BitDefender : Des vagues de spams sur FaceBook et MySpace
Internet
PostÃ© par : JerryG
PubliÃ©e le : 13/4/2010 0:00:00

Des vagues de **spams inondent deux des rÃ©seaux sociaux les plus populaires** avec une frÃ©quence pouvant atteindre 500 messages toutes les 10 minutes

Câ□□est de nouveau lâ□□heure du spam ! La lÃ©gÃ¨re diffÃ©rence avec les campagnes prÃ©cÃ©dentes, est que le volume est beaucoup plus important tant en termes de messages envoyÃ©s que de cibles potentiellement touchÃ©es. Cette dÃ©ferlante atteint cette fois une taille critique qui pourrait sâ□□avÃ©rer dâ□□autant plus nuisible quâ□□elle charrie avec elle un ensemble de malwares.

Ces campagnes jumelles sont Â« nÃ©es sous le mÃªme thÃ¨me Â», une fausse demande de modification de mot de passe. Que ce soit sur FacebookÂ® ou sur MySpaceâ□¢, les utilisateurs sont informÃ©s que leur mot de passe a Ã©tÃ© modifiÃ©, en consÃ©quence de quoi, ils sont cordialement invitÃ©s Ã ouvrir le fichier .Zip attachÃ© au message afin de dÃ©couvrir le nouveau mot de passe qui leur a Ã©tÃ© assignÃ©.

Fig 1 : les e-mails servant dâ□□ Â« appÃ¢ts Â» pour FacebookÂ® et MySpaceâ□¢

Â« Un clic plus tard Â», cette expression pourrait bien laisser un gout amer dans la bouche de ceux qui ouvriront effectivement la piÃ¨ce jointe de ces emails, et dans les deux cas, la surprise pour eux se prÃ©sentera sous la forme dâ□□un code malveillant.

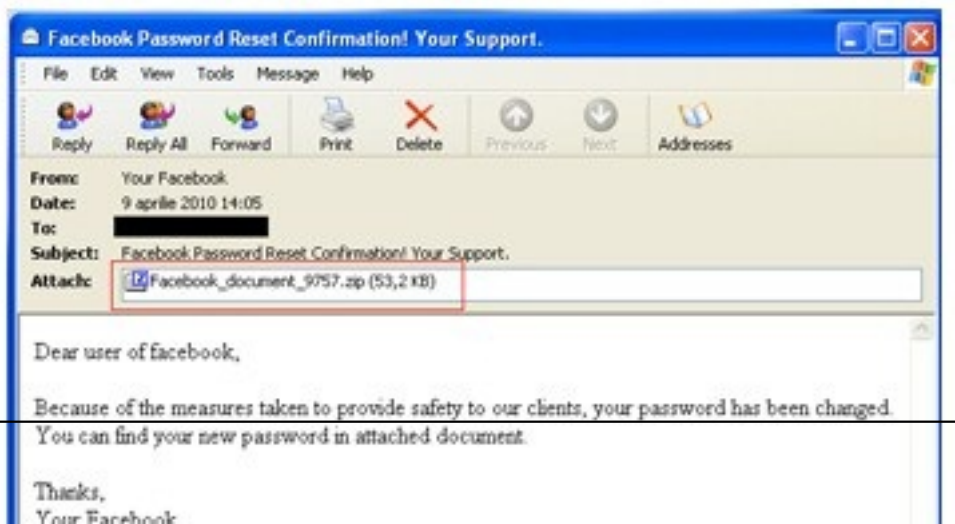
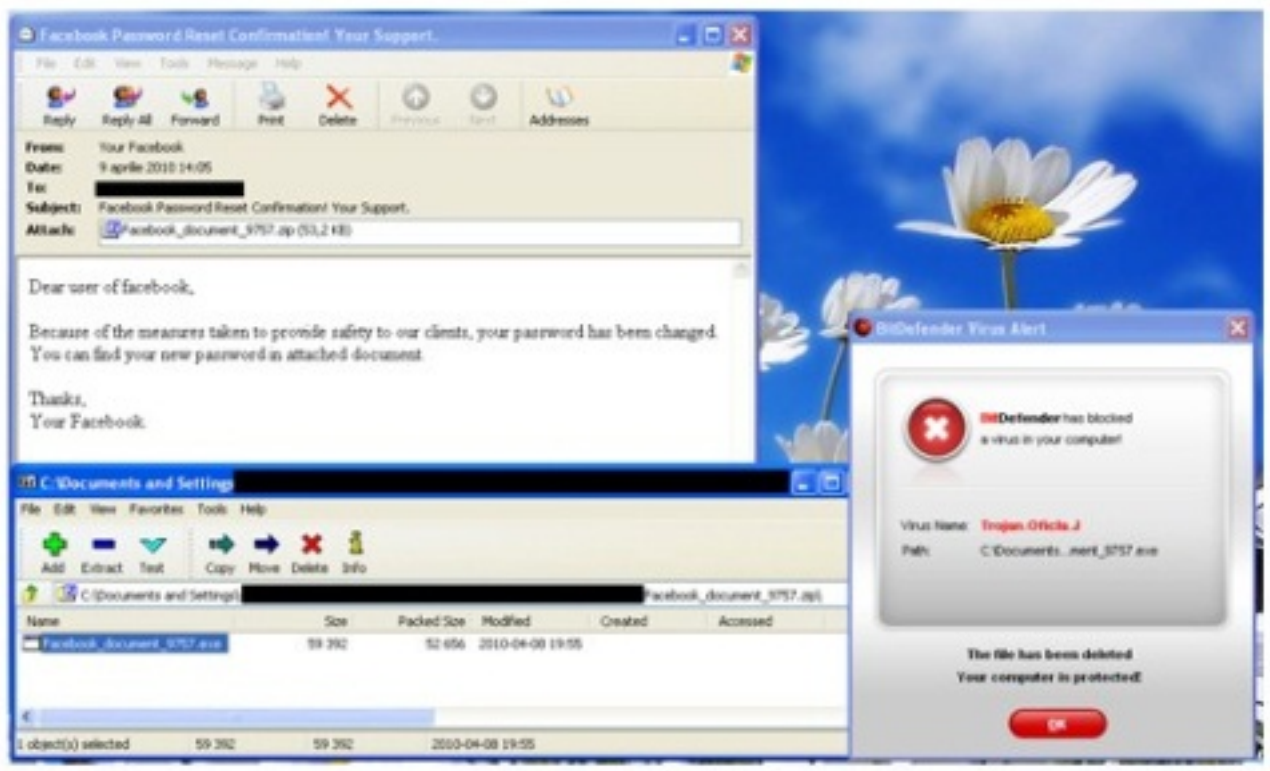


Fig 2 : Le Trojan envoyÃ© pendant la campagne qui a touchÃ© FacebookÂ®

En lieu et place du mot de passe promis, le fichier .Zip qui arrive dans les boÃ®tes e-mails des utilisateurs Facebook contient Â« Trojan.Oficla.J Â». Ce malware contient des codes malveillants qui sont dÃ©posÃ©s et installÃ©s sur le systÃ¨me. Il permet lâ□□ouverture dâ□□une porte dÃ©robÃ©e Â« backdoor Â» autorisant un accÃ¨s distant et clandestin aux systÃ¨mes infectÃ©s.

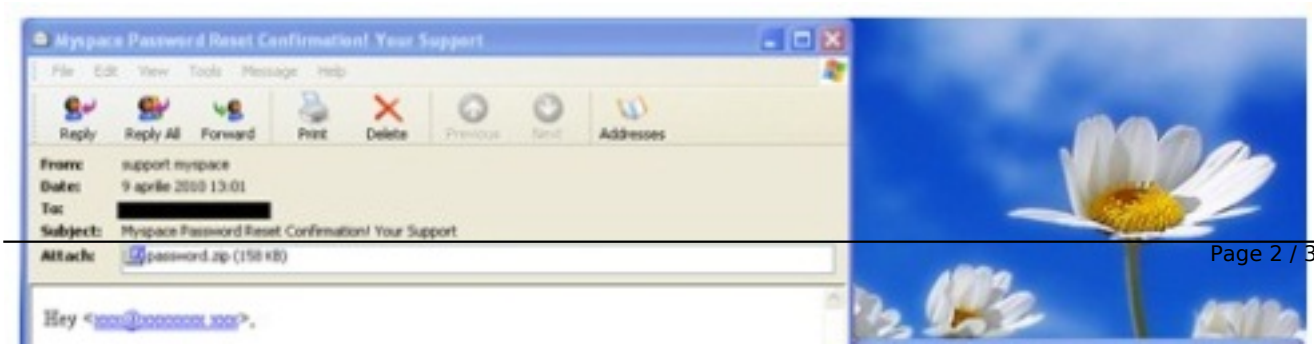


Cette backdoor pourra ensuite Ãªtre utilisÃ©e par des cybercriminels pour installer dâ□□autres logiciels indÃ©sirables ou malveillants sur lâ□□ordinateur de la victime.

Fig. 4 Les utilisateurs de MySpaceâ□¢ auront la surprise dâ□□Ãªtre infectÃ©s par un faux antivirus (rogue)

Les utilisateurs de MySpaceâ□¢ recevront un autre type de malware : un faux antivirus (rogue).

Le comportement de Trojan.Fakealert.BZZ est comparable Ã celui de tout autre rogue. La fenÃªtre du navigateur se rÃ©duit automatiquement et un message dâ□□alerte sâ□□affiche en parallÃ¨le. Ce message prÃ©vient lâ□□utilisateur que son ordinateur est infectÃ© par des soit-disant menaces et lâ□□avertit quâ□□il est nÃ©cessaire dâ□□installer une solution de sÃ©curitÃ©.



Que ce soit en cliquant sur les boutons Â« Ok Â» ou Â« Annuler Â» des diffÃ©rentes fenÃªtres pop-up qui apparaissent Ã lâ□□Ã©cran, lâ□□utilisateur activera une analyse antivirus factice. Ce processus imite une analyse classique et dÃ©tecte une multitude de malwares sur le systÃ¨me, alors que dans le mÃªme temps, une fausse pop-up tente de tromper lâ□□utilisateur en lui demandant de tÃ©lÃ©charger un programme malicieux, en le faisant passer pour lâ□□antivirus.

Avec chacune de ces prÃ©tendues analyses, le nombre dâ□□annonces dâ□□infections augmente et lâ□□utilisateur est mis sous pression afin de le pousser Ã tÃ©lÃ©charger le faux antivirus (rogue). Une fois installÃ©, il modifie ou endommage irrÃ©mÃ©diablement le contenu de nombreux fichiers systÃ¨me, et active de nombreuses pop-up annonÃ§ant de faux problÃ¨mes systÃ¨me et de fausses infections, tout en continuant de demander Ã lâ□□utilisateur dâ□□acheter ou de renouveler une licence.