BitDefender : Analyse lâ□□exploitation d'une nouvelle faille Adobe PDF
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 6/3/2009 15:00:00

Les spammeurs et les voleurs dâ□□informations trouvent tous les jours de nouvelles maniÃ¨res d'exploiter cette vulnÃ©rabilitÃ©
BitDefenderÂ® analyse lâ□□utilisation de **la derniÃ¨re faille touchant le format PDF dâ□□Adobe**, dÃ©couverte pour la toute premiÃ¨re fois le 4 novembre 2008.

L'analyse BitDefender a dÃ©montrÃ© que les principaux dangers qui affectent lâ□□utilisateur comprennent diffÃ©rents malwares :

Backdoor.Poisonivy.GK est une porte dÃ©robÃ©e qui permet au spammeur de se connecter Ã distance Ã l'ordinateur infectÃ© et d'exÃ©cuter des commandes non autorisÃ©es. Il surveille et enregistre Ã©galement toutes les applications et les versions des applications que la victime utilise.

Â

Trojan.Spammer.Tedroo.BA est un cheval de Troie qui transforme un ordinateur infectÃ© en un ordinateur envoyant du spam.

Trojan.Spy.Goldun.NEP, lui surveille les fenÃªtres Internet Explorer et vole les informations d'authentification des utilisateurs pour le systÃ¨me de paiement en ligne e-gold.

Pour plus de sÃ©curitÃ© et afin d'Ã©viter de telles atteintes Ã leur vie privÃ©e, nous recommandons aux utilisateurs de mettre Ã jour leurs solutions de sÃ©curitÃ©, ainsi que d'installer toutes les mises Ã jour de sÃ©curitÃ© Adobe existantes.

Depuis la diffusion de la mise Ã jour de sÃ©curitÃ© Adobe, on sait qu'**Adobe Reader 8** et Adobe **Acrobat 8** (versions antÃ©rieures Ã la 8.1.3) sont sujets Ã de multiples dÃ©nis de service et exploits. Ces informations essentielles nâ□□ont pas Ã©chappÃ© non plus ni aux spammeurs, ni aux voleurs dâ□□informations.

Le 6 novembre, la faille sur la fonction â□□util.printf()â□□ d'Adobe Ã©tait publiÃ©e et le lendemain, le premier cheval de Troie Ã©tait repÃ©rÃ© dans des spams et sur des sites Internet malicieux. DÃ©tectÃ© par BitDefender comme Exploit.PDF.A, le code JavaScrit Ã l'intÃ©rieur du PDF tentait de tÃ©lÃ©charger d'autres malwares Ã partir de l'adresse : http: // adxdnet.n [removed]un. php aprÃ¨s une exploitation rÃ©ussie.

Le code de commandes Ã©tait encodÃ© en caractÃ¨res ASCII en clair et exÃ©cutÃ© 5 secondes aprÃ¨s l'ouverture du document.

Plusieurs variantes de ce PDF malicieux sont apparues dans les mois suivants, modifiant le code d'exploitation et la charge utile.

Â

Des versions plus rÃ©centes contiennent du code cryptÃ©.

Une exploitation de faille pour la fonction â□□Collab.collectEmailInfo()â□□ a Ã©galement Ã©tÃ© ajoutÃ©e afin d'augmenter le taux d'infection.

Ã□ propos de BitDefenderÂ®

BitDefender est la sociÃ©tÃ© crÃ©atrice de lâ□□une des gammes de solutions de sÃ©curitÃ© la plus complÃ¨te et la plus certifiÃ©e au niveau international reconnues comme Ã©tant parmi les plus rapides et les plus efficaces du marchÃ©.

Depuis sa crÃ©ation en 2001, BitDefender nâ□□a cessÃ© dâ□□Ã©lever le niveau et dâ□□Ã©tablir de nouveaux standards en matiÃ¨re de protection proactive des menaces. Chaque jour, BitDefender protÃ¨ge des dizaines de millions de particuliers et de professionnels Ã travers le monde â□□ en leur garantissant une utilisation sereine et sÃ©curisÃ©e de lâ□□univers informatique.

Les solutions de sÃ©curitÃ© BitDefender sont distribuÃ©es dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiÃ©s. Dans les pays francophones, BitDefender est Ã©ditÃ© en exclusivitÃ© par Ã□ditions Profil.

Visitez le site