Tor : l'anonymat n'est pas toujours synonyme de sécurité

Si le système Tor protège l'anonymat de ses utilisateurs, il n'est pas forcément immunisé contre toutes les menaces. Un chercheur en sécurité du nom de **Josh Pitts** vient de mettre au jour un nœud de sortie Tor infecté. Situé en Russie, ce dernier aurait été utilisé par des assaillants non identifiés pour **insérer du code malicieux dans des fichiers téléchargés par les utilisateurs Tor**. Depuis, ce nœud a été signalé par les administrateurs du réseau d'anonymisation (via le signal BadExit) permettant aux utilisateurs de l'éviter.

Dans l'architecture Tor, les requêtes sont cryptées et routées de façon distribuée afin de masquer l'adresse IP des utilisateurs. Elles parviennent sur le Web public via un nœud de sortie. Il en existe entre 1 100 et 1 200 dans le monde.

La découverte de Josh Pitts s'inscrit dans le cadre de ses **recherches sur les binaires non chiffrés disponibles sur Internet**, des fichiers très faciles à modifier par un assaillant via une technique de type Man-in-the-middle avait-il montré lors de la conférence DerbyCon en début d'année. C'est en étudiant ce phénomène sur les nœuds de sortie Tor, via un module spécifique qu'il a écrit pour l'outil exitmap, que le chercheur de la société Leviathan a découvert le pot aux roses.

L'erreur de Windows Update « *pose problème* »

« *Sur les 1 100 nœuds de sortie du réseau Tor, c'est le seul que j'ai détecté comme patchant les binaires (pour les compromettre, NDLR) ; ce nœud essaie de modifier à peu près tous les binaires que j'ai testés. (…) Cela ne signifie pas que d'autres nœuds Tor ne patchent pas les binaires ; il est possible que je ne les ai pas détectés ou qu'ils ne modifient qu'un nombre limité de binaires* », écrit Josh Pitts dans un billet de blog.

Sur ce nœud russe, des **mises à jour Windows** étaient ainsi modifiées lorsqu'elles étaient téléchargées, y compris quand elles l'étaient au travers de Windows Update. Si l'outil du premier éditeur mondial détecte la modification et émet alors une erreur, cette alerte même « *pose problème* », estime le chercheur. Après une recherche sur le code d'erreur émis par Windows Update, Microsoft propose en effet de résoudre le problème via le téléchargement d'un utilitaire… qui sera lui aussi modifié par le nœud malicieux ! Et comme il sera téléchargé en dehors de Windows Update, sa transformation en malware ne générera plus aucun message d'erreur.

Pour le leader du projet Tor, **Roger Dingledine**, « *la meilleure approche serait d'avoir des applications qui n'accordent pas une confiance aveugle à des bits non authentifiés qu'elles récupèrent d'Internet* ». Dans son billet de blog, Pitts explique que tous les utilisateurs devraient avoir à disposition un moyen de **vérifier l'empreinte et la signature d'un binaire avant son exécution**, afin de s'assurer que le fichier qu'ils ont téléchargé est bien le même que celui qu'ils ont demandé.

A lire aussi :

Anonabox, le routeur Tor déchu de Kickstarter
Anonymat sur le Net : Tor bientôt intégré à Firefox ?