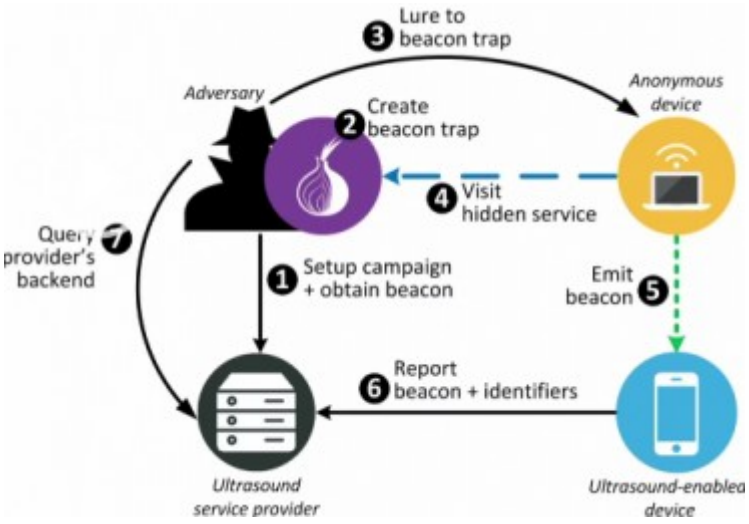
Quand les ultrasons désanonymisent les utilisateurs de Tor

Les moyens de désanonymiser les utilisateurs du réseau Tor se multiplient, comme le montre « la faille publiquement inconnue » trouvée par le FBI. La dernière en date a été présentée par six chercheurs lors du Chaos Communication Congress (CCC) à Hambourg à la fin décembre 2016. Et la méthode est pour le moins originale, car elle repose sur le traçage des ultrasons.

Plus exactement, elle se sert de la technologie nommée uXDT (Ultrasonic cross-device tracking). Les annonceurs cachent dans leurs publicités des ultrasons. Quand la publicité est diffusée sur une télévision, sur une radio ou en ligne, elle émet des ultrasons pouvant être captés à proximité par les micros des ordinateurs ou des smartphones. Ces terminaux peuvent ensuite interpréter les instructions cachées des ultrasons via une application. En général, elles demandent d'effectuer un ping vers le serveur de l'annonceur. Objectif de ce dernier avec l'uXDT : connaître les liens d'une personne avec l'ensemble de ses terminaux et proposer de la publicité ciblée.

Un piège redoutable

Mais cette technologie peut-être un piège redoutable pour les utilisateurs de Tor. Vasilios Mavroudis, un des six chercheurs cités précédemment, a détaillé une attaque de désanonymisation sur les utilisateurs de Tor en obtenant *in fine* la vraie adresse IP et d'autres détails. Première étape de l'attaque, amener l'utilisateur du réseau Tor vers une page web contenant des publicités émettant des ultrasons ou une page web intégrant un code JavaScript caché qui force le navigateur à émettre des ultrasons via l'API Audio HTML5.



Si un smartphone est à proximité et qu'il dispose d'applications supportant uXDT, une agence gouvernementale ou un Etat pourrait assigner une liste d'annonceurs à fournir les détails sur les utilisateurs.

Des attaques multiples pour forcer les ultrasons

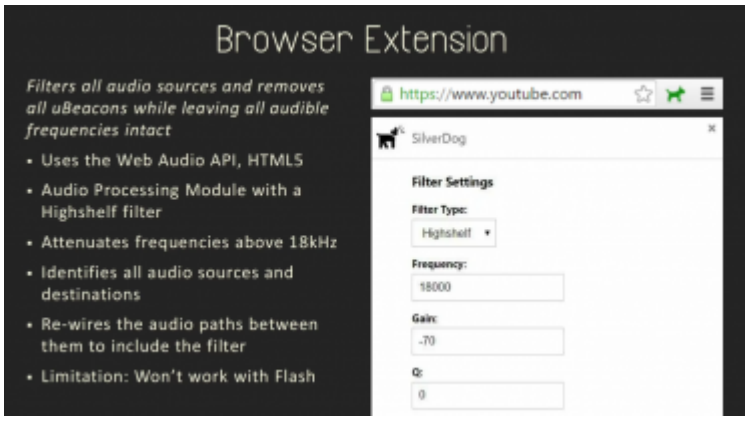
Et les tests réalisés par l'équipe de Vasilios Mavroudis sont concluants. En analysant le trafic émis par les ultrasons vers le smartphone, elle a pu découvrir l'adresse IP réelle de l'utilisateur, les coordonnées de géolocalisation, le numéro de téléphone, l'ID d'Android, le code IMEI et l'adresse MAC du PC.

Les spécialistes ont également trouvé d'autres moyens pour mener à bien leurs attaques contre les utilisateurs de Tor. Ainsi, des pirates pourraient se servir de failles XSS pour injecter du code JavaScript malveillant au sein de pages web vulnérables. Autre technique, créer un faux nœud de sortie Tor à travers une attaque de type homme du milieu (MiTM) pour injecter du code et forcer à l'émission d'ultrasons.

Des techniques d'atténuation

Le FBI pourrait donc s'intéresser à cette technologie des ultrasons dans le cadre des enquêtes pour lutter contre la pédopornographie, le trafic de drogue, le terrorisme et autres crimes. Surtout que l'uXDT n'est pas régulé. La FTC évalue actuellement l'impact des publicités dotées d'ultrasons. Les chercheurs proposent des moyens pour atténuer les risques.

Ils ont par exemple créé une extension pour le navigateur Chrome baptisé SilverDog. Elle se charge de filtrer les fonctions audio HTML5 et de supprimer les ultrasons. Petit hic, l'extension ne supprime pas les sons joués dans Flash et n'est pas compatible avec le navigateur Tor (basé sur Firefox).



Autre technique, la création d'une règle de permission sur Android pour savoir quelles applications peut écouter des ultrasons. Enfin, les chercheurs militent pour la création d'un standard pour ces technologies s'adossant aux ultrasons (uXDT, Beacons audio, etc.) et d'instaurer des bonnes pratiques. Le chemin sera long…

A lire aussi :

Mozilla corrige une faille critique touchant Tor dans Firefox

Le projet Tor avance sur un Tor Phone