L’anonymat de l’OS Linux sécurisé Tails compromis

The Amnesic Incognito Live System plus connu sous son acronyme **Tails** est encore plus connu pour être l’OS utilisé par le lanceur d’alerte Edward Snowden pour dévoiler les documents de la NSA. Tails a pour objectif de permettre de naviguer et de communiquer sur Internet de façon anonyme. Cet OS ultra sécurisé s’appuie une base Linux (d’origine Debian), et le réseau Tor.

Or l’anonymat des utilisateurs de l’OS pourrait être compromis par **une faille de sécurité** découverte par Exodus Intelligence, une société spécialisée dans le chiffrement des données. La faille en question se situe dans l’**Invisible Internet Project (I2P)**, une connexion réseau cryptée développée par la communauté Open Source pour maintenir les communications privées. Les experts ont réussi à tromper le logiciel pour révéler l’adresse IT utilisateur.

I2P a été intégrée dans les dernières versions de l’OS et les responsables du projet ont indiqué à Reuters qu’ils travaillaient sur un correctif. Ils recommandent aux utilisateurs de Tails de désactiver temporairement JavaScript pour éviter l’identification. Sur le blog d’Exodus, on peut lire que « *nous espérons rappeler aux utilisateurs de Tails qu’aucun logiciel n’est infaillible* ».

Les solutions d’anonymisation sous surveillance

Pour mémoire, Tails peut être exécuté depuis un DVD, une clé USB ou une carte SD. Il a été conçu pour ne laisser aucune trace numérique sur une machine. Cela signifie en théorie une impossibilité de suivre les utilisateurs. En début de semaine, **la version 1.1 de Tails a été publiée** en apportant des améliorations en matière de sécurité et de stabilité, mais elle contient toujours la faille détectée par Exodus. L’OS fonctionne toujours sur Debian, comprend du chiffrement OpenPGP et le support du réseau Tor. En plus du navigateur Firefox pré-configuré, il intègre Pidgin un client de messagerie instantanée et Claw Mail pour les courriels. Sur la partie applicative, on retrouve OpenOffice, GIMP et Audacity. Il est enfin livré avec un clavier virtuel pour contrer les keyloggers.

Récemment la NSA s’est intéressée de près à Tails et au réseau Tor à travers son outil de surveillance KeyScore avec en filigrane la quête d’un second Snowden. Le sujet des outils d’anonymisation sur le web est très sensible au point qu’une session de la prochaine Black Hat sur la désanonymisation du réseau Tor a été annulée.

crédit photo © Sashkin – shutterstock

A lire aussi :

Le service de messagerie anti-NSA, Protonmail, arrive en test