SÃ©curitÃ© : StoneGate IPS protÃ¨ge des derniÃ¨res failles Adobe et Microsoft
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 18/6/2010 15:00:00

Stonesoft, fournisseur innovant de solutions intÃ©grÃ©es de sÃ©curitÃ© rÃ©seau et de continuitÃ© de service, annonce aujourdâ□□hui que son **appliance StoneGate IPS** est non seulement capable de protÃ©ger efficacement les utilisateurs contre lâ□□exploitation des toutes derniÃ¨res vulnÃ©rabilitÃ©s du Flash Player, dâ□□Adobe Reader et dâ□□Acrobat mais Ã©galement contre celles des failles Microsoft.

Selon le dernier bulletin de sÃ©curitÃ© Ã©mis par Adobe le 10 juin 2010, la toute derniÃ¨re vulnÃ©rabilitÃ© (CVE-2010-1297) pourrait propager une infection et permettre au pirate de prendre le contrÃ´le du systÃ¨me touchÃ©. La ruse consiste Ã persuader un utilisateur dâ□□ouvrir un PDF contenant du code malveillant. Le code malveillant sâ□□exÃ©cute, attaque le poste de lâ□□utilisateur via le navigateur web et provoque alors de graves dÃ©gÃ¢ts. On dit que ces vulnÃ©rabilitÃ©s sont largement exploitÃ©es Â« dans la nature Â» et ciblent notamment Adobe Flash Player, Adobe Reader et Acrobat.

STONESOFT

Secure Information Flow

De la mÃªme faÃ§on, pour lâ□□exploitation dâ□□une faille Microsoft, lâ□□utilisateur est dirigÃ© vers une page web de tÃ©lÃ©chargement, qui se sert du programme dâ□□aide Windows pour pÃ©nÃ©trer le poste client. Si lâ□□exploit rÃ©ussit, le cybercriminel peut, Ã distance, exÃ©cuter des commandes arbitraires grÃ¢ce aux droits administrateurs sur lesquels il a pris le contrÃ´le.

Lâ□□appliance StoneGate IPS dÃ©livre une protection efficace contre lâ□□ensemble des menaces mentionnÃ©es ci-dessus. Lâ□□appliance sait identifier et stopper les attaques au moment oÃ¹ la page web ou le PDF sont ouverts et/ou tÃ©lÃ©chargÃ©s. Le systÃ¨me StoneGate sait aussi arrÃªter les emails qui contiennent le PDF, en piÃ¨ces jointes. Il sait Ã©galement, lorsque le plus haut niveau de protection est activÃ©, empÃªcher le tÃ©lÃ©chargement de tout contenu Adobe Flash. Ainsi, lâ□□ensemble des clients utilisant la solution StoneGate IPS pour la protection de leur rÃ©seau ne risque pas dâ□□Ãªtre touchÃ© par ces vulnÃ©rabilitÃ©s.

Les derniÃ¨res failles Adobe et Microsoft sont autant dâ□□exemples dâ□□attaques survenant

cÃ´tÃ© client, attaques qui se multiplient chaque jour. Elles sont particuliÃ¨rement dangereuses : en effet, elles pÃ©nÃ¨trent via les firewalls traditionnels et touchent un trÃ¨s grand nombre dâutilisateurs. Lorsque ces attaques sont correctement menÃ©es, elles permettent non seulement aux pirates de lire et de modifier nâimporte quel fichier mais Ã©galement de dÃ©rober des informations personnelles comme des identifiants et/ou des mots de passe. Les hÃ´tes corrompus sont Ã©galement intÃ©grÃ©s Ã des rÃ©seaux de botnets (PC zombies).

Selon **LÃ©onard Dahan**, country manager Stonesoft France et Benelux : Â« *ces vulnÃ©rabilitÃ©s ont commencÃ© Ã Ãªtre exploitÃ©es avant mÃªme que des correctifs de sÃ©curitÃ© aient Ã©tÃ© publiÃ©s. Il est donc extrÃªmement difficile de prÃ©server les hÃ´tes de ces attaques sans un Ã©quipement supplÃ©mentaire comme la solution StoneGate IPS* Â»

Â« *MalgrÃ© la crise financiÃ¨re que nous traversons actuellement, les malwares continuent de se rÃ©pandre via Internet. Les entreprises ne doivent donc pas Ã©conomiser sur la sÃ©curitÃ©. Nettoyer un rÃ©seau est toujours plus coÃ»teux que de se prÃ©munir contre les attaques. Les entreprises nâÃ©tant pas Ã©quipÃ©es dâun systÃ¨me de prÃ©vention des intrusions devront dâabord la facture correspondant au nettoyage du rÃ©seau puis y installer un IPS. Les clients StoneGate IPS sont donc intÃ©gralement protÃ©gÃ©s contre les menaces en mouvement et peuvent ainsi se concentrer sur leur activitÃ©* Â» continue **LÃ©onard Dahan**.