U.S. Department of Homeland Security
Cybersecurity & Infrastructure Security Agency
Office of the Director
Washington, DC 20528

April 21, 2020

INFORMATION

MEMORANDUM FOR AGENCY CHIEF INFORMATION OFFICERS

FROM: Christopher C. Krebs
Director

SUBJECT: **Addressing Domain Name System Resolution on Federal Networks**

The purpose of this memorandum, issued pursuant to authorities under section 3553(b) of Title 44, U.S. Code, and Title XXII of the Homeland Security Act of 2002, as amended, is to remind agencies[1] of their legal requirement to use EINSTEIN 3 Accelerated (E3A)'s Domain Name System (DNS) sinkholing capability for DNS resolution and provide awareness about recent security and privacy enhancements to DNS resolution protocols – in particular, DNS over HTTPS (DoH) and DNS over TLS (DoT).

Background

Title XXII of the Homeland Security Act of 2002, as amended, requires the Secretary of Homeland Security to deploy, operate, and maintain capabilities to detect and prevent cybersecurity risks in network traffic.[2] In turn, the head of each agency is required to apply and continue to utilize these capabilities to all information traveling between an agency information system and any information system other than an agency information system.[3] One of these capabilities is E3A's DNS sinkholing service, which blocks access to malicious infrastructure by, in effect, overriding public DNS records that have been identified as harmful.

Compliance with the above requirement protects federal agencies and provides the Cybersecurity and Infrastructure Security Agency (CISA) insight into DNS requests made from agency networks. This insight is further enhanced when agencies share details about their infrastructure

---

[1] This memorandum does not apply to national security systems or to systems operated by the Department of Defense or the Intelligence Community. 44 U.S.C. §3553(b), (d), (e)(2), (e)(3).
[2] 6 U.S.C. §663(b).
[3] 6 U.S.C. §663 note, "Agency Responsibilities". This requirement does not apply to the Department of Defense, a national security system, or an element of the intelligence community. *Id*.

with CISA, helping to minimize the burden placed on CISA and federal agencies resulting from traffic analysis based on incomplete information.

Currently, there are two protocols that introduce transit encryption to DNS resolution, which increases user security and privacy by preventing eavesdropping and manipulation of DNS data:

- DNS over HTTPS enables DNS resolution over a Hypertext Transfer Protocol Secure (HTTPS) connection,[4] and was published as RFC 8484 by the Internet Engineering Task Force (IETF) in October 2018.[5]
- DNS over TLS has effectively the same security outcomes as DoH, but establishes a Transport Layer Security (TLS) connection directly to a DNS resolver instead of relying on HTTPS. DoT was published as RFC 7858 by the IETF in May 2016.[6]

In September 2019, Mozilla announced plans to enable DoH in Firefox[7]. On February 25, 2020, Firefox began the rollout of DoH by default for the users in the United States[8]. This change shifts in-browser DNS requests from the resolver set at the operating system to providers Firefox deems trustworthy.[9] Firefox will still respect enterprise policies that disable DoH and attempt to detect when a managed network expresses a preference to not use externally hosted DNS available over DoH.[10]

Also in September, Google announced that its Chrome 78 release (subsequently postponed to Chrome 79) would begin a DoH experiment with a limited set of users.[11] While DoH would similarly be enabled by default for these users, Google's approach differs in that Chrome will only upgrade the *protocol* used for DNS resolution – upgrading the connection from plaintext to encrypted – while leaving a user's DNS *provider* unchanged.

---

[4] https://https.cio.gov/#what-https-does
[5] https://tools.ietf.org/html/rfc8484
[6] https://tools.ietf.org/html/rfc7858
[7] https://blog.mozilla.org/futurereleases/2019/09/06/whats-next-in-making-dns-over-https-the-default/
[8] https://blog.mozilla.org/blog/2020/02/25/firefox-continues-push-to-bring-dns-over-https-by-default-for-us-users/
[9] https://wiki.mozilla.org/Security/DOH-resolver-policy
[10] Mozilla's use of a 'canary domain', one where the domain's resolution/non-resolution results in an application disabling DoH, might be feasible in agencies' local DNS resolver. However, the way E3A performs DNS filtering is to redirect known-malicious domain names to "safe" IP addresses; it cannot return predetermined DNS response codes (e.g., NXDOMAIN). Thus, this feature to signal a preference against DoH at the network level is unavailable with E3A. To date, Firefox is the only browser known to check for a canary domain. https://support.mozilla.org/en-US/kb/canary-domain-use-application-dnsnet
[11] https://blog.chromium.org/2019/09/experimenting-with-same-provider-dns.html

In November 2019, Microsoft announced its intent to offer encrypted DNS resolution (prioritizing DoH support) in the Windows DNS client in a future release.[12] Their approach is similar to Google's in that only the protocol used for DNS resolution is upgraded, not the provider.

CISA encourages efforts to make network communications encrypted by default. Doing so increases user security, making it harder for attackers to monitor and modify communication. DoH and DoT add desirable security features to DNS resolution; however, federal agencies that use DNS resolvers other than E3A lose the protection that defensive DNS filtering provides, and E3A does not currently offer encrypted DNS resolution.[13] CISA intends to offer a DNS resolution service that supports DoH and DoT in time. Until then, agencies must use E3A for DNS resolution.

Required Action

1. In accordance with 6 U.S.C. §663 note, "Agency Responsibilities," ensure local DNS recursive resolvers use E3A as their primary (or ultimate) upstream DNS resolver.[14]

Recommended Actions

1. Configure local DNS recursive resolvers to utilize well-known public resolvers as fallback upstream DNS resolvers.

   While CISA does not endorse any particular resolver and agencies are at liberty to choose their own fallback upstream DNS resolvers, examples of well-known public resolvers include[15]:
   - Cisco (208.67.222.222 and 208.67.220.220)
   - Cloudflare (1.1.1.1 and 1.0.0.1)
   - Google (8.8.8.8 and 8.8.4.4)
   - Quad9 (9.9.9.9 and 149.112.112.112)

   Agencies should notify CISA at dns.support@cisa.dhs.gov regarding which public resolvers they decide to utilize.[16]

2. Configure agency policy enforcement points[17] to:

---

[12] https://techcommunity.microsoft.com/t5/Networking-Blog/Windows-will-improve-user-privacy-with-DNS-over-HTTPS/ba-p/1014229

[13] DNS queries from agency networks to E3A occur via an encrypted tunnel or a private network, though this protection is limited to those devices physically or virtually on the network.

[14] Information systems and applications must use DHS-provided DNS sinkholing capability. CISA recognizes there are challenges associated with administering DNS resolution settings on cloud and mobile devices and is exploring options for these systems. Agencies may operate encrypted DNS resolvers inside their own infrastructure.

[15] These providers also offer IPv6 support.

[16] This reporting will help CISA more accurately understand traffic flows and reduce false positive incident tickets.

[17] Policy Enforcement Point (PEP): A security device, tool, function or application that enforce security policies through technical capabilities. For additional information, see

a. Drop all inbound/outbound IPv4 and IPv6 traffic on port 53 (TCP and UDP), except to/from authorized DNS infrastructure (e.g., authoritative name servers, recursive resolvers, etc.).
b. Drop all inbound/outbound IPv4 and IPv6 DoT traffic on port 853 (TCP and UDP) (unless DoT is explicitly supporting mission needs, in which case notify CISA at dns.support@cisa.dhs.gov).

3. Until DoH and DoT resolution services are available from CISA, set and enforce enterprise-wide policy (e.g., Group Policy Objects [GPO] for Windows environments) for installed browsers to disable DoH use.[18]

4. If CISA provides an agency with analysis highlighting potential DNS traffic anomalies, review the reports and provide feedback to CISA at dns.support@cisa.dhs.gov if anomalies are confirmed.

Note: NIST SP 800-81-2 *Secure DNS Deployment Guide* also recommends that DNS infrastructure servicing external DNS requests is separate from DNS infrastructure servicing internal requests.[19]

CISA Actions

1. CISA will continue to monitor DNS traffic across the federal enterprise.
2. CISA will begin providing agencies with reports highlighting potential DNS traffic anomalies.
3. Six months after the issuance of this memo, CISA will evaluate the state of federal DNS security and consider follow-on action, as necessary. This could involve the issuance of a directive.
4. CISA can provide agencies operational and technical assistance to support their adoption of the required and recommended actions above.

Point of Contact

For inquiries regarding this memo, contact dns.support@cisa.dhs.gov.

---

https://www.cisa.gov/sites/default/files/publications/Draft%20TIC%203.0%20Vol.%202%20Reference%20Architecture.pdf#page=19

[18] For example, for Firefox, see https://support.mozilla.org/en-US/products/firefox-enterprise/policies-customization-enterprise/policies-overview-enterprise

[19] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-81-2.pdf#page=50, §7.2.9