Sécurité - Une mise à jour des Macs permet de boucher la vulnérabilité...Le ver est dans la pomme: une variante du cheval de Troie Flashback aurait infecté plus de 600.000 Macs, selon la firme d'antivirus DrWeb. Ce «trojan» avait déjà fait la Une en 2011, mais le nombre de machines touchées a récemment explosé à cause d'une vulnérabilité Java.

Dans l'affaire, Apple est pointé du doigt. Oracle a en effet bouché la faille Java en février, mais la firme à la pomme a mis six semaines avant de proposer la mise à jour sur Mac OS X. Attention, l'update empêche les nouvelles contaminations, mais les utilisateurs déjà infectés doivent malgré tout faire du ménage manuellement.

Si vous êtes en France, la probabilité d'être infecté est faible: seulement 0,56% du botnet (le réseau de machines dites «zombies» potentiellement contrôlées par des pirates) est situé dans l'Hexagone, soit environ 3.000 Macs. Pour savoir si vous êtes touchés, il faut passer par des commandes à entrer dans la console. Cnet explique la procédure pas à pas. En cas d'infection, d'autres commandes sont nécessaires. La liste se trouve ici.

Les Macs pas immunisés

Cet épisode rappelle une vérité longtemps ignorée par Apple et ses utilisateurs: les Macs ne sont pas intrinsèquement immunisés contre les virus et malwares. Si les machines d'Apple ont jusqu'ici globalement été épargnées, «c'est avant tout pour des raisons de parts de marché», explique l'expert David Perry.

Sauf qu'aux Etats-Unis, Apple est le seul fabricant d'ordinateurs dont les ventes ont progressé au trimestre dernier, à 11% (on ne compte pas les smartphones et tablettes). Face au déclin du PC, viser les Macs, les smartphones et les tablettes, sous iOS et Android, commence à devenir intéressant pour les cybercriminels.

Si Apple inclut désormais une protection contre les malwares avec OS X, il est possible, pour être plus tranquille, d'installer un antivirus. Surtout qu'il en existe des gratuits, de Sophos ou encore ClamXav.

Source : 20 minutes.fr

Plus de 600 000 Macs piratés à travers le monde : l'analyse de Guillaume Lovet

L'encre vient de couler en abondance au sujet de Flashback, un cheval de Troie ayant infecté plus de 600 000 Macs dans le monde. Etats-Unis, UK, France, Allemagne, Espagne, Italie, Suisse, Japon, Australie... sont autant de pays touchés. Se propageant depuis 2011, ce virus récupère les mots de passes et identifiants bancaires des victimes.

Face à ces faits, Guillaume Lovet, expert en cybercriminalité chez Fortinet, nous explique les motivations d'une telle attaque, les hypothèses concernant l'auteur des faits ainsi que les techniques utilisées. Et accessoirement, il nous livre ses conseils pratiques pour permettre de savoir si votre Macintosh est ou non infecté par Flashback.

Quel est le processus adopté par FlashBack ? Quelles sont les techniques utilisées ?

La dernière version de Flashback utilise la technique dite de "Drive-by install" pour infecter les utilisateurs de Mac: L'utilisateur visite un site malicieux qui exploite une vulnérabilité dans son système afin d'installer silencieusement un cheval de Troie ou un virus.

Dans le cas de Flashback, cette vulnérabilité (dont le nom de référence est CVE-2012-0507) porte sur la version de Java utilisée par MacOS, avant qu'Apple ne propose un patch le 4 Avril.

Une fois installé, le cheval de Troie contacte un serveur "mère", depuis lequel les cybercriminels contrôlent le parc de machines infectées. Jusqu'à présent, les "payloads" (c'est-à-dire que les cybercriminels chargent les machines infectées d'exécuter des programmes) qui leur furent transmis concernent l'espionnage du trafic réseau, et la manipulation des résultats retournés par un moteur de recherche.

Quelle est l'étendue des dégâts ?

A l'échelle mondiale, grande: 600 000 Macs infectés, soit 1% du parc total de Macs. Proportionnellement, c'est une "prévalence" comparable à celle qu'a eu un super-vers comme Conficker, sur Windows.

En France, environ 4 000 machines sont infectées.

Pour quelle raison le Mac jusqu'à présent épargné est-il aujourd'hui la cible des cyber-pirates ?

La part de marché du Mac est passée de moins de 3% en 2004, à plus de 10% aujourd'hui. Il commence donc à devenir rentable pour un cybercriminel de consacrer du temps et de l'énergie à fabriquer et distribuer du malware pour Mac. D'autant qu'ils peuvent (à raison ou à tort) percevoir les utilisateurs de Mac comme plus fortunés que les utilisateurs de PC.

Quelles sont les motivations des auteurs de l'attaque ?

Au vu des payloads décrits ci-dessus, les motivations sont, sans surprises, vénales: interception des identifiants (dont les identifiants bancaires), et détournement de trafic internet vers des liens "commerciaux" en modifiant les pages de résultats des moteurs de recherche, dans le navigateur des utilisateurs infectés.

Quelle est la réponse d'Apple ? quelle parade est proposée par le constructeur et les éditeurs ?

Apple a (enfin) fourni la mise-à-jour Java qui patche la vulnérabilité exploitée lors du "Drive-by install". Par contre, il n'y a pas d'outil de détection ou de nettoyage en vue.

Que peuvent faire les utilisateurs de Mac ?

Vérifier s'ils sont infectés, en suivant ces instructions:
http://mashable.com/2012/04/05/mac-flashback-trojan/

Eventuellement, enlever le cheval de Troie "à la main", pour celà les internautes trouveront des instructions à suivre sur Internet.

Et dans tous les cas, installer la mise à jour de Java fournie par Apple.

Source : ITRnews