Le réseau Tor victime d'un piratage pendant 6 mois

Tor a été victime d'un piratage, a annoncé le le réseau d'anonymisation par voie de blog. *« Le 4 Juillet 2014, nous avons trouvé un groupe de relais dont nous supposons qu'**ils tentaient de dé-anonymiser les utilisateurs**. Ils semblent avoir ciblé les personnes qui exploitent ou accèdent aux services cachés de Tor. L'attaque a consisté à modifier les en-têtes de protocole Tor afin de faire des attaques de type trafic confirmation. »* Une technique utilisée pour repérer les activistes du réseau même si elle ne permet pas de savoir ce qu'ils y font.

Rappelons que Tor (**The Onion Router**) est un réseau informatique mondial distribué et décentralisé qui, selon un principe de réseau mélangé, permet de transmettre les flux TCP de manière anonyme et, donc, rendre les échanges Internet anonymes. Le logiciel de réseau propose ainsi des services cachés qui permettent de cacher l'identité du serveur qui les héberge (données IP et géographiques cachées). C'est ce type de services qui a été la cible des attaquants.

Localiser les utilisateurs

L'installation des relais, ou nœuds de réseau qui reçoivent et transmettent les requêtes IP, ayant servi à l'attaque remonte de fait au **30 janvier** 2014 et les administrateurs de Tor n'ont supprimé ces sondes que le 4 juillet dernier. *« Bien que nous ne sachons pas quand ils ont démarré l'attaque, les utilisateurs qui ont opéré ou ont accédé à des services cachées entre début février et le 4 juillet doivent estimer qu'ils ont été affectés. »*

Néanmoins, les auteurs du billet avouent ne pas savoir comment ni jusqu'à quel niveau les victimes ont été affectées. De toute évidence, les attaquants cherchaient à localiser les services cachés et, donc, **cibler au mieux l'identité de leurs administrateurs**. *« En théorie, l'attaque pourrait également être utilisée pour relier les utilisateurs à leurs destinations sur les circuits normaux de Tor, mais nous n'avons trouvé aucune preuve que les attaquants ont opérés sur les relais de sortie, ce qui rend cette attaque moins probable. »* Toujours est-il que les modification des entêtes de protocole ont pu aider d'autres attaquants à dé-anonymiser les utilisateurs.

Sale temps pour Tor

De par son système de navigation anonyme, le réseau Tor est réputé pour **attirer aussi bien les criminels** surfant sur des sites plus ou moins légaux **que les utilisateurs soucieux de leur sécurité** et de leur vie privée. Si bien qu'il attire aussi l'intérêt des gouvernements et agences de sécurité. A commencer par la NSA dont les pratiques d'infiltration ont été révélées par son ancien employé **Edward Snowden**. Plus récemment, la Russie a offert une récompense pour casser le réseau Tor. Parallèlement, une conférence qui devait démontrer comment identifier les utilisateurs Tor a été retirée du programme du prochain Black Hat de Las Vegas dédié à la sécurité. Les nuages s'accumulent sur la tête de Tor.

crédit photo © Glebstock – shutterstock

Lire également

[La NSA traque un autre Snowden en surveillant Tor et Tails ?]
[Microsoft supprime Tor à distance pour bloquer un botnet]
[Prism : Le réseau Tor résiste aux attaques de la NSA]