BitDefender : Faux billets d'avion pour vrais malwares
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 18/9/2008 0:00:00

Un malware utilise des noms de compagnies aÃ©riennes amÃ©ricaines pour se propager
Suite au bombardement de faux billets Ã©lectroniques de **JetBlue Airways** cet Ã©tÃ©, les crÃ©ateurs de malwares ont lancÃ© une offensive de Trojan via des messages frauduleux prÃ©sentant une utilisation abusive des identitÃ©s des principales compagnies aÃ©riennes.

Â

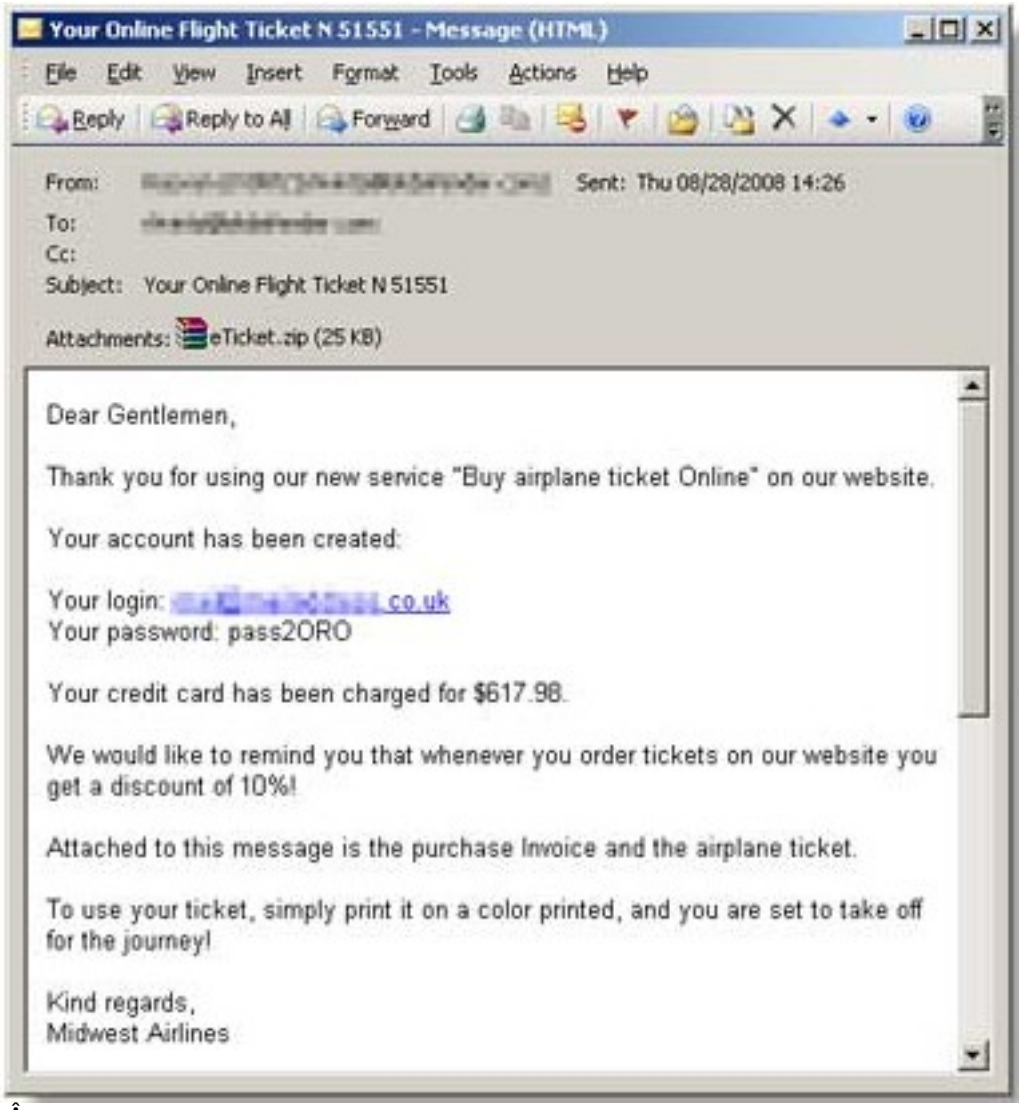
Ces deux derniÃ¨res semaines, les messageries du monde entier ont Ã©tÃ© inondÃ©es par une nouvelle campagne de spam prÃ©tendant dÃ©livrer des billets Ã©lectroniques et des factures aux clients prÃ©sumÃ©s dâ□□un service intitulÃ© Â« **Achat de billets dâ□□avion en ligne** Â», sauf que derriÃ¨re les archives zip apparemment inoffensives, se trouve dissimulÃ©e une nouvelle sÃ©rie de malwares amÃ©liorÃ©s.

Avec la fin de la pÃ©riode estivale et la rentrÃ©e, les auteurs de la vague de spam de cet Ã©tÃ©, ont probablement souhaitÃ© lui donner une seconde chance, avec le mÃªme modÃ¨le utilisÃ© et diffusÃ© massivement â□□ mais avec des compagnies aÃ©riennes diffÃ©rentes et quelques codes malicieux supplÃ©mentaires.

Au lieu de lâ□□identitÃ© dÃ©tournÃ©e de jetBlue Airways de ce mois de juillet, avec lâ□□automne, dâ□□autres compagnies aÃ©riennes ont Ã©tÃ© mises sous les projecteurs : Delta Air Lines, Virgin America, United Airlines, Continental Airlines, mais Ã©galement SouthWest Airlines, Northwest Airlines, Midwest Airlines, etc.

Prenez Ã©galement garde aux messages contrefaits envoyÃ©s au nom dâ□□opÃ©rateurs aux consonances plus exotiques : Sun Country Airlines, Spirit Airlines, Allegiant Air, Frontier Airlines, AirTran Airlines, Hawaiian Airlines et Alaska Airlines.

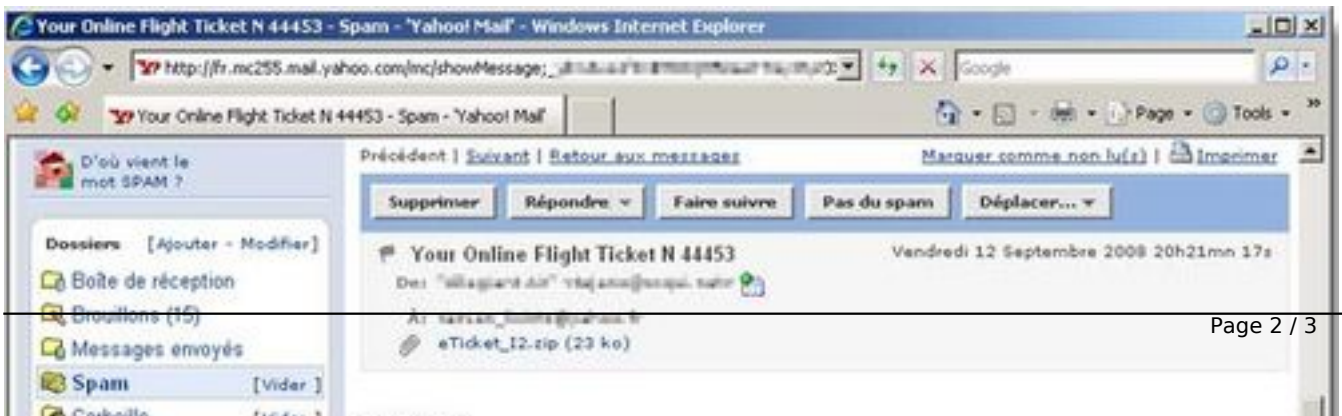
Comme un goÃ»t de dÃ©jÃ vu, nous avons les malwares Â« **habituels** Â» **Trojan.Spy.Zbot.KJ** et **Trojan.Spy.Wsnpoem.HA** - vous vous en souvenez probablement quand nous vous les avions prÃ©sentÃ©s lors des faux e-mails UPS et FedEx -, sans oublier le Â« challenger Â» **Trojan.Injector.CH**.



Â

Les anciens comme les nouveaux malwares ont des composants de rootkits leur permettant de sâ□□installer et de se cacher sur la machine infectÃ©e soit dans le rÃ©pertoire Windows, soit dans le rÃ©pertoire Program Files.

Ils injectent leur code dans plusieurs processus et ajoutent des exceptions aux rÃ¨gles du Pare-feu MicrosoftÂ® WindowsÂ®, offrant des fonctionnalitÃ©s de backdoor et de serveur. Tous envoient des informations sensibles et surveillent les diffÃ©rents ports du Pare-feu Ã lâ□□Ã©coute dâ□□une Ã©ventuelle commande de pirates.



Â

Les Trojans tentent Ã©galement de se connecter et de tÃ©lÃ©charger des fichiers Ã partir de serveurs ayant des noms de domaines apparemment enregistrÃ©s en Russie.

â***Les utilisateurs doivent savoir que sans une solution de sÃ©curitÃ© appropriÃ©e, lâintÃ©gritÃ© de leur systÃ¨me est exposÃ©e Ã un risque trÃ¨s important.***

Les Trojans distribuÃ©s via cette nouvelle campagne et lâimportant taux dâinfection prouvent une fois encore, non pas seulement lâingÃ©niositÃ© des auteurs de malwares, mais Ã©galement le peu dâintÃ©rÃªt portÃ© par les utilisateurs aux systÃ¨mes de dÃ©fense et de protection des donnÃ©es sensibleâ, a dÃ©clarÃ© **Sorin Dudea**, Directeur de la recherche Antimalware de BitDefenderÂ®.

Visitez le site de BitDefender