Symantec-MessageLabs Intelligence Report de septembre 2009
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 1/10/2009 0:00:00

Les derniÃ¨res recherches concernant les spams des botnets dÃ©montrent leur dÃ©veloppement rapide et lâ□□arrivÃ©e de tout nouveaux acteurs

Symantec Corp. (Nasdaq: SYMC) annonce la publication de lâ□□Ã©dition de septembre 2009 de son rapport trimestriel **MessageLabs Intelligence Report**. Il apparaÃ®t que les botnets sont responsables de lâ□□envoi de 87,9 % des spams. Maazben, un tout nouveau botnet de spams liÃ©s aux casinos, a connu une croissance fulgurante depuis son lancement fin mai, tandis que Rustock, un ancien botnet parmi les plus dÃ©veloppÃ©s, a doublÃ© de volume depuis juin avec un mode dâ□□envoi de spam dÃ©sormais prÃ©visible.

Dâ□□aprÃ¨s **MessageLabs Intelligence**, le dÃ©veloppement de Maazben sâ□□est accÃ©lÃ©rÃ© le mois dernier pour passer de 0,5 % de tous les spams en aoÃ»t Ã 1,4 % de tous les spams en septembre. Si Rustock est le plus important en nombre de bots (entre 1,3 et 1,9 millions dâ□□ordinateurs zombies), sa production par bot reste relativement faible. Mais le mode dâ□□envoi de spams de Rustock est Ã prÃ©sent prÃ©visible : il dÃ©marre tous les jours Ã 3h00 (heure de lâ□□est), avec un pic dâ□□envoi Ã 7h00 (heure de lâ□□est) pour sâ□□arrÃªter Ã 19h00 (heure de lâ□□est).

Il fait donc une pause de huit heures avant de recommencer Ã envoyer des spams. Rustock est le seul botnet connu au cycle dâ□□envoi rÃ©gulier. Et câ□□est lâ□□un des plus dominants puisquâ□□il est Ã lâ□□origine de 10 % des spams. Son mode de fonctionnement se reflÃ¨te donc dans le schÃ©ma quotidien de distribution des spams.

Â« *Lâ□□an dernier, plusieurs FAI ont dÃ» fermer pour avoir hÃ©bergÃ© des rÃ©seaux de machines zombies parmi leurs abonnÃ©s. Bien entendu, ces fermetures ont largement affaibli les botnets* Â», explique **Paul Wood**, analyste senior pour MessageLabs Intelligence chez Symantec. Â« *Les botnets dominants ont Ã©tÃ© frappÃ©s de plein fouet, comme ce fut le cas de Cutwail, Ã la faveur de nouveaux botnets, Ã lâ□□image de Maazben. Mais ceci ne va pas durer car la technologie des botnets a su Ã©voluer depuis fin 2008 et les fermetures de FAI les plus rÃ©centes nâ□□ont plus*

autant dâ□□impact puisquâ□□elles ne durent plus que quelques heures contre des semaines voire des mois auparavant. Â»

Depuis la fermeture de FAI au cours des trois derniers mois, deux autres botnets rivalisent pour sâ□□emparer de la position occupÃ©e jusque-lÃ par Cutwail, celle du botnet le plus actif. Il sâ□□agit de Grum, qui fait la moitiÃ© de la taille de Rustock mais distribue 23,2 % de tous les spams, et de Bobax, qui reprÃ©sente 15,7 % de tous les spams. Au plus fort, Cutwail distribuait 45,8 % de tous les spams.

Egalement en septembre, MessageLabs Intelligence constate quâ□□un dÃ©clin de la pÃ©riode dâ□□essai des noms de domaine, la possibilitÃ© dâ□□annuler une inscription pendant un dÃ©lai de grÃ¢ce de 5 jours, signalÃ© par ICANN en juin 2009 peut Ãªtre Ã lâ□□origine dâ□□un changement de la nature malveillante des sites Web, suggÃ©rant que les noms de domaine malveillants sont probablement aujourdâ□□hui davantage dâ□□anciens sites corrompus plutÃ´t que de nouvelles inscriptions actives depuis peu, contrairement Ã il y a un an.

Une analyse des sites Web crÃ©Ã©s dÃ©libÃ©rÃ©ment pour distribuer des programmes malveillants rÃ©vÃ¨le que les noms de domaine Â« jeunes Â», actifs depuis trois mois au plus Ã la date de leur premiÃ¨re interdiction pour hÃ©bergement de contenus malveillants, sont relativement peu nombreux mais quâ□□ils sont dans leur grande majoritÃ© repÃ©rÃ©s comme malveillants et bloquÃ©s et quâ□□ils comportent du contenu malveillant dÃ¨s le dÃ©part. 90 % des noms de domaine Â« jeunes Â» sont arrÃªtÃ©s dans les 38 jours qui suivent lâ□□inscription.

M. Wood poursuit ainsi : Â« *Avec une fenÃªtre dâ□□action aussi petite, il nâ□□est pas surprenant que les agresseurs inscrivent les noms de domaine de plus en plus vite, ce qui sous-entend quâ□□ils travaillent trÃ¨s dur pour crÃ©er de nouveaux domaines et corrompre de nouveaux sites Web. En rÃ¨gle gÃ©nÃ©rale, les programmes malveillants que distribuent ces sites Web nâ□□Ã©voluent pas rapidement et le rythme dâ□□apparition de nouveaux programmes correspond Ã un tiers seulement du rythme de crÃ©ation de noms de domaine malveillants.* Â»

Une analyse des noms de domaine plus anciens, ceux inscrits depuis plus de trois mois et corrompus pour distribuer des programmes malveillants, montre que 90 % de ces sites Web ne sont fermÃ©s quâ□□aprÃ¨s 138 jours dâ□□activitÃ©, soit longtemps aprÃ¨s leurs cadets. MessageLabs Intelligence a dÃ©couvert que 80 % des noms de domaine bloquÃ©s comme malveillants sont des sites Web lÃ©gitimes ayant Ã©tÃ© corrompus.

Â« *Un agresseur a davantage intÃ©rÃªt Ã compromettre un site Web lÃ©gitime quâ□□Ã crÃ©er un nom de domaine spÃ©cialement pour distribuer des programmes malveillants* Â», conclut M. Wood. Â« *Fondamentalement, il perdra moins de temps Ã dÃ©tourner des sites Web et il peut compter sur une durÃ©e plus longue de distribution de ses programmes malveillants. De plus, avec le dÃ©lai de grÃ¢ce, cette rÃ¨gle qui autorise lâ□□inscription gratuite dâ□□un nom de domaine et son annulation dans les cinq jours, les cybercriminels sâ□□en donnent Ã cÅ□ur joie puisquâ□□ils peuvent profiter du systÃ¨me sans jamais payer la distribution de leurs programmes malveillants.* Â»

Voici quelques-unes des autres conclusions du rapport :

Spam : en septembre 2009, la proportion des e-mails Ã©changÃ©s dans le monde sâ□□avÃ©rant Ãªtre des spams de sources nouvelles ou inconnues jusque-ici est de 86,4 % (1 pour 1,2 e-mail), soit une augmentation de 2,1 % depuis le mois dâ□□aoÃ»t. Les volumes de spams au troisiÃ¨me trimestre 2009 sont autour de 88,1 %, contre 81 % au troisiÃ¨me trimestre 2008.

Virus : la proportion des e-mails Ã©changÃ©s dans le monde vÃ©hiculant des virus de sources nouvelles ou inconnues jusque-ici est de 0,25 % (1 pour 399,2 e-mails) en septembre, soit une diminution de 0,09 % depuis le mois dâ□□aoÃ»t. En septembre, 39,8 % des programmes malveillants vÃ©hiculÃ©s par e-mail consistaient en des liens vers des sites Web malveillants, soit une augmentation de 22 % depuis aoÃ»t. Au troisiÃ¨me trimestre 2009, on compte 1 e-mail malveillant pour 330,3 e-mails, alors que le chiffre Ã©tait dâ□□1 pour 122,5 au troisiÃ¨me trimestre 2008.

Phishing : En septembre, on compte 1 tentative de phishing pour 437,1 e-mails (0,23 %), une augmentation de 0,06 % depuis aoÃ»t. 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 11,1 % pour reprÃ©senter 75,8 % de toutes les menaces vÃ©hiculÃ©es par e-mail interceptÃ©es en septembre. En moyenne, lâ□□activitÃ© de phishing au troisiÃ¨me trimestre 2009 concerne 1 e-mail pour 368,6, alors que le chiffre Ã©tait dâ□□1 pour 330,5 au troisiÃ¨me trimestre 2008.

SÃ©curitÃ© Web : les statistiques de sÃ©curitÃ© sur le Web montrent que 33,5 % des programmes malveillants interceptÃ©s sur le Web en septembre Ã©taient nouveaux, en diminution de 2,6 % depuis aoÃ»t. Et 12,3 % des programmes malveillants sur le Web en septembre Ã©taient nouveaux, une augmentation de 0,4 % depuis aoÃ»t. MessageLabs Intelligence a Ã©galement identifiÃ© une moyenne de 2 337 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 33,4 % depuis aoÃ»t.

Tendances gÃ©ographiques :

Â· Les volumes de spams au Danemark ont atteint 95,6 % des e-mails Ã©changÃ©s en septembre, en faisant le pays le plus victime des spams.

Â· Les volumes de spams ont atteint 91,8 % aux Etats-Unis et 91,2 % au Canada. Le chiffre est de 91,7 % au Royaume-Uni.

Â· La plus forte augmentation est celle de la SuÃ¨de, Ã 7,2 %, avec une proportion de 89,6 %. Aux Pays-Bas, les volumes de spams ont atteint 91,9 %. Ils restent inchangÃ©s en Autriche Ã 90,7 % et atteignent 93,4 % Ã Hong Kong et 89,4 % au Japon.

Â· Les attaques par des virus ont augmentÃ© de 0,08 % en Suisse, ce qui en fait le pays le plus attaquÃ© en septembre.

Â· La proportion des e-mails comportant un virus est de 1 pour 552,5 aux Etats-Unis et de 1 pour 393,8 au Canada. Elle est de 1 pour 358,5 en Allemagne, 1 pour 666,2 aux Pays-Bas, 1 pour 626,5 en Australie, 1 pour 328,7 Ã Hong Kong et 1 pour 552 au Japon.

Â· La Suisse est le pays oÃ¹ les attaques de phishing sont les plus nombreuses, avec 1 e-mail de phishing pour 246,4 e-mails Ã©changÃ©s. Vient ensuite le Royaume-Uni, avec 1 attaque de phishing pour 252,3.

Tendances sectorielles :

Â· En septembre, le secteur de lâ□□industrie le plus victime des spams est celui de lâ□□ingÃ©nierie avec un taux de 94,7 %.

Â· Les volumes de spams ont atteint 93,8 % dans le secteur de lâ□□Ã©ducation, 92 % dans celui des produits chimiques et pharmaceutiques ; 92,2 % dans le secteur de la vente au dÃ©tail, 90,6 % dans le secteur public et 90,6 % dans le secteur des finances.

Â· Les attaques par des virus ont diminuÃ© de 0,36 % dans le secteur de lâ□□Ã©ducation, mais ce secteur conserve la premiÃ¨re place avec 1 e-mail infectÃ© pour 209,7 e-mails reÃ§us en septembre.

Â· La proportion des e-mails comportant un virus est de 1 pour 288,2 dans le secteur des produits chimiques et pharmaceutiques, de 1 pour 346,4 dans le secteur des services informatiques, de 1 pour 682 dans le secteur de la vente au dÃ©tail, de 1 pour 262,2 dans le secteur public et de 1 pour 579,2 dans celui des finances.

Vous trouverez de plus amples dÃ©tails sur les tendances et les statistiques citÃ©es ici, ainsi que sur les tendances gÃ©ographiques et sectorielles dans le **rapport complet MessageLabs Intelligence** de septembre 2009,

MessageLabs Intelligence, une division de Symantec, est une source fiable dâ□□information et dâ□□analyse des problÃ©matiques, tendances et statistiques de sÃ©curitÃ© des solutions de messagerie. MessageLabs Intelligence vous informe sur les menaces pour la sÃ©curitÃ© informatique en sâ□□appuyant sur les flux de donnÃ©es permanents des tours de contrÃ´le installÃ©es partout dans le monde par Symantec et qui analysent des milliards de messages chaque semaine.