Forum: Sécurité

Topic: Microsoft veut intégrer DNS over HTTPS dans Windows 10

Subject: Microsoft veut intégrer DNS over HTTPS dans Windows 10

Publié par: Wullfk

Contribution le : 22/11/2019 17:30:01

Citation :
Microsoft travaille sur le support du protocole DNS over HTTPS (DoH) dans une prochaine version de Windows 10. L'éditeur n'écarte cependant pas le support de DNS over TLS (DoT).
https://www.lemondeinformatique.fr/act ... ans-windows-10-77123.html

Pour info ce protocole est existant sur Firefox 70, mais il n'est pas activé par défaut.

Dans le menu Firefox, choisissez Outils >> Préférences, section "*Généralités*", descendre jusqu'à "*Paramètres du réseau*", cliquez sur le bouton "*Paramètres*".

descendre et sélectionnez "*Activer DNS over HTTPS*"

configurez le résolveur DoH de votre choix. Vous pouvez utiliser le résolveur Cloudflare intégré (une société avec laquelle Mozilla a conclu un accord pour enregistrer moins de données sur les utilisateurs de Firefox), ou utiliser un de votre choix dans cette liste : ICI

Via **about:config**

Rechercher la clé : **network.trr.mode**

mettre la valeur à **2**

Ça active le support DoH. Ce réglage prend en charge quatre valeurs :

Valeur par défaut **5** sur un profil standard de Firefox, **ce qui signifie que DoH est désactivé.**

1 - DoH activé, mais Firefox choisit s'il utilise DoH ou un DNS régulier basé sur celui qui renvoie des réponses de requête plus rapides
2 - DoH activé, et le DNS régulier fonctionne comme une sauvegarde
3 - DoH activé, et le DNS régulier est désactivé
5 - DoH désactivé

La valeur 2 fonctionne le mieux.

Rechercher la clé : **network.trr.uri**

C'est l'URL du serveur DNS compatible DoH où Firefox enverra les requêtes DNS DoH. Par défaut, Firefox utilise le service DoH de Cloudflare situé sur https://mozilla.cloudflare-dns.com/dns-query. Cependant, les utilisateurs peuvent utiliser leur propre URL de serveur DoH. Ils peuvent en choisir un parmi les nombreux serveurs disponibles ICI.

On en profite pour activer le chiffrement du SNI (*Encrypted SNI*)

SNI (*Server Name Indication*) est une extension du protocole TLS 1.3 qui améliore la confidentialité des utilisateurs Internet en empêchant les observateurs sur le trajet, par exemple, votre FAI peut connaître les sites que vous visitez à travers les résolutions DNS.

Rechercher la clé : **network.security.esni.enabled**

Double clic sur la clé afin de passer sa valeur à **True**

Pour vérifier si ces protocoles sont actifs, CloudFlare fournit un site de test à cette adresse : https://www.cloudflare.com/ssl/encrypted-sni/#

Chez moi sur mon PC de test j'obtiens ceci :

300) this.width=300" />

Mais sur deux autres de mes configs, j'ai toujours DNSSEC qui est considéré comme non sécurisé.