BitDefender : Angelina Jolie, vecteur de diffusion dâ□□un Malware
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 17/7/2008 0:00:00

Les Laboratoires BitDefender ont identifiÃ© une nouvelle vague de spam utilisant de faux Ã©vÃ¨nements concernant lâ□□actrice Angelina Jolie dans le but de tromper les utilisateurs afin quâ□□ils tÃ©lÃ©chargent et installent un Trojan sur leurs ordinateurs.
Cette nouvelle campagne de diffusion de malwares se propage principalement via des spams au sujet dâ□□**une supposÃ©e vidÃ©o pour adulte** qui mettrait en scÃ¨ne la star de cinÃ©ma. Pour voir le film, les utilisateurs doivent tÃ©lÃ©charger un fichier binaire, **video-nude-angelina.avi.exe** , qui est infectÃ© par **Trojan.Agent.ACGZ**.

Â

Le message spam est composÃ© dâ□□une image explicite dâ□□Angelina Jolie, accompagnÃ©e de textes prÃ©tendant que le mail a Ã©tÃ© envoyÃ© dans le cadre du programme des offres MSN. Par ce biais, le message spam joue un double rÃ´le en essayant, dâ□□une part, de tromper lâ□□utilisateur en lui faisant penser que câ□□est un e-mail dâ□□information lÃ©gitime et dâ□□autre part, en Ã©vitant que les filtres antispams classent le mail comme un spam.

Â« ***Cette vague de spams appartient Ã une catÃ©gorie plus large dâ□□e-mails non sollicitÃ©s, qui reposent sur des techniques de Â« social engineering*** Â» ***de faÃ§on Ã pousser les utilisateurs imprudents Ã installer des trojans*** Â», dÃ©clare **Vlad Valceanu**, Directeur de la Recherche antispam BitDefender.

Â Â« ***Ce type dâ□□attaque semble avoir beaucoup de succÃ¨s comme le montre la progression importante dont ils sont lâ□□objet ces derniers mois. Afin dâ□□atteindre leurs buts, les spammeurs sâ□□appuient habituellement sur des cÃ©lÃ©britÃ©s internationales et leurs photos, accompagnÃ©es de titres accrocheurs et cependant faux*** . Â»

Ce nâ□□est pas le premier incident impliquant Angelina Jolie .

Â

Dâ□□autant plus que, lâ□□actrice a rÃ©cemment donnÃ© naissance Ã 2 enfants, et les spammeurs ont tirÃ© avantage de cet Ã©vÃ¨nement pour infecter encore plus dâ□□ordinateurs.

La campagne de spam qui a suivi lâ□□Ã©vÃ¨nement a annoncÃ© quâ□□Angelina avait donnÃ© naissance Ã pas moins de 5 enfants, et proposait mÃªme aux utilisateurs un lien vers un site Web qui prÃ©tendait proposer une petite vidÃ©o de lâ□□Ã©vÃ¨nement. Lâ□□annonce, combinÃ©e Ã la cÃ©lÃ©britÃ© dâ□□Angelina Jolie, Ã©tait destinÃ©e Ã tirer avantage de lâ□□intÃ©rÃªt des utilisateurs pour les Ã©vÃ¨nements sensationnels.

Une fois sur la page, les utilisateurs pouvaient voir une image reprÃ©sentant un lecteur vidÃ©o en flash. Quand lâ□□utilisateur arrivait sur la page web corrompue, le tÃ©lÃ©chargement dÃ©marrait immÃ©diatement, sans intervention de lâ□□utilisateur (un procÃ©dÃ© aussi appelÃ© le Â« **Drive by download** Â»).

Le fichier binaire Ã©tait infectÃ© par le troyen : **Trojan.Downloader.Exchanger.Gen.1**, un bout de code malveillant qui a Ã©tÃ© largement utilisÃ© dans une autre campagne de spam qui mettait en avant **un soi-disant utilitaire antivirus, appelÃ© Antivirus XP 2008.**

Bien que l'approche soit relativement nouvelle, la technique sous-jacente a largement Ã©tÃ© utilisÃ©e par le passÃ©. Cette campagne vise surtout des utilisateurs qui ne sont pas trop au fait des questions de sÃ©curitÃ©â□□ Ã©tant donnÃ© que ces derniers ne sont pas au courant de lâ□□existence de scanners en ligne gratuits mis Ã disposition par les principaux Ã©diteurs de logiciels de sÃ©curitÃ©.

Â

Le message du spam dirige l'utilisateur vers une page web lÃ©gitime dont la page d'index a Ã©tÃ© doublÃ©e pour faciliter l'attaque. Par exemple, si la page dâ□□accueil normale est index.php, l'**URL dangereuse se terminera par index1.php.**

Cette deuxiÃ¨me page dâ□□index est prÃ©sentÃ©e Ã la maniÃ¨re de Windows Vista (***fond dâ□□Ã©cran Aero et icÃ´nes***). Lâ□□aspect professionnel contribue grandement Ã inspirer confiance aux utilisateurs, bien que quelques dÃ©tails devraient alerter les visiteurs au sujet de lâ□□escroquerie.

Par exemple, en haut Ã droite de lâ□□Ã©cran, le spam affiche les virus les plus actifs durant le mois de mai â□□ ce qui signifie que la page nâ□□a pas Ã©tÃ© mise Ã jour. DeuxiÃ¨mement les autres Ã©lÃ©ments du texte sont Ã©crits en Anglais basique avec des explications ambiguÃ«s (comme "les attaques de Trojan endommagent plus de 3 million $ /heure.")

Le message du spam lui-mÃªme est Ã©crit avec une grammaire pauvre, et de multiples zones pas trÃ¨s nettes visant Ã duper les filtres Antispam.

Â« ***Cette vague de spam utilise une vieille technique qui consiste Ã obscurcir certaine zone de texte de faÃ§on importante, afin dâ□□empÃªcher les filtres Antispam dâ□□identifier le message et de le catÃ©goriser en tant que spam*** Â» a dÃ©clarÃ© Vlad Valceanu.

Â« ***Le message lui-mÃªme devrait pourtant Ãªtre un avertissement suffisant pour l'utilisateur pour quâ□□il comprenne que le logiciel n'est pas lÃ©gitime et provient dâ□□une source suspecte. IndÃ©pendamment de cela, les utilisateurs devraient faire beaucoup plus attention aux pages web qui tentent de tÃ©lÃ©charger automatiquement un fichier sur leurs ordinateurs*** Â».

Une fois installÃ© sur l'ordinateur, le faux utilitaire antivirus installe discrÃ¨tement dâ□□autres fichiers Ã haut risque comme des adwares, des spywares ou autres malwares Ã partir de multiples serveurs ou sources issues dâ□□Internet.

De plus, une fois lancÃ©, lâ□□antivirus affichera diffÃ©rents messages rÃ©pertoriant de multiples fausses menaces de sÃ©curitÃ© sur la machine. C'est une mÃ©thode habituelle pour les fausses applications de sÃ©curitÃ© pour induire en erreur les utilisateurs non-avertis et les faire payer une version "complÃ¨te" d'un faux logiciel.