BitDefender : Nouvelle utilisation simultanÃ©e de plusieurs techniques de spams
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 9/10/2008 15:00:00

Les spammeurs tentent de piÃ©ger les utilisateurs en les poussant Ã confirmer la validitÃ© de leur adresse e-mail.
Les chercheurs des laboratoires BitDefender ont dÃ©tectÃ© une nouvelle vague de spams de produits pharmaceutiques et autres â□□â□□**remÃ¨des**â□□â□□ visant Ã amÃ©liorer les performances sexuelles. La nouveautÃ© de cette campagne de spams tient dâ□□une part Ã son amplitude et dâ□□autre part au mixage de plusieurs technique de confirmation dâ□□adresses e-mail suite Ã ces messages non sollicitÃ©s.

Â

La premiÃ¨re technique vise Ã exploiter une caractÃ©ristique commune Ã la plupart des logiciels de messagerie - les accusÃ©s de rÃ©ception ou avis de lecture. Dans les conditions dâ□□utilisation normales les accusÃ©s de rÃ©ception servent Ã confirmer la rÃ©ception et la lecture dâ□□un message.

Dans le cas de campagnes massives de spams, cela sert uniquement Ã confirmer aux spammeurs la validitÃ© de lâ□□adresse visÃ©e.

Si lâ□□utilisateur se doute de quelque chose et choisit de ne pas envoyer dâ□□accusÃ© de rÃ©ception, les spammeurs ont mis en place une deuxiÃ¨me technique pour valider lâ□□adresse e-mail : un lien vers une image stockÃ©e sur un serveur distant. Les clients de messagerie bloquent

gÃ©nÃ©ralement ce type de contenu.

Pour la visualiser les utilisateurs doivent donc accepter le chargement de lâ□□image ce qui revient Ã confirmer la lecture de lâ□□e-mail en question.

Â

DerniÃ¨re technique mais non des moindres, si les deux niveaux de confirmation prÃ©cÃ©dents ont Ã©chouÃ©, un troisiÃ¨me niveau peut sâ□□avÃ©rer efficace, particuliÃ¨rement quand les utilisateurs rÃ©alisent quâ□□ils sont tombÃ©s dans le piÃ¨ge en ouvrant un spam et quâ□□ils ne connaissent pas le â□□classiqueâ□□ faux lien de dÃ©sinscription.

Bien entendu, le prÃ©tendu lien de dÃ©sinscription ne permet pas de sortir de la base dâ□□e-mails, mais sert une nouvelle fois Ã confirmer la validitÃ© de lâ□□adresse e-mail, ce qui la rend dâ□□autant plus sujette Ã recevoir des vagues de spam encore plus nombreuses.

Pour se prÃ©munir contre les spams, voici quelques recommandations Ã suivre :

- Installer, activer et mettre Ã jour une solution de sÃ©curitÃ© anti-malware, antispam et antiphishing.
- Ne pas activer la confirmation automatique de lecture des e-mails dans votre client de messagerie.
- Toujours effacer les messages de spam et ne pas les conserver; si vous ouvrez par erreur lâ□□un dâ□□entre eux ou affichez une image ou cliquez sur un des liens quâ□□il contient, cela revient Ã confirmer la validitÃ© de votre adresse e-mail, ce qui dâ□□une part vous expose Ã recevoir encore plus de spams et dâ□□autre part peut provoquer lâ□□installation dâ□□un malware.
- Nâ□□ouvrez pas les e-mails et les piÃ¨ces jointes des expÃ©diteurs que vous ne connaissez pas.
- Nâ□□ouvrez pas les e-mails dont lâ□□objet vous semble bizarre ou Ã©trange.
- Ne cliquez sur aucun des liens contenus dans les e-mails de spam, y compris le lien â□□dÃ©sinscriptionâ□□, vous risquez de dÃ©clencher lâ□□envoi dâ□□autre malware ou de mettre en pÃ©ril la sÃ©curitÃ© de votre systÃ¨me.
- Ne vous dÃ©sinscrivez pas et ne rÃ©pondez pas aux e-mails de spam, pour les raisons Ã©voquÃ©es ci-dessus.
- Ne diffusez pas vos coordonnÃ©es personnelles sur des pages Internet dont vous nâ□□Ãªtes pas sÃ»r lors de votre navigation sur Internet.

Â

Lorsque vous effectuez des achats en ligne, essayez de limiter au maximum le fait de vous inscrire pour recevoir les services ou les promotions complÃ©mentaires qui vous sont proposÃ©es sur les sites marchands.

Utilisez au moins deux adresses e-mail. CrÃ©ez un compte de messagerie pour correspondre avec les personnes que vous connaissez et une deuxiÃ¨me adresse destinÃ©e aux formulaires et autres sites web qui nÃ©cessitent que vous donniez une adresse e-mail.

Ã□vitez dâ□□utiliser ou de diffuser votre adresse e-mail sur des sites web, des livres dâ□□or, des forums, des listes de contact ou des â□□listes de souhaitsâ□□ ou dâ□□achats.

Â« ***Les utilisateurs doivent avoir conscience du fait que sans utiliser une solution de sÃ©curitÃ© adÃ©quate ils mettent clairement en danger lâ□□intÃ©gritÃ© de leur systÃ¨me*** Â» rappelle **Vlad Valceanu**, Directeur du centre de Recherche Antispam de BitDefender.

Â Â« ***La validation de leur adresse e-mail par les utilisateurs revient Ã signer lâ□□Â« arrÃªt de mort Â» de leur boÃ®te de messagerie. Le prochain mail envoyÃ© par les spammeurs pourra contenir un malware ou un code malveillant qui peut effacer leur disque dur ou rÃ©colter des informations confidentielles et les faire sortir de lâ□□ordinateur, comme par exemple les numÃ©ros de cartes bancaire qui sont utilisÃ©s pour les achats en ligne*** Â».