Le projet Tor avance sur un Tor Phone

Un Tor Phone en approche. Non il ne s'agit pas d'un fantasme, mais bel et bien un projet développé par l'équipe derrière le réseau d'anonymisation. Mike Perry, développeur pour Tor, a indiqué dans un billet de blog que « *ce prototype doit être vu comme une possible orientation de Tor dans le mobile* ». Ce prototype repose sur Android, mais une version profondément remaniée de l'OS de Google.

Pour le développeur, « *l'écosystème Android évolue rapidement et dans cette transformation, nous sommes préoccupés de la menace qui pèse sur la liberté des utilisateurs à étudier, partager et améliorer le système d'exploitation* ». Et d'ajouter : « *Nous essayons de réaliser un téléphone qui respecte le choix et la liberté des utilisateurs, réduit considérablement la vulnérabilité aux menaces et donne à l'écosystème une orientation pour garantir un haut niveau de sécurité.* »

Basé sur Copperhead avec OrWall

Le Tor Phone est basé sur Copperhead OS, une distribution Android, comprenant des améliorations de sécurité en corrigeant de nombreuses failles. Les développeurs de Tor ont ajouté un firewall Android baptisé OrWall, qui force les applications à router leur trafic sur le réseau anonymisé et bloque les flux indésirables. L'application laisse la main à l'utilisateur pour déterminer si un programme comme la VoIP peut contourner le firewall et améliorer la qualité des appels. Par contre OrWall vérifiera que la localisation et les données personnelles des parties sont bien anonymisées.

Le prototype fonctionne pour l'instant sur les Google Nexus 6P et prochainement sur les Pixel, capables de gérer la dernière version de la fonction « verified Boot », qui garantit l'intégrité du système au démarrage.

Mission Improbable

Répondant au doux nom de « Mission Improbable », ce prototype est prêt à être téléchargé (sur GitHub) et à être installé (des connaissances sur les environnements Linux sont les bienvenues). Mike Perry l'a mis sur son téléphone et indique dans le blog qu'il l'utilise pour « *l'e-mail, Signal, XMPP+OTR, Mumble, les cartes en mode déconnecté, la prise de photo et la lecture de magazines ou livres* ».

Le développeur rappelle qu'il n'est pas dans l'intention de Tor de s'occuper du matériel, mais bien de proposer une solution logicielle, réellement Open Source, transparente et garante de la confidentialité des données. Un coup de gueule à destination de la politique de Google sur Android et aux OEM qui prennent quelques libertés sur la personnalisation de l'OS mobile.

A lire aussi :

Une seconde backdoor chinoise nichée dans les terminaux Android
Foxconn laisse des backdoor trainer dans des smartphones Android