Hornet, un réseau d'anonymisation à la mode Tor en haut débit

Traduit en français par « frelon », le terme anglais « hornet » a d'autres acceptions. Illustration en sécurité IT : une équipe de chercheurs basée entre Londres et Zurich l'utilise tout en capitales (**HORNET**), comme acronyme pour « High-speed Onion Routing at the NETwork layer »).

Derrière cette appellation se cache une technologie d'**anonymisation du trafic** sur les réseaux informatiques. Sa particularité : elle associe le haut niveau de sécurité d'une solution comme Tor aux performances de protocoles tels que LAP et Dovetail.

Les expérimentations menées sur un routeur logiciel d'une capacité maximale de 120 Gbit/s ont permis de transmettre des données à un débit de 93,5 Gbit/s ; soit près de 12 Go à la seconde. De quoi satisfaire très largement des activités comme la navigation Internet et la messagerie instantanée.

C'est précisément à ces usages que se destine HORNET, le principal objectif étant de protéger les utilisateurs contre les tentatives d'écoute, y compris celles qui émanent d'entités dotées d'une grande force de frappe – typiquement, les agences de renseignement.

Le timing de publication du rapport (document PDF de 15 pages daté du 21 juillet 2015) est idéal si l'on considère d'une part que la conscience du public à l'égard du cyber-espionnage s'éveille au fil des révélations d'Edward Snowden. Et de l'autre, que de nombreux États légifèrent actuellement pour renforcer leurs pouvoirs en la matière.

Du Tor amélioré ?

En termes de sécurité, HORNET est dit résistant aux attaques passives. Ses créateurs se sont notamment assurés qu'un tiers cherchant à écouter du trafic ne puisse pas déterminer d'où provient la communication, ni quelle est sa destination (concept baptisé « end-to-end unlinkability » en anglais »).

Parmi les autres garanties évoquées, l'impossibilité pour des tiers de modifier les en-têtes de paquets sans être détectés ou encore de faire le lien entre différentes sessions de connexion. Sur le volet des performances, le défi est le suivant : comment accélérer la transmission de données sachant alors que la nature même des protocoles d'anonymisation, avec leurs opérations de chiffrement répétées, ne s'y prête pas ?

A l'instar de Tor, HORNET chiffre les données par cryptographie symétrique en s'appuyant de façon aléatoire sur les différents nœuds (serveurs, passerelles) qui composent le réseau. Mais il traite différemment les informations de routage au niveau des nœuds intermédiaires (ceux situés entre le client et le serveur), de sorte qu'ils peuvent rediriger plus rapidement le trafic.

Les chercheurs pointent aussi du doigt les limites de Tor en matière de montée en charge. Pour résoudre ce problème, le protocole HORNET, tout comme LAP et Dovetail, ne se superpose pas à la

couche réseau : il s'y intègre, souligne ITespresso.

A défaut de tests plus poussés par la communauté, on restera prudent sur l'avancée concrète que représente HORNET. Non sans se demander si les réseaux exploités commercialement proposeront un jour l'anonymisation du trafic par défaut…

A lire aussi :

Miné par des bugs, le projet Tor Cloud ferme ses portes
Tor à la recherche de financements moins gouvernementaux

Crédit Photo @ Glebstock-Shutterstock