Microsoft reveló planes para integrar el soporte nativo para DNS sobre HTTPS en el sistema operativo Windows 10 en noviembre de 2019.

El anunció fue publicado en el blog Networking de Microsoft, el 17 de noviembre de 2019. DNS sobre HTTPS está diseñado para mejorar la privacidad, la seguridad y la confiabilidad mediante el cifrado de las consultas DNS que se manejan actualmente en texto sin formato.

El DNS sobre HTTPS ha ido en aumento en los últimos años. Mozilla, Google, Opera, y varios proveedores de DNS públicos, también anunciaron soporte para el estándar.

La compatibilidad con programas, como un navegador web por ejemplo, significa que las consultas DNS que se originan en ese programa están encriptadas. Sin embargo, otras consultas desde otro navegador que no admite DNS por medio de HTTPS, o está configurado para no usarlo, no se beneficiará con esta integración.

El anuncio de Microsoft brinda soporte DNS sobre HTTPS para el sistema operativo Windows. La compañía planea presentarlo para obtener una vista previa de las compilaciones de Windows 10 en el futuro antes de lanzarlo a una versión final del sistema.

Microsoft quiere seguir la implementación de Google, en un inicio. Google reveló hace tiempo que implementará DNS a través de HTTPS en Chrome, pero solo en sistemas que utilizan un servicio DNS que se admite por medio de HTTPS. En otras palabras, Google no alterará el proveedor de DNS del sistema.

Mozilla y Opera decidieron elegir un proveedor, lo que significa que el proveedor DNS local puede ser anulado en el navegador.

Microsoft afirma que no realizará cambios en la configuración del servidor DNS de la máquina Windows. Los administradores tienen el control cuando se trata de la selección del proveedor de DNS en Windows y la introducción de soporte para DNS sobre HTTPS en Windows no cambiará eso.

El cambio podrá beneficiar a los usuarios sin que lo sepan. Si un sistema está configurado para utilizar un proveedor de DNS que admita DNS por medio de HTTPS, ese sistema usará de forma automática el nuevo estándar para que los datos de DNS se cifren.

La compañía planea introducir *«formas más amigables con la privacidad»* para que sus clientes descubran la configuración de DNS en Windows y concienticen sobre DNS a través de HTTPS en el sistema operativo.

Microsoft reveló cuatri principios para esta implementación:

- El DNS de Windows debe ser lo más privado y funcional posible de forma predeterminada sin la necesidad de una configuración de usuario o administrador porque el tráfico de DNS de Windows representa una instantánea del historial de navegación del usuario.
- Los usuarios y administradores de Windows con mentalidad de privacidad, deben ser guiados a la configuración de DNS aún si no saben qué es DNS.
- Los usuarios y administradores de Windows deben poder mejorar su configuración de DNS con la menor cantidad de acciones simples posible.
- Los usuarios y administradores de Windows deben permitir explícitamente la recuperación de DNS cifrado una vez configurado.