BitDefender : RÃ©trospective des e-Menaces en 2009
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 5/1/2010 15:00:00

Une enquÃªte de BitDefender sur les malwares et le spam rÃ©vÃ¨le une recrudescence des e-menaces favorisÃ©e par les **Ã©vÃ©nements internationaux actuels et la popularitÃ© grandissante du Web 2.0**

Les cybercriminels continuent de trouver dâ□□ingÃ©nieux moyens de diffusion de malwares au cours du deuxiÃ¨me semestre 2009

Les auteurs de malwares ont poursuivi leurs attaques habituelles via le Web tout en recherchant activement de nouvelles mÃ©thodes pour dissÃ©miner leurs produits, indique BitDefender, Ã©diteur de solutions de sÃ©curitÃ© antimalwares, qui publie aujourdâ□□hui les rÃ©sultats de son enquÃªte sur les malwares et le spam, menÃ©e entre juillet et dÃ©cembre 2009. Lâ□□enquÃªte fait Ã©tat de la recrudescence dâ□□un grand nombre de menaces, allant de lâ□□exploitation des Ã©vÃ©nements internationaux Ã lâ□□envoi de trÃ¨s fortes quantitÃ©s de spam, qui se rÃ©pandent Ã travers les plateformes de rÃ©seaux sociaux afin de rÃ©duire les coÃ»ts de marketing dans une Ã©conomie en repli.

Les menaces de type malwares

Au cours des six derniers mois, les auteurs de malwares ont poursuivi leurs tentatives dâ□□infecter les ordinateurs pour obtenir un profit financier immÃ©diat au dÃ©triment des utilisateurs et/ou prendre le contrÃ´le de leurs machines. Trojan.Clicker.CM est la menace Ã©lectronique numÃ©ro un du deuxiÃ¨me semestre de lâ□□annÃ©e. Elle est utilisÃ©e pour imposer des publicitÃ©s dans les navigateurs des utilisateurs lorsque ces derniers visitent les zones dâ□□ombre du web (comme les sites pornographiques ou les services proposant des logiciels de type Â« warez Â»). Le taux alarmant dâ□□infection fait apparaÃ®tre que les auteurs de malwares sont attirÃ©s par le gain, tandis que les cybercriminels sont motivÃ©s par la fraude du type Â« pay-per-click Â».

Comme les dÃ©jÃ Â« traditionnelles Â» infections dues au Trojan.Clicker.CM, Win32.Worm.Downadup sâ□□est rÃ©vÃ©lÃ©e Ãªtre lâ□□une des e-menaces les plus notoires des six derniers mois. Si le web reste lâ□□un des moyens favoris des auteurs de malwares pour camoufler leurs menaces, les techniques utilisant la fonction Autorun ont rapidement gagnÃ© du terrain. Par dÃ©faut, les supports de stockage amovibles contiennent tous un script autorun.ini qui

indique Ã lâ□□ordinateur quel fichier exÃ©cuter quand le pÃ©riphÃ©rique est branchÃ©. Il est cependant frÃ©quent que les auteurs de malwares falsifient le fichier pour quâ□□il lance diverses applications malveillantes. Bien quâ□□elle soit extrÃªmement utile aux utilisateurs peu expÃ©rimentÃ©s, la fonctionnalitÃ© a Ã©tÃ© supprimÃ©e dans Windows Vista SP2 et Windows 7 pour Ã©viter les contaminations.

Â« *Au cours du deuxiÃ¨me semestre 2009, des Ã©vÃ©nements internationaux, comme la grippe H1N1, ont Ã©tÃ© exploitÃ©s au maximum par les auteurs de malware pour lancer de nouvelles infections* Â» signale **Vlad VÃ¢lceanu**, Directeur des Laboratoires de Recherches Antispam de BitDefender. Â« *Dans la mesure oÃ¹ les cybercriminels continuent, aujourdâ□□hui plus que jamais, Ã rechercher tous les moyens de perfectionner leurs menaces Ã©lectroniques, il est essentiel que les utilisateurs installent sur leurs ordinateurs une solution de sÃ©curitÃ© capable de leur procurer une protection proactive avancÃ©e.* Â»

Au cours des six derniers mois, les pays les plus actifs en termes de propagation de logiciels malveillants ont Ã©tÃ© la Chine, la France et les Etats-Unis, suivis par lâ□□Australie (qui avance dâ□□une place dans le classement depuis le premier semestre 2009), la Roumanie (qui avance dâ□□une place Ã©galement) et lâ□□Espagne qui recule dâ□□une place.

Le top 10 du malware mondial entre juillet et dÃ©cembre 2009

01. Trojan.Clicker.CM 8,97%

02. Trojan.AutorunINF.Gen 8,41%

03. Trojan.Wimad.Gen.1 4,41%

04. Win32.Worm.Downadup.Gen 4,13%

05. Exploit.PDF-JS.Gen 3,39%

06. Win32.Sality.OG 2,60%

07. Trojan.Autorun.AET 1,97%

08. Worm.Autorun.VHG 1,59%

09. Trojan.JS.PYV 1,50%

10. Exploit.SWF.Gen 1,47%

Types de spam au cours du deuxiÃ¨me semestre 2009

Au cours de la seconde moitiÃ© de 2009, le paysage du spam est restÃ© Ã peu prÃ¨s le mÃªme, avec les produits pharmaceutiques canadiens occupant le rang le plus Ã©levÃ© Ã lâ□□Ã©chelle mondiale. La plupart des messages contiennent de la publicitÃ© pour des produits augmentant la vigueur sexuelle, alternatives au Cialis, Viagra et Levitra. Cette catÃ©gorie de spam est extrÃªmement lucrative, car les produits commandÃ©s en ligne ne sont gÃ©nÃ©ralement jamais livrÃ©s au client, qui nâ□□ose pas le signaler aux autoritÃ©s. Plus grave encore ces paiements en ligne sont extrÃªmement risquÃ©s. Le spammeur, ayant accÃ¨s Ã toutes les donnÃ©es de la carte de crÃ©dit utilisÃ©e, peut retirer autant dâ□□argent quâ□□il le souhaite.

Le spam reprÃ©sente 88,9 % du montant total des messages Ã©lectroniques envoyÃ©s dans le monde entier. Les messages textuels constituent la forme la plus frÃ©quente du spam, tandis que le spam image est extrÃªmement rare, avec un pourcentage se situant entre 2,3 et 2,5. La taille

moyenne dâ□□un message spam est de 3,5 Ko, mais peut sâ□□Ã©chelonner entre 2 et 9 Ko en fonction de son type.

Au cours du deuxiÃ¨me semestre 2009, les spammeurs se sont particuliÃ¨rement servis des Ã©vÃ©nements internationaux ou nationaux pour inciter leurs victimes Ã ouvrir les messages. Lâ□□une des plus importantes vagues de spam a Ã©tÃ© lancÃ©e aprÃ¨s la mort controversÃ©e de Michael Jackson. En juillet dernier, BitDefender a identifiÃ© de multiples courants de spam prÃ©tendant dÃ©voiler plus dâ□□informations sur lâ□□assassin de Michael Jackson, mais vÃ©hiculant en fait de la publicitÃ© pour des produits amÃ©liorant la performance sexuelle et des malwares.

Le Top 10 des spams du deuxiÃ¨me semestre 2009, triÃ©s par contenu, est le suivant :

1 Produits pharmaceutiques

2 Liens de hameÃ§onnage (phishing)

3 Spam pour produits/contrefaÃ§ons

4 Malware en piÃ¨ces jointes

5 Logiciels/OEM

6 PrÃªts/Assurances

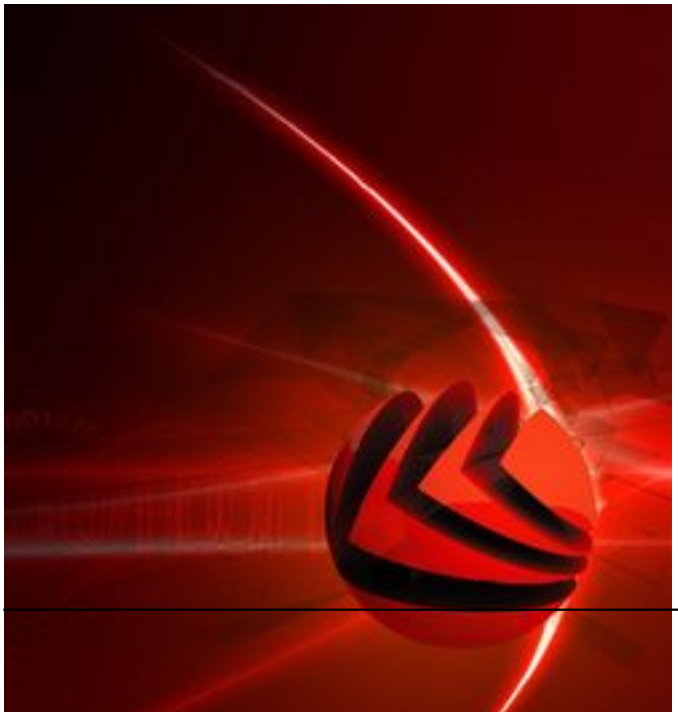
7 Offres dâ□□emploi

8 Education

9 Pornographie (autre que Rencontres)

10 Rencontres

Menaces Web 2.0



Le spamming est Ã©galement une pratique courante parmi les utilisateurs de services Web 2.0, comme les rÃ©seaux sociaux. Tandis que Twitter et Facebook ont imposÃ© des politiques trÃ¨s strictes concernant le spamming, dâ□□autres services de rÃ©seaux sociaux ont Ã peine tenu compte de cette possibilitÃ©. Par exemple, le rÃ©seau professionnel LinkedIn est devenu le terrain de jeu favori dâ□□individus et dâ□□organisations proposant des services divers. Les spammeurs tentent de pÃ©nÃ©trer les rÃ©seaux dâ□□utilisateurs professionnels et les bombardent de messages publicitaires vantant leurs produits ou services.

Au cours des six derniers mois, BitDefender a identifiÃ© de multiples versions du spam LinkedIn â□□ un avertissement qui montre que lâ□□Ã©tat instable de lâ□□Ã©conomie mondiale pousse de plus en plus de fournisseurs Ã vanter leurs services par lâ□□intermÃ©diaire des rÃ©seaux sociaux.

Au moment oÃ¹ le spam et l'hameÃ§onnage atteignent 80 % des e-menaces concernant les rÃ©seaux sociaux, on constate une montÃ©e rapide des vers exploitant de larges plateformes. Au cours du deuxiÃ¨me semestre 2009, de nombreuses familles de vers ont pris d'assault les plus importants rÃ©seaux sociaux que sont Twitter, MySpace et Facebook.

Apparu en aoÃ»t 2008, le ver Koobface sâ□□est rÃ©vÃ©lÃ© Ãªtre lâ□□une des e-menaces les plus destructrices pour les rÃ©seaux sociaux. Les Ã©quipes de cybercriminels Ã lâ□□origine de ce ver en ont libÃ©rÃ© de multiples versions pour augmenter la portÃ©e de leur action et atteindre le plus grand nombre possible de ces rÃ©seaux. Les infections virales ont pris la plupart des plateformes par surprise et les dommages infligÃ©s aux utilisateurs ont dÃ©passÃ© lâ□□imagination, dÃ©sactivant certains des antivirus et exportant des donnÃ©es sensibles comme des rÃ©fÃ©rences bancaires et des mots de passe de messagerie instantanÃ©e. La technique Ã©tait simple mais efficace : le ver utilisait des comptes compromis pour inciter des amis du rÃ©seau Ã cliquer sur les liens infectÃ©s.

Le paysage de l'hameÃ§onnage (phishing)

Par rapport au premier semestre 2009, le nombre de messages de l'hameÃ§onnage est restÃ© relativement stable, bien que leurs auteurs aient choisi pour victimes des institutions susceptibles de leur apporter le plus de profit dans le plus court laps de temps. Les cibles principales sont PayPal, Visa et eBay, suivis par HSBC, American Express et Abbey Bank. Ally Bank et Bank of America figurent en dernier avec un peu plus de 1% seulement du nombre total de messages de phishing. Ces messages visent pour la plupart des utilisateurs anglophones utilisant les services dâ□□au moins une des institutions citÃ©es.

Les laboratoires de BitDefender ont constatÃ© que les tentatives de l'hameÃ§onnage Web 2.0 de la premiÃ¨re moitiÃ© de 2009 Ã©taient basÃ©es sur Â« lâ□□ingÃ©nierie sociale Â» et spÃ©culaient sur la candeur des utilisateurs. Lâ□□arnaque Twitter Porn Name en donne un bon exemple. Les utilisateurs Ã©taient invitÃ©s Ã fournir le nom de leur premier animal de compagnie et le nom de la premiÃ¨re rue oÃ¹ ils avaient habitÃ©. Ces noms sont gÃ©nÃ©ralement utilisÃ©s en rÃ©ponse aux questions de rattrapage en cas dâ□□oubli dâ□□un mot de passe. Lâ□□escroc en possession du nom dâ□□utilisateur de la personne et de ces Â« indices Â» peut facilement rÃ©cupÃ©rer le mot de passe et sâ□□en servir ensuite pour accÃ©der au compte, envoyer des spams, accÃ©der aux transactions ou utiliser le compte de toutes les maniÃ¨res possibles pour gagner de lâ□□argent, y compris en exigeant une ranÃ§on pour libÃ©rer le compte piratÃ©.

Â« *2009 a permis dâ□□observer une grande quantitÃ© de menaces pour la sÃ©curitÃ©, visant Ã la fois des utilisateurs finaux et des rÃ©seaux dâ□□entreprise* Â» a dÃ©clarÃ© VÃ¢lceanu. Â« *Des prÃ©cautions exceptionnelles et une solution trÃ¨s efficace comprenant des modules antispam, antiphishing et antimalware sont impÃ©ratifs pour toute personne naviguant sur le Web en 2010*. "

Pour plus dâ□□informations sur cette enquÃªte

Pour Ãªtre informÃ© des derniÃ¨res e-menaces et informations sur nos produits et Ã©vÃ©nements, inscrivez-vous au **service RSS de BitDefender.**