and "Phone" corresponds to a mobile phone.

Device type	Greece		Portugal		Singapore	
	ssdpall	upnp	ssdpall	upnp	ssdpall	upnp
Broadband router	5 (0.08)	4 (0.05)	2 (1.79)	2 (1.83)	1 (0.79)	(–)
Firewall	3 (0.05)	3 (0.03)	2 (1.79)	2 (1.83)	0 (–)	0 (–)
Media device	11 (0.17)	11 (0.13)	0 (–)	0 (–)	0 (–)	0 (–)
PBX	1 (0.02)	1 (0.01)	0 (–)	0 (–)	0 (–)	0 (–)
Phone	92 (1.39)	92 (1.06)	1 (0.89)	1 (0.92)	1 (0.79)	0 (–)
Power-device	0 (–)	0 (–)	1 (0.89)	1 (0.92)	0 (–)	0 (–)
Printer	8 (0.12)	10 (0.12)	1 (0.89)	1 (0.92)	0 (–)	0 (–)
Remote management	1 (0.02)	6 (0.07)	0 (–)	0 (–)	0 (–)	0 (–)
Router	23 (0.35)	24 (0.28)	0 (–)	0 (–)	0 (–)	0 (–)
Specialized	4 (0.06)	4 (0.05)	0 (–)	0 (–)	0 (–)	0 (–)
Storage-misc	19 (0.29)	22 (0.25)	2 (1.79)	2 (1.83)	1 (0.79)	0 (–)
Switch	1 (0.02)	0 (–)	0 (–)	0 (–)	1 (0.79)	0 (–)
VoIP phone	9 (0.14)	9 (0.10)	0 (–)	0 (–)	1 (0.79)	0 (–)
WAP	20 (0.30)	20 (0.23)	18 (16.07)	16 (14.68)	3 (2.36)	4 (6.35)
Webcam	1 (0.02)	1 (0.01)	0 (–)	0 (–)	0 (–)	0 (–)
General purpose	271 (4.10)	273 (3.16)	60 (53.57)	57 (52.29)	75 (59.06)	28 (44.44)
Unknown	6147 (92.91)	8169 (94.45)	25 (22.32)	27 (24.77)	44 (34.65)	31 (49.21)
Total	6616 (100)	8649 (100)	112 (100)	109 (100)	127 (100)	63 (100)

Table 15
Detailed view of fingerprinting results regarding the general purpose category per country (E1).

Device type	Greece		Portugal		Singapore	
	ssdpall	upnp	ssdpall	upnp	ssdpall	upnp
FreeBSD 6	0 (–)	1 (0.37)	0 (–)	0 (–)	0 (–)	0 (–)
Linux 2	227 (83.76)	229 (83.88)	17 (28.33)	17 (29.82)	19 (25.33)	5 (17.86)
Linux 3	37 (13.65)	36 (13.19)	43 (71.67)	40 (70.18)	55 (73.33)	23 (82.14)
MS Windows 7	1 (0.37)	1 (0.37)	0 (–)	0 (–)	0 (–)	0 (–)
MS Windows XP	4 (1.48)	4 (1.47)	0 (–)	0 (–)	0 (–)	0 (–)
MS Windows Server 2008	1 (0.37)	1 (0.37)	0 (–)	0 (–)	1 (1.33)	0 (–)
VxWorks	1 (0.37)	1 (0.37)	0 (–)	0 (–)	0 (–)	0 (–)
Total	271 (100.00)	273 (100.00)	60 (100.00)	57 (100.00)	75 (100.00)	28 (100.00)

Table 16
Fingerprinting results by OS type per country (E2).

Device type	Greece		Portugal		Singapore	
	ssdpall	upnp	ssdpall	upnp	ssdpall	upnp
Broadband router	4 (0.25)	4 (0.27)	1 (0.91)	3 (2.89)	1 (0.63)	1 (0.67)
Firewall	3 (0.19)	3 (0.20)	2 (1.82)	2 (1.92)	3 (1.90)	3 (2.01)
Media device	4 (0.25)	4 (0.27)	1 (0.91)	1 (0.91)	2 (1.27)	2 (1.34)
Phone	22 (1.39)	22 (1.47)	2 (1.82)	2 (1.82)	1 (0.63)	1 (0.67)
Printer	4 (0.25)	3 (0.20)	1 (0.91)	1 (0.91)	1 (0.63)	1 (0.67)
Remote management	23 (1.45)	2 (0.13)	0 (–)	0 (–)	0 (–)	0 (–)
Router	10 (0.63)	10 (0.67)	0 (–)	0 (–)	0 (–)	0 (–)
Specialized	3 (0.19)	3 (0.20)	1 (0.91)	1 (0.91)	1 (0.63)	1 (0.67)
Storage-misc	9 (0.57)	9 (0.60)	1 (0.91)	1 (0.91)	1 (0.63)	1 (0.67)
Terminal	1 (0.06)	1 (0.07)	0 (–)	0 (–)	0 (–)	0 (–)
VoIP phone	1 (0.06)	0 (–)	0 (–)	0 (–)	3 (1.90)	3 (2.01)
WAP	20 (1.26)	19 (1.27)	11 (10.00)	10 (9.62)	16 (10.13)	15 (10.07)
webcam	1 (0.06)	1 (0.07)	0 (–)	0 (–)	0 (–)	0 (–)
General purpose	149 (9.41)	148 (9.89)	61 (43.86)	56 (53.85)	67 (42.41)	67 (44.97)
Unknown	1329 (83.95)	1268 (84.65)	29 (26.36)	27 (25.96)	62 (39.24)	54 (36.24)
Total	1583 (100.00)	1498 (100.00)	110 (100.00)	104 (100.00)	158 (100.00)	149 (100.00)

of services. On the contrary, for Greece, the results demonstrate that a significant portion of the identified OSs fall under the SOHO category, like networking, telecommunication, and IP-based IoT devices. Lastly, according to the detailed view of the general purpose OS in Tables 15 and 17, most of the OSs families are server-related distributions, like Linux. Particularly, during E2 the majority of the discovered devices run Linux v2.6, for which the last stable release was back in May 2011. The second most popular category is Linux v3 with the last stable release in February 2015. In the list, we notice also some popular but old versions of MS Windows, including Server 2000, and Server 2008.

5.3.3. Query evaluation

The evildoers can take advantage of the ssdp:all and upnp: rootdevice queries to generate surges of amplified traffic against their victim. As already pointed out in Section 4.2, a single query may trigger a multitude of responses, which typically have a UDP payload of around 100 bytes, depending on the length of the advertised service. The outcomes are grouped according to these two query types and summarized in Tables 18 and 19 for BAF and PAF, respectively. The highest score is indicated with an asterisk, while in boldface is shown the highest score per quartile across the two query types.

Table 17
Detailed view of fingerprinting results regarding the general purpose category per country (E2).

Device type	Greece		Portugal		Singapore	
	ssdpall	upnp	ssdpall	upnp	ssdpall	upnp
Linux 2.4	1 (0.67)	1 (0.69)	1 (1.64)	10 (47.62)	0 (–)	0 (–)
Linux 2.6	99 (66.44)	94 (63.51)	24 (39.34)	11 (52.38)	19 (28.36)	18 (26.87)
Linux 3	45 (30.20)	44 (29.73)	33 (44.10)	0 (–)	45 (67.16)	45 (67.16)
Linux 4	1 (0.67)	0 (–)	2 (3.29)	0 (–)	2 (2.99)	2 (2.99)
UNIX 5	0 (–)	0 (–)	0 (–)	0 (–)	1 (1.49)	1 (1.49)
MS Windows 7	1 (0.67)	1 (0.69)	0 (–)	0 (–)	0 (–)	0 (–)
MS Windows XP	0 (–)	1 (0.69)	0 (–)	0 (–)	0 (–)	0 (–)
MS Windows Server 2000	0 (–)	0 (–)	1 (1.64)	0 (–)	0 (–)	0 (–)
MS Windows Server 2008	2 (1.34)	3 (2.03)	0 (–)	0 (–)	0 (–)	0 (–)
MS Windows Server 2012	0 (–)	4 (2.70)	0 (–)	0 (–)	0 (–)	1 (1.49)
Total	149 (100.00)	148 (100.00)	61 (100.00)	56 (100.00)	67 (100.00)	67 (100.00)

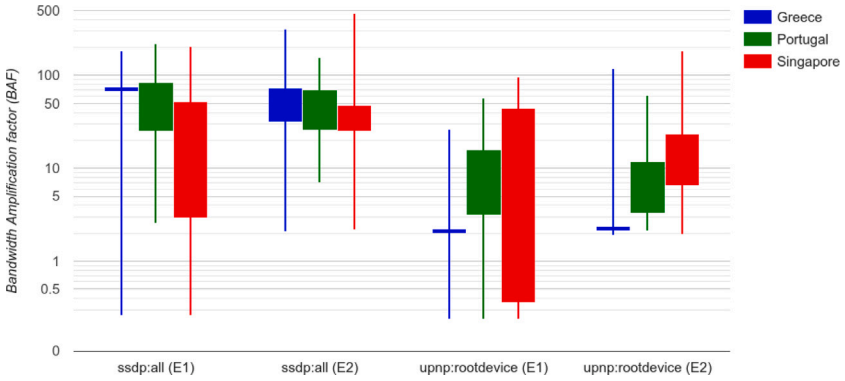

Fig. 3. SSDP ssdp:all vs. upnp:rootdevice in terms of BAF per country.

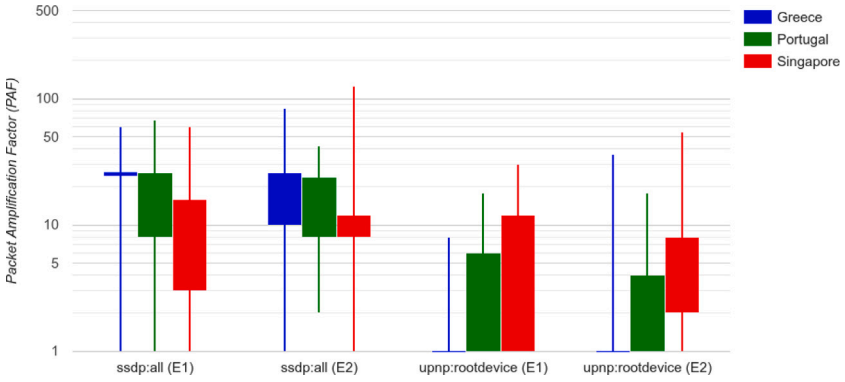

Fig. 4. SSDP ssdp:all vs. upnp:rootdevice in terms of PAF per country.

As illustrated in Table 18, the BAF for the evaluated queries can reach up to 470.22, which corresponds to a response stream of 126 packets. This worst case result pertains to E2 for Singapore. The query type ssdp:all returned a greater number of responses in terms of both multitude of packets (PAF) and accumulated packet length (BAF). In more detail, this query seems the most efficient amplifier when involving the Greek IP address pool, as the top 75% of the identified IP addresses yielded an accumulated response with a BAF between 31.38 and 313.20 or a PAF ranging from 10 to 84. On the other hand, the upnp:rootdevice query also exhibited a high maximum BAF of 119.36, however the low first and third quartile of BAF with values 2.20 and 2.39, respectively, rendered the majority of the devices unsuitable for amplification purposes. For E1, the results were even higher for the query type ssdp:all, as the first quartile provided a BAF of 73.24 or PAF of 26, but with a maximum BAF of 183.85 or PAF of 60.

Likewise, for the Portuguese IP address pool and for the ssdp:all, the accumulated responses generated a BAF between 25.40 and 156.81 or a PAF between 8 and 42 for the 75% of all the exploitable IP addresses. This outcome constitutes the Portuguese IP addresses as the second most prolific amplifier. For E1, the maximum response was even higher, with a BAF of 219.04 or a packet count of 68. Lastly, the Singaporean IP address pool exhibited somehow lower values compared to the other two countries. Particularly, the first quartile provided a BAF of 25.34 or a PAF of 8, while the third quartile generated a BAF of 47.78 or a PAF of 12. However, a Singaporean IP address set the record of the highest BAF observed throughout the experiments.

According to the box-and-whisker format illustration of BAF and PAF measurements in Figs. 3 and 4, respectively, we can note that the query type ssdp:all is more beneficial for an attacker's purposes, as it demonstrates higher BAF and PAF values in all quartiles, than

Table 18
BAF and length of accumulated responses in bytes per country.

	ssdp:all				upnp:rootdevice			
	E1		E2		E1		E2	
Greece	BAF	Bytes	BAF	Bytes	BAF	Bytes	BAF	Bytes
Min	0.26	26	2.06	206	0.24	26	1.89	202
25%	**73.24**	**7,324**	31.38	3138	2.20	235	2.20	235
75%	**73.24**	**7,324**	**73.24**	**7324**	2.20	235	2.39	256
Max	183.85	18,384	**313.20**	**31,320**	26.47	3,832	119.36	12,771
Portugal	BAF	Bytes	BAF	Bytes	*BAF*	Bytes	BAF	Bytes
Min	2.53	253	6.94	694	0.24	26	2.11	226
25%	25.34	2,534	**25.40**	**2540**	3.12	334	3.27	350.25
75%	**84.99**	**8,499**	69.86	6986	15.87	1,698	11.93	1277
Max	**219.04**	**21,904**	156.81	15,681	56.78	6,075	61.21	6549
Singapore	BAF	Bytes	BAF	Bytes	BAF	Bytes	BAF	Bytes
Min	0.26	26	2.16	216	0.24	26	1.96	210
25%	2.96	296	**25.34**	**2534**	0.36	39	6.57	702.50
75%	**51.91**	**5,191**	47.78	4778	44.06	4,714	23.69	2534
Max	206.34	20,634	**470.22***	**47,022***	96.56	10,332	183.53	19,638

Table 19
PAF and number of packets of accumulated responses per country.

	ssdp:all		upnp:rootdevice	
	E1	E2	E1	E2
Greece	PAF	PAF	PAF	PAF
Min	1	1	1	1
25%	**26**	10	1	1
75%	**26**	**26**	1	1
Max	60	**84**	8	36
Portugal	PAF	PAF	PAF	PAF
Min	1	2	1	1
25%	**8**	**8**	1	1
75%	**26**	24	6	4
Max	**68**	42	18	18
Singapore	PAF	PAF	PAF	PAF
Min	1	1	1	1
25%	3	**8**	1	2
75%	**16**	12	12	8
Max	60	**126***	30	54

the query type upnp:rootdevice. Nevertheless, since the majority of the identified devices for all countries responded to both query types, a potential perpetrator can exploit them simultaneously to magnify the impact on the target; this is in line with the fact that the total number of the available SSDP reflectors are scarce. Finally, once more, it is evident that the Greek's cyberspace security requires more attention compared to the other two evaluated countries.

5.3.4. Ephemeral source ports

As mentioned above, when examining the SSDP responses, we noticed that they were originating from various random UDP source ports, rather than the predefined one, e.g., UDP port 1900 [18]. To shed more light on this situation, we further analyse the SSDP responses pertaining to all the probes.

Depending on the source port of a response, the corresponding device is classified either as "normal", namely the source port of the response is 1900 as per the standard, or "abnormal", namely the source port ranges from 0 to 65,000 but not the standard one. This, means that the device uses an ephemeral port to send back the SSDP response. The abnormal cases were further divided into groups of 5000 each, i.e., ports 0 to 5000 (excluding 1900), 5001 to 10,000, and so on. Based on [26], we assume that the randomness of the source port is related to the OS on which the protocol is implemented. For instance, services running on the MS Windows platform utilize lower port ranges, namely from 1025 to 5000 as an ephemeral port. Those running on Linux platform usually choose from a higher pool of ports, i.e., 32,768 to 61,000. The obtained results depicted in Fig. 5 for E2 do verify that the majority of the identified SSDP devices are based on Linux. The first column represents the normal, while the remaining the abnormal behaviour. The figures for E1 are similar and thus are omitted for brevity.

In detail, for the Greek IP addresses, nearly 95.7% of the total responses fall into the "normal" category, while a 3.7% indicate that they are coming from Linux-based devices and a small portion of 0.7% originating from Windows-based. On the other hand, for Portugal and Singapore, all but one of the responses are "abnormal". Both countries demonstrate a small percentage of around 1% on the group of 0–5000 ports (excluding 1900), which correspond to the Windows-based behaviour. Furthermore, they exhibit a uniform distribution on the groups that correspond to the ports 30,000 to 65,535, meaning that the associated Linux-based software picks the source port in a round-robin fashion.

5.3.5. Information leakage

Another particularly interesting finding stemming from the SSDP results is that misconfigured SSDP servers can be straightforwardly exploited by remote opponents for reconnoitring the internal network. Table 20, collocates some of the most interesting responses from the SSDP probing per country. By observing the table, it becomes evident that the advertised services do reveal valuable and private information about the type, OS, software, and even the firmware version of the probed device. For instance, the fourth cell of the first column (CB-DIM2028FW) identifies a 1080P Vandal IR Mini Dome Camera, the fifth and ninth cells of the second column identify a Panasonic and LG TV, respectively, and the third cell of the third column (DIR-868L) reveals a D-Link Wireless AC1750 dual-band Gigabit cloud router. Naturally, such information can be particularly handy to remote (external) opponents performing network enumeration. In fact, this is an interesting avenue for future work, that is, delving deeper to the information a potential perpetrator can acquire through SSDP or other service discovery protocols and to the ways this information can be exploited in the context of specific attacks.

6. Related work

In the literature, there exist a significant mass of works investigating the contribution of UDP-based protocols to amplification/reflection DoS attacks in terms of BAF and PAF and the detection of potential strong reflector agents. Table 21 recapitulates the key characteristics of such key works based on 14 different criteria.

In the first documented study of DNS amplification attack, Vaughn and Evron [27] observed that the perpetrators tend to exploit large

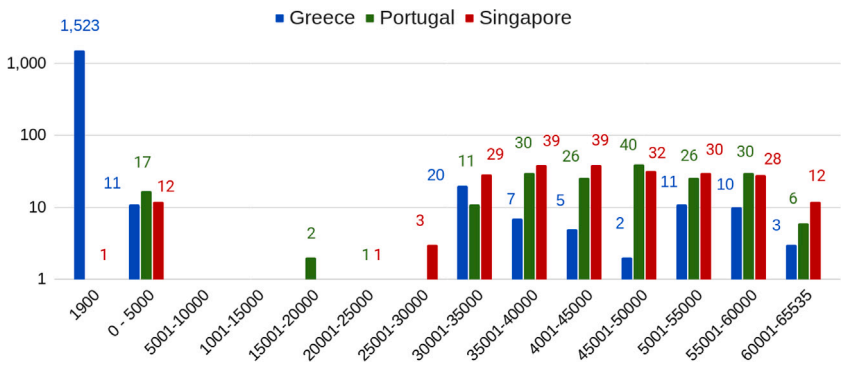

Fig. 5. Mapping of the SSDP source ports per country (E2).

Table 20
Instances of information leakage through SSDP probing.

Greece	Portugal	Singapore
AirTies/ASP 1.0 UPnP/1.0 miniupnpd/1.0	LPUX/1.3 UPnP/1.0 Aficio MP 2510/1.0	DLNADOC/1.50 Linux/4.4.159 UPnP/1.0 RKDLNALib/2.0
ASUSTeK UPnP/1.0 MiniUPnPd/1.4	Cellvision UPnP/1.0	FreeBSD/8.0 UPnP/1.0 Panasonic-MIL-DLNA-SV/1.0
Canon IJ-UPnP/1.0 UPnP/1.0 UPnP-Device-Host/1.0	CE/6.0 UPnP/1.0 domovea/3.7.0.1	Linux, UPnP/1.0, DIR-868L Ver 1.03SHC
CB-DIM2028FW, UPnP/1.0	DNS-320L, UPnP/1.0, POSIX/1.0	Linux/3.3.0 UPnP/1.0 YunOSTV/1.0
EPSON Linux UPnP/1.0 Epson UPnP SDK/1.0	FreeBSD/8.0 UPnP/1.0 Panasonic-MIL-DLNA-SV/1.0	Linux/i686 UPnP/1,0 DLNADOC/1.50 LGE WebOS TV/v0.9
FreeBSD/8.0 UPnP/1.0 Panasonic-MIL-DLNA-SV/1.0	GIGABYTE-UPnP-Server/1.0 UPnP/1.0	Mac OS X UPnP/1.0 DLNADOC/1.50 Serviio/2.0
FreeRTOS/6.0.5, UPnP/1.0, IpBridge/0.1	Linux UPnP/1.0 DLNADOC/1.50 Serviio/2.1	SHP, UPnP/1.0, Samsung UPnP SDK/1.0
Linux UPnP/1.0 Huawei-ATP-IGD	Linux, UPnP/1.0, DHP-W610AV Ver 1.02EU	Synology/DSM/58.185.196.X
Linux, UPnP/1.0, DAP-1665 Ver 2.06	Linux/i686 UPnP/1,0 DLNADOC/1.50 LGE WebOS TV/v0.9	Unix/Linux v5.4.0-65-generic (buildd@lcy01-amd64-018)
Linux/2.6.17.WB WPCM450.1.3 UPnP/1.0, Intel SDK for UPnP devices/1.3.1	POSIX, UPnP/1.0, Intel MicroStack/1.0.2777	UPnP/1.0 RSSDP/1.0
Linux/2.6.5-it0, UPnP/1.0, Intel SDK for UPnP devices /1.2	SHP, UPnP/1.0, Samsung UPnP SDK/1.0	UPnP/1.0 UniFi/6.1.71
Linux/3.4.103 UPnP/1.0 ASRock Media Server/1.0	Synology/DSM/192.168.1.89	WebOS/1.5 UPnP/1.0 webOSTV/1.0
Linux/i686 UPnP/1,0 DLNADOC/1.50 LGE WebOS TV/v0.9	UPnP/1.0 DLNADOC/1.50 Kodi	Windows/10.0 UPnP/1.0 EmbyServer/4.5
Linux/i686 UPnP/1.0 DLNADOC/1.50 Platinum/1.0.3.0	WebOS/1.5 UPnP/1.0 webOSTV/1.0	Windows/10.0.17763 UPnP/1.1 uTorrent(client)(native)/355
LPUX/1.3 UPnP/1.0 Aficio MP 2510/1.0	Windows/10.0 UPnP/1.0 EmbyServer/4.5	Windows/6.3.9600 UPnP/1.1 BitTorrent(client)(native)/7105

TXT RR for amplifying their attack network traffic and open DNS resolvers as reflectors. The authors reported a BAF of 60. The first comprehensive study of DNS amplification attack involving DNSSEC-related RRs is that given in [9]. The authors took advantage of the increased size of DNSSEC-related RRs for amplifying the DoS traffic, along with the multitude of SOHO devices operating as open DNS forwarders for reflecting this traffic. According to their experiments, the authors recorded a maximum BAF of 44. Moreover, the same group of authors investigated the amplification and reflection capabilities of the dedicated ANS for the TLDs [15]. In particular, they reported that almost 70% of the ANSs responded with a BAF of 60 for at least one of the examined query types and a 7% with greater than 100. Furthermore, they concluded that 9.5% of the ANSs reflected their ingress traffic, with a success rate of 90%, i.e., they responded to 9 out of 10 requests, after amplifying its volume by a weighty factor that exceeds 50.

Similarly, Rijswijk-Deij et al. [12] investigated the feasibility of exploiting DNSSEC-related RR to augment the BAF of a DNS amplification attack. To this purpose, they calculated the provided BAF of 2.5 million DNSSEC-signed zones under 6 major TLDs. They concluded that the ANY query type could generate a factor of around 47 on average, with the worst case of 179. Moreover, Rossow [10] evaluated the potential of exploiting 14 UDP-based network protocols for launching amplification attacks. For the case of DNS, they calculated that the "ANY" query type produced a BAF of 54.6 on average, with the top 10% yielding a BAF of 98. Regarding the SSDP protocol, the authors discovered that SSDP-enabled devices could provide a BAF of 30.8 with the top 10% accomplishing a BAF of 75.9. Lastly, an alarming finding by Rossow is that the *monlist* request of the NTP protocol, fortunately now deprecated, could trigger a BAF of 4670 and a PAF of up to 100.

Gondim et al. [29] evaluated in a local area network (LAN) testbed the amplification capabilities of SSDP and DNS protocol among other UDP-based protocols. They recorded a BAF of at most 38 and 48, and a PAF of 10 and 3 for SSDP and DNS, respectively. However, they recognized that protocols such as SSDP, which are mainly deployed in IoT devices, suffer from saturation when they are exploited for DoS

Table 21
Comparison of related work.

	Vaughn and Evron [27]	Anagnostopoulos et al. [9]	Rijswijk-Deij et al. [12]	Rossow [10]	Kührer et al. [28]	Gondim et al. [29]	Current
Year of study	2006	2013	2014	2014	2014	2020	2021
Scale	Internet wide	Multi country-wide	Internet wide	Internet wide	Internet wide	LAN	Multi country-wide
Method	Log file investigation	IP scanning	Active DNS probing of TLD	IP scanning	IP scanning	IP scanning	IP scanning
DNS Resolvers/ forwarders	N/A	✓	N/A	No differentiation	✓	N/A	✓
Fingerprinting of hosts	N/A	✓	N/A	✗	✓	N/A	✓
DNS	✓	✗	✓	✓	✓	✓	✓
DNSSEC	✗	✓	✓	✓	✓	✗	✓
SSDP	✗	✗	✗	✓	✓	✓	✓
Other Protocols examined	–	–	–	SNMP, NTP, NetBios, CharGen, QOTD, BitTorrent, Kad, Quake 3, Steam	SNMP, CharGen, QOTD, NTP, NetBIOS	SNMP, NTP	–
Calculation of BAF	Unavailable	UDP payload	UDP payload	UDP payload	UDP payload	IP packet	UDP Payload
Max BAF for DNS	60 (TXT based response)	✗	80.90 (query for .nl TLD)	✗	✗	✗	Top 25%:18.25/Max: 72.45[a]
Max BAF for DNSSSEC	✗	44 (ANY query)	178.60 (query for .net TLD)	Top 10%: 64.1 (ANY query)	✗	43,81	Top 25%: 43.97/Max: 47.48[b]
Max BAF for SSDP	N/A	N/A	N/A	Top 10%: 75.9 (SEARCH query)	✗	38,23	Top 25%: 47.78/Max: 470.22[c]
Max PAF for SSDP	N/A	N/A	N/A	9.92 (all)	✗	10	Top 25%: 12/Max: 126[c]

[a]For Q2 from Greek IP pool (E2).
[b]For Q8 from Greek IP pool (E2).
[c]For ssdp:all from Singaporean IP pool (E2).

purposes. Meaning that the amplification effect is decreasing proportionally to the ingress traffic, due to the computation capabilities of the reflecting IoT device and the congestion on the outbound traffic.

Kührer et al. [28] conducted an Internet-wide scanning for discovering potential reflectors. They focused on several UDP-based protocols, including DNS and SSDP, and they noticed that throughout their experiment there existed a number of 23 to 25.5M open DSN resolvers and around 5M SSDP reflectors. Furthermore, in agreement to our results, they deduced that these reflectors migrate to different IP addresses with a high rate. Specifically, only about 50% of the initial discovered reflectors were still accessible after one week, while the following weeks their population slightly decreased until reached an almost steady level of around 30%–40%. The main difference of [28] with our work is that beside the identification of the reflectors for DNS and SSDP, we also meticulously evaluate their amplification capabilities. Moreover, regarding the devices that provide DNS services, we differentiate DNS resolvers from forwarders, as it is rather straightforward that the majority of open DNS forwarders are misconfigured to operate as such, and thus their operation should be ceased. The investigation of the SSDP ephemeral ports phenomenon and the underlining of the information leakage issue due to the same protocol is also a plus for the work at hand.

It is also to be noted that on top of any novel contribution, Internet measurement works, especially those elaborating on security issues, need to be updated from time to time in order to present a recent snapshot of the current state of affairs. This aids in directly comparing the current situation with previous results and therefore obtaining a clear estimation of the progress made, i.e., the uptake of mitigations over the course of time. For instance, the work in [28] revealed that the "ANY" type of query was the most impactful at that time, while the work at hand pinpoints that this observation does not stand true anymore.

7. Conclusions

DoS type of attacks capitalizing on the amplification effect along with the still inadequate implementation of BCP 38 comprise a persistent threat and a growing major concern in the cyberspace. While some vulnerabilities relevant to specific UDP-based protocols, such as the NTP's *monlist* debugging command have been cured [28], other protocols with strong amplification potential continue to draw the attention of both the security community and the aspiring cybercrooks. Through multi-countrywide Internet scans, this work attempts to shed light on the DNS and SSDP amplifiers, which are among the most favourable for mounting or orchestrating impactful volumetric DDoS assaults. We offer up-to-date, wholemeal, and novel answers to several key questions regarding (a) the demographics of such amplifiers across three countries in two continents, (b) the hardware and software characteristics of such devices via painstaking fingerprinting, and (c) a detailed assessment of their amplification capacity. The most important takeaways from this endeavour can be summarized as follows:

- The number of potentially exploitable amplifiers remain substantial, and for some countries quite alarming, although progress is being made especially for SSDP; on top of that, a great portion of such devices yield a high amplification factor.

- The use of outdated OSs is the norm for "general purpose" machines hosting DNS forwarders. With reference to the E2 column of Table 5, the great majority of DNS forwarders hosted by this type of devices in both Greece and Portugal, more than 75 and 80%, respectively, run on a Linux v2 kernel; the situation is better for Singapore where the majority of forwarders runs on MS Windows Server 2012 (≈63%), but still around 28% uses a Linux v2 kernel.
- A great mass of SSDP open services run on SOHO devices, often with obsolete OSs indicating an "install and forget" mentality.
- The concerned organizations that operate open resolvers differ considerably depending on the country.
- In all cases, DNS amplifiers are more productive in terms of BAF if queried for DNSSEC-related RRs, say, Q8 or Q9, while the "ANY" type is less effective or eventually unusable due to the increasing adoption of RCF 8482.
- The third quartile of the DNS BAF distribution for E2 reaches an average of 17.5 and 15 for Greece and Portugal, respectively, and around 12 for Singapore. The same figures for E1 are calculated to ≈15 in every case, thus indicating a slight improvement (−3) for Singapore and an almost equal deterioration (+2.5) for the other two countries. Interestingly, for E1, the aforesaid scores pertain to Q9 in all cases, while for E2 the most fruitful type of query is Q9 for both Greece and Portugal and Q8 only for Greece.
- The population of amplifiers does not show steep variations in the considered biennium, but exceptions do exist and are mostly attributed either to the augmentation of IP addresses, as in the case of forwarders in Singapore.
- From a bird's-eye view, for the considered biennium, DNS forwarders show fluctuations from approximately +.01 (Portugal) to +.06 (Singapore), resolvers remain more or less static (only Greece demonstrates a negligible (+.001) increase), while SSDP amplifiers present major fluctuations from around −89.3% (Singapore) to +100% (Portugal), from −98.7% (Greece) to +100% (Portugal), and from −77.5% (Greece) to +512.5% (Singapore) for ssdp:all, upnp:rootdevice, and both query types, respectively.
- For SSDP, the implementations do not abide by the standard in regard to the network port, thus complicating monitoring and defencive schemes.

All in all, the current work can be used as a reference to anyone interested in contributing to DDoS defences, including security professionals, scholars, policy makers, and service providers, and it is also anticipated to stimulate research efforts in this timely and high stakes area. Furthermore, the results of the current study can be used in raising the awareness of the community about the imminent potential of this threat and impel the stakeholders towards taking the appropriate mitigation actions in a prompt manner. A straightforward direction for future work is the exploration and assessment of the amplification potential of other major UDP-based protocols, including NTP, simple network management protocol (SNMP), and constrained application protocol (CoAP) with a special focus on IP-based IoT SOHO devices.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] Cisco Annual Internet Report (2018–2023) White Paper. URL https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html.

[2] Luckie MJ, Beverly R, Koga R, Keys K, Kroll JA, kc claffy. Network hygiene, incentives, and regulation: Deployment of source address validation in the internet. In: Cavallaro L, Kinder J, Wang X, Katz J, editors. Proceedings of the 2019 ACM SIGSAC conference on computer and communications security, CCS 2019, London, UK, November 11-15, 2019. ACM; 2019, p. 465–80. http://dx.doi.org/10.1145/3319535.3354232.

[3] Heinrich T, Obelheiro RR, Maziero CA. New kids on the DRDoS block: Characterizing multiprotocol and carpet bombing attacks. In: Hohlfeld O, Lutu A, Levin D, editors. Passive and active measurement. Cham: Springer International Publishing; 2021, p. 269–83.

[4] NexusGuard, Threat Report FHY 2021 Distributed Denial of Service (DDoS). URL https://blog.nexusguard.com/threat-report/ddos-threat-report-fhy-2021.

[5] Donno MD, Dragoni N, Giaretta A, Spognardi A. DDoS-Capable IoT malwares: Comparative analysis and mirai investigation. Secur Commun Netw 2018;2018:7178164:1–30. http://dx.doi.org/10.1155/2018/7178164.

[6] Kolias C, Kambourakis G, Stavrou A, Voas JM. DDoS in the IoT: Mirai and other botnets. Computer 2017;50(7):80–4. http://dx.doi.org/10.1109/MC.2017.201.

[7] Spathoulas G, Giachoudis N, Damiris G-P, Theodoridis G. Collaborative blockchain-based detection of distributed denial of service attacks based on internet of things botnets. Future Internet 2019;11(11):226.

[8] Anagnostopoulos M. Amplification DoS attacks. In: Jajodia S, Samarati P, Yung M, editors. Encyclopedia of cryptography, security and privacy. Berlin, Heidelberg: Springer Berlin Heidelberg; 2019, p. 1–3. http://dx.doi.org/10.1007/978-3-642-27739-9_1486-1.

[9] Anagnostopoulos M, Kambourakis G, Kopanos P, Louloudakis G, Gritzalis S. DNS amplification attack revisited. Comput Secur 2013;39, Part B:475–85.

[10] Rossow C. Amplification hell: Revisiting network protocols for DDoS abuse. In: Proceedings of the 2014 network and distributed system security symposium (NDSS). 2014, URL https://www.ndss-symposium.org/ndss2014/.

[11] Majkowski M. Stupidly simple DDoS protocol (SSDP) generates 100 Gbps DDoS. 2018, URL https://blog.cloudflare.com/ssdp-100gbps/.

[12] van Rijswijk-Deij R, Sperotto A, Pras A. DNSSEC and its potential for DDoS attacks: A comprehensive measurement study. In: Proceedings of the 2014 conference on internet measurement conference. IMC '14, New York, NY, USA: ACM; 2014, p. 449–60.

[13] Ismail S, Hassen HR, Just M, Zantout H. A review of amplification-based distributed denial of service attacks and their mitigation. Comput Secur 2021;109:102380.

[14] Cloudflare. Memcached DDoS attack. 2020, URL https://https://www.cloudflare.com/learning/ddos/memcached-ddos-attack/.

[15] Anagnostopoulos M, Kambourakis G, Gritzalis S, Yau DKY. Never say never: Authoritative TLD nameserver-powered DNS amplification. In: NOMS 2018 - 2018 IEEE/IFIP network operations and management symposium. 2018, p. 1–9. http://dx.doi.org/10.1109/NOMS.2018.8406224.

[16] Anagnostopoulos M, Kambourakis G, Konstantinou E, Gritzalis S. DNSSEC vs. DNSCurve: A side-by-side comparison. In: Situational awareness in computer network defense: Principles, methods and applications. IGI Global; 2012, p. 201.

[17] Abley J, Gudmundsson O, Majkowski M, Hunt E. RFC 8482: Providing minimal-sized responses to DNS queries that have QTYPE=ANY. Tech. rep., IETF; 2019, URL https://tools.ietf.org/html/rfc8482.

[18] Goland Y, Cai T, Leach P, Gu Y, Albright S. Simple service discovery protocol/1.0 operating without an arbiter. Internet draft, IETF; 1999, URL https://tools.ietf.org/html/draft-cai-ssdp-v1-03.txt.

[19] Dagon D, Provos N, Lee CP, Lee W. Corrupted DNS resolution paths: The rise of a malicious resolution authority. In: Proceedings of network and distributed security symposium (NDSS08); 2008.

[20] Park J, Jang R, Mohaisen M, Mohaisen D. A large-scale behavioral analysis of the open DNS resolvers on the internet. IEEE/ACM Trans Netw 2021;1–14. http://dx.doi.org/10.1109/TNET.2021.3105599.

[21] Weber R. Better than Best Practices for DNS Amplification Attacks. URL https://archive.nanog.org/sites/default/files/mon_general_weber_defeat_23.pdf.

[22] Kolkman O, Mekking M, Gieben M. RFC 6781: DNSSEC operational practices, version 2. 2012, URL https://tools.ietf.org/html/rfc6781.

[23] Vixie P, Schryver V. DNS response rate limiting (DNS RRL). 2012, http://ss.vix.com/~vixie/isc-tn-2012-1.txt.

[24] Morishita S, Hoizumi T, Ueno W, Tanabe R, Gañán C, van Eeten MJ, Yoshioka K, Matsumoto T. Detect me if you…oh wait. An internet-wide view of self-revealing honeypots. In: 2019 IFIP/IEEE symposium on integrated network and service management (IM). IEEE; 2019, p. 134–43.

[25] Portable SDK for UPnP Devices. URL https://pupnp.sourceforge.io/.

[26] Bing M. A new twist in SSDP attacks. 2018, URL https://www.netscout.com/blog/asert/new-twist-ssdp-attacks.

[27] Vaughn R, Evron G. DNS amplification attacks (preliminary release). 2006.

[28] Kührer M, Hupperich T, Rossow C, Holz T. Exit from hell? Reducing the impact of amplification DDoS attacks. In: 23rd USENIX security symposium (USENIX security 14). 2014, p. 111–25.

[29] Gondim JJ, de Oliveira Albuquerque R, Sandoval Orozco AL. Mirror saturation in amplified reflection distributed denial of service: A case of study using SNMP, SSDP, NTP and DNS protocols. Future Gener Comput Syst 2020;108:68–81.