Des experts en sécurité hackent le client Dropbox

Dhiru Kholia et **Przemyslaw Wegrzyn**, deux développeurs œuvrant dans de multiples domaines, dont les outils de sécurité open source, se sont attaqués au client **Dropbox**. Avec succès.

Ils ont pu décoder l'exécutable de l'application, qui comprend en fait un ensemble de fichiers écrits en Python, lancés par un interpréteur intégré. Ils ont ensuite décrypté ce code, qui était rendu illisible par des techniques d'obscurcissement du source.

Une fois ceci fait, ils ont pu découvrir comment intercepter les communications SSL en provenance des serveurs de Dropbox, comment contourner l'identification à deux facteurs utilisée et comment mettre au point un client open source alternatif à celui fournit par la société.

Les techniques utilisées sont décrites au sein d'une publication qui a été présentée dans le cadre de la conférence **Usenix Woot'13** (*Workshop on Offensive Technologies*) de Washington D.C. (plus de détails ici). Elles pourront être utilisées avec d'autres applications cachant du code Python.

Pourquoi verrouiller le client ?

Les deux experts en sécurité s'interrogent sur le pourquoi de l'utilisation de telles techniques de protection du code source par Dropbox.

« Nous nous demandons ce que Dropbox espère gagner en appliquant de telles mesures », expliquent-ils dans les colonnes de *SD Times*. *« La majeure partie de la recette secrète de Dropbox se trouve côté serveur et est déjà bien protégée. Nous ne croyons pas que ces mesures anti-rétro-ingénierie soient bénéfiques pour Dropbox et ses utilisateurs. »*

La société ne fournit par ailleurs aucune API permettant de créer des clients alternatifs. Heureusement toutefois, les techniques de rétro-ingénierie, telles que celles utilisées ici, sont autorisées en Europe (et dans une moindre mesure aux États-Unis) dans un objectif d'améliorer l'interopérabilité d'un produit avec des solutions tierces.

Voir aussi
Quiz Silicon.fr – Crimes et châtiments sur Internet