Mardi 5 janvier 2010

Une enquête de BitDefender sur les malwares et le spam révèle une recrudescence des e-menaces favorisée par les événements internationaux actuels et la popularité grandissante du Web 2.0

Les cybercriminels continuent de trouver d'ingénieux moyens de diffusion de malwares au cours du deuxième semestre 2009

Les auteurs de malwares ont poursuivi leurs attaques habituelles via le Web tout en recherchant activement de nouvelles méthodes pour disséminer leurs produits, indique BitDefender, éditeur de solutions de sécurité antimalwares, qui publie aujourd'hui les résultats de son enquête sur les malwares et le spam, menée entre juillet et décembre 2009. L'enquête fait état de la recrudescence d'un grand nombre de menaces, allant de l'exploitation des événements internationaux à l'envoi de très fortes quantités de spam, qui se répandent à travers les plateformes de réseaux sociaux afin de réduire les coûts de marketing dans une économie 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 immédiat au détriment des utilisateurs et/ou prendre le contrôle de leurs machines. Trojan.Clicker.CM est la menace électronique numéro un du deuxième semestre de l'année. Elle est utilisée pour imposer des publicités 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 apparaître que les auteurs de malwares sont attirés par le gain, tandis que les cybercriminels sont motivés par la fraude du type « pay-per-click ».

Comme les déjà « traditionnelles » infections dues au Trojan.Clicker.CM, Win32.Worm.Downadup s'est révélée être 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 gagné du terrain. Par défaut, les supports de stockage amovibles contiennent tous un script autorun.ini qui indique à l'ordinateur quel fichier exécuter quand le périphérique est branché. Il est cependant fréquent que les auteurs de malware falsifient le fichier pour qu'il lance diverses applications malveillantes. Bien qu'elle soit extrêmement utile aux utilisateurs peu expérimentés, la fonctionnalité a été supprimée dans Windows Vista SP2 et Windows 7 pour éviter les contaminations.

« Au cours du deuxième semestre 2009, des événements internationaux, comme la grippe H1N1, ont été exploités au maximum par les auteurs de malware pour lancer de nouvelles infections » signale Vlad Vâlceanu, Directeur des Laboratoires de Recherches Antispam de BitDefender. « Dans la mesure où les cybercriminels continuent, aujourd'hui plus que jamais, à rechercher tous les moyens de perfectionner leurs menaces électroniques, il est essentiel que les utilisateurs installent sur leurs ordinateurs une solution de sécurité capable de leur procurer une protection proactive avancée. »

Au cours des six derniers mois, les pays les plus actifs en termes de propagation de logiciels malveillants ont été 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 également) et l'Espagne qui recule d'une place.

Le top 10 du malware mondial entre juillet et décembre 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 deuxième semestre 2009

Au cours de la seconde moitié de 2009, le paysage du spam est resté à peu près le même, avec les produits pharmaceutiques canadiens occupant le rang le plus élevé à l'échelle mondiale. La plupart des messages contiennent de la publicité pour des produits augmentant la vigueur sexuelle, alternatives au Cialis, Viagra et Levitra. Cette catégorie de spam est extrêmement lucrative, car les produits commandés en ligne ne sont généralement jamais livrés au client, qui n'ose pas le signaler aux autorités. Plus grave encore ces paiements en ligne sont extrêmement risqués. Le spammeur, ayant accès à toutes les données de la carte de crédit utilisée, peut retirer autant d'argent qu'il le souhaite.

Le spam représente 88,9 % du montant total des messages électroniques envoyés dans le monde entier. Les messages textuels constituent la forme la plus fréquente du spam, tandis que le spam image est extrêmement 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'échelonner entre 2 et 9 Ko en fonction de son type.

Au cours du deuxième semestre 2009, les spammeurs se sont particulièrement servis des événements internationaux ou nationaux pour inciter leurs victimes à ouvrir les messages. L'une des plus importantes vagues de spam a été lancée après la mort controversée de Michael Jackson. En juillet dernier, BitDefender a identifié de multiples courants de spam prétendant dévoiler plus d'informations sur l'assassin de Michael Jackson, mais véhiculant en fait de la publicité pour des produits améliorant la performance sexuelle et des malwares.

Le Top 10 des spams du deuxième semestre 2009, triés par contenu, est le suivant :

1 Produits pharmaceutiques

2 Liens de hameçonnage (phishing)

3 Spam pour produits/contrefaçons

4 Malware en pièces jointes

5 Logiciels/OEM

6 Prêts/Assurances

7 Offres d'emploi

8 Education

9 Pornographie (autre que Rencontres)

10 Rencontres

Menaces Web 2.0

Le spamming est également une pratique courante parmi les utilisateurs de services Web 2.0, comme les réseaux sociaux. Tandis que Twitter et Facebook ont imposé des politiques très strictes concernant le spamming, d'autres services de réseaux sociaux ont à peine tenu compte de cette possibilité. Par exemple, le réseau professionnel LinkedIn est devenu le terrain de jeu favori d'individus et d'organisations proposant des services divers. Les spammeurs tentent de pénétrer les réseaux d'utilisateurs professionnels et les bombardent de messages publicitaires vantant leurs produits ou services.

Au cours des six derniers mois, BitDefender a identifié de multiples versions du spam LinkedIn – un avertissement qui montre que l'état instable de l'économie mondiale pousse de plus en plus de fournisseurs à vanter leurs services par l'intermédiaire des réseaux sociaux.

Au moment où le spam et l'hameçonnage atteignent 80 % des e-menaces concernant les réseaux sociaux, on constate une montée rapide des vers exploitant de larges plateformes. Au cours du deuxième semestre 2009, de nombreuses familles de vers ont pris d'assault les plus importants réseaux sociaux que sont Twitter, MySpace et Facebook.

Apparu en août 2008, le ver Koobface s'est révélé être l'une des e-menaces les plus destructrices pour les réseaux sociaux. Les équipes de cybercriminels à l'origine de ce ver en ont libéré de multiples versions pour augmenter la portée de leur action et atteindre le plus grand nombre possible de ces réseaux. Les infections virales ont pris la plupart des plateformes par surprise et les dommages infligés aux utilisateurs ont dépassé l'imagination, désactivant certains des antivirus et exportant des données sensibles comme des références bancaires et des mots de passe de messagerie instantanée. La technique était simple mais efficace : le ver utilisait des comptes compromis pour inciter des amis du réseau à cliquer sur les liens infectés.

Le paysage de l'hameçonnage (phishing)

Par rapport au premier semestre 2009, le nombre de messages de l'hameçonnage est resté 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 citées.

Les laboratoires de BitDefender ont constaté que les tentatives de l'hameçonnage Web 2.0 de la première moitié de 2009 étaient basées sur « l'ingénierie sociale » et spéculaient sur la candeur des utilisateurs. L'arnaque Twitter Porn Name en donne un bon exemple. Les utilisateurs étaient invités à fournir le nom de leur premier animal de compagnie et le nom de la première rue où ils avaient habité. Ces noms sont généralement utilisés en réponse 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 récupérer le mot de passe et s'en servir ensuite pour accéder au compte, envoyer des spams, accéder aux transactions ou utiliser le compte de toutes les manières possibles pour gagner de l'argent, y compris en exigeant une rançon pour libérer le compte piraté.

« 2009 a permis d'observer une grande quantité de menaces pour la sécurité, visant à la fois des utilisateurs finaux et des réseaux d'entreprise » a déclaré Vâlceanu. « Des précautions exceptionnelles et une solution très efficace comprenant des modules antispam, antiphishing et antimalware sont impératifs pour toute personne naviguant sur le Web en 2010.

Pour télécharger cette enquête

Pour être informé des dernières e-menaces et informations sur nos produits et événements, inscrivez-vous au service RSS de BitDefender.

À propos de BitDefender®

*BitDefender est la société créatrice de l'une des gammes de **solutions de sécurité** la plus complète et la plus certifiée au niveau international, reconnue comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les **solutions de sécurité** BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le **Centre de presse**. Retrouvez également sur le site **www.malwarecity.fr** les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.*

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et de contrôle parental Parental Filter 2, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.