Firefox unveils major security upgrade: DoH protocol boosts user privacy

February 26 2020, by Peter Grad

Credit: CC0 Public Domain

In a major step to curb eavesdroppers from tapping into users' web browsing habits, Mozilla today launched a major security initiative for all Firefox users in the United States.

Beginning Tuesday, Firefox browsers will use encrypted means of accessing web addresses to help keep activities of users private. It will curb malicious activity by hackers and block surreptitious data collection by merchants who use "super cookies" to track every website a user visits.

The protocol is called DNS over HTTPS, or DoH. Every website is assigned a digital Internet Protocol address containing up to 12 digits. To make it easy for users to find websites without memorizing long numerical strings, the Domain Name System, DNS, links the digits to a user-friendly name such as TechXplore.com.

But when browsers transmit the name to a server that fetches the matching numerical IP address, the request is not encrypted. At that moment, internet providers and third-party interests can siphon that information and use it for marketing efforts or sell it to other interested parties. Lurking hackers might use it for more nefarious purposes, such as quietly redirecting users to phony websites.

DoH aims to plug that security gap by encrypting all data entered into the browser address bar.

DoH has actually been around for a while. It has been an option is Firefox, as well as other major browsers, for about a year. But Firefox reported that few users are taking advantage of the security feature. Beginning today, DoH will be the default setting on all Firefox releases. The rollout will be staggered over several weeks as Firefox monitors early usage for any problems.

A post on the official Mozilla blog this morning explained: "DNS lookups are sent to servers that can spy on your website browsing history without either informing you or publishing a policy about what they do with that information. At the creation of the internet, these kinds of threats to people's privacy and security were known, but not being exploited yet."

"Today," the post continued, "we know that unencrypted DNS is not only vulnerable to spying but is being exploited, and so we are helping the internet to make the shift to more secure alternatives."

Adoption of DoH protocols has not been without controversy. Some security experts say DoH implementation will make it harder to track down illicit web activity. Police officials say it will interfere with efforts to track down child pornography rings and other criminal activities.

In Great Britain last summer, DoH implementation caused such an uproar that the United Kingdom's ISP umbrella organization named Mozilla "Internet Villain of the Year." And when the DoH protocol was formally adopted in 2018, Paul Vixie, one of the architects of DNS, called it "a cluster duck for internet security." He added, "The inmates have taken over the asylum."

More information: Read Mozilla's announcement here: blog.mozilla.org/blog/2020/02/ … efault-for-us-users/

© 2020 Science X Network

Citation: Firefox unveils major security upgrade: DoH protocol boosts user privacy (2020, February 26) retrieved 1 May 2024 from https://techxplore.com/news/2020-02-firefox-unveils-major-doh-protocol.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.