

BitDefender : R trospective des e-Menaces en 2009

S curit 

Post  par : JerryG

Publi e le : 5/1/2010 15:00:00

Une enqu te de BitDefender sur les malwares et le spam r v le une recrudescence des e-menaces favoris e par les ** v nements internationaux actuels et la popularit  grandissante du Web 2.0**

Les cybercriminels continuent de trouver d ring nieux moyens de diffusion de malwares au cours du deuxi me semestre 2009

Les auteurs de malwares ont poursuivi leurs attaques habituelles via le Web tout en recherchant activement de nouvelles m thodes pour diss miner leurs produits, indique BitDefender,  diteur de solutions de s curit  antimalwares, qui publie aujourd hui les r sultats de son enqu te sur les malwares et le spam, men e entre juillet et d cembre 2009. L enqu te fait  tat de la recrudescence d un grand nombre de menaces, allant de l exploitation des  v nements internationaux   l envoi de tr s fortes quantit s de spam, qui se r pandent   travers les plateformes de r seaux sociaux afin de r duire les co ts de marketing dans une  conomie en repli.

Les menaces de type malwares

Au cours des six derniers mois, les auteurs de malwares ont poursuivi leurs tentatives d infecter les ordinateurs pour obtenir un profit financier imm diat au d triment des utilisateurs et/ou prendre le contr le de leurs machines. Trojan.Clicker.CM est la menace  lectronique num ro un du deuxi me semestre de l ann e. Elle est utilis e pour imposer des publicit s dans les navigateurs des utilisateurs lorsque ces derniers visitent les zones d ombre du web (comme les sites pornographiques ou les services proposant des logiciels de type  warez  ). Le taux alarmant d infection fait appara tre que les auteurs de malwares sont attir s par le gain, tandis que les cybercriminels sont motiv s par la fraude du type  pay-per-click  .



Comme les d j   « traditionnelles   infections dues au Trojan.Clicker.CM, Win32.Worm.Downadup s est r v l e  tre l une des e-menaces les plus notoires des six derniers mois. Si le web reste l un des moyens favoris des auteurs de malwares pour camoufler leurs menaces, les techniques utilisant la fonction Autorun ont rapidement gagn  du terrain. Par d fait, les supports de stockage amovibles contiennent tous un script autorun.ini qui

indique   l ordinateur quel fichier ex cuter quand le p riph rique est branch . Il est cependant fr quent que les auteurs de malwares falsifient le fichier pour qu il lance diverses applications malveillantes. Bien qu elle soit extr mement utile aux utilisateurs peu exp riment s, la fonctionnalit  a  t  supprim e dans Windows Vista SP2 et Windows 7 pour  viter les contaminations.

 « Au cours du deuxi me semestre 2009, des  v nements internationaux, comme la grippe H1N1, ont  t  exploit s au maximum par les auteurs de malware pour lancer de nouvelles infections  » signale **Vlad V lcianu**, Directeur des Laboratoires de Recherches Antispam de BitDefender.  « Dans la mesure o ¹ les cybercriminels continuent, aujourd hui plus que jamais,   rechercher tous les moyens de perfectionner leurs menaces  lectroniques, il est essentiel que les utilisateurs installent sur leurs ordinateurs une solution de s curit  capable de leur procurer une protection proactive avanc e.  »

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

Le top 10 du malware mondial entre juillet et d 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 deuxi me semestre 2009

Au cours de la seconde moiti  de 2009, le paysage du spam est rest    peu pr s le m me, avec les produits pharmaceutiques canadiens occupant le rang le plus  lev    l  chelle mondiale. La plupart des messages contiennent de la publicit  pour des produits augmentant la vigueur sexuelle, alternatives au Cialis, Viagra et Levitra. Cette cat gorie de spam est extr mement lucrative, car les produits command s en ligne ne sont g n ralement jamais livr s au client, qui n ose pas le signaler aux autorit s. Plus grave encore ces paiements en ligne sont extr mement risqu s. Le spammeur, ayant acc s   toutes les donn es de la carte de cr dit utilis e, peut retirer autant d argent qu il le souhaite.

Le spam repr sente 88,9 % du montant total des messages  lectroniques envoy s dans le monde entier. Les messages textuels constituent la forme la plus fr quente du spam, tandis que le spam image est extr mement rare, avec un pourcentage se situant entre 2,3 et 2,5. La taille

moyenne d un message spam est de 3,5 Ko, mais peut s  chelonner entre 2 et 9 Ko en fonction de son type.

Au cours du deuxi me semestre 2009, les spammeurs se sont particuli rement servis des  v nements internationaux ou nationaux pour inciter leurs victimes   ouvrir les messages. L une des plus importantes vagues de spam a  t  lanc e apr s la mort controvers e de Michael Jackson. En juillet dernier, BitDefender a identifi  de multiples courants de spam pr tendant d voiler plus d informations sur l assassin de Michael Jackson, mais v hiculant en fait de la publicit  pour des produits am liorant la performance sexuelle et des malwares.

Le Top 10 des spams du deuxi me semestre 2009, tri s par contenu, est le suivant :

- 1 Produits pharmaceutiques
- 2 Liens de hame onnage (phishing)
- 3 Spam pour produits/contrefa sons
- 4 Malware en pi ces jointes
- 5 Logiciels/OEM
- 6 Pr ats/Assurances
- 7 Offres d emploi
- 8 Education
- 9 Pornographie (autre que Rencontres)
- 10 Rencontres

Menaces Web 2.0



Le spamming est  galement une pratique courante parmi les utilisateurs de services Web 2.0, comme les r seaux sociaux. Tandis que Twitter et Facebook ont impos  des politiques tr s strictes concernant le spamming, d autres services de r seaux sociaux ont   peine tenu compte de cette possibilit . Par exemple, le r seau professionnel LinkedIn est devenu le terrain de jeu favori d individus et d organisations proposant des services divers. Les spammeurs tentent de p n trer les r seaux d utilisateurs professionnels et les bombardent de messages publicitaires vantant leurs produits ou services.

Au cours des six derniers mois, BitDefender a identifi  de multiples versions du spam LinkedIn   un avertissement qui montre que l  tat instable de l  conomie mondiale pousse de plus en plus de fournisseurs   vanter leurs services par l  interm diaire des r seaux sociaux.

Au moment o ¹ le spam et l'hame sonnage atteignent 80 % des e-menaces concernant les r seaux sociaux, on constate une mont e rapide des vers exploitant de larges plateformes. Au cours du deuxi me semestre 2009, de nombreuses familles de vers ont pris d'assault les plus importants r seaux sociaux que sont Twitter, MySpace et Facebook.

Apparu en ao t 2008, le ver Koobface s est r v l   tre l une des e-menaces les plus destructrices pour les r seaux sociaux. Les  quipes de cybercriminels   l origine de ce ver en ont lib r  de multiples versions pour augmenter la port e de leur action et atteindre le plus grand nombre possible de ces r seaux. Les infections virales ont pris la plupart des plateformes par surprise et les dommages inflig s aux utilisateurs ont d pass  l imagination, d sactivant certains des antivirus et exportant des donn es sensibles comme des r f rences bancaires et des mots de passe de messagerie instantan e. La technique  tait simple mais efficace : le ver utilisait des comptes compromis pour inciter des amis du r seau   cliquer sur les liens infect s.

Le paysage de l'hame sonnage (phishing)

Par rapport au premier semestre 2009, le nombre de messages de l'hame sonnage est rest  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 d au moins une des institutions cit es.

Les laboratoires de BitDefender ont constat  que les tentatives de l'hame sonnage Web 2.0 de la premi re moiti  de 2009  taient bas es sur   l ing nierie sociale   et sp culaient sur la candeur des utilisateurs. L arnaque Twitter Porn Name en donne un bon exemple. Les utilisateurs  taient invit s   fournir le nom de leur premier animal de compagnie et le nom de la premi re rue o ¹ ils avaient habit . Ces noms sont g n ralement utilis s en r ponse aux questions de rattrapage en cas d oubli d un mot de passe. L escroc en possession du nom d utilisateur de la personne et de ces   indices   peut facilement r cup rer le mot de passe et s en servir ensuite pour acc der au compte, envoyer des spams, acc der aux transactions ou utiliser le compte de toutes les mani res possibles pour gagner de l argent, y compris en exigeant une ran on pour lib rer le compte pirat .

  2009 a permis d observer une grande quantit  de menaces pour la s curit , visant   la fois des utilisateurs finaux et des r seaux d entreprise   a d clar  V lceanu.   Des pr cautions exceptionnelles et une solution tr s efficace comprenant des modules antispam, antiphishing et antimalware sont imp ratifs pour toute personne naviguant sur le Web en 2010. "

[Pour plus d informations sur cette enqu te](#)

Pour  tre inform  des derni res e-menaces et informations sur nos produits et  v nements, inscrivez-vous au [service RSS de BitDefender.](#)