BitDefender : Listes des pays les plus touchÃ©s par les malwares Zbot
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 15/1/2010 15:00:00

13 % des systÃ¨mes aux Ã□tats-Unis sont infectÃ©s par le Â« cocktail Â» de malwares explosif â□□Zbotâ□□ Ces infections montent en flÃ¨che en **ciblant les utilisateurs de Microsoft Office Outlook Web Access**

BitDefenderÂ®, Ã©diteur de solutions de sÃ©curitÃ© antimalwares met en garde aujourdâ□□hui contre la rapide diffusion de malwares conÃ§us pour les utilisateurs de Microsoft Office Outlook Web Access.

Le message non sollicitÃ© invite les utilisateurs Ã Â« appliquer une nouvelle configuration Â» Ã leur boÃ®te de rÃ©ception afin de mettre Ã jour plusieurs Â« Mises Ã niveau de sÃ©curitÃ© Â» qui sont disponibles. Le lien de l'e-mail conduit vers une page Web avec les logos de Microsoft Office et demande aux utilisateurs de tÃ©lÃ©charger et de lancer un fichier exÃ©cutable censÃ© mettre Ã jour les paramÃ¨tres de leur messagerie.

Au lieu de cela, ils reÃ§oivent un puissant Â« cocktail de malwares Â» comprenant Trojan.SWF.Dropper.E, nom gÃ©nÃ©rique dâ□□une famille de chevaux de Troie au comportement similaire : il sâ□□agit de fichiers Flash qui nâ□□affichent habituellement aucune animation/image particuliÃ¨re mais dÃ©posent et exÃ©cutent plusieurs fichiers malveillants (en exploitant la vulnÃ©rabilitÃ© Shockwave Flash de logiciels Adobe). Les fichiers dÃ©posÃ©s sont susceptibles dâ□□Ã©voluer (diffÃ©rentes variantes peuvent dÃ©poser et exÃ©cuter diffÃ©rents programmes malveillants).

Les statistiques indiquent une augmentation importante du nombre de fichiers infectÃ©s par Trojan.SWF.Dropper.E. Une comparaison entre la premiÃ¨re moitiÃ© du mois de janvier et la premiÃ¨re moitiÃ© du mois de dÃ©cembre rÃ©vÃ¨le une augmentation du nombre total de fichiers infectÃ©s de presque 60 %.

Les pays les plus touchÃ©s par Trojan.SWF.Dropper.E entre le 1er et le 13 janvier sont les suivants :

PaysÂ et % des systÃ¨mes infectÃ©s

Ã□tats-Unis 13 - Espagne 11 - France 9 - Roumanie 9 - Canada 5 - Royaume-Uni 3 - Australie 3 - Allemagne 3 - ThaÃ¯lande 3 - Turquie 2 - Autres pays 39

Lâ□□attaque comprenait Ã©galement dâ□□autres malwares prolifiques parmi lesquels :

1) Lâ□□un des plus anciens chevaux de Troie - Trojan.Spy.ZBot.EKF, largement utilisÃ© dans la campagne de diffusion de malwares liÃ©e au virus AH1N1.

Zbot injecte du code dans plusieurs processus et ajoute des exceptions au Pare-feu MicrosoftÂ® WindowsÂ®, offrant ainsi des fonctionnalitÃ©s de backdoor et de serveur aux pirates. Il envoie Ã©galement des informations sensibles et surveille diffÃ©rents ports, Ã lâ□□Ã©coute dâ□□une Ã©ventuelle exÃ©cution distante de commande par des pirates. Les derniÃ¨res variantes peuvent aussi dÃ©rober des informations bancaires, des donnÃ©es de connexion, lâ□□historique des sites Web visitÃ©s et dâ□□autres Ã©lÃ©ments saisis par lâ□□utilisateur. Elles prennent Ã©galement des captures dâ□□Ã©cran du bureau de la machine compromise.

2) Exploit.HTML.Agent.AM, qui utilise les vulnÃ©rabilitÃ©s permettant dâ□□exÃ©cuter arbitrairement du code en chargeant un objet flash spÃ©cialement construit dans une page Web. Une fois quâ□□une page Web infectÃ©e est ouverte, le cheval de Troie crÃ©e un objet SWF spÃ©cialement conÃ§u permettant lâ□□exÃ©cution dâ□□une charge utile (au moment oÃ¹ nous rÃ©digeons cet article, le fichier tÃ©lÃ©chargÃ© est dÃ©tectÃ© sous le nom de Trojan.Spy.ZBot.EKG, mais cela est susceptible de changer).

Les donnÃ©es fournies par le systÃ¨me Â« RTVR Â», Reporting des Virus en Temps RÃ©el de BitDefender, permettent de se faire une idÃ©e de lâ□□importance de la diffusion de ce malware : aux Ã□tats-Unis, le nombre de fichiers infectÃ©s a augmentÃ© de 10 %t pendant la premiÃ¨re moitiÃ© du mois de janvier, alors quâ□□en Espagne, lâ□□augmentation a Ã©tÃ© de plus de 400% en comparaison avec la seconde moitiÃ© du mois de dÃ©cembre.

3) Exploit.PDF-JS.Gen, est le nom gÃ©nÃ©rique de fichiers PDF spÃ©cialement conÃ§us exploitant diffÃ©rentes vulnÃ©rabilitÃ©s dÃ©tectÃ©es dans le moteur Javascript de PDF Reader, afin dâ□□exÃ©cuter du code malveillant sur les ordinateurs des utilisateurs.

Les donnÃ©es de BitDefender indiquent Ã©galement une progression pour Exploit.PDF-JS.Gen. Les deux premiÃ¨res semaines de janvier ont rÃ©vÃ©lÃ© que les systÃ¨mes les plus touchÃ©s Ã©taient ceux des Ã□tats-Unis, de lâ□□Espagne et du Canada.

Afin de profiter dâ□□Internet en toute sÃ©curitÃ©, BitDefender recommande aux utilisateurs de ne jamais cliquer sur les liens contenus dans des messages provenant dâ□□expÃ©diteurs inconnus et leur conseille Ã©galement dâ□□installer et de mettre Ã jour une solution antimalware complÃ¨te. Les utilisateurs doutant de lâ□□efficacitÃ© de leur solution antimalware peuvent vÃ©rifier gratuitement que leur ordinateur nâ□□a pas de virus avec **BitDefender online scanner, disponible aussi sur notre site**.