Les hackers qui ont piraté les réseaux Xbox et PlayStation visent maintenant Tor

Après avoir mis hors service les deux principaux réseaux de jeu en ligne de la planète (Xbox Live et PlayStation Network) via des attaques DDoS – les services ont depuis été remis sur pied -, **les hackers de la Lizard Squad** ciblent maintenant le réseau d'anonymisation Tor. Rappelons que ce dernier fonctionne grâce à des routeurs administrés par des individus ou organisations participant au réseau et transmettant de manière anonyme des flux TCP.

Vendredi dernier, des milliers de nouveaux nœuds sont apparus sur Tor, avec des **appellations débutant par 'LizardNSA'**. Le compte Twitter de la Lizard Squad a confirmé que l'équipe de hackers était bien derrière l'ouverture de ces quelque 3 000 serveurs (selon les affirmations du groupe). Une menace potentielle pour les utilisateurs de Tor, l'opérateur d'un grand nombre de nœuds pouvant en théorie compromettre leur anonymat en surveillant le trafic sortant.

Beaucoup de nœuds, peu de trafic

Le fait d'ouvrir un grand nombre de nœuds ne suffit toutefois pas à mettre à mal la sécurité du réseau d'anonymisation. Comme l'explique le projet Tor dans un billet de blog paru en 2013, les nouveaux relais passent par un **processus d'approbation** durant plusieurs jours, au cours desquels le trafic qui y transite est limité. Dans une interview par chat avec le Washington Post, une personne indiquant faire partie de la Lizard Squad a expliqué que le groupe est désormais en possession de plus de la moitié des nœuds du réseau Tor, mais a reconnu que seule une petite partie du trafic y transite. En dehors du processus d'approbation, les utilisateurs disposent aussi d'**options pour éviter d'utiliser les serveurs suspects** (comme le marquage BadExit).

Selon le hacker interrogé par nos confrères, l'objectif de cette opération est de **montrer les faiblesses structurelles de Tor**. « *Ajoutez ces nœuds au réseau sur une période d'un mois environ et il n'y aurait alors aucune façon simple d'identifier ces serveurs* », a expliqué le contact anonyme joint par nos confrères. De facto, remarquons que la Lizard Squad a choisi ici d'ajouter 3 000 nœuds d'un coup et de les identifier clairement (avec le préfixe LizardNSA).

Un des volontaires du projet Tor, Kate Krauss, a expliqué que ces milliers de nouveaux relais ne faisaient transiter que moins de 1 % du trafic du réseau et que l'équipe du projet travaille à les retirer du réseau.

Selon le blogueur spécialisé Brian Krebs, la Lizard Squad serait constitué de jeunes hackers en mal de notoriété, **inspirés par LulzSec**, autre gang dont les membres fondateurs ont été arrêtés en 2012 et placés en détention.

A lire aussi :

Tor : 8 utilisateurs sur 10 pourraient être identifiés
Tor : l'anonymat n'est pas toujours synonyme de sécurité

crédit photo © GlebStock – Shutterstock