Un ancien de la NSA se joue de la sécurité de Mac OS X

A l'occasion de la conférence CansSecWest qui se déroule à Vancouver, Patrick Wardle directeur de la recherche chez SynAck, fournisseur de solutions de sécurité 'as a service', a indiqué à nos confrères de ThreatPost, avoir découvert des techniques de détournement de DLL dans OS X d'Apple. L'intervenant n'est pas un novice. Il a travaillé comme chercheur en sécurité auprès de **la NSA** et de **la NASA**.

Pour lui, les **Dylib**, qui sont les librairies d'OS X, peuvent être substituées par des versions malveillantes. Ces dernières fournissent exactement les mêmes attaques que le détournement de DLL (Dymanic Linked Librairy) qui a frappé Windows depuis plus de 15 ans. Patrick Wardle explique que « *le détournement de DLL est assez répandu sur Windows, je me suis demandé si c'était envisageable sur OS X et j'ai trouvé une attaque similaire. Certes sous le capot, il y a des différences techniques, mais les capacités sont les mêmes. Etant donné que vous avez une application vulnérable sur OS X, vous pouvez attaquer de la même façon que sur Windows* ».

Les librairies dynamiques sont des composants intégrés dans les couches basses du système d'exploitation en tant que ressource commune mise à disposition des développeurs. Sous Mac OS X, ces fichiers se définissent par l'extension .dylib (DLL pour Windows). On les retrouve notamment dans les API, les pilotes, les widgets ou les polices de caractères.

Xcode, iMovie, Dropbox, Java…

Parmi les différentes méthodes, Patric Wardle a développé **un scanner** pour trouver les applications qui sont vulnérables au contournement de Dylib. Sur son propre Mac, il a trouvé **144 binaires sensibles dont Xcode, iMovie, les plugins Quicktime, Word, Excel et PowerPoint de Microsoft** et des apps tierces comme **Java, Dropbox, GPG Tools et des plugins Adobe**. Pour sa démonstration lors de la conférence, l'ancien chercheur de la NSA s'est basé sur un binaire Apply dans Photostream Agent qui démarre automatiquement avec iCloud. « *C'est une méthode idéale pour une attaque persistante. On copie la Dylib infectée dans le répertoire de PhotoStream et elle est chargée au démarrage de l'application sans avoir modifié de fichier ou créé de nouveaux processus* », constate Patrick Wardle.

La protection de Gatekeeper déjouée

Une autre méthode lui a permis d'exécuter du code via un processus d'injection dans **Xcode**, la plateforme de développement d'Apple. De même, il a trouvé un procédé pour contourner la protection de l'outil de sécurité d'Apple **Gatekeeper,** en charge de l'identification de malware. Ce dernier « *fait du très bon travail* », reconnaît le spécialiste de la sécurité, mais « *en utilisant ce système de contournement, on peut infecter des utilisateurs sans problème* ». Ces différentes méthodes ont été transmises à Apple pour apporter d'éventuels correctifs. Patrick Wardle prévoit de publier un programme qui vérifiera le niveau de vulnérabilité des applications et de l'OS installé.

Cette présentation intervient après les révélations des documents Snowden relatant des réunions secrètes des experts en sécurité de la CIA notamment. L'objectif de ces réunions était de trouver des techniques pour casser la sécurité de certains logiciels et terminaux dont ceux d'Apple. En particulier, les documents montrent comment les spécialistes de la CIA ont travaillé sur **une version modifiée de Xcode** qui avait pour ambition de **placer des backdoors**.

A lire aussi :

Mac OS X Yosemite à l'assaut de la convergence

Google déniche 3 failles Zero Day dans Mac OS X

Crédit Photo : GaudiLab-Shutterstock