Bitdefender : Le nombre de Spams contenant des PJ malveillantes augmente
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 8/6/2012 11:30:00

Selon une Ã©tude de **Bitdefender**, les messages de Spam sont moins nombreux, mais plus dangereux, alors que dans le mÃªme temps les messages contenant des piÃ¨ces jointes malveillantes sont plus nombreux. Cela signifie que le Spam, bien que moins prÃ©sent, devient plus dangereux.

Les chercheurs de Bitdefender indiquent que le nombre de piÃ¨ces jointes malveillantes en janvier a augmentÃ© de 4% par rapport Ã la mÃªme pÃ©riode lâ□□an dernier, et ce alors que le nombre global de messages de spam envoyÃ©s a diminuÃ© de plus de 16% entre le dernier trimestre 2011 et le premier trimestre 2012. Sur les 264,6 milliards de messages de spam envoyÃ©s tous les jours dans le monde, 1,14% dâ□□entre eux comprenaient des piÃ¨ces jointes et 300 millions Ã©taient malveillants.

AprÃ¨s une hausse en janvier, lâ□□augmentation du nombre de piÃ¨ces jointes malveillantes sâ□□est stabilisÃ©e dans un contexte apparent de suspension des campagnes de spam, et ce alors que le spam a continuÃ© Ã diminuer globalement. Les piÃ¨ces jointes peuvent Ãªtre des formulaires de phishing qui trompent les utilisateurs en leur faisant divulguer les informations confidentielles concernant leur(s) carte(s) bancaire(s), permettant ainsi aux scammeurs de les utiliser Ã leur grÃ©. Elles peuvent aussi contenir des malwares tels que des chevaux de Troie, des vers et des virus.

Ce type de piÃ¨ce jointe Ã©tant devenu une source de prÃ©occupation croissante sur Internet, Bitdefender a cherchÃ© Ã savoir quels malwares exactement se retrouvaient dans les boÃ®tes de rÃ©ception des utilisateurs. Vous trouverez ci-dessous les cinq malwares les plus intÃ©ressants et les plus souvent joints Ã des e-mails de spam.

Le ver de Â« mass mailing Â» MyDoom, dÃ©couvert pour la premiÃ¨re fois en 2008, continue Ã faire partie des malwares les plus tenaces qui sâ□□introduisent dans les boÃ®tes de rÃ©ception des utilisateurs. Une fois que les e-mails dâ□□ingÃ©nierie sociale habilement conÃ§us ont convaincu les utilisateurs dâ□□ouvrir la piÃ¨ce jointe, le ver sâ□□auto-expÃ©die Ã toutes les adresses e-mail

trouvÃ©es sur le systÃ¨me en utilisant divers expÃ©diteurs, sujets et corps de texte.

MyDoom dÃ©pose Ã©galement un composant backdoor sur le systÃ¨me-hÃ´te afin de permettre Ã lâ□□attaquant Ã distance dâ□□accÃ©der Ã lâ□□ensemble de lâ□□ordinateur de lâ□□utilisateur. Il actualise Ã©galement une liste dâ□□adresses IP infectÃ©es sur un serveur distant. De cette faÃ§on, tous les systÃ¨mes corrompus apparaissent dans une base de donnÃ©es commune des ordinateurs infectÃ©s accessibles au ver. MyDoom est connu pour Ãªtre utilisÃ© dans des attaques par dÃ©ni de service contre des sites Web dâ□□antivirus et dâ□□Ã©diteurs de logiciels.

La deuxiÃ¨me piÃ¨ce jointe malveillante la plus frÃ©quente est un tÃ©lÃ©chargeur Javascript gÃ©nÃ©rique se prÃ©sentant sous la forme dâ□□un code Javascript obscurci Ã lâ□□intÃ©rieur de la piÃ¨ce jointe HTML. Lorsque lâ□□utilisateur ouvre le fichier HTML, le code Javascript obscurci sâ□□exÃ©cute et injecte un iFrame dans la page HTML dans laquelle il se trouve. Cet iFrame charge du contenu malveillant depuis des serveurs tiers, corrompant ainsi le systÃ¨me.

La troisiÃ¨me position est occupÃ©e par Netsky, un autre mass mailer. En plus de sâ□□expÃ©dier Ã toutes les adresses e-mail trouvÃ©es sur le systÃ¨me corrompu, il se diffuse via FTP, peer-to-peer ou fichiers partagÃ©s. Les sujets ingÃ©nieux utilisÃ©s vont des accusations et des messages dâ□□erreur aux dÃ©clarations dâ□□amour et transactions financiÃ¨res et incluent des noms de personnes cÃ©lÃ¨bres afin dâ□□attirer les victimes. Si lâ□□utilisateur ouvre la piÃ¨ce jointe, le ver affiche un message (conÃ§u pour ressembler Ã un message de la solution antivirus locale) indiquant quâ□□aucun virus nâ□□a Ã©tÃ© trouvÃ© sur le systÃ¨me.

Notons que Netsky ne sâ□□expÃ©die jamais Ã des adresses e-mail contenant des mots liÃ©s Ã la sÃ©curitÃ© et Ã lâ□□industrie antivirus (@antivirus, @FBI, @freeav, bitdefender etc.).

Le ver Mytob arrive en quatriÃ¨me position. Il sâ□□agit dâ□□un ver connu pour empÃªcher que les utilisateurs ne se connectent Ã des sites commercialisant des solutions de sÃ©curitÃ©, tout en ouvrant une backdoor afin de permettre lâ□□accÃ¨s Ã distance Ã des personnes mal intentionnÃ©es. De cette faÃ§on, le systÃ¨me est vulnÃ©rable Ã toutes sortes dâ□□exploitation malveillante.

Ce classement sâ□□achÃ¨ve avec le ver Bagle, un Â« mass mailer Â» recueillant des adresses et sâ□□expÃ©diant Ã toutes les adresses e-mail quâ□□il trouve sur le systÃ¨me corrompu. Il tÃ©lÃ©charge Ã©galement dâ□□autres adresses Ã partir dâ□□une liste intÃ©grÃ©e dâ□□emplacements en ligne. Afin dâ□□Ã©viter dâ□□Ãªtre dÃ©tectÃ©, il termine les processus liÃ©s pour la plupart aux solutions antivirus installÃ©es en local. Il tÃ©lÃ©charge et exÃ©cute ensuite des fichiers provenant de nombreux sites web suspects.