

SÃ©curitÃ© : Les conseils de Qualys pour bien sÃ©curiser Mac OS X

Mac et Linux

PostÃ© par : JulieM

PubliÃ© le : 10/12/2008 15:00:00

Depuis toujours, **Apple dÃ©clare que Mac OS X est suffisamment sÃ©curisÃ© pour se passer d'antivirus**. **Qualys® 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 d'Apple est en train de se dÃ©velopper Ã une vitesse fulgurante. Il y a encore quelques annÃ©es, Apple ne reprÃ©sentait qu'une faible partie du marchÃ© informatique. Aujourd'hui, grÃ¢ce au succÃ©s du systÃ©me d'exploitation OS X et des IMacs, Apple est devenu le troisiÃ©me plus important constructeur de PC avec une part de marchÃ© d'environ **8%**.



Ã

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

D'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 d'affaiblir la configuration du firewall.

De plus, les vulnÃ©rabilitÃ©s au sein du systÃ©me d'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 l'annÃ©e.



Mais en mati re de s curit , Apple ne reste pas les bras crois s. En effet, certaines nouvelles fonctionnalit s inh rentes   OS X 10.5, participant   la s curisation du syst me, ont  t  apport es   la version diffus e   l automne 2007 :

Taggage et avertissement lors de la premi re ex cution : Mac OS X 10.5 marque les fichiers qui sont t l charg s pour emp cher les utilisateurs d ex cuter par inadvertance des applications malveillantes qu ils ont t l charg es.

Protection runtime : de nouvelles technologies telles que la d sactivation de l ex cution, la randomisation des biblioth ques et le sandboxing aident   pr venir les attaques destin es   capturer ou   modifier les logiciels syst me.

Firewall am lior  : apr s activation du nouveau firewall applicatif, ce dernier s auto-configure afin que les utilisateurs profitent de sa protection sans devoir  tre pour autant des experts en ports et en protocoles r seau.

Contr le d acc s obligatoire : des restrictions sont appliqu es pour l acc s aux ressources syst me. Pas m me un utilisateur   racine   compromis peut modifier des param tres.

Signature applicative : elle permet aux utilisateurs de v rifier l int grit  et l identit  d applications pr sentes sur le Mac.

Connectivit  encore plus fiable : le support du r seau priv  virtuel (VPN) a  t  am lior  pour permettre des connexions   davantage de serveurs VPN parmi les plus utilis s, le tout sans logiciels suppl mentaires.

Au mois d ao t 2008, Apple a  galement publi  le   Mac OS X Security Configuration Guide  , un guide sur la configuration de la s curit    la fois tr s d taill  et pr cieux pour tous ceux qui souhaitent verrouiller le syst me d exploitation ou qui sont charg s de prot ger le r seau de leur entreprise.



Cependant, comme l  crit Apple dans son propre d ni de responsabilit  pour ce guide, il est important de disposer d une certaine exp rience pour utiliser l interface de ligne de commande de l application Terminal d Apple.

  **Comme quiconque travaillant dans le domaine de la s curit  informatique le sait, aucun syst me d exploitation n est imp n trable. Mais si pour certains professionnels de la s curit , la s curisation d OS X appara t comme un d fi, il s agit bien plut t d un simple manque de ma trise du syst me**

d  exploitation   , d  clare **Leif Krenkow**, Technical Account Manager chez Qualys.

   Ce guide (disponible ici) permet    coup s  r de r  soudre ce probl  me. Il traite de tous les sujets, depuis l  introduction    l  architecture de la s  curit   d  OS X, jusqu   la gestion des comptes en passant par FileVault (chiffrement du disque du Mac), par la protection physique du mat  riel contre les attaques    base d    coutes des radiofr  quences et par la s  curit   Bluetooth.

Ce guide m  rite toute l  attention des utilisateurs d  Apple, surtout s  ils doivent garantir la s  curit   des syst  mes Mac de leur environnement. Et m  me si personne ne pr  voit des attaques massives contre le syst  me MAC OS X dans un avenir proche, il n  est pas inutile de se pr  parer avant que cela finisse par se produire.   

A propos de Qualys

Qualys, Inc. est le principal fournisseur de solutions de gestion des risques pour la s  curit   et de conformit   en mode       la demande    - fournies comme un service. Les solutions en mode SaaS de Qualys peuvent   tre d  ploy  es    tout moment, n  importe o  ¹ dans le monde, et peuvent fournir aux clients une vue imm  diate de leur politique de s  curit   et de conformit  .

Le service QualysGuard   est utilis   aujourd'hui par plus de 3.500 entreprises dans 85 pays, dont 35 issues de    Fortune Global 100    et ex  cute plus de 200 millions de scans d  adresses IP par an. Qualys dispose   galement du plus grand d  ploiement d  outils de gestion des vuln  rabilit  s au sein des plus importantes entreprises mondiales (Fortune Global 50).

Qualys a   tabli des accords strat  giques avec les principaux fournisseurs de    managed services    et cabinets de conseils tels que BT, Etisalat, Fujitsu, IBM, I(TS) 2, LAC, SecureWorks, Symantec, TELUS et VeriSign.

[Pour plus d'informations](#)