National Cyber Security Centre
Ministry of Justice and Security

DNS-monitoring will get harder

Be prepared for the modernisation of transport protocols

Factsheet FS-2019-01 | versie 1.0 | 30 September 2019

New DNS transport protocols make it harder to monitor or modify DNS requests. This is **beneficial on today's untrusted networks. At the** same time the shift may render your **organisation's security controls ineffective,** expose internal naming or break connectivity. These negative side effects are hard to mitigate at a network level and require mitigation at DNS infrastructure and individual devices.
The NCSC recommends organisations to decide on preferred (DNS) resolvers, configure these on devices under administrative control and take note of the benefits provided by modern DNS transport protocols.

Background

DNS is one of the most important protocols in the internet stack. Increased concern over the monitoring of DNS traffic by ISPs has led to standardisation of modern DNS transport protocols ('DNS transports'), that make use of encryption. A DNS transport is used by an endpoint and its recursive caching name server ('resolver') to exchange DNS requests and answers. Users who want to prevent their ISP from reading their DNS requests can utilize an encrypted DNS transport. By also using a resolver provided by a third party, the ISP is no longer involved in the handling of their DNS requests.

Target audience

System or network administrators and security officers

What is happening?

Encrypted transports for DNS are gaining popularity

System or network administrators and security professionals have come to expect DNS traffic to arrive without encryption on port 53 (tcp and udp). In recent years, new encrypted DNS transports have been standardized that utilize encryption to provide confidentiality or integrity in the presence of attackers on the network.

Key facts

1. Encrypted transports for DNS are gaining popularity.
2. Increasingly software no longer uses system level DNS resolving. Your organisation may unwittingly start to hand off responsibility for DNS resolving to a third party.
3. This can render security controls ineffective, expose internal naming or break connectivity.

Perspective for action

- Decide on preferred resolvers.
- Configure these preferred resolvers on all devices under administrative control.
- Take note of the benefits provided by modern DNS transports.

These new DNS transports are gaining popularity to transport DNS queries between endpoints and the recursive caching name server ('resolver') they are configured to use.

DNS over TLS (DoT)[1] transports DNS queries over a TLS tunnel on tcp/853. DNS over HTTPS (DoH)[2] transports DNS queries over a TLS encrypted HTTP transport, typically over tcp/443. Both can can provide confidentiality and integrity in the presence of an active attacker on the network.[3] It is likely that future transport protocols such as QUIC are likewise used to transport DNS queries with useful security properties.

Mainstream operating systems have not (yet) shipped support for the new encrypted transports, with the notable exception of Android. Android 9 Pie upgrades plaintext DNS over tcp/udp port 53 to DoT if the resolver supports it.[4] This opportunistic use of DoT provides confidentiality in the presence of a passive observer on the network, but does not protect against an active attacker.

Increasingly software no longer uses system level DNS resolving

Application developers have long used programming libraries shipped with the various operating systems to perform their DNS resolving. As a consequence, all applications used a single (system level) DNS stub resolver. Its configuration determined where queries were sent for the whole system.

Some application developers have integrated DNS resolving directly into their applications. This enables them to make use of the benefits provided by the new encrypted transports, in the absence of operating system support. The developer is then able to determine which resolver is used by the application. Some developers use this possibility. As a result, the DNS requests sent by these applications use the DNS resolver configured at a system level.

Mozilla provides its own functionality for DNS resolvering in Firefox, that also supports DoH. Mozilla experiments in the US[5] with a Firefox configuration that sends DNS requests to Cloudflare. Google conducts world wide experiments in Chrome[6], testing DoH functionality that sends sends DNS queries over DoH when the configured system level resolver is in a whitelist of third parties known to support DoH.

What does this mean for me?

Ineffective security controls

Organisations relying on the ability to inspect clear text DNS traffic will likely see their visibility decrease over time. Organisations that implement security monitoring or filtering on the provisioned system level resolvers will find these measures ineffective once applications start using an alternative resolver.

Leaking Informations and exposing internal resource naming

DNS queries can contain a lot of sensitive information, including websites visited and destinations for e-mail. Many organisations consider resource records for internal systems and networks sensitive information.

The choice of a resolver is a matter of trust. When devices under your administrative control start using resolvers run by third parties unrelated to your organisation, they will process queries that contain sensitive information. Depending on your trust in these third parties and the legal context they operate in, this may be a risk.

Breaking connectivity

Organisations who limit the visibility of internal resource naming to internal networks run an additional risk once devices start using third party resolvers. The third party may not be able to answer queries for internal resource records, if these are not answered by your authoritative name servers on the public internet. This may break connectivity on internal networks, including popular VPN setups.

[1] DNS over TLS is specified in RFC 7857, available from https://datatracker.ietf.org/doc/rfc7858/
[2] DNS over HTTPS is specified in RFC 8484, available from https://datatracker.ietf.org/doc/rfc8484/
[3] The endpoint does require a hostname of the resolver, used for TLS authentication. For more information, see section 6.6 of RFC 8310, available from https://datatracker.ietf.org/doc/rfc8310/

[4] Source: https://android-developers.googleblog.com/2018/04/dns-over-tls-support-in-android-p.html
[5] Source: https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/
[6] Source: https://www.chromium.org/developers/dns-over-https

What can I do?

The NCSC recommends organisations to decide on preferred resolvers and to configure these on systems under administrative control. Consider enabling and using DoT or DoH on your preferred resolvers once supported. These recommendations are further detailed in Table 1.

Accept or mitigate risks on your networks for unmanaged clients, such as internet access for visitors or private devices. This recommendation is further detailed in Table 2.

In conclusion

There is time to prepare while DoT and DoH experiments are conducted on a limited scale. But the trend is unmistakable: DNS monitoring will get harder.

To retain DNS monitoring as an effective measure, it is necessary to make changes to your own DNS infrastructure and endpoints. While centralized DNS monitoring on networks has been feasible up to this point, this centralized approach will continue to decrease in effectiveness over time.

The remaining time for centralized DNS monitoring as an effective measure depends strongly on the pace Mozilla and Google choose to activate support in their software. If your organisation starts changing your DNS monitoring today, you will not be surprised by the upcoming changes.

Table 1 Use preferred resolvers on systems under administrative control

Decide where you prefer clients to send their queries.

- Do you run your own resolvers, or is this outsourced to a third party?
- What are the consequences when clients switch to a non-preferred resolver? Consider:
  a. Query confidentiality
  b. DNS zones that are not resolvable on the public internet (split-horizon DNS)
  c. Performance and availability
  d. Security controls, such as DNS filtering or security monitoring
  e. Visibility for performance measurement or debugging

Understand how clients under your administrative control learn where to send their queries.

- Understand how system level DNS configuration is provisioned in your organisation.
  a. Most networks provide resolver configuration through a DHCP option.
  b. Network flow data may help you to understand which resolvers are in use in your organisation.
- Understand which applications[7] are provisioned with alternative resolvers. Consider:
  a. Web browsers and plugins
  b. Apps on mobile devices

Provision resolver configuration to clients if changing the default is necessary.

- Mozilla Firefox provides policy knobs to toggle DoH and to provide a preferred resolver.[8] Mozilla says DoH defaults to off when enterprise roots are installed[9] for TLS interception[10].
- Google Chrome is expected to offer policy knobs to toggle DoH and to provide a preferred resolver.[11]

Table 2 Accept or mitigate limited visibility for DNS queries from unmanaged clients

Many organisations provide internet access for visitors or private devices. The devices on these networks tend not to be under administrative control of the organisation. This precludes control over resolver configuration. Over time, it is likely that devices will either start encrypting their queries, choose non-preferred resolvers from the perspective of the organisation, or both.

- Be aware that any security controls that rely on query visibility will likely decrease in effectiveness over time.
- Some applications allow for mitigation at the network level, but these may be discontinued on short notice.
  a. Mozilla Firefox allows networks to signal their use of DNS filtering at a resolver by means of canary domain.[9]
- Take into account the level of access provided to unmanaged clients, the risks this entails and the required trade-off for guest and private use when deciding to accept or mitigate.

[7] See for example https://en.wikipedia.org/wiki/DNS_over_HTTPS#Client_support and https://dnsprivacy.org/wiki/display/DP/DNS+Privacy+Clients
[8] An overview of existing policy knobs is available from https://github.com/mozilla/policy-templates/blob/master/README.md#dnsoverhttps
[9] Source: https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https
[10] See also the factsheet TLS Interception by the NCSC, available from https://english.ncsc.nl/publications/factsheets/2019/juni/01/factsheet-tls-interception
[11] These are described in the design documentation, available from https://www.chromium.org/developers/dns-over-https

Publication
National Cyber Security Centre (NCSC)
P.O. Box 117, 2501 CC The Hague
Turfmarkt 147, 2511 DP The Hague
+31 (70) 751 5555

More information
www.ncsc.nl
info@ncsc.nl
@ncsc_nl

FS-2019-01 | version 1.0 | 30 September 2019