EUROPEAN UNION AGENCY
FOR CYBERSECURITY

SECURITY AND PRIVACY OF PUBLIC DNS RESOLVERS

FEBRUARY 2022

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use resilience@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

AUTHORS

Evangelos Kantas, Marnix Dekker, ENISA

ACKNOWLEDGEMENTS

We would like to thank the members of NIS CG WS10, a group of experts from national authorities supervising the Digital Infrastructure sector under the NIS Directive. For this project we contracted the support of DNV (Maria Jinert Johansson, Shaun Reardon), who supported us with desktop research, interviews with industry experts and analysis.

Above all, we would like to thank all the experts who participated in the interviews and shared their valuable experience: Anne-Marie Eklund Lowinder (Internetstitifelse), Bill Woodcock and John Todd (Quad9), Byron Holland, Mark Gaudet, Dave Chiswell and Vivek Kumar (CIRA), Francois Zamora and Jeanmarie Mele (Orange), Giovane Moura (SIDN), Jari Arkko (Ericsson), Marco Hogewoning (RIPE NCC), Michael Hausding (Internet Society, Switzerland Chapter), Roxana Radu (Graduate Institute Geneva), Miguel Angel Carnero Fernandez, Alejandro Becerra Gonzalez, Cristina Vela Marimon, Diego Lopez, Alberto Sempere Blanco, Sergio de los Santos Vilchez, Antonio Augustin Pastor Perales and Patricia Diez Muñoz (Telefonica), subject matter experts at Google, Patrik Fältström (Netnod), Paul Vixie (Farsight Security), Robbie Grue and Reda Jaaouani (CISCO), subject matter experts at Cloudflare, Ross Creelman (ETNO), Stéphane Bortzmeyer (AFNIC), Stephen Hermanson, Polly Cameron, Gianpaolo Angelo Scalone, Andreas Kohring and Javier Villegas-Burgos (Vodafone Group), Thomas Tschersich and Philipp Trinius (Deutsche Telecom).

LEGAL NOTICE

This publication represents the views and interpretations of ENISA, unless stated otherwise. It does not endorse a regulatory obligation of ENISA or of ENISA bodies pursuant to Regulation (EU) No 2019/881.

ENISA has the right to alter, update or remove this publication or any of its contents. It is intended for information purposes only and it must be accessible free of charge. All references to it or its use as a whole or partly must show ENISA as its source.

Third-party sources are quoted as appropriate. ENISA is not responsible or liable for the content of the external sources including external websites referenced in this publication.

Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

ENISA maintains its intellectual property rights in relation to this publication.

COPYRIGHT NOTICE

ISBN: 978-92-9204-558-6 - DOI: 10.2824/288837 - Catalogue number: TP-08-22-030-EN-N

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Domain Name System (DNS) resolution is a distributed system of protocols and registers, whose main purpose is to map the human friendly domain names, such as www.example.com, to machine readable IP addresses, such as 123.123.123.123. DNS resolution is both highly critical and highly sensitive, and traditionally this service is provided locally by internet access providers for their customers.

For years there has been a shift towards public DNS resolvers, either large-scale ones such as Google and Cloudflare or smaller ones like the European non-profit Quad9 and Canadian Shield, a DNS resolution service provided by the Canadian top-level domain registry CIRA to Canadian citizens. These resolvers tend to offer advanced security and protection features out-of-the-box, such as encryption of user requests and blocking of malicious domains, that aim to attract users to their services.

In this paper, we analyse this shift in the market and discuss some of the major drivers for these changes, such as:

- **Encryption -** Many public DNS resolvers offer encryption of DNS requests via the newer resolution protocols;
- **Service outages –** Sometimes, a service outage of regular internet access provider DNS resolvers can trigger customers to switch to a global public DNS resolver;
- **DNS blocking –** Anyone who wishes to view online content that is blocked by their own provider (under national policies) can use public DNS resolvers to circumvent the blockage.

Furthermore, the resolution protocols are evolving as well. Currently in many settings DNS requests are sent unencrypted by the endpoint (a laptop or smartphone) to the telecom provider or internet service provider. There are mainly two new protocols that are growing in importance and which will be discussed, **DNS over HTTPS** (DoH) and **DNS over TLS** (DoT).

In this paper we also analyse the different security and resilience advantages (such as **geographic spread**) and drawbacks (such as **loss of enterprise network traffic visibility**) of public DNS resolvers. Finally, based on the analysis, we identify concerns in this area and we conclude with certain recommendations to address them, such as:

- providing citizens and organisations with a robust European alternative to large scale US DNS resolvers, such as DNS4EU;
- issuing specific and actionable guidelines to help organisations avoid the disruption of security controls caused by encrypted DNS traffic;
- closely monitoring the matter of national blocking policies, as this is one of the main drivers causing users to switch to global public DNS resolvers.

1. INTRODUCTION

In the DNS resolution market there is a shift towards large-scale public DNS resolvers, such as Google, Cloudflare and Quad9, using new DNS resolution protocols like DoH and DoT. These encryption protocols mean that there is an inflection point where changes are being made in DNS settings, consciously by the user or by the service provider within the applications or operating system during upgrades. This brings an opportunity to change not only the protocol itself, but the server from which answers are obtained. This means that DNS queries, which are critical and sensitive, are starting to be handled with different protocols and by different entities that are often based in a different country or even continent than the user.

In this paper, we present and analyse the main drivers for the shift to public DNS resolvers, and the evolution in the DNS resolution protocols. We look at the security and resilience aspects of these changes, we discuss data protection, legal and other considerations briefly, and we conclude with recommendations for policy makers and national authorities.

1.1 TARGET AUDIENCE

This paper aims to inform policy makers and national authorities about public DNS resolvers, which are an increasingly important part of the DNS resolution market.

1.2 SCOPE

In this paper we only focus on DNS resolution and the shift from the local private DNS resolvers offered by telecom providers and ISPs towards the global public DNS resolvers offered by internet companies.

1.3 POLICY CONTEXT

1.3.1 NIS Directive

Under the NIS Directive (Article 14 and Annex II) national authorities are required to supervise the security of operators of essential services offering DNS resolution.

The requirements for supervision are described in Article 14 of the NIS Directive. These specifically mention that Member States must ensure that Operators of Essential Services[1]:

1. take measures to **manage their security risks;**
2. take measures to **prevent and minimise the impact of security incidents;**
3. **notify** the national competent authority or CSIRT of **incidents with a significant impact.**

Under the NIS Directive, Member States need to identify operators of essential services and consider the criticality of the essential services offered by the provider. As NIS Directive Annex II states, operators offering DNS are within the scope of the Digital Infrastructure sector, together with IXPs and TLD name registries.

Note that the DNS resolvers offered by telecom providers and internet access providers, as part of the internet connection, are within the scope of the EU’s telecom directives (the EECC), rather than the NIS Directive.

[1] https://eur-lex.europa.eu/eli/dir/2016/1148/oj

In several Member States, some of the larger public DNS resolvers have been identified as operators of essential services, depending on the number of users, their criticality, etc.

1.3.2 Cybersecurity package – DNS4EU

At the end of 2020, the European Commission announced a new cybersecurity strategy, introducing a package of new cybersecurity initiatives, including legislative proposals but also initiatives by the Commission. One of the elements of the new strategy is the so-called DNS4EU proposal.

DNS4EU aims to establish a public European DNS resolver service that offers an alternative to the public DNS resolvers that currently dominate the market (which are mostly US-based internet companies). DNS4EU aims to be transparent and in line with the latest security, data protection and privacy-by-design standards and rules by default. DNS4EU will be part of the European Industrial Alliance for Data and Cloud.

2. DNS RESOLUTION MARKET

In this section we take a look at the DNS resolution market, how it is shifting and what are the drivers for these shifts. It should be noted that measuring market share of DNS resolvers presents a series of challenges, as relevant data are scarce, many resolvers do not publish relevant reports, and analysis is usually built upon sample datasets.

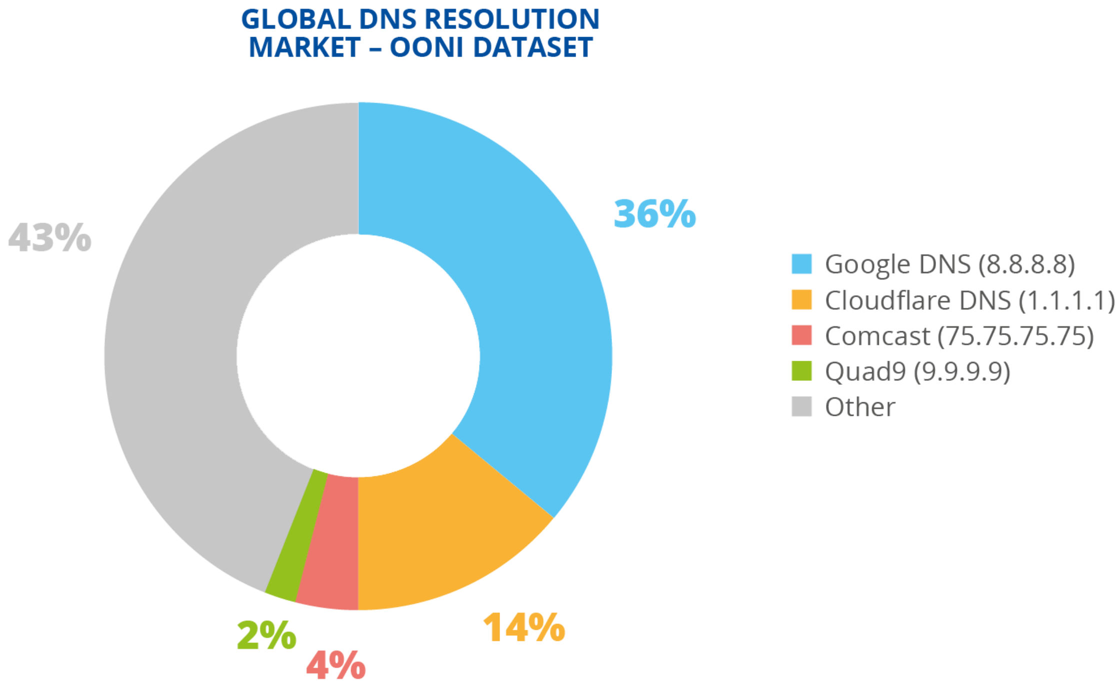
2.1 STATE OF PLAY OF THE DNS RESOLUTION MARKET

In the last years there has been a shift away from the DNS resolution services provided by telecom providers, towards global players offering public DNS resolvers. These large global public DNS resolvers are growing in importance, handling an increasing number of DNS requests.

Please note that because DNS is a complex distributed system and because DNS queries can be resolved at many different layers, sometimes using a cache, it is not easy to get hard data about the DNS resolution market.

In 2020 Radu and Hausding published an article in an academic journal in which they measured market share using data from the OONI project[2] (Open Observatory of Network Interference). Their data taken in 2019 (see the pie chart below) confirms that Google has the largest share of the market by a substantial margin[3], though it must be noted that the OONI data is limited to mobile devices and OONI probes.

Figure 1: Distribution of global DNS resolution traffic – OONI dataset (2019)



[2] https://ooni.org/about/
[3] Radu, R. and Hausding, M., 2020. Consolidation in the DNS resolver market–how much, how fast, how dangerous?. Journal of Cyber Policy, 5(1), pp.46-64

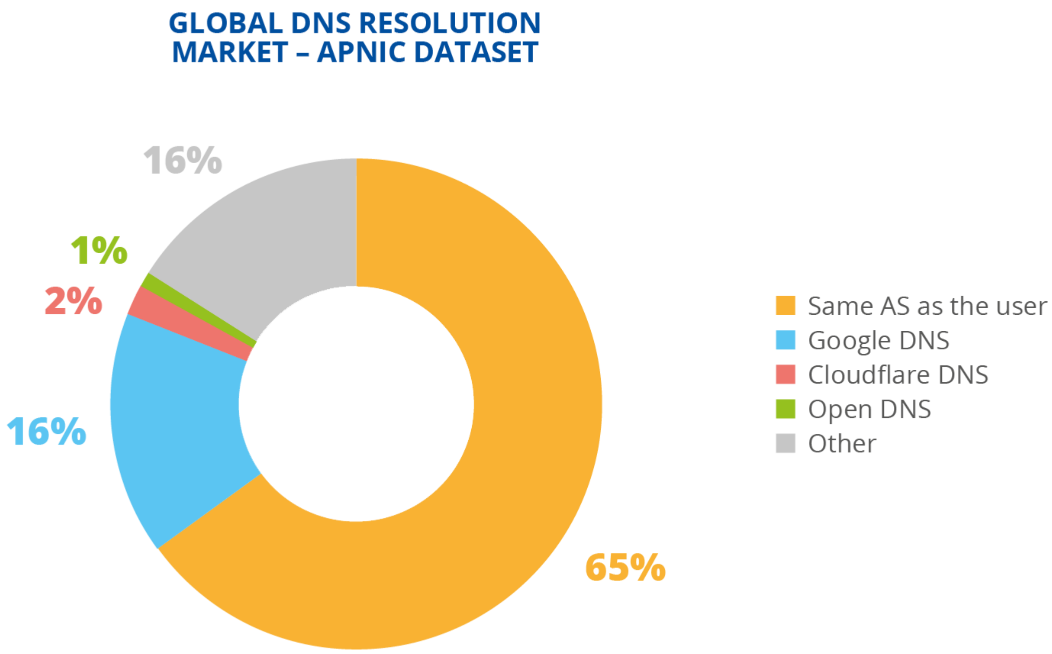
Based on the data collected, in 2019 half of the DNS requests were being resolved by two public resolvers, Google and Cloudflare. Both resolvers are owned by companies based in the USA, which has raised concerns about how these providers can be supervised regarding resilience and the protection of personal data.

Radu and Hausding also compare the data for 2019 with historical data from 2016, which shows that global public DNS resolvers are growing rapidly: Google DNS grew from 15% to 36% of the market, Cloudflare from 0% to 14% in just three years.

According to research done in 2020 and data based on the Open Observatory of Network Interference, almost half of the global DNS requests were resolved by two large-scale public DNS resolvers. This creates a significant dependency on the infrastructure of just two large organisations.

When looking at alternative methods to measure the market share of DNS resolvers, one can look also at APNIC[4], the regional internet registry administering IP addresses for the Asia and Pacific regions. APNIC publishes a nearly real time report on DNS traffic based on their data and uses a larger and more diverse dataset than OONI. The market distribution, according to APNIC's much more recent dataset of October 2021, can be seen in Figure 2 below

Figure 2: Distribution of global DNS resolution traffic – APNIC dataset (October 2021)



The data form APNIC shows a somewhat different picture, with 65% of DNS requests being resolved by a resolver within the same Autonomous System as the user (their own internet access provider's DNS), while Google is resolving 16%, Cloudflare 2% and Open DNS 1% of the requests.

There are no established ways to accurately measure the distribution of DNS requests over the various DNS resolvers. Measuring methods are not straightforward, while many resolvers do not publish relevant reports.

[4] https://www.apnic.net/about-apnic/

2.2 APPLICATIONS USING PUBLIC DNS RESOLVERS

One of the public global DNS resolvers (Cloudflare) publishes statistics about where the DNS requests are coming from, in terms of devices and applications[5]. It must be noted that the data published by Cloudflare are possibly being combined with CDN data as well, in order to provide information about aspects not present in the DNS requests, such as user browser. Figure 3 shows data published by Cloudflare and captured in October 2021.

Figure 3; Distribution of mobile vs desktop DNS resolution traffic - Cloudflare

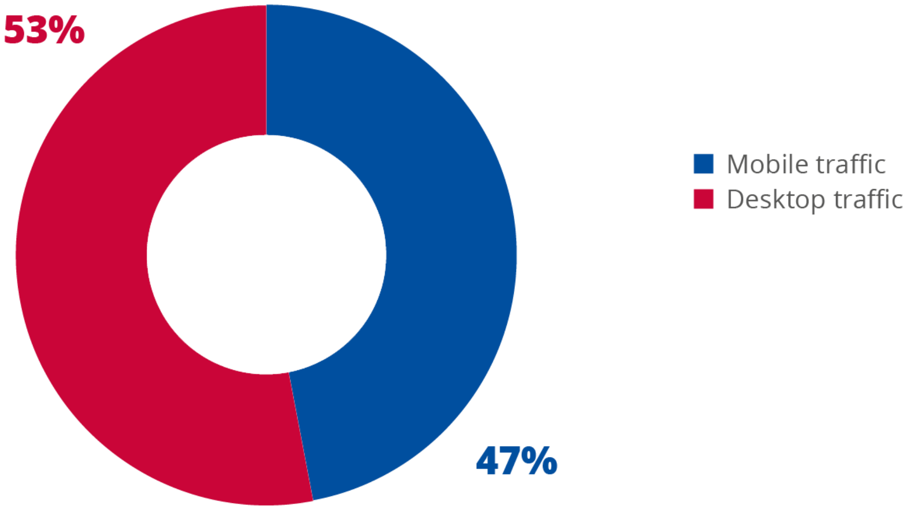
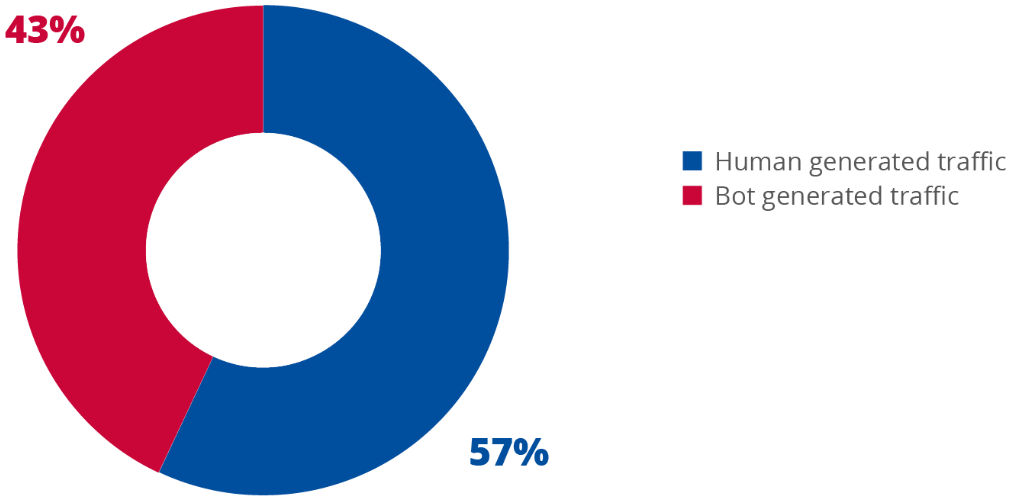
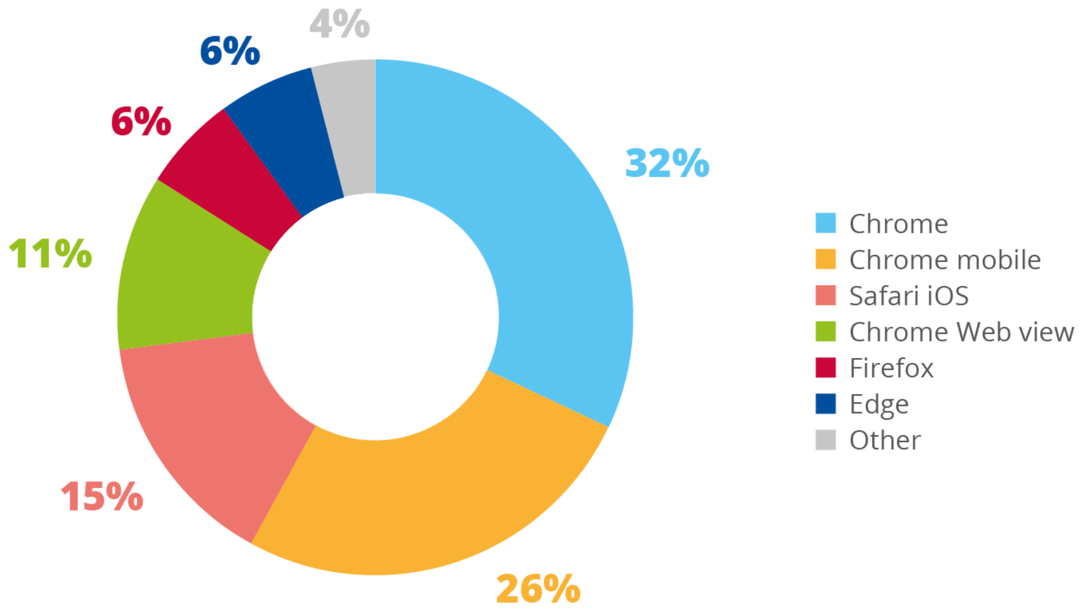


Figure 4: Distribution of bot vs human generated DNS resolution traffic – Cloudflare



[5] https://radar.cloudflare.com/

Figure 5: Distribution of DNS resolution traffic per browser - Cloudflare



More than half of the DNS requests come from mobile devices. Note that, especially on mobile devices, users may struggle to manually configure their DNS resolver.

Although the only data that could be gathered was from Cloudflare, this represents a significant share of the users of public DNS resolvers. It is worth noting that more than 50% of the requests originate from mobile devices, where users rarely go to lengths to manually change their DNS resolver. This indicates that in many cases DNS selection is based on the default configuration of the products that people use.

DNS resolver selection is in many cases based on the default configuration of applications and devices, rather than conscious user selection.

It must be noted that measuring the distribution of DNS requests over the various DNS resolvers presents significant challenges, hence the difficulty in obtaining more recent data on market share. In addition, as there are no established methods for accurately measuring this distribution, there is reliance on large-scale exercises performed by individual researchers.

Measuring the distribution of DNS requests over various applications, agents and devices presents difficulties. Such measurements could help researchers and organisations gain more insight around the DNS resolution market.

2.3 DRIVERS CHANGING THE MARKET

During desktop research and in-depth interviews with experts, we identified several drivers that are pushing the shift towards public DNS resolvers. These drivers range from user-related preferences or concerns to incentives or the limitations of larger organisations. We present the main drivers identified by our analysis in the following table.

Table 1: Drivers for the shifts in the market

Drivers for the shift	Explanation
Encryption offered by the new players or protocols	The added encryption offered by the new players and by the new protocols is attracting users towards public DNS resolvers. The underlying reasons for end user interest in encryption are many fold. These range from critical revelations concerning privacy and surveillance being made public, to concerns about easy-to-use network snooping tools on local networks or the fear that financial services sessions can be hijacked via DNS corruption.
Avoidance of national blocking policies or restrictions	As national blocking policies and geographic restrictions are becoming more prevalent, there is a significant increase in the desire to avoid them and view blocked online content (such as geographically restricted entertainment, file sharing, and sports)
Data protection considerations	Customers have become more aware of data protection issues. They are concerned about what happens to the information about their DNS requests and many consider the global public resolvers as more transparent in that regard compared to DNS resolution by their internet access providers.
Service outage	Sometimes customers switch to global public DNS resolvers because their traditional DNS resolution service suffers an outage. After the outage is resolved they often remain with the global public resolver.
Service performance or latency	Sizable public DNS resolvers usually have large numbers of nodes around the world and so are able to offer users lower latency by load-balancing the traffic and sending requests to the nearest available node. There are cases though where the DNS infrastructure of the internet access provider is much closer to the client and thus can offer the user higher performance.
Value added services that can be offered – such as security blocking and family filters	Public DNS resolvers can offer value-added services on top of the usual DNS resolution, ranging from family filters and parental controls to security blocking to protect customers from phishing, scams, malicious websites, etc. However, there are internet access providers that offer similar security services to their clients.
Speed of adoption of newer protocols	Traditional DNS resolvers at the telecom providers are perceived as being slow with the adoption of new standards for DNS resolution.
Complexity and limited incentives for traditional providers of DNS resolution	For telecom providers, DNS resolution is typically a ‘free’ service integrated as part of the internet access service. Therefore, there is little financial incentive for providers to invest in this service. At the same time DNS resolution has become complex. Up until 2021 there were 281 relevant RFCs on various aspects of DNS[6] and the number is growing very rapidly.
Economies of scale for global players	Telecom providers mostly operate within country borders, serving a customer base in one country. This means they cannot operate on the scale of global public DNS resolvers, which has an impact on the cost-efficiency and quality of the services offered.
Outsourcing or forwarding of DNS queries by smaller ISPs	Some smaller telecom providers are outsourcing or forwarding DNS requests to global public DNS resolvers to save costs, to comply with GDPR regulations, to access additional service features (blocklists, etc.) or simply to decrease the complexity of their networks.
Default configurations included in applications such as browsers	Some applications, such as the Mozilla Firefox browser, have started to configure their products to use global public DNS resolvers by default in some regions.

[6] https://www.statdns.com/rfc/

3. DNS RESOLUTION PROTOCOLS

When discussing the observed shift towards public DNS resolvers, it is important to present and analyse the various current and newer DNS security protocols, as these represent a significant security-related driver for this shift. In addition, the support of these protocols by the public DNS resolvers that were interviewed will be presented.

During the traditional DNS resolution process, the user queries are sent over the network to the DNS resolver of the internet access provider. In the majority of cases, these requests are sent in an unencrypted form over the network, leaving them open to sniffing or man-in-the-middle attacks. Recently however, two new protocols have been standardised that aim to remediate that:

- DNS over HTTPS (DoH)
- DNS over TLS (DoT)

In addition, other DNS resolution protocols are being developed and adopted, such as DNSCrypt, DNSCurve and Oblivious DoH (ODoH). In this section we look at current and future DNS security resolution protocols.

3.1 CURRENT AND UPCOMING DNS RESOLUTION PROTOCOLS

3.1.1 DNS over HTTPS (DoH)

DoH is a security protocol for DNS resolution over HTTPS. It aims to increase user privacy and security by preventing eavesdropping and manipulation through man-in-the-middle (MITM) attacks. It uses TLS as an underlying encryption layer to encrypt the DNS request between the client and the DNS resolver. For DoH to work, the client must have access to a DoH-compatible server that will answer the query.

There are three common usage scenarios for DoH.

- *Using DoH within an application, such as a browser*: this method originally bypassed the operating system's own DNS lookup configurations, as the application took over the name lookup process. The application may or may not try to use the local network resolver via DoH and may communicate with an off-network cloud resolver as a default. There is a shift, however, by operating systems (such as Windows and MacOS) to support DoH at the OS level.

- *Installing a DoH proxy on an organisation's own local name server inside the network, while leaving the existing DNS configurations in place for the operating systems on the network*: clients can continue using traditional DNS querying to the local name server which then gathers replies by sending them to DoH-capable servers on the Internet. This encrypts the query between the local nameserver ('forwarding cache') and the upstream DoH-capable recursive resolver, but does not encrypt the query between the client and the local forwarding cache. This provides encryption outside the shelter of the local network but trusts traffic inside the network to be secure without encryption.

- *Installing a DoH-capable upgrade on the DNS server residing on the local network, so that the operating system is configured to directly query a local DoH system*: That system can then either be a fully-recursive DNS server, or it can forward queries to an upstream

DoH-capable server. This would encrypt the traffic from the client to the local DNS server and, optionally, would encrypt it to the upstream cloud server if that configuration was chosen. If the local DNS server was DoH-capable but was a fully recursive resolver, queries to authoritative systems would be unencrypted.

Advantages

The main advantages of DoH can be summarised as follows:

- **Confidentiality - Encryption** – by encrypting user DNS queries between the user device and the resolver, DoH can protect users against man-in-the-middle attacks. In comparison, traditionally DNS queries are sent in plain-text leaving them open to interception.

- **Protection from unauthorised access** – the encryption of user DNS queries with DoH can protect sensitive information that could be sniffed by third-parties or the user's own internet service provider.

Disadvantages

The main concerns about using DoH are:

- **Disruption of cybersecurity controls and content filters** – as DoH encrypts name resolution requests and 'hides' them in normal HTTPS traffic, it poses challenges for organisations or individuals who monitor or filter DNS requests to log or block access to malicious or inappropriate sites[7]. This is particularly important for organisation networks where system administrators use local DNS servers and DNS-based software for filtering and monitoring local traffic. Using external DoH in such cases would bypass these cybersecurity defences, rendering them useless[8].

- **Difficulties in monitoring** – by 'hiding' the DNS resolution traffic in HTTP data, DoH makes it hard to monitor DNS traffic. This is a disadvantage that can also be exploited by malwares (such as the Godlua malware[9]) that use this feature to evade monitoring and analysis of the traffic they produce.

- **Potentially revealing more information about the client** – DoH sessions naturally have more information about the end user than standard DNS or DoT transactions. Browsers include significant 'fingerprint' data in HTTPS transactions, potentially allowing DoH service operators to consistently identify users based on those signature patterns. There are ways to minimise this fingerprint ability, but it is the case that HTTPS is a much more complex encapsulating protocol than either the legacy DNS or DoT, which creates more opportunity for risks to privacy.

- **Leaking of internal network information** – when using DoH, the leaking of internal network information is possible when trying to resolve the domains of internal organisations. This happens because the browser initially attempts to contact the external DoH resolver, practically revealing the internal domain it is attempting to resolve.

- **Failure to inform user of issues** – in cases where the name lookup process is not performed by the operating system, the application could fail to inform the user of any DoH issues, as the operating system's logging and alerting functions are not engaged.

[7] https://searchsecurity.techtarget.com/definition/DNS-over-HTTPS-DoH
[8] https://www.cyberonsecurity.no/2020/03/11/dns-over-https-doh/
[9] https://www.bleepingcomputer.com/news/security/new-godlua-malware-evades-traffic-monitoring-via-dns-over-https/

According to some of the interviewees, deployment of DoH is becoming increasingly more common.

As DoH becomes increasingly more common, its use with public DNS resolvers by users of organisations can disrupt the network security controls of these organisations and prevent them from monitoring and filtering malicious network traffic.

3.1.2 DNS over TLS (DoT)

DoT is a security protocol for encrypting and wrapping DNS queries and replies through the TLS protocol. It aims to increase user privacy and security by preventing eavesdropping and manipulation through MITM attacks. So far, DoT has been implemented by Quad9, Google and Cloudflare, and is supported by most large resolvers.

At first glance, DoH and DoT look very similar as they both employ TLS for encrypting users' DNS queries. The most important difference between the two is the network port used for the DNS requests. DoT uses only port 853, while DoH uses port 443 which, as mentioned previously, is the port that is used for all other HTTPS traffic.

With a dedicated port, DoT traffic streams can be observed on the network and identified as DoT-based DNS, even though the content cannot be determined since the requests and responses are encrypted. With DoH on the other hand, DNS queries are hidden in other HTTPS traffic, as they all go through the same port. Disambiguating DoH traffic from other HTTPS traffic is difficult without deep-packet analysis, and may eventually become impossible.

Advantages

- **Confidentiality - Encryption –** the main advantage of DoT, as with DoH, is that it offers encryption of the DNS resolution data, improving security and user privacy.

- **Protection from unauthorised access –** similarly to DoH, the advanced protection of user DNS requests prevents malicious tampering that could take place by intercepting and modifying DNS queries or responses.

Disadvantages

- **Disruption of cybersecurity controls and content filters** – as with DoH, the encryption of DNS requests with DoT prevents network administrators from viewing the requested domains and applying security blocklists. However, the use of a dedicated port by the protocol allows network administrators to monitor and block DNS queries, which is important for identifying and stopping abnormal network behaviour and malicious traffic.

- **Use of dedicated port –** DoT's observability is considered a significant weak point, as it can be blocked by network administrators who are seeking to manage malware or content on their networks. DoT provides an easily-blocked protocol, while DoH purposefully disguises itself amongst other HTTPS traffic, raising the stakes of any blocking actions.

This list of disadvantages helps explain the lack of enthusiasm amongst interviewees for DoT. It was not perceived as popular because of its inaccessibility to application developers, which makes ad-hoc adoption more difficult by developers who are not involved in the operating system. (Currently Apple iOS, Mac OS and Android support DoT, but only in their most modern versions). Many developers expressed a strong desire that the browser and application space protect user privacy at all costs, but both perceived speed and difficulty of implementation, as well as potential blocking of the protocol, have made DoT a less-favoured solution than DoH.

It must be noted that significant work is being done in IETF on the specification of Discovery of Designated Resolvers (DDR) around adaptive DNS resolver discovery. This standard aims to allow clients to automatically upgrade unencrypted DNS connections to DoH or DoT, provided that this is supported[15].

3.1.3 DNSCrypt

DNSCrypt is a protocol that encrypts, authenticates and optionally anonymises the user's IP address, which prevents DNS spoofing. It uses cryptographic signatures to verify that responses originate from the chosen DNS resolver and have not been tampered with.

With DNSCrypt the client and the resolver initially generate a short-term key pair for preliminary communication. The client sends a non-authenticated request to the resolver. This request encodes the certificate versions supported by the client and the public identifier of the provider requested by the client. The resolver responds with a public set of signed certificates, which must be verified by the client using the resolver's public key.

Each certificate contains, apart from its basic parameters, a magic string (a number defined in code, activating otherwise hidden functionality[10]) that the client must prefix its queries with in order for the resolver to know which certificate to use. The DNS queries are then encrypted using the resolver's public key, the client magic string and its public key. Using the client's public key, the certificate and the corresponding secret key, the resolver verifies and decrypts the query and finally encrypts the response using the same parameters.

DNSCrypt has been adopted by several DNS resolvers[11].

Advantages

- **Confidentiality - Encryption –** As with DoH and DoT, DNSCrypt offers encryption of the DNS resolution data, thus protecting user queries.

- **Client anonymisation –** DNSCrypt has the option to hide the user's IP address from the servers. By doing so, it not only protects the data containing the user's online activity, it also anonymises the user as well.

Disadvantages

- **Not submitted to IETF** –The main disadvantage of DNSCrypt is that it is yet to be submitted to IETF[12] for review. As a result, it has not been peer-reviewed and tested by experts, and the work to keep the protocol current with other DNS standards has lagged significantly.

3.1.4 DNSCurve

DNSCurve is a secure protocol designed for DNS, using 256-bit elliptic-curve cryptography (estimated by NIST to be equivalent to about 3072-bit RSA). It uses per-query public key cryptography, and 96-bit nonces to protect against replay attacks[13]. In contrast to other encrypted DNS protocols that encrypt the traffic between the client and the resolver, DNSCurve

[10] https://en.wikipedia.org/wiki/Magic_string
[11] https://en.wikipedia.org/wiki/DNSCrypt#Deployment
[12] https://dnscrypt.info/faq
[13] https://en.wikipedia.org/wiki/DNSCurve#Implementations

only encrypts the DNS traffic between resolvers and authoritative servers, with the public key of the authoritative server being placed in DNS records.

There are certain similarities between DNSCurve and DNSCrypt, such as they both use the same cryptography mechanism and the same magic string for the DNS answer. The main difference, however, is that DNSCurve is established between the resolver and the authoritative server, while DNSCrypt sits between the client and the resolver[14]. In that respect, it operates with the resolver sending a packet to the server with a DNSCurve public key, a nonce and the encrypted query. The encryption is done using the private key from the resolver and the public key from the server. The response from the server contains the nonce and the encrypted answer for the query.

Advantages

- **Confidentiality - Encryption** — compared to traditional DNS resolution, DNSCurve offers data confidentiality by encrypting the user's DNS request.

- **Integrity** — traditional DNS offers some minimal protection but a patient attacker can sniff and forge DNS records. With DNSCurve this is prevented by using cryptographic authentication.

- **Availability** — traditional DNS offers no protection against denial of service (DoS) by an attacker sending several forged packets per second. DNSCurve recognises and discards forged DNS packets, providing some protection.

Disadvantages

- **Limited support** – As of 2021, there is limited support of the protocol by public DNS resolvers. OpenDNS started to support DNSCurve in 2010[15], but no other significant DNS provider is using it[16].

3.1.5 ODoH

Oblivious DNS over HTTPS, or ODoH, is a new proposed standard being developed by IETF, for DNS that separates information about client IP addresses from the queries those clients send. This means that both pieces of data (IP address & query) cannot be seen by any one organisation at the same time. It has been hailed by Cloudflare, who say it could help in closing privacy holes in DNS.

Cloudflare has been quoted as saying "*Until there is wider deployment among Internet service providers, Cloudflare is one of only a few providers to offer a public DoH or DoT service. This has raised two main concerns […] One concern is that the centralization of DNS introduces single points of failure (although, with data centres in more than 100 countries, Cloudflare is designed to always be reachable). The other concern is that the resolver can still link all queries to client IP addresses*"[17].

ODoH aims to solve such issues by adding public key encryption and a network proxy to separate user IPs and DNS requests. These two elements ensure that only the user has access to both DNS messages and their own IP address simultaneously.

There are three key features in ODoH[18]:

1. the target resolver only sees the query and proxy's IP address;

[14] https://dnscurve.io/faq/
[15] https://umbrella.cisco.com/blog/opendns-dnscurve
[16] https://en.wikipedia.org/wiki/DNSCurve#Implementations
[17] https://www.cyberscoop.com/cloudflare-odoh-ech-opaque-doh-dot/
[18] https://blog.cloudflare.com/oblivious-dns/

2. the proxy cannot see the DNS message, neither request nor reply;
3. only the intended resolver can read the query content and respond.

Advantages

- **Confidentiality – Encryption** – As with other encrypting DNS protocols, ODoH offers data confidentiality by encrypting the user DNS request as it is sent to the DNS resolver.
- **User Privacy** – ODoH improves user privacy, while also maintaining the security and integrity of the queries. So long as there is no collusion between proxy and the target, an attacker can only succeed if both proxy and target are compromised[18].

Disadvantages

- **Increased Complexity** – One of the main drawbacks of this protocol is the increased complexity which also adds fragility, as instead of one server in the chain of DNS recursive resolution, ODOH requires two servers – the proxy and the target. These by definition will have to be on separate networks run by two separate (possibly competing) operators, doubling the risk profile of recursive DNS flowing through those systems. Additionally, any problems relating to DNS will be extremely challenging to solve as there will be unclear demarcations of responsibility in the resolution chain, and the end user will need to understand some of the complexities in order to even start to diagnose any problems.

DNS is becoming increasingly complex, as new protocols are constantly being introduced. This is a complexity barrier that could discourage new smaller-scale public DNS resolvers from entering the market, thus leaving users with a choice of only a few large resolvers.

3.2 OTHER SECURITY FEATURES OF PUBLIC DNS RESOLVERS

Apart from the various DNS resolution protocols, public DNS resolvers usually offer additional security features that aim to enhance security and offer more customised services to users. These additional security features are usually in the form of blocking packages that allow for a more secure online experience, such as the protection of children and the blocking of malicious content.

According to interviewees, there are several ways for a resolver to develop their security blocklists. Smaller scale public DNS resolvers usually tend to prefer commercial threat feeds, while large scale public DNS resolvers might have the capacity and resources to complement such commercial threat feeds with in-house threat intelligence, based also on the huge amount of DNS requests they process daily.

In the table below, we present an overview of the different security features and DNS resolution protocols supported by some of the DNS resolvers in the market.

Table 2: DNS protocols and other security features supported by public DNS resolvers (October 2021)

DNS Provider	Nodes	DNSSEC	DNS over TLS	DNS over HTTPS	DNSCrypt[19]	DNSCurve	Additional Security Features
Cloudflare[2021]	250	Yes	Yes	Yes	No	No	- Normal: only DNS resolution - Security: malware and phishing protection - Family: malware, phishing and adult content
CIRA Canadian Shield[22]	3	Yes	Yes	Yes	No	No	- Private: only DNS resolution - Protected: malware and phishing protection - Family: blocks adult content
Google[23]	296	Yes	Yes	Yes	No	No	- Offers no blocking
OpenDNS (CISCO)[24]	37	Yes	No	Yes	Yes	Yes	- Family shield: blocks adult content - Home: customisable filtering set by user - Home VIP: home package and one-year use of stats and optional allow-list - Umbrella Prosumer: protects personal laptops anywhere
Quad9[25]	162	Yes	Yes	Yes	Yes	No	- Blocks malicious domains - Has optional non-filtered service

Based on the information presented in the table above, the following observations can be made.

- There is significant variance in the number of nodes that public DNS resolvers use. This is affected by their intended coverage – for example Canadian Shield is mostly aimed at Canadian citizens – but also by taking advantage of their already established infrastructure that supports their other core services – Google and Cloudflare already have a significant number of datacentres around the world
- There is a significant difference in the number and type of additional security features offered by various DNS resolvers. Some choose to offer no blocking at all, like Google, while others offer a variety of protection packages for family, home and children, some of which even require a paid subscription
- It is worth noting that DoH is supported by every one of the public DNS resolvers interviewed, while newer protocols like DNSCrypt and DNSCurve are currently supported only by OpenDNS (for both DNSCrypt and DNSCurve) and Quad9 (for DNSCrypt). The support of DNS protocols by major DNS resolvers usually plays a significant role in their community expansion, research and evolution.

[19] https://dnscrypt.info/public-servers/
[20] https://www.cloudflare.com/network/
[21] https://developers.cloudflare.com/1.1.1.1/
[22] https://www.cira.ca/cybersecurity-services/canadian-shield/
[23] https://developers.google.com/speed/public-dns/docs/intro
[24] https://www.opendns.com/data-center-locations/
https://support.opendns.com/hc/en-us/articles/360038086532-Using-DNS-over-HTTPS-DoH-with-OpenDNS
[25] https://www.quad9.net/support/faq/

4. SECURITY AND DATA PROTECTION

The DNS protocol hasn’t been created with security built-in and there have been frequent cyberattacks on DNS in the past. Most organisations report having experienced a cyberattack on their DNS infrastructure[26]. Public DNS resolvers also get targeted.

In 2016, DNS provider Dyn experienced a series of DDoS attacks caused by the Mirai botnet. The attack rendered several Internet platforms and services unavailable in Europe and North America. Websites affected included sites such as Airbnb, Twitter, and the Swedish Civil Contingencies Agency (MSB). The attack on Dyn came in several waves, causing outages of several hours spread out over the day[27]. It is important to note that Dyn is an authoritative DNS resolver and not a recursive resolver, but the impact of the attack underlines the criticality of DNS infrastructure.

Traditional DNS resolution, as provided by telecom providers and internet service providers, is unencrypted, offering no protection for the customer’s DNS requests and responses. Often they do not support newer DNS protocols.

The public DNS resolvers, on the other hand, offer security protocols, like DoH or DoT (see previous section) which encrypt DNS queries, protecting user traffic[28] [29]. Combined with the additional security features that some public DNS resolvers offer, such as blocking lists for malware, phishing domains, family protection, this creates a compelling package for users who want fast and secure or private DNS resolutions.

4.1 SECURITY AND RESILIENCE

In this section we discuss the different security and resilience advantages and drawbacks of the market shift towards public DNS resolvers.

4.1.1 Encrypted protocols (better privacy, better security)

A key benefit of the move towards global public DNS resolvers is the fact that they support DNSSEC and encrypted DNS protocols like DoH and DoT. Encryption protects the integrity, authenticity and privacy of the DNS requests and this prevents a number of cyberattacks such as network sniffing, man-in-the-middle attacks and redirection to malicious domains[30]. So there are clear security benefits.

It should be noted that the privacy benefits of encrypting the DNS protocol are currently limited, as much of the information that is being encrypted leaks to the internet access providers via other means. For example, most of the internet websites today use TLS/HTTPS and in the TLS/HTTPS handshake the website domain name is also sent to the server in clear text (Server Name Indication tag at the beginning of the TLS handshake). This means that encrypting the

[26] https://www.efficientip.com/news/idc-dns-threat-report-2020/
[27] https://en.wikipedia.org/wiki/DDoS_attack_on_Dyn
[28] https://www.howtogeek.com/664608/why-you-shouldnt-be-using-your-isps-default-dns-server/
[29] https://whatismyipaddress.com/switch-dns
[30] https://www.cloudflare.com/learning/dns/what-is-1.1.1.1/

original DNS resolution query works against tampering with the DNS resolution, but it does not really increase the privacy (when visiting TLS/HTTPs websites).

It must be noted that internet companies like Cloudflare and Mozilla are implementing new standards to address this privacy issue, first with Encrypted Server Name Indication – ESNI – that encrypts the requested domain from the first part of the TLS handshake, and now with Encrypted Client Hello – ECH – that encrypts the full TLS handshake[31].

Secondly, it should be noted that even when DNS requests are encrypted, there is still a lot of relevant metadata that can be sniffed from the IP traffic at the network layer. There are still many webpages and internet resources that do not encrypt their network traffic. For example, many IP addresses can be analysed and mapped back to domain names and websites using Reverse DNS.

Even with the use of TLS encryption for the DNS protocols, there are cases where parts of users' DNS requests (such as the requested domain) are leaked and exposed to interception.

4.1.2 Single point of failure

The consolidation in the DNS resolver market is creating a situation where a few public DNS resolvers have become critical. The impact would be very high should something happen with these resolvers. Resilience and single points of failure are a risk to be taken into account and this means that national authorities should supervise this segment of the market.

It should be noted that due to economies of scale (see below), and using techniques such as Anycast, it is easier for global public DNS resolvers to offer a high level of continuity and resilience. But this does not mean that all global public DNS resolvers offer the same level of resilience. Different DNS resolvers take different approaches, as was also shown in the scorecards in section 3.3.

As DNS resolution is essential to view online content, the resilience and redundancy of the DNS infrastructure is enormously important. DNS resolvers with smaller geographical footprints have an apparent disadvantage against global-scale DNS resolvers with multiple datacentres, and need to develop alternative controls to increase their resilience.

4.1.3 Geographic spread

The public DNS resolvers can offer multiple points of presence that are geographically spread, for reasons of speed and failover. This ensures that people can reach the DNS resolvers quickly from many different locations. Using Anycast, a global public DNS resolver would be able to handle requests, even when some of the points of presence are down or disconnected.

It should be noted that the local private DNS resolvers do not have this kind of geographic spread. Because they only offer services to devices connected to their own network, the resilience requirements are different.

DNS resolvers are frequently targeted by cyberattacks, and particularly DNS flood DDoS types of attack. With Anycast DNS, a single IP is given to a number of DNS servers, and any one of them can respond to DNS queries. Anycast provides protection against DDoS attacks as the attacking traffic is spread across a large number of servers preventing saturation of resources.

[31] https://blog.cloudflare.com/encrypted-client-hello/ & https://www.securityweek.com/firefox-improves-privacy-protections-encrypted-client-hello

An additional benefit of Anycast is that typically the server that is geographically closest to the customer will provide the DNS response. This reduces latency and provides significant uptime improvement for the DNS resolving service. Anycast also focuses potential risk closer to the origin of any attack, as networks that generate more attack traffic will focus those results on Anycast nodes closer to that origin, localising bad results to systems nearby or within badly-managed networks.

> Using wide geographic spread of their nodes and Anycast DNS, large public DNS providers can offer increased performance, redundancy and resilience in case of DDoS types of attacks against their services.

4.1.4 Economies of scale

Some global DNS resolvers are operating on a greater scale, handling large numbers of DNS requests. At scale certain security mechanisms can be implemented better, and the costs of security investments are spread across a larger group of users. For instance, it may be easier to spot certain anomalies or attacks when monitoring a large number of DNS requests.

The larger public DNS resolvers usually have a global reach, maintaining datacentres in many countries around the world, often counting DNS nodes in the hundreds. Some of the public DNS resolvers already have a vast infrastructure underpinning other services (cloud services or content delivery for example), making it cheaper to invest in capacity, redundancy, and security. Scale, global presence and redundant infrastructure offers significant protection against outages and DDoS attacks.

It should be noted that (as mentioned above), the downside of operating at scale is that these larger DNS resolvers are also more attractive as a target, and they are more critical overall. The security and resilience requirements for global public DNS resolvers are typically higher.

Outsourcing

Economies of scale also drive outsourcing. DNS has become complex and DNS infrastructure is often targeted by attacks, and this means that some smaller organisations and smaller telecom providers have started to forward DNS requests to a global public resolver, effectively outsourcing their local DNS resolution to a third-party. This has the obvious benefits of outsourcing, such as savings on infrastructure, reduced needs for expertise and reduced risks, but on the other hand it creates new dependencies and failure points.

> Increasing complexity of DNS resolution make it inefficient for smaller internet access providers to invest in secure DNS infrastructure. These smaller providers sometimes start outsourcing DNS resolution to larger public DNS resolvers. This drives even further market concentration towards a few large players and introduces new dependencies.

4.1.5 Protective DNS and DNS block lists

Larger global public DNS resolvers can filter or block DNS requests to malicious websites, phishing websites, etc. at scale, using local or global threat intelligence feeds. This is sometimes referred to as ‘protective DNS’.

Note that smaller local private DNS resolvers often do DNS filtering or blocking as well, but it is more costly for them to implement this with the same scope and accuracy. An important issue here is that a DNS resolver would need a good threat intelligence feed – large in scope and with good accuracy. Typically this would require commercial agreements with multiple security vendors.

Blocklists

Public DNS resolvers typically have block lists that block domain names used by malware, botnets, phishing campaigns, etc. based on threat intelligence feeds. Others offer family-filters or block offending or illegal content. Blocking is often implemented with RPZ validation, based on a variety of private and public threat intelligence sources.

Many public DNS resolvers provide different service addresses for different flavours of DNS blocking. Some of the public DNS resolvers offer these additional security features for free, or bundle them in monthly subscription services. See the scorecards in section 3.2.

Response Policy Zones – RPZ

The RPZ standard (DNS Response Policy Zones) was developed[32] to standardise DNS blocking policies. The DNS resolver implementing RPZ offerings checks DNS requests against threat intelligence and, depending on the outcome, does not resolve certain DNS requests in order to prevent the client from reaching the malicious site.

As mentioned, blocklists and RPZ can be bypassed by cyberattackers and malware by using IP addresses directly that require no DNS lookups. It cannot be relied upon as a waterproof measure[33].

> Blocklists and RPZ can offer an additional layer of protection for users, acting as a DNS firewall that blocks malicious or unwanted domain. It is important though not to rely fully on this control, as it can be bypassed by using IP addresses directly and skipping the domain name resolution step.

4.1.6 Loss of enterprise network traffic visibility

Inside an enterprise, the extra encryption offered by the global public DNS resolvers reduces, or even eliminates entirely, the visibility of traffic inside the enterprise network[34]. Security and network monitoring tools, intrusion detection tools and even forensics often rely on logged traces of DNS traffic. These tools will have to be adapted to rely on other information or network administrators will have to deny access to external encrypted resources (DoT, DoH or HTTPS) in order to force all traffic through a proxy which provides in-depth analysis and the mitigation of threats, potentially introducing new risks for the privacy of network users.

Note that in general the filtering, blocking or monitoring of DNS traffic can be evaded by cyberattackers and malware by, for example, using IP addresses directly or by using a pre-set DoH DNS resolver.

> End-to-end encrypted DNS traffic, as offered by protocols such as DoH, effectively 'blind' network security teams, as it disrupts network monitoring and other security controls. Further guidance is required for organisations in order to securely implement encrypted DNS without compromising network security.

[32] https://datatracker.ietf.org/doc/html/draft-vixie-dns-rpz-04
[33] https://media.defense.gov/2021/Mar/03/2002593055/-1/-1/0/CSI_Selecting-Protective-DNS_UOO11765221.PDF
[34] A similar argument can be made against HTTPS, and to retain network visibility of the encrypted HTTP protocol, some organisations have resorted to terminating the TLS connections with a local proxy.

4.2 PRIVACY AND OTHER CONSIDERATIONS

During the interviews, several experts raised concerns related to the rules for the protection of personal data, privacy and content blocking. We mention these issues briefly below.

4.2.1 Data protection and DNS resolvers

The shift towards global public DNS resolvers raises concerns with regards to the protection of personal data as, more often than not, the global public DNS resolvers are based outside the EU. Given that DNS requests contain personal data, such as IP addresses, which is collected as part of the DNS resolution and that processing could result in the profiling of the user's geolocation and browsing habits, there are privacy risks that should be properly addressed both by the policy makers and industry.

As also highlighted by the Spanish DPA[35], any processing that comes on top of the domain name resolution service requires user consent and/or a relevant legal basis from the provider's side in order to adhere to GDPR requirements. As discussed in Section 2, privacy protection and transparency are also some of the reasons that customers start to use global public DNS resolvers.

It was noted by interviewees that the publication of strong privacy policies which adhere to the GDPR is a challenge for many DNS recursive operators. There is an ongoing effort to create an industry-supported standard set of European DNS Recursive Resolver Privacy guidelines[36] that provides additional resolver-specific suggestions in addition to the GDPR's set of requirements.

There is usually a lack of transparency when it comes to the use of personal data by the DNS resolution infrastructure of local internet access providers.

4.2.2 National content blocking policies

At the national level, under national legislation, the telecom providers and internet service providers are often required to block certain websites, for example websites offering gambling or websites infringing on copyrights. This content blocking is usually implemented by the local private DNS resolver. Public DNS resolvers usually do not implement content blocking according to these national policies. However, it has been strongly noted by several interviewees that the desire to avoid such blocking can be considered the most important driver for users to leave their local internet access resolution and switch to public DNS resolvers.

Desire to escape the national blocking policies for online content is one of the strongest drivers causing end users to switch to global public DNS resolvers.

[35] AEPD (2019) DNS PRIVACY Available at https://www.aepd.es/sites/default/files/2019-12/nota-tecnica-privacidad-dns-en.pdf
[36] https://europeanresolverpolicy.com/

5. RECOMMENDATIONS

The DNS resolution market has been shifting from local private DNS resolvers at the telecom providers to larger public DNS resolvers offered by either larger internet companies like Google and Cloudflare or smaller ones like Quad9 and the Canadian CIRA. We analysed the major drivers that push for this trend, both from the perspective of the end user, as well as from the organisations offering DNS resolution, and we noted that this trend is not expected to change soon, as increasingly more applications use public DNS resolvers as their default configuration and people want to view online content that is blocked by national policies employed by their countries.

The protocol implementation of DNS resolution is also changing. New DNS protocols are rapidly being adopted by the large public DNS resolvers offering DoH and DoT, while other protocols, such as DNSCurve and DNSCrypt are not as widely supported. In addition, we considered the benefits and drawbacks of public DNS resolvers such as scale and resilience, the disruption of the network security controls of organisations and the concerns of many experts around the protection of personal data and privacy at public DNS resolvers.

Recommendations

In general, it should be stressed that DNS resolution is a critical component of the digital infrastructure, underpinning all internet connections and that the data involved with DNS resolution is highly sensitive. Based on our analysis and considering the issues we identified in this paper, we make a number of recommendations for national authorities and policy makers.

- Share information and establish methods to measure and monitor the market share and customer base of public DNS resolution providers. This is important to help EU Member States with the identification of DNS providers under the NIS Directive.

- Decrease the dependency on very few DNS resolution providers by providing citizens and organisations with sufficient and robust alternatives to ensure and promote diversification and guarantee that these meet EU privacy, security, and resilience goals (such as DNS4EU).

- Monitor the introduction of default configurations of DNS resolvers in software applications and devices, as this can have a quick and major impact on the criticality of a DNS resolver.

- National authorities should issue specific guidelines for organisations to address the disruption of network monitoring and security controls caused by the shift in the market and the uptake of encrypted DNS queries via public DNS resolvers.

- There should be an incentive (such as funding for resilience) for telecom providers and internet access providers to expand, secure and update their DNS resolver infrastructure, instead of outsourcing their requirements to major global public DNS resolvers. This will avoid a situation where many end-users rely on a few large public DNS resolvers for their internet access.

- Policy makers and national authorities should pay particular attention to enforcing the blocking of online content via the DNS resolution services of telecom providers and internet service providers, because for end-users blocked online content is an important driver for shifting to global public DNS resolvers.

TP-08-22-030-EN-N

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-558-6
DOI 10.2824/288837