September 20, 2019

TLP White: Distribution Unlimited

Upcoming Browser DNS Changes and Impact to University IT Operations

Executive Summary

Changes to how Firefox and Chrome browsers conduct domain name resolution will impact your users and IT operations. When a user navigates to a web page, domain names on that page need to be translated ("resolved") to their corresponding server IP addresses. This includes the name of the server hosting the page itself, as well as servers hosting content embedded in the page. Name-to-address resolution is typically conducted by university-operated servers or by a university-selected third-party resolver operator. Firefox and Chrome plan to implement a new protocol "DNS over HTTPS" ("DoH", pronounced "dough") for this domain name resolution.

Chrome will automatically enable DoH only when the browser has already been configured to use specific alternative DoH-capable resolvers (such as Google DNS, OpenDNS, Quad9, etc.)

Firefox will automatically enable DoH for all resolutions and substitute its own preferred DNS resolver unless users or IT administrators take certain steps (described below).

These changes, intended to improve user privacy and security, provide value when users have reason to distrust their DNS or network provider. However, within institutional networks, the Firefox approach presents challenges to IT security operations, protections, and user support. The institution can take action to mitigate the impact of these changes.

We recommend that institutions:

- Understand how domain name resolution is conducted at their institution.
- Understand how DNS choices can impact user privacy and security.
- Identify how their IT security operations and protections may be impacted.
- Identify how user support may be impacted.
- Understand how reliability, availability, and performance may be impacted.
- Decide on a response.
- Communicate with your users about this issue.

REN-ISAC welcomes questions or feedback on this document. Please contact us at soc@ren-isac.net

What is Changing

FIREFOX WEB BROWSER

- Starting in late September 2019, the Mozilla Foundation will begin changing how Domain Name Service (DNS) queries are handled in the Firefox web browser.[1] Rather than using the DNS settings configured by the user or assigned by the user's network provider, Firefox will substitute its **own** preferred DNS recursive resolvers operated by Cloudflare on behalf of the Mozilla Foundation.
- This DNS traffic will be encrypted using a new protocol known as "DNS over HTTPS," ("DoH").[2]
- Individual Firefox users can take steps to disable this change in their browser if they (a) know to do so, and (b) are technically comfortable doing so.
- Enterprises can use technical methods to deter Firefox from changing their users' DNS settings. However, individual users can override their provider's expressed preference if they choose to do so and opt-in to DoH. Because Firefox is using DoH by default, it will be difficult for institutions to completely prevent Firefox's alternative third-party DoH activity.

[1] https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/
[2] https://en.wikipedia.org/wiki/DNS_over_HTTPS

CHROME WEB BROWSER

- Chrome is enabling DoH when it detects the user is already using one of a set of third-party DNS providers capable of supporting DoH; it will upgrade the user's DNS traffic to use DoH with that provider.[3] This is scheduled to happen with Chrome version 78, expected on October 22, 2019.
- The main difference between Chrome's implementation of DoH and Firefox's implementation is that, with Chrome, only users who've voluntarily selected a third-party DNS service are affected (the user or network service provider's DNS resolver specification is respected).

Why This is Important

- **User Privacy and Security:** DoH is intended to increase user privacy by limiting eavesdropping on domain name resolution requests ("what web sites is this person visiting?").

However,

- **DNS is a Fundamental and Mission Critical Protocol:** DNS is a technology that average users know little about but underlies everything users do on the Internet. Anything that impacts DNS operations deserves careful review and management.
- **Bypassing Institutional DNS "Firewalls":** Universities often protect users from phishing and malware by blocking access to known bad domains.[4] These protections are conducted on locally managed DNS recursive resolvers or contracted to a service provider. Users of alternative third-party resolvers bypass these protections and may be more likely to become victimized. Some of the alternative providers may provide a level of known bad protections; however, the values, integrity, comprehensiveness, and operational controls are outside of institutional control. The capability for local network and security operators to firewall malicious domains based on information received through threat intelligence sharing or local discovery is bypassed.
- **Loss of Visibility to DNS Traffic Used to Identify Compromised Systems:** Many university cybersecurity teams leverage DNS telemetry to identify compromised systems on campus. When browsers move to third-party DoH, that telemetry is lost to university cybersecurity teams.
- **Split-Horizon DNS Configurations Could Be Impacted:** In certain configurations, DNS servers will answer with different responses based on the location of the client on the enterprise network (typically internal versus external). In some cases, use of third-party resolvers may impact the ability to properly resolve a DNS record because records will always be resolved from the perspective of an outside client regardless of client location. Mozilla has specific heuristics to detect this behavior and refer to the system resolver, but this may not be comprehensive. Chrome does not currently offer the ability to detect this behavior.
- **Use of Third-Party Recursive Resolvers Complicates End-User Support:** Diagnosing Internet issues can be challenging at the best of times. A change to DNS operations, which the user may not be aware of, increases complexity particularly if different applications end up using different DNS services (i.e., the browser uses different DNS services from every other application on the user's computer). Additionally, one's user experience may differ from another nearby user.
- **Performance May Be Impacted:** While third-party recursive resolver services often tout their speed as a selling point, user experiences may vary as a result of distant third-party recursive resolvers or subtle protocol nuances. For example, in an effort to respect user privacy, some third-party recursive resolver services don't transmit what's known as EDNS Client Subnet information.[5] Without hints as to the user's location, content distribution networks can't optimize delivery of content from nearby cache servers. This, plus the additional latency involved in reaching a remote third-party resolver, may result in users perceiving (and potentially complaining about) "the network being slow."
- **Reliability and Availability May Be Impacted:** When DNS operations are run locally or by an institutionally selected third-party provider, the CIO knows who's responsible; has service level agreements, commitments concerning protection from malicious domains; and has recourse in the case of outages.

---

[3] https://www.chromium.org/developers/dns-over-https
[4] RPZ is one technology commonly used for this, see https://dnsrpz.info/
[5] https://en.wikipedia.org/wiki/EDNS_Client_Subnet

- **User Privacy May Be Adversely Impacted:** While local network administrators may no longer be able to see user DNS traffic, control of this private data is ceded outside the institution to the third-party operators. These operators may not be subject to the same compliance obligations as the institution itself and have no contractual obligation to the user or institution. Additionally, because of various EDNS extensions, user trackability can actually be enhanced.[6]
- **An Insufficient Privacy and Security Solution:** Although DoH affords some privacy and security benefits, it is an insufficient solution when operating outside the institutional network, such as at a coffee shop or while on a mobile device. Much more than just DNS requests is exposed; therefore, an institutional VPN is a more comprehensive choice.

Recommendations

- **Understand Who is Currently Providing Recursive Resolver DNS Service for Your Institution:** Is it your IT department or a third-party service? Knowing who's doing DNS for your school may impact your options. Whether using local or contracted responsible parties, you should ensure you've heard their perspective on this important issue.
- **Understand the Mix of Browser Use at Your Institution:** Worldwide, Firefox has a small percentage of the browser market (~5%); Chrome has over 60%. In the U.S., Chrome's percentage is lower (~50%) due to use of Safari; however, Firefox stays at ~5%.[7] These percentages may vary in higher ed. A local survey can be performed by looking at the institution's own web logs for user-agent strings.
- **Decide if You Want to Allow, Discourage, or Disallow Use of Third-Party DNS Services.** This is a policy decision that should be made by the institution following normal institutional procedures, typically including an understanding of the risks involved and a consultation with interested stakeholders. If you choose to discourage or disallow, refer to:
    - the section of this document *Technical Options for Controlling Browser Behavior*, and/or
    - the institutional network blocking approach described in the *block-doh*[8] resource
- **Communicate with Your Users About this Issue:** Ensure your users are aware of the changes that will be forthcoming (whether those changes are the browser vendor's or the institution's) and their options for helping to shape what happens. In addition, communicate with concerned users about the pros and cons of DoH as a privacy solution, particularly noting they should not develop a false sense of privacy; that DoH is an incomplete privacy solution.
- **Evaluate Running Your Own DNS Privacy (DoH or DoT) Server[9]:** By running your own DNS Privacy Server, your users gain the enhanced privacy and security benefits. An institutional DNS Privacy Server ensures that private data stays with the institution, a consistent user experience is maintained, and the institution retains capabilities for security controls (e.g. DNS firewall and incident investigation).
- **Be Cognizant of the Bigger Picture:** While this alert focuses on changes to web browser DNS practices, a growing number of users may eventually choose to use a third-party Virtual Private Network (VPN). A VPN typically sends all user Internet traffic (DNS and other types alike) over an encrypted tunnel, dramatically limiting the ability of network administrators and security teams to manage institutional network traffic and protect users and assets. Some web browsers, such as Opera, currently bundle a free VPN service.

Background/Context

- Normally, university DNS services are provided by the university itself or by a university-selected third-party DNS service provider. Communications between users and those DNS servers have historically been unencrypted.

[6] https://nlnog.net/static/nlnogday2019/5_NLNOG_day_2019_Bert_Hubert_DNS_TLS_Privacy.pdf
[7] https://gs.statcounter.com/browser-market-share/all/
[8] https://github.com/bambenek/block-doh
[9] https://dnsprivacy.org/wiki/display/DP/Running+a+DNS+Privacy+server

- Over time, third-party DNS services (such as Google's 8.8.8.8, Cloudflare's 1.1.1.1, or the Global Cyber Alliance/IBM's 9.9.9.9 name server services) have become freely available to end-users. Use of these servers has been a matter of user preference, on an opt-in basis, and the traffic has remained unencrypted.
- Following Edward Snowden's disclosures in June 2013, the IETF and other Internet standards organizations devoted much attention to encrypting network traffic, including web traffic. Now that most web traffic is encrypted, the community's attention has broadened to include encryption of DNS.
- There are multiple standards that may be used for DNS encryption, including DNSCrypt (not IETF standardized), DNS over TLS (DoT), and DNS over HTTPs (DoH). All deliver roughly equivalent functional protection against eavesdropping, but DNS over HTTPS is deliberately engineered to be particularly difficult for network administrators to block.
- Discussions around DNS over HTTPS and its deployment are ongoing in the IETF. Those interested in detailed technical discussions of these issues should see https://datatracker.ietf.org/wg/dprive/about/ and https://datatracker.ietf.org/wg/doh/about/

Technical Options for Controlling Browser Behavior

FIREFOX WEB BROWSER

- **Disable via Canary Domain**: Configuring DNS resolvers to return an NXDOMAIN response for "*use-application-dns.net*" will disable DoH services on endpoints utilizing those resolvers.[10] Several options exist for implementing a canary domain. Two common approaches are the use of RPZ[11] or Unbound local zones.[12]
- **Configure via Group/System Policy**: Mozilla provides group policy options for controlling Firefox behavior on managed endpoints. DoH will be disabled if any enterprise security policy is detected unless explicitly enabled by the user. DoH can be explicitly enabled/disabled or directed at a custom DoH server using the DNSOverHTTPS policy.[13]
- **Configure Manually**: DoH can be manually enabled/disabled in the Network Settings section of *about:preferences*.[14]

CHROME WEB BROWSER

- **Configure via Group/System Policy**: Chrome will make group policy templates available to control browser behavior when Chrome 78 is released.[15]
- **Configure Manually:** DoH can be manually enabled/disabled via the flag at *chrome://flags/#dns-over-https* once Chrome 78 is released.[16]

Additional References

- Encrypted DNS Deployment Initiative
  https://www.encrypted-dns.org/
- DNS Privacy Project Homepage
  https://dnsprivacy.org/wiki/

Credits

Thanks to the members of the REN-ISAC Technical Advisory Group[17] for assistance in developing this Advisory!

[10] https://support.mozilla.org/en-US/kb/configuring-networks-disable-dns-over-https
[11] https://dnsrpz.info/
[12] https://nlnetlabs.nl/documentation/unbound/unbound.conf/
[13] https://github.com/mozilla/policy-templates/blob/master/README.md#dnsoverhttps
[14] https://support.mozilla.org/en-US/kb/firefox-dns-over-https#w_enabling-and-disabling-dns-over-https
[15] https://www.chromium.org/developers/dns-over-https
[16] Ibid
[17] https://www.ren-isac.net/about/governance/tag.html