Tor sous la menace d’une attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs Directory Authorities dans le viseur

Tor sous la menace d’une attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs

Depuis les révélations d’Edward Snowden sur les pratiques d’espionnage de la NSA et du GHCQ, le réseau anonyme Tor a largement gagné en popularité, ce qui l’a rendu inévitablement le centre des convoitises des agences gouvernementales et la cible de plusieurs attaques.

C’est dans ce contexte que le directeur du projet Tor – Roger Dingledine – a annoncé que le réseau anonyme serait sous la menace d’une attaque informatique ou d’une procédure judiciaire dans les prochains jours.
Dans son billet de blog, Dingledine a tenu à rassurer les utilisateurs que des dispositifs techniques ont été pris pour assurer l’anonymat des utilisateurs, alors qu’ils seront notifiés en cas d’attaques dans les plus brefs délais via le blog et le compte Twitter du projet. De plus, la redondance de l’infrastructure du réseau devrait permettre le fonctionnement de Tor même en cas d’attaque selon le même responsable.
Toutefois, des réserves peuvent être émises quant à la capacité de Tor à résister à cette menace, en effet ladite attaque/procédure cible principalement les serveurs DA (Directory Authorities) via une attaque de type DDoS ou encore par la saisie des serveurs physiques, hors ces derniers qui sont au nombre limité de 10, jouent un rôle crucial dans l’anonymat du réseau, en mettant à disposition des utilisateurs une liste de relais potentiels qui seront par la suite utilisés pour débuter toute communication.
Ainsi, la perturbation du bon fonctionnement des serveurs DA devrait impacter le réseau, pire encore ces serveurs sont aussi responsables de la validation de la liste des relais utilisables, validation qui se fait chaque heure par l’aval de la majorité (au moins 5 serveurs), dès lors le contrôle d’au moins 5 serveurs DA permettrait à l’attaquant de réorienter le trafic vers des relais non sécurisés et déjà sous son emprise, ce qui pourrait signer le coup d’arrêt temporaire de tout le réseau Tor.
À noter aussi que les serveurs DA sont les premiers à être contactés par les utilisateurs, de ce fait leurs adresses IP sont inscrites en dur dans le code du client, ce qui limite le champ d’action et de riposte des responsables du projet.
Quant à la cause d’une telle entreprise, les spéculations vont bon train, allant même à affirmer que cela est relatif au récent piratage de Sony, même si aucune information n’a filtrée lors de l’annonce officielle.
Finalement, le mystère reste entier et les risques sont accrus pour les utilisateurs, ce qui laisse place à la vigilance et à la prudence comme étant les seules consignes en vigueur.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Sources :
http://www.developpez.com/actu/79522/Tor-sous-la-menace-d-une-attaque-en-mesure-de-corrompre-l-anonymat-des-utilisateurs-les-serveurs-Directory-Authorities-dans-le-viseur/
https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network
par Arsene Newman