SÃ©curitÃ© : Les conseils de Qualys pour bien sÃ©curiser Mac OS X
Mac et Linux
PostÃ© par : JulieM
PubliÃ©e le : 10/12/2008 15:00:00

Depuis toujours, ***Apple dÃ©clare que Mac OS X est suffisamment sÃ©curisÃ© pour se passer dâ□□antivirus*** . ***QualysÂ® Inc.***, principal fournisseur de solutions pour la gestion des vulnÃ©rabilitÃ©s et de mise en conformitÃ© en mode Â« Ã la demande Â», ***conseille les utilisateurs pour garantir la sÃ©curitÃ© de Mac OS X, face aux vulnÃ©rabilitÃ©s.***
En effet, les virus ne sont pas les seules menaces qui peuvent mettre en pÃ©ril la sÃ©curitÃ© de la plate-forme Mac OS X.

La plate-forme Mac dâ□□Apple est en train de se dÃ©velopper Ã une vitesse fulgurante. Il y a encore quelques annÃ©es, Apple ne reprÃ©sentait quâ□□une faible partie du marchÃ© informatique. Aujourdâ□□hui, grÃ¢ce au succÃ¨s du systÃ¨me dâ□□exploitation OS X et des IMacs, Apple est devenu le troisiÃ¨me plus important constructeur de PC avec une part de marchÃ© dâ□□environ **8%**.

Â

Cette engouement nâ□□est pas passÃ© inaperÃ§u aux yeux des pirates qui ont multipliÃ© les attaques contre cette plate-forme.

Dâ□□ailleurs, quelques cas de chevaux de Troie ciblant des utilisateurs Mac, notamment un cheval de Troie Flash, sont Ã dÃ©plorer cette annÃ©e et un autre, dÃ©couvert en juin dernier, tentait de dÃ©rober des mots de passe et dâ□□affaiblir la configuration du firewall.

De plus, les vulnÃ©rabilitÃ©s au sein du systÃ¨me dâ□□exploitation sont en augmentation certaine : en 2002, il y en avait moins de 20 annoncÃ©es pour Apple, contre plus de 100 en 2007. DÃ©but juillet 2008, Apple a mÃªme intÃ©grÃ© 25 vulnÃ©rabilitÃ©s Ã sa quatriÃ¨me mise Ã jour de sÃ©curitÃ© de lâ□□annÃ©e.

Mais en matiÃ¨re de sÃ©curitÃ©, Apple ne reste pas les bras croisÃ©s. En effet, certaines nouvelles fonctionnalitÃ©s inhÃ©rentes Ã OS X 10.5, participant Ã la sÃ©curisation du systÃ¨me, ont Ã©tÃ© apportÃ©es Ã la version diffusÃ©e Ã lâautomne 2007 :

Taggage et avertissement lors de la premiÃ¨re exÃ©cution : Mac OS X 10.5 marque les fichiers qui sont tÃ©lÃ©chargÃ©s pour empÃªcher les utilisateurs dâexÃ©cuter par inadvertance des applications malveillantes quâils ont tÃ©lÃ©chargÃ©es.

Protection runtime : de nouvelles technologies telles que la dÃ©sactivation de lâexÃ©cution, la randomisation des bibliothÃ¨ques et le sandboxing aident Ã prÃ©venir les attaques destinÃ©es Ã capturer ou Ã modifier les logiciels systÃ¨me.

Firewall amÃ©liorÃ© : aprÃ¨s activation du nouveau firewall applicatif, ce dernier sâauto-configure afin que les utilisateurs profitent de sa protection sans devoir Ãªtre pour autant des experts en ports et en protocoles rÃ©seau.

ContrÃ´le dâaccÃ¨s obligatoire : des restrictions sont appliquÃ©es pour lâaccÃ¨s aux ressources systÃ¨me. Pas mÃªme un utilisateur Â« racine Â» compromis peut modifier des paramÃ¨tres.

Signature applicative : elle permet aux utilisateurs de vÃ©rifier lâintÃ©gritÃ© et lâidentitÃ© dâapplications prÃ©sentes sur le Mac.

ConnectivitÃ© encore plus fiable : le support du rÃ©seau privÃ© virtuel (VPN) a Ã©tÃ© amÃ©liorÃ© pour permettre des connexions Ã davantage de serveurs VPN parmi les plus utilisÃ©s, le tout sans logiciels supplÃ©mentaires.

Au mois dâaoÃ»t 2008, Apple a Ã©galement publiÃ© le Â« Mac OS X Security Configuration Guide Â», un guide sur la configuration de la sÃ©curitÃ© Ã la fois trÃ¨s dÃ©taillÃ© et prÃ©cieux pour tous ceux qui souhaitent verrouiller le systÃ¨me dâexploitation ou qui sont chargÃ©s de protÃ©ger le rÃ©seau de leur entreprise.

Cependant, comme lâÃ©crit Apple dans son propre dÃ©ni de responsabilitÃ© pour ce guide, il est important de disposer dâune certaine expÃ©rience pour utiliser lâinterface de ligne de commande de lâapplication Terminal dâApple.

Â« ***Comme quiconque travaillant dans le domaine de la sÃ©curitÃ© informatique le sait, aucun systÃ¨me dâexploitation nâest impÃ©nÃ©trable. Mais si pour certains professionnels de la sÃ©curitÃ©, la sÃ©curisation dâOS X apparaÃ®t comme un dÃ©fi, il sâagit bien plutÃ´t dâun simple manque de maÃ®trise du systÃ¨me***

dâ□□exploitation Â», dÃ©clare **Leif Krenkow**, Technical Account Manager chez Qualys.

Â« Ce guide (disponible ici) permet Ã coup sÃ»r de rÃ©soudre ce problÃ¨me. Il traite de tous les sujets, depuis lâ□□introduction Ã lâ□□architecture de la sÃ©curitÃ© dâ□□OS X, jusquâ□□Ã la gestion des comptes en passant par FileVault (chiffrement du disque du Mac), par la protection physique du matÃ©riel contre les attaques Ã base dâ□□Ã©coutes des radiofrÃ©quences et par la sÃ©curitÃ© Bluetooth.

Ce guide mÃ©rite toute lâ□□attention des utilisateurs dâ□□Apple, surtout sâ□□ils doivent garantir la sÃ©curitÃ© des systÃ¨mes Mac de leur environnement. Et mÃªme si personne ne prÃ©voit des attaques massives contre le systÃ¨me MAC OS X dans un avenir proche, il nâ□□est pas inutile de se prÃ©parer avant que cela finisse par se produire. Â»

A propos de Qualys

Qualys, Inc. est le principal fournisseur de solutions de gestion des risques pour la sÃ©curitÃ© et de conformitÃ© en mode Â« Ã la demande Â» - fournies comme un service. Les solutions en mode SaaS de Qualys peuvent Ãªtre dÃ©ployÃ©es Ã tout moment, nâ□□importe oÃ¹ dans le monde, et peuvent fournir aux clients une vue immÃ©diate de leur politique de sÃ©curitÃ© et de conformitÃ©.

Le service QualysGuardÂ® est utilisÃ© aujourd'hui par plus de 3.500 entreprises dans 85 pays, dont 35 issues de Â« Fortune Global 100 Â» et exÃ©cute plus de 200 millions de scans dâ□□adresses IP par an. Qualys dispose Ã©galement du plus grand dÃ©ploiement dâ□□outils de gestion des vulnÃ©rabilitÃ©s au sein des plus importantes entreprises mondiales (Fortune Global 50).

Qualys a Ã©tabli des accords stratÃ©giques avec les principaux fournisseurs de Â« managed services Â» et cabinets de conseils tels que BT, Etisalat, Fujitsu,'IBM, l(TS) 2, LAC, SecureWorks, Symantec, TELUS et VeriSign.

Pour plus d'informations