Le ver qui touche MySpace fera-t-il trembler la Toile?

Le site de '*social networking*' **MySpace.com** est la cible de ce que les experts en sécurité appellent *« une recrudescence suspecte d'activité ».* Le réseau est en effet ciblé par un ver qui vole les identifiants des utilisateurs du site de partage de vidéo.

« Ce ver contamine les profils MySpace avec une grande efficacité. Sur 150 profils scannés près d'un tiers étaient infectés », déclare Christopher Boyd, directeur des recherches de sécurité de FaceTime Communications.

MySpace, détenu par News Corp, compte **73 millions d'utilisateurs** enregistrés. La menace est donc prise très au sérieux, d'autant qu'elle semble difficile à éradiquer.

Le ver en question utilise une faille dans le '*cross scripting*' de MySpace, une vulnérabilité découverte il y a deux semaines. Il se sert également d'une fonction dans le lecteur multimédia d'Apple QuickTime.

Cet exploit commence par la visite d'un usager sur un profil Myspace infecté et contenant une vidéo au format QuickTime. Une fois en marche, la vidéo charge un code JavaScript qui permet d'agir sur le profil et de le modifier via un petit menu.

Une fonction QuickTime, nommée le '*HREF track*', peut obliger le lecteur à utiliser des commandes JavaScript pour charger des pages Web dans une fenêtre classique ou un moteur de recherche.

Cette fonctionnalité de QuickTime trouve aussi une utilisation légitime, mais comme le souligne Ross Paul, senior product manager chez Websense : « *Il y a de nombreuses technologies dont la fonction est détournée par et pour les pirates* »(ndlr: par exemple la virtualisation).

Si l'utilisateur du site clique sur une option dans le menu buggué, il est renvoyé vers une fausse page de log hébergée sur un autre serveur où ses détails personnels sont récupérés par un pirate.

Ce ver placé dans une vidéo au format QuickTime contamine tous les utilisate urs qui se rendent sur ledit profil. Qui plus est, ce code a également été conçu pour diffuser du spam à la liste de contact de la personne dont le poste est infecté.

Ces messages de 'spam' se font passer pour un film pornographique, mais ils contiennent en réalité un lien vers un site qui héberge du 'adware' de la société Zango, ex 180 solutions, une société bien connue de la justice qui a été condamnée par la FTC (*US Federal Trade Comission*) à payer une douloureuse de 3 millions de dollars suite à des plaintes pour avoir installé des 'adware' sur des postes sans l'autorisation de l'utilisateur.

Cette nouvelle affaire met en exergue le fait que la condamnation de 180 solutions n'a pas été assez forte et qu'il devient primordial de prendre des mesures encore plus fermes contre cette société qui aime jouer avec le feu.

D'après Boyd, certains utilisateurs plus expérimentés ont réussi à supprimer le ver JavaScript

manuellement, mais ce dernier s’est réinstallé automatiquement, car certains de leurs amis avaient des profils également infectés.