Symantec annonce la publication de l'édition de septembre et du troisième trimestre 2009 de son rapport MessageLabs Intelligence Report

Les dernières recherches concernant les spams des botnets démontrent leur développement rapide et l'arrivée de tout nouveaux acteurs

CUPERTINO, Californie – 29 septembre 2009 – Symantec Corp. (Nasdaq: SYMC) annonce la publication de l'édition de septembre 2009 de son rapport trimestriel MessageLabs Intelligence Report. Il apparaît que les botnets sont responsables de l'envoi de 87,9 % des spams. Maazben, un tout nouveau botnet de spams liés aux casinos, a connu une croissance fulgurante depuis son lancement fin mai, tandis que Rustock, un ancien botnet parmi les plus développés, a doublé de volume depuis juin avec un mode d'envoi de spam désormais prévisible.

D'après MessageLabs Intelligence, le développement de Maazben s'est accéléré le mois dernier pour passer de 0,5 % de tous les spams en août à 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 d'ordinateurs zombies), sa production par bot reste relativement faible. Mais le mode d'envoi de spams de Rustock est à présent prévisible : il démarre tous les jours à 3h00 (heure de l'est), avec un pic d'envoi à 7h00 (heure de l'est) pour s'arrêter à 19h00 (heure de l'est). Il fait donc une pause de huit heures avant de recommencer à envoyer des spams. Rustock est le seul botnet connu au cycle d'envoi régulier. Et c'est l'un des plus dominants puisqu'il est à l'origine de 10 % des spams. Son mode de fonctionnement se reflète donc dans le schéma quotidien de distribution des spams.

« *L'an dernier, plusieurs FAI ont dû fermer pour avoir hébergé des réseaux de machines zombies parmi leurs abonnés. Bien entendu, ces fermetures ont largement affaibli les botnets* », explique Paul Wood, analyste senior pour MessageLabs Intelligence chez Symantec. « *Les botnets dominants ont été frappés de plein fouet, comme ce fut le cas de Cutwail, à la faveur de nouveaux botnets, à l'image de Maazben. Mais ceci ne va pas durer car la technologie des botnets a su évoluer depuis fin 2008 et les fermetures de FAI les plus récentes n'ont plus autant d'impact puisqu'elles ne durent plus que quelques heures contre des semaines voire des mois auparavant.* »

Depuis la fermeture de FAI au cours des trois derniers mois, deux autres botnets rivalisent pour s'emparer de la position occupée jusque-là par Cutwail, celle du botnet le plus actif. Il s'agit de Grum, qui fait la moitié de la taille de Rustock mais distribue 23,2 % de tous les spams, et de Bobax, qui représente 15,7 % de tous les spams. Au plus fort, Cutwail distribuait 45,8 % de tous les spams.

Egalement en septembre, MessageLabs Intelligence constate qu'un déclin de la période d'essai des noms de domaine, la possibilité d'annuler une inscription pendant un délai de grâce de 5 jours, signalé par ICANN en juin 2009 peut être à l'origine d'un changement de la nature malveillante des sites Web, suggérant que les noms de domaine malveillants sont probablement aujourd'hui davantage d'anciens sites corrompus plutôt que de nouvelles inscriptions actives depuis peu, contrairement à il y a un an.

Une analyse des sites Web créés délibérément pour distribuer des programmes malveillants révèle que les noms de domaine « jeunes », actifs depuis trois mois au plus à la date de leur première interdiction pour hébergement de contenus malveillants, sont relativement peu nombreux mais qu'ils sont dans leur grande majorité repérés comme malveillants et bloqués et qu'ils comportent du contenu malveillant dès le départ. 90 % des noms de domaine « jeunes » sont arrêtés dans les 38 jours qui suivent l'inscription.

M. Wood poursuit ainsi : « Avec une fenêtre d'action aussi petite, il n'est pas surprenant que les agresseurs inscrivent les noms de domaine de plus en plus vite, ce qui sous-entend qu'ils travaillent très dur pour créer de nouveaux domaines et corrompre de nouveaux sites Web. En règle générale, les programmes malveillants que distribuent ces sites Web n'évoluent pas rapidement et le rythme d'apparition de nouveaux programmes correspond à un tiers seulement du rythme de création de noms de domaine malveillants. »

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 fermés qu'après 138 jours d'activité, soit longtemps après leurs cadets. MessageLabs Intelligence a découvert que 80 % des noms de domaine bloqués comme malveillants sont des sites Web légitimes ayant été corrompus.

« Un agresseur a davantage intérêt à compromettre un site Web légitime qu'à créer un nom de domaine spécialement pour distribuer des programmes malveillants », conclut M. Wood. « Fondamentalement, il perdra moins de temps à détourner des sites Web et il peut compter sur une durée plus longue de distribution de ses programmes malveillants. De plus, avec le délai de grâce, cette règle qui autorise l'inscription gratuite d'un nom de domaine et son annulation dans les cinq jours, les cybercriminels s'en donnent à cœur joie puisqu'ils peuvent profiter du système sans jamais payer la distribution de leurs programmes malveillants. »

Voici quelques-unes des autres conclusions du rapport :

Spam : en septembre 2009, la proportion des e-mails échangés dans le monde s'avérant être 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 d'août. Les volumes de spams au troisième trimestre 2009 sont autour de 88,1 %, contre 81 % au troisième trimestre 2008.

Virus : la proportion des e-mails échangés dans le monde véhiculant 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 d'août. En septembre, 39,8 % des programmes malveillants véhiculés par e-mail consistaient en des liens vers des sites Web malveillants, soit une augmentation de 22 % depuis août. Au troisième trimestre 2009, on compte 1 e-mail malveillant pour 330,3 e-mails, alors que le chiffre était d'1 pour 122,5 au troisième trimestre 2008.

Phishing : En septembre, on compte 1 tentative de phishing pour 437,1 e-mails (0,23 %), une augmentation de 0,06 % depuis août. En proportion de toutes les menaces par e-mail, comme les virus et chevaux de Troie, le nombre des e-mails de phishing a diminué de 11,1 % pour représenter 75,8 % de toutes les menaces véhiculées par e-mail interceptées en septembre. En moyenne, l'activité de phishing au troisième trimestre 2009 concerne 1 e-mail pour 368,6, alors que le chiffre était d'1 pour 330,5 au troisième trimestre 2008.

Sécurité Web : les statistiques de sécurité sur le Web montrent que 33,5 % des programmes malveillants interceptés sur le Web en septembre étaient nouveaux, en diminution de 2,6 % depuis août. Et 12,3 % des programmes malveillants sur le Web en septembre étaient nouveaux, une augmentation de 0,4 % depuis août. MessageLabs Intelligence a également identifié une moyenne de 2 337 nouveaux sites Web par jour hébergeant des programmes malveillants et d'autres programmes indésirables, de type logiciels espions et publicitaires, soit une baisse de 33,4 % depuis août.

Tendances géographiques :

- Les volumes de spams au Danemark ont atteint 95,6 % des e-mails échangés en septembre, en faisant le pays le plus victime des spams.

- 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.

- La plus forte augmentation est celle de la Suède, à 7,2 %, avec une proportion de 89,6 %. Aux Pays-Bas, les volumes de spams ont atteint 91,9 %. Ils restent inchangés en Autriche à 90,7 % et atteignent 93,4 % à Hong Kong et 89,4 % au Japon.

- Les attaques par des virus ont augmenté de 0,08 % en Suisse, ce qui en fait le pays le plus attaqué en septembre.

- 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 à Hong Kong et 1 pour 552 au Japon.

- La Suisse est le pays où les attaques de phishing sont les plus nombreuses, avec 1 e-mail de phishing pour 246,4 e-mails échangés. Vient ensuite le Royaume-Uni, avec 1 attaque de phishing pour 252,3.

Tendances sectorielles :

- En septembre, le secteur de l'industrie le plus victime des spams est celui de l'ingénierie avec un taux de 94,7 %.

- Les volumes de spams ont atteint 93,8 % dans le secteur de l'éducation, 92 % dans celui des produits chimiques et pharmaceutiques ; 92,2 % dans le secteur de la vente au détail, 90,6 % dans le secteur public et 90,6 % dans le secteur des finances.

- Les attaques par des virus ont diminué de 0,36 % dans le secteur de l'éducation, mais ce secteur conserve la première place avec 1 e-mail infecté pour 209,7 e-mails reçus en septembre.

- 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 détail, de 1 pour 262,2 dans le secteur public et de 1 pour 579,2 dans celui des finances.

Vous trouverez de plus amples détails sur les tendances et les statistiques citées ici, ainsi que sur les tendances géographiques et sectorielles dans le rapport complet MessageLabs Intelligence de septembre 2009, disponible à l'adresse suivante : http://www.messagelabs.com/intelligence.aspx.

MessageLabs Intelligence, une division de Symantec, est une source fiable d'information et d'analyse des problématiques, tendances et statistiques de sécurité des solutions de messagerie. MessageLabs Intelligence vous informe sur les menaces pour la sécurité informatique en s'appuyant sur les flux de données permanents des tours de contrôle installées partout dans le monde par Symantec et qui analysent des milliards de messages chaque semaine.

A propos de Symantec

Leader mondial dans le domaine des solutions logicielles d'infrastructure, Symantec permet aux entreprises et aux particuliers d'avoir confiance dans le monde connecté. Symantec aide ses clients à protéger leurs infrastructures, informations et interactions en proposant des solutions logicielles et des services ayant pour but de réduire les risques en matière de sécurité, disponibilité, conformité et performances. Symantec est présente dans plus de 40 pays à travers le monde. Plus d'informations à trouver sur : www.symantec.com

###

NOTE AUX REDACTEURS : si vous souhaitez des informations complémentaires sur la Symantec Corporation et ses produits, merci de visiter la News Room de Symantec à l'adresse http://www.symantec.com/news. Tous les prix mentionnés sont en dollars américains et ne sont valables qu'aux États-Unis.