Des vagues de spams déferlent sur FaceBook® et MySpace™

Des vagues de spams inondent deux des réseaux sociaux les plus populaires avec une fréquence pouvant atteindre 500 messages toutes les 10 minutes.

C’est de nouveau l’heure du Spam ! La légère différence avec les campagnes précédentes, est que le volume est beaucoup plus important tant en terme de messages envoyés que de cibles potentiellement touchées. Cette déferlante atteint cette fois une taille critique qui pourrait s’avérer d’autant plus nuisible qu’elle charrie avec elle un ensemble de malware.

Ces campagnes jumelles sont « nées sous le même thème », une fausse demande de modification de mot de passe. Que ce soit sur Facebook® ou sur MySpace™, les utilisateurs sont informés que leur mot de passe a été modifié, en conséquence de quoi, ils sont cordialement invités à ouvrir le fichier .Zip attaché au message afin de découvrir le nouveau mot de passe qui leur a été assigné.

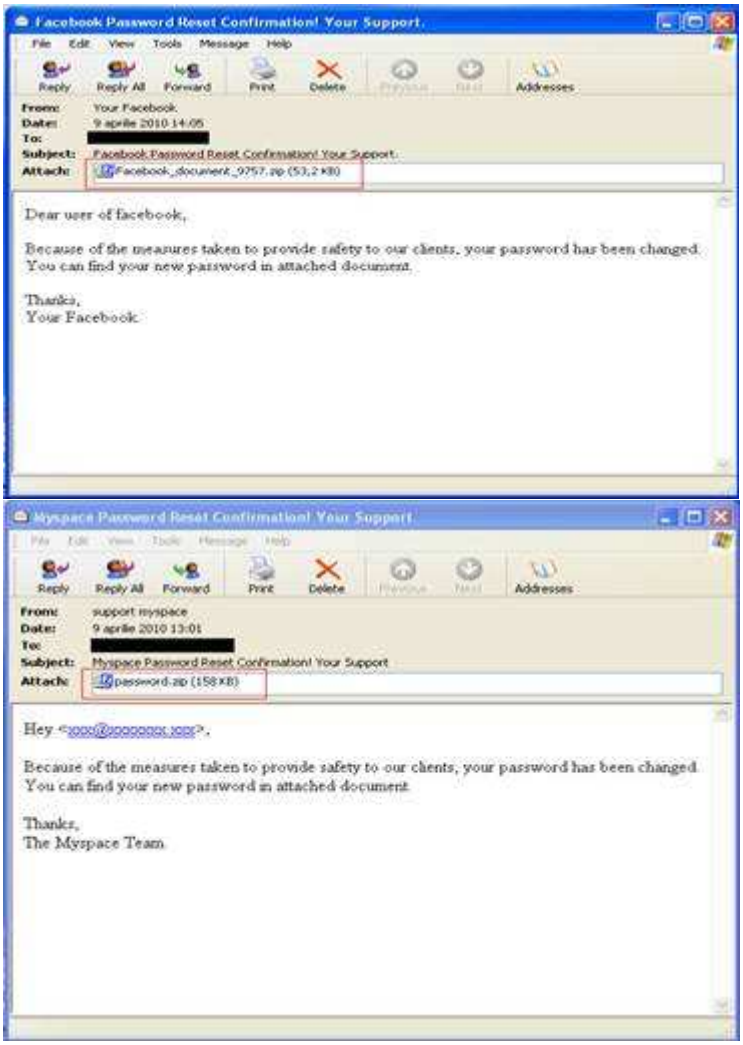

Fig 1 : les e-mails servant d'"appâts" pour Facebook et MySpace

« Un clic plus tard », cette expression pourrait bien laisser un gout amer dans la bouche de ceux qui ouvriront effectivement la pièce jointe de ces emails, et dans les deux cas, la surprise pour eux se présentera sous la forme d'un code malveillant.

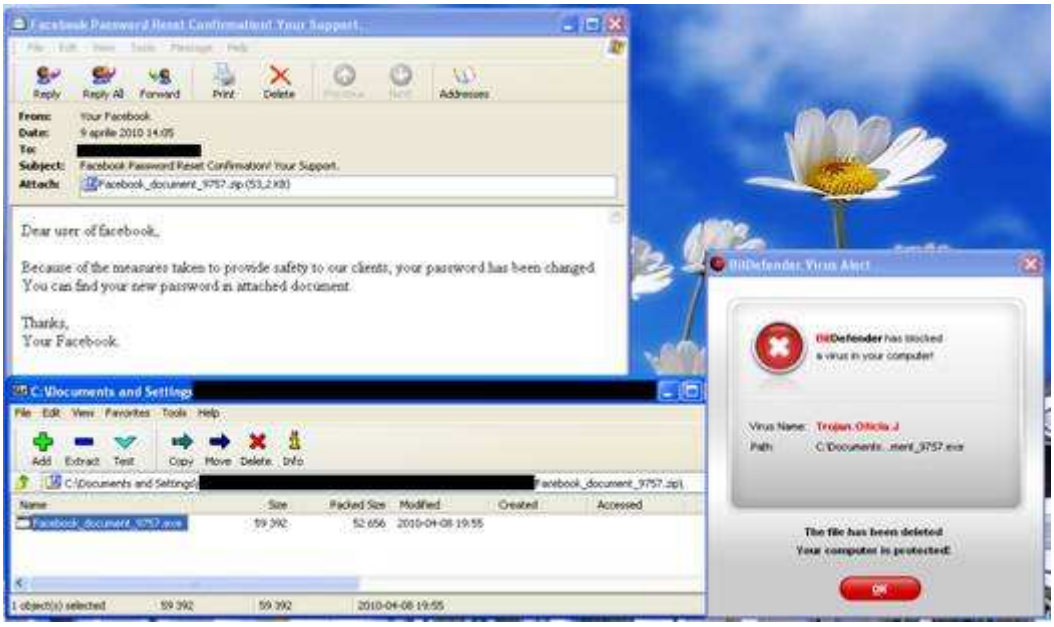

Fig 2 : Le Trojan envoyé pendant la campagne qui a touché Facebook®

En lieu et place du mot de passe promis, le fichier .Zip qui arrive dans les boîtes e-mail des utilisateurs Facebook contient « Trojan.Oficla.J ». Ce malware contient des codes malveillants qui sont déposés et installés sur le système touché. Il permet l'ouverture d'une porte dérobée « backdoor » autorisant un accès distant et clandestin aux systèmes infectés. Cette backdoor pourra ensuite être utilisée par des cybercriminels pour installer d'autres logiciels indésirables ou malveillants sur l'ordinateur de la victime.

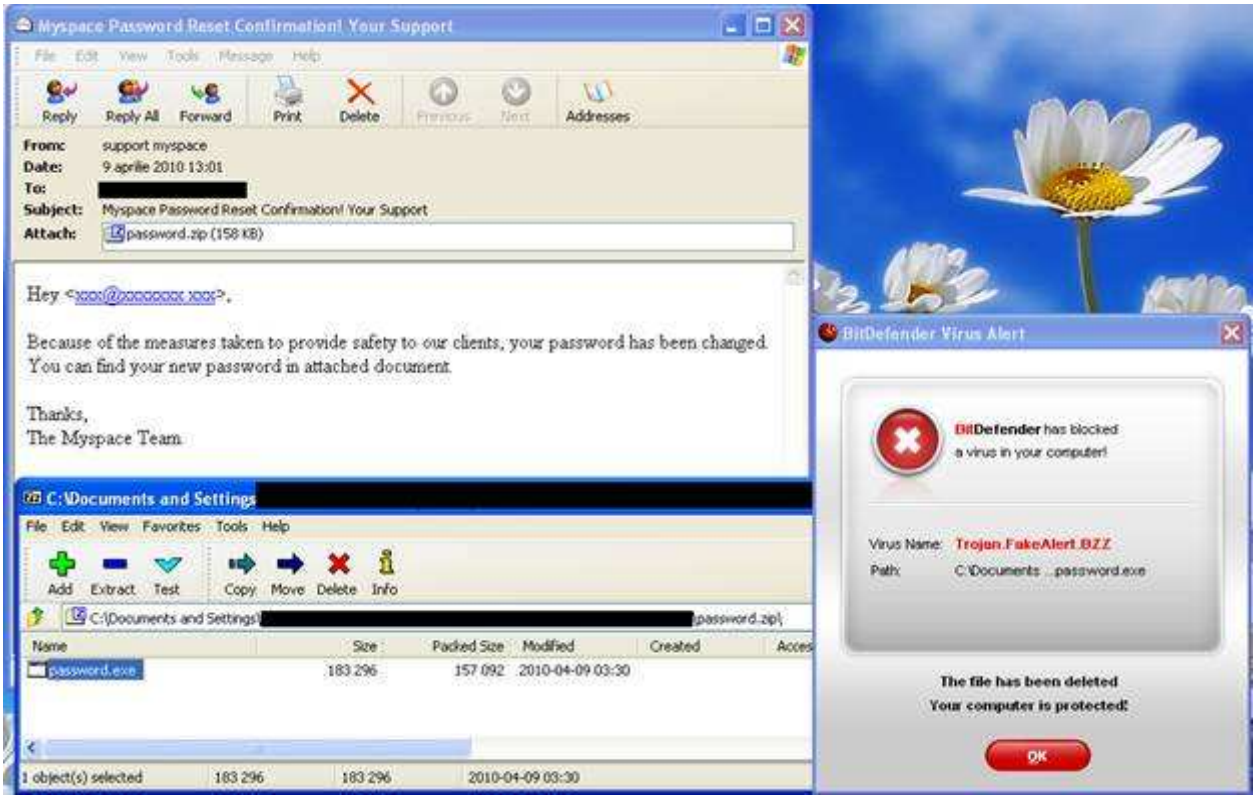

Fig. 4 Les utilisateurs de MySpace™ auront la surprise d'être infectés par un faux antivirus (rogue)

Les utilisateurs de MySpace™ recevront un autre type de malware : un faux antivirus (rogue).

Le comportement de Trojan.Fakealert.BZZ est comparable à celui de tout autre rogue. La fenêtre du navigateur se réduit automatiquement et un message d'alerte s'affiche en parallèle. Ce message prévient l'utilisateur que son ordinateur est infecté par des soit disant menaces et l'avertit qu'il est nécessaire d'installer une solution de sécurité.

Que ce soit en cliquant sur les boutons « Ok » ou « Annuler » des différentes fenêtres pop-up qui apparaissent à l'écran, l'utilisateur activera une analyse antivirus factice. Ce processus imite une analyse classique et détecte une multitude de malwares sur le système, alors que dans le même temps, une fausse pop-up tente de tromper l'utilisateur en lui demandant de télécharger un programme malicieux, en le faisant passer pour l'antivirus.

Avec chacune de ces prétendues analyses, le nombre d'annonces d'infections augmente et l'utilisateur est mis sous pression afin de le pousser à télécharger le faux antivirus (rogue). Une fois installé, il modifie ou endommage irrémédiablement le contenu de nombreux fichiers système, et active de nombreuses pop-up annonçant de faux problèmes système et de fausses infections, tout en continuant de demander à l'utilisateur d'acheter ou de renouveler une licence.