Un nouveau malware vise les Mac, 17.000 machines affectées ?

Un nouveau malware vise les Mac, 17.000 machines affectées ?

Selon la firme russe Dr.Web un malware visant spécifiquement les possesseurs de Mac serait actuellement actif, affectant plus de 17.000 machines à travers le monde. Pas une première, mais ce malware possède quelques spécificités amusantes.

Pas la peine de se mentir, les produits Apple eux aussi sont parfois victimes de malwares. En 2011, le Trojan Flashback avait ainsi infecté des centaines de milliers d'ordinateurs Apple. Le malware détecté par Dr Web est en revanche bien moins diffusé : 17.000 utilisateurs seulement seraient infectés.
Ce malware se range sous la catégorie des Botnets, infectant l'ordinateur de l'utilisateur afin de permettre à l'attaquant de l'exploiter pour d'autres fonctions à l'insu de son utilisateur. Le malware a été baptisé, un peu rapidement, iWorm par Doctor Web, bien que le mode exact de propagation du virus reste encore peu clair.
La particularité qui a retenu l'attention des chercheurs, c'est la façon dont les ordinateurs infectés récupèrent les adresses IP des serveurs de command&control. Les machines du botnet vont ainsi chercher sur Reddit les adresses de leurs centre de command&control : celles-ci sont postées à intervalles régulier dans la section commentaire d'un sujet destiné à recenser des serveurs Minecraft via un compte tenu par les individus responsables de la propagation du malware.

Reddit est innocent !
Reddit n'a rien à se reprocher, le site n'a pas été altéré ou son utilisation n'a pas été techniquement détournée, mais cette approche originale mérite d'être notée. Comme le relève le chercheur Graham Cluley, même en supprimant le compte utilisé pour router vers ces adresses IP, cela n'empêcherait pas les pirates de recréer un compte et de continuer leur activité.
Comme souvent néanmoins, il convient de rester prudent avec les alertes lancées par les firmes spécialisées dans la vente d'antivirus. Dr.Web annonce ainsi 17.000 ordinateurs infectés à travers le monde, mais ne précise pas du tout quel mode de diffusion a été choisi pour propager le malware. Selon des sources anonymes, le principal mode d'infection se ferait via le téléchargement de logiciels Adobe et Microsoft piratés sur les plateformes de partage en P2P.
De la même manière, peu d'informations sont disponibles pour ceux qui souhaitent se prémunir de ce malware, si ce n'est la solution vendue par Dr.Web… Mais selon MacRumors, l'outil de protection maison proposé par Apple à ses clients Xprotect, a été mis à jour pour détecter et empêcher la propagation de cette menace.
Attention Livo !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/un-nouveau-malware-vise-les-mac-17000-machines-affectees-39807339.htm
Par Louis Adam | Lundi 06 Octobre 2014