Symantec janvier 2010, rapport MessageLabs Intelligence Report
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 25/1/2010 15:00:00

Symantec Corp. annonce la publication de lâ□□Ã©dition de janvier 2010 de son rapport **MessageLabs Intelligence Report**. On y apprend que les spammeurs ont lancÃ© de nouvelles campagnes inspirÃ©es des Ã©vÃ©nements de 2010 en vue de maintenir **le volume de leurs spams Ã un niveau similaire** Ã celui de la fin 2009.

MessageLabs Intelligence a analysÃ© les offres spÃ©ciales Nouvelle annÃ©e 2010 proposant des produits pharmaceutiques, accessoires de mode, montres, produits de rÃ©gime, prÃªts et offres dâ□□emploi. Ses experts ont ainsi dÃ©couvert que 7,7 % du nombre total de spams distribuÃ©s en une journÃ©e concernaient le Nouvel an et que plus de la moitiÃ© de ceux-ci provenaient des botnets Grum et Cutwail. AprÃ¨s le thÃ¨me de la Nouvelle annÃ©e, les spammeurs devraient sâ□□intÃ©resser Ã prÃ©sent Ã celui de la Saint-Valentin. Et, tout comme les pros du phishing, ils nâ□□ont pas Ã©tÃ© longs Ã exploiter la tragÃ©die dâ□□HaÃ¯ti sous la forme de Â« scams Â» pour demander des fonds. Alors que de nombreux pays sâ□□efforcent dâ□□apporter leur aide humanitaire, les experts du Â« scam Â» ne manquent pas dâ□□imagination lorsquâ□□il sâ□□agit de profiter de lâ□□empathie du public pour tromper sa vigilance et dÃ©tourner des dons.

Avec 83,4 % des spams provenant de botnets fin 2009, MessageLabs Intelligence estime que le reste des spams, soit 0,9 % ou 900 millions de spams, provenait de comptes de messagerie Ã©lectronique gratuits. Par ailleurs, plus de 79 % de ces 900 millions de spams ont Ã©tÃ© envoyÃ©s depuis 3 services de messagerie en ligne bien connus.

Â« *Les fournisseurs de services de messagerie Web auront beau tout mettre en Å□uvre pour lutter contre ce genre dâ□□abus, il existe bel et bien un marchÃ© souterrain dâ□□achat et de vente de comptes de messagerie en ligne lÃ©gaux et exploitables* Â», explique **Paul Wood**, analyste senior pour MessageLabs Intelligence chez Symantec.

Au mois de dÃ©cembre 2009, une nouvelle vulnÃ©rabilitÃ© Â« zero-day Â» a Ã©tÃ© dÃ©tectÃ©e dans une version largement diffusÃ©e dâ□□un visionneur de .PDF. MessageLabs Intelligence en avait bloquÃ© les premiÃ¨res versions en circulation en novembre 2009, protÃ©geant ainsi les utilisateurs des services hÃ©bergÃ©s de Symantec avant quâ□□ils nâ□□aient Ã en pÃ¢tir. Cette attaque ciblait des individus haut placÃ©s de lâ□□administration, de lâ□□enseignement, des services financiers et de multinationales. DistribuÃ©e sous la forme dâ□□un fichier .PDF intÃ©grant du code Javascript, elle procÃ©dait Ã©galement dâ□□une technique dâ□□ingÃ©nierie sociale pour sâ□□adapter selon lâ□□individu et lâ□□organisme ciblÃ©s.

En dÃ©cembre 2009, MessageLabs a commencÃ© Ã traquer un nouveau botnet baptisÃ© Lethic, rapidement incriminÃ© dans 2,5 % du nombre total de spams. DÃ¨s la premiÃ¨re semaine de janvier, le volume des spams diffusÃ©s par Lethic avait dÃ©jÃ presque atteint 4 % avec un pic Ã 5,25 % le 8 janvier, juste avant de ne plus donner signe de vie.

Â« *Lethic sâ□□est Ã©vaporÃ© aussi rapidement quâ□□il est apparu* Â», dÃ©clare **M. Wood**. Â« *Il envoyait autant de spams de promotion de produits pharmaceutiques que de rÃ©pliques de montres. Le botnet Bagle envoyait exactement les mÃªmes messages avec les mÃªmes liens hypertextes que Lethic, et sur une mÃªme pÃ©riode, ce qui nous amÃ¨ne Ã penser que soit Lethic et Bagle ont Ã©tÃ© crÃ©Ã©s par les mÃªmes personnes, soit les crÃ©ateurs de ces spams ont recrutÃ© les cybercriminels se cachant derriÃ¨re plusieurs botnets pour diffuser plus largement.* Â»

Pour finir, MessageLabs Intelligence a Ã©tudiÃ© lâ□□Ã©volution par rapport Ã lâ□□annÃ©e passÃ©e du prix de vente de 100 mg pour le mÃ©dicament contre les problÃ¨mes dâ□□Ã©rection, objet de spam rÃ©current, ainsi que les Ã©ventuels effets de la crise financiÃ¨re sur les spammeurs. AprÃ¨s avoir atteint un pic de 6 $ les 100 mg en dÃ©but dâ□□annÃ©e 2009, le prix du mÃ©dicament a rapidement chutÃ© aux mois de juin et juillet 2009 entre 2 et 3 $. Il sâ□□est stabilisÃ© Ã 1,60 $ depuis la fin 2009.

Â« *On ne peut pas affirmer aujourdâ□□hui que cette Ã©volution des prix reflÃ¨te la conjoncture Ã©conomique du marchÃ© des spams. Aussi, sommes-nous dÃ©cidÃ©s chez MessageLabs Intelligence Ã poursuivre nos investigations pour observer sâ□□il y a bien un retour aux prix dâ□□origine Ã mesure que la reprise Ã©conomique se confirme* Â», indique **M. Wood.**

Voici quelques-unes des autres conclusions du rapport :

Spam : en janvier 2010, la proportion des e-mails Ã©changÃ©s dans le monde sâ□□avÃ©rant Ãªtre des spams de sources nouvelles ou inconnues jusquâ□□ici est de 83,9 % (1 pour 1,2 e-mail), soit une baisse de 0,3 % depuis le mois de dÃ©cembre 2009.

Virus : la proportion des e-mails Ã©changÃ©s dans le monde vÃ©hiculant des virus de sources nouvelles ou inconnues jusquâ□□ici est de 0,31 % (1 pour 326,9 e-mails) en janvier, soit une diminution de 0,03 % depuis le mois de dÃ©cembre 2009. En janvier, 13,2 % des programmes malveillants vÃ©hiculÃ©s par e-mail contenaient des liens vers des sites malveillants, soit une diminution de 5,9 % par rapport Ã dÃ©cembre.

Phishing : en janvier, on compte 1 tentative de phishing pour 562,3 e-mails (0,18 %), soit une augmentation de 0,11 % depuis dÃ©cembre 2009. En proportion de toutes les menaces par e-mail, comme les virus et chevaux de Troie, le nombre des e-mails de phishing a diminuÃ© de 14,3 % pour reprÃ©senter 65,3 % de toutes les menaces vÃ©hiculÃ©es par e-mail.

SÃ©curitÃ© Web : les statistiques de sÃ©curitÃ© sur le Web montrent que 41,4 % des programmes malveillants interceptÃ©s sur le Web en janvier Ã©taient nouveaux, soit 0,6 % de plus quâ□□en dÃ©cembre. MessageLabs Intelligence a Ã©galement identifiÃ© une moyenne de 1 760 nouveaux sites Web par jour hÃ©bergeant des programmes malveillants et dâ□□autres programmes indÃ©sirables, de type logiciels espions et publicitaires, soit une baisse de 56,2 % depuis dÃ©cembre.

Tendances gÃ©ographiques :

â¢ Les volumes de spams au Danemark ont beau avoir baissÃ© de 0,6 % en janvier Ã 94,8 % de tous les e-mails, le pays conserve la premiÃ¨re place des victimes de spams.

â¢ Les volumes de spams sont en baisse aux Etats-Unis et au Canada, avec respectivement 91,6 % et 89,7 % de tous les e-mails. Le chiffre est de 90 % au Royaume-Uni, en baisse Ã©galement.

â¢ Aux Pays-Bas, les volumes de spams ont atteint 92,4 %, tandis quâen Australie ils atteignent 90,6 %.

â¢ A Hong Kong, ils atteignent 92,1 % et 88,2 % au Japon.

â¢ Les attaques par des virus ont augmentÃ© de 0,13 % en Chine, soit 1 virus pour 121,4 e-mails, ce qui en fait le pays le plus attaquÃ© en janvier.

â¢ La proportion des e-mails comportant un virus est de 1 pour 440,3 aux Etats-Unis et de 1 pour 383,1 au Canada. Elle est de 1 pour 271,6 en Allemagne, 1 pour 496,4 aux Pays-Bas, 1 pour 644,1 en Australie, 1 pour 331,9 Ã Hong Kong et 1 pour 396,5 au Japon.

â¢ Le Royaume-Uni est le pays oÃ¹ les attaques de phishing sont les plus nombreuses, avec 1 e-mail de phishing pour 253,6 e-mails Ã©changÃ©s.

Tendances sectorielles :

â¢ En janvier, le secteur de lâindustrie le plus victime des spams est celui de lâingÃ©nierie avec un taux de 95,1 %.

â¢ Les volumes de spams ont atteint 92,1 % dans le secteur de lâÃ©ducation, 91 % dans celui des produits chimiques et pharmaceutiques, 91,5 % dans le secteur des services informatiques, 92,3 % dans celui de la vente au dÃ©tail et enfin 89,3 % et 90,1 % dans les secteurs public et des finances, respectivement.

â¢ Les attaques par des virus ont diminuÃ© de 0,33 % dans le secteur public, mais ce secteur est passÃ© Ã la premiÃ¨re place avec 1 e-mail infectÃ© pour 109,7 e-mails reÃ§us en janvier.

â¢ La proportion des e-mails comportant un virus est de 1 pour 230,9 dans le secteur des produits chimiques et pharmaceutiques, de 1 pour 353,4 dans le secteur des services informatiques, de 1 pour 607,2 dans le secteur de la vente au dÃ©tail, de 1 pour 187,7 dans le secteur de lâenseignement et de 1 pour 391,5 dans celui des finances.

Le rapport de sÃ©curitÃ© de MessageLabs pour janvier 2010 offre des informations plus dÃ©taillÃ©es sur toutes les tendances et tous les chiffres mentionnÃ©s ci-dessus, ainsi que sur les tendances gÃ©ographiques et verticales. **Le rapport complet.**