Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

	Alerte sur Apple, le Trousseau d’accès mis en défaut par un nouveau malware

Faut-il y voir la rançon du succès des Mac ? Toujours est-il qu'OSX/Keydnap est le deuxième malware de la semaine sur OS X, après Backdoor.MAC.Eleanor. Découvert par ESET, ce nouveau logiciel malveillant est pour le moment d'origine inconnue, mais on connait son mode de fonctionnement.

Téléchargé en pièce jointe ou depuis un site interlope, Keydnap se présente sous une forme bien innocente : une archive ZIP qui contient ce qui ressemble à une image (.jpg) ou un document texte (.txt). Sauf que le suffixe du document contient une espace, ce qui lance un Terminal, et non Aperçu ou TextEdit comme on peut s'y attendre.

En cliquant sur le document, un mécanisme se met en place qui fait prendre des vessies pour des lanternes. L'application attendue s'ouvre et présente le document qui va bien… sauf que dans l'intervalle, le fichier aura ouvert un Terminal (l'icône du Terminal apparait brièvement dans le dock avant d'être remplacée par celle de l'application standard). Une fois l'exécutable lancé, Gatekeeper prévient que le fichier provient d'un développeur non enregistré et qu'il ne peut pas ouvrir le document :

Ce message d'alerte intervient si et seulement si Gatekeeper n'autorise que les applications provenant du Mac App Store et des développeurs identifiés. Sur OS X El Capitan, on peut choisir de lancer une app téléchargée depuis « n'importe où », mais plus sous macOS Sierra.

Une fois lancé, le malware crée une porte dérobée et remplace le contenu de l'exécutable par un leurre téléchargé sur internet ou intégré dans le code du logiciel malveillant – il peut s'agir du document effectivement attendu, comme une image :

La porte dérobée créée par Keydnap est persistante, même si on multiplie les redémarrages du Mac. Il demandera aussi le mot de passe de la session, déguisé sous la forme d'icloudsyncd. Une fois en possession de cette information, il transforme le Mac en open-bar : l'objectif du malware est de récupérer les informations du Trousseau d'accès, qui contient les identifiants et mots de passe de vos logiciels et services en ligne.

À la lumière de cette nouvelle affaire, on comprend mieux pourquoi Apple exige maintenant des logiciels signés sur macOS Sierra.

Merci à Mickaël Bazoge pour son enquête et son article

Réagissez à cet article

Original de l’article mis en page : Nouveau malware sur OS X : OSX/Keydnap détrousse le Trousseau d’accès | MacGeneration