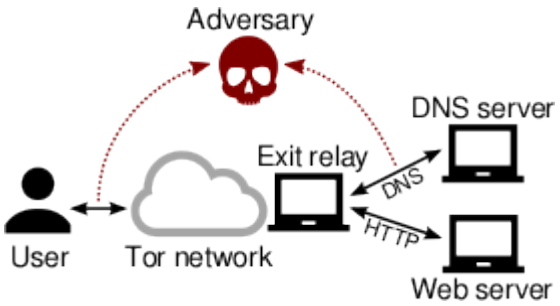
DefecTor : s'appuyer sur le DNS pour désanonymiser Tor

Des chercheurs de Princeton, aux État-Unis, et des universités Karlstad et KTH, en Suède, ont étudié la faisabilité d'une méthode permettant de démasquer les utilisateurs du réseau d'anonymisation Tor. Leurs travaux orientés sur le DNS sont en ligne (*« The Effect of DNS on Tor's Anonymity »*).

L'attaque nommée DefecTor est une variante d'une attaque par corrélation centrée sur les requêtes DNS (Domain Name System). Elle est possible car Tor Browser, le navigateur qui permet aux internautes d'accéder au réseau Tor, regroupe et chiffre le trafic HTTP et le trafic DNS. Ensuite la requête DNS est traitée au niveau du noeud de sortie, et le trafic HTTP est envoyé vers sa destination.



Google pourrait voir clair dans Tor

Selon les chercheurs, un tiers peut utiliser des requêtes DNS pour : mener des attaques de type *« website fingerprinting »* (empreinte de site web), cartographier le trafic DNS avec précision, et corréler les différents sites observés. Les scientifiques disent également avoir constaté *« qu'un ensemble de relais de sortie, représentant parfois jusqu'à 40 % de la bande passante de sortie de Tor, utilise les serveurs DNS publics de Google »*. C'est *« un taux alarmant pour une seule organisation »*, préviennent-ils.

Ils préconisent davantage de diversité sur ce plan. Mais ne croient pas à l'existence d'une menace imminente… *« Nos attaques [DefecTor] ont bien fonctionné lors de simulations,* expliquent-ils, *mais peu d'entités sont en mesure de les mener. Par ailleurs, ces attaques nécessitent un effort d'ingénierie non négligeable »*, et le projet Tor propose des parades aux attaques de type website fingerprinting.

Lire aussi :

Tor perd un de ses pionniers et un nœud critique

Tor envahi par des noeuds espions ?

Le FBI a recruté chez Tor pour démasquer les utilisateurs