Les sites cachés Tor exposés grâce au serveur Apache

Les sites web, qui s'appuient sur le réseau d'anonymisation Tor pour masquer leur adresse serveur, doivent se méfier d'un paramétrage par défaut dans les serveurs Apache. Ces derniers largement utilisés sur le web ont fait l'objet d'une attention particulière de la part d'un hacker qui a donné sur un site les détails de la faille.

Sur cette page, il rend d'abord hommage à d'autres hackers pour leurs travaux sur les serveurs Apache. Il explique ensuite que *« si vous utilisez un serveur Apache pour faire tourner un site caché Tor, assurez-vous de désactiver mod_status avec l'instruction: $ a2dismod status »*. Il poursuit son explication en précisant : *« Dans plusieurs distributions, Apache est livré avec une fonctionnalité pratique appelée mod_status qui est activée. C'est une fonctionnalité située à /server-status qui donne quelques statistiques comme la disponibilité, l'utilisation des ressources, le trafic total, les hôtes virtuels activés et les requêtes actives HTTP. Pour des raisons de sécurité, elle est accessible uniquement depuis localhost par défaut. »*

Un espionnage en toute transparence

Dès lors, si le daemon Tor fonctionne sur le localhost, le site caché sur Tor a donc sa page /server-status et expose plusieurs statistiques pouvant intéresser des gens malintentionnés. Un pirate peut ainsi déduire à partir du fuseau horaire la longitude approximative du service ou déterminer l'adresse IP du site. Adieu donc anonymat.

Comme le rappelle le hacker anonyme, cette vulnérabilité n'est pas nouvelle. Mais elle est remise au goût du jour, car elle est persistante. Le projet Tor conscient du problème a tenté d'y remédier. Las, le hacker constate qu'il *« a découvert plusieurs expositions à ce problème depuis 6 mois »*. A chaque fois, il assure avoir contacté les personnes pour modifier ce paramètre. Pire il a trouvé un moteur de recherche de site .onion qui n'avait pas désactivé le module status et *« le résultat n'est pas beau à voir »*. Il recommande aux utilisateurs de vérifier leur site sur l'adresse http://your.onion/server-status : *« Si vous avez une réponse autre que 404 et 403, ouvrez un shell sur votre serveur et exécutez $ sudo a2dismod status. »*

La sécurité de Tor est souvent prise pour cible comme le montre les accointances entre le FBI et Carnegie Mellon pour casser le réseau d'anonymisation. Les promoteurs du projet ont lancé en décembre dernier un programme de chasse aux bugs pour renforcer cette sécurité. La faille dans les serveurs Apache souligne que la fragilité de Tor est à chercher en dehors du projet.

A lire aussi :

Un gourou du chiffrement lance PrivaTegrity, une alternative à Tor
Bounty Factory : la recherche de bugs made in Europe est née