Les botnets dÃ©veloppent de nouvelles techniques de survie
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 11/12/2009 0:00:00

Symantec Corp. annonce la publication de lâ□□Ã©dition 2009 de son rapport sur la sÃ©curitÃ© **MessageLabs Intelligence Report**. Ce rapport annuel fait le point sur les techniques de survie imaginÃ©es par les cybercriminels et dÃ©crit comment leurs activitÃ©s ont Ã©voluÃ© en termes de volume et de diversitÃ© tout au long de lâ□□annÃ©e 2009.

Lâ□□activitÃ© de spams a connu des turbulences tout au long de lâ□□annÃ©e , avec des volumes moyens atteignant 87,7 % des e-mails Ã©changÃ©s, mais avec des hauts et des bas Ã 90,4 % en mai et 73,3 % en fÃ©vrier. 83,4 % des 107 milliards de courriers indÃ©sirables distribuÃ©s chaque jour en moyenne dans le monde Ã©tant envoyÃ©s par des ordinateurs infectÃ©s, la fermeture de FAI hÃ©bergeant des botnets, comme McColo fin 2008 et Real Host en aoÃ»t 2009, semble inciter les botnets Ã rÃ©Ã©valuer et amÃ©liorer leur stratÃ©gie de commande et de contrÃ´le pour que la restauration ne prenne plus que quelques heures et non plus des semaines, voire des mois. Il est trÃ¨s probable quâ□□en 2010 les botnets soient plus autonomes et intelligents, avec chaque nÅ□ud comportant un programme autonome qui lui permette de coordonner et de prolonger sa propre survie.

Les botnets ont continuÃ© de dominer le paysage de la cybersÃ©curitÃ© en 2009.

Les dix botnets les plus dÃ©veloppÃ©s, dont Cutwail, Rustock et Mega-D, contrÃ´lent dÃ©sormais au moins cinq millions dâ□□ordinateurs infectÃ©s. Cutwail a dominÃ© lâ□□univers des spams et des programmes malveillants en 2009, avec 29 % de tous les spams en circulation ou 8 500 milliards de spams envoyÃ©s entre avril et novembre 2009. Cutwail a Ã©galement utilisÃ© sa force pour distribuer des e-mails comportant le cheval de Troie Bredolab, dÃ©guisÃ© en fichier .zip joint. Lâ□□une des principales menaces de 2009, le cheval de Troie Bredolab, permettait Ã celui qui lâ□□envoyait de prendre le contrÃ´le total de lâ□□ordinateur attaquÃ©, qui pouvait alors Ãªtre utilisÃ© pour dÃ©ployer dâ□□autres programmes malveillants, logiciels espions et publicitaires du botnet sur lâ□□ordinateur de la victime. Le pourcentage des spams relayant le cheval de Troie Bredolab Ã©tait en augmentation constante fin 2009 et a culminÃ© en octobre 2009, avec des estimations portant Ã 3,6 milliards le nombre dâ□□e-mails de diffusion de Bredolab en circulation.

Â« *En 2009, les menaces ont gagnÃ© en sophistication. PlutÃ´t que les traditionnels envois massifs de spams et les attaques par des programmes malveillants, nous avons interceptÃ© davantage de variantes plus complexes et efficaces, faisant appel Ã©galement Ã des technologies plus Ã©voluÃ©es* Â», explique **Paul Wood**, analyste senior pour MessageLabs Intelligence, Symantec.

Â« *Nous avons mis fin Ã plus de 21 millions de types diffÃ©rents de campagnes de spams en 2009, plus du double par rapport Ã 2008. Et le nombre de variantes de programmes malveillants a augmentÃ© de 23 % par rapport Ã lâ□□annÃ©e prÃ©cÃ©dente. Ces chiffres Ã la hausse laissent penser que, du fait de la plus grande accessibilitÃ© dâ□□outils du parfait cybercriminel, il est devenu plus simple que jamais de crÃ©er des spams et programmes malveillants et de les diffuser, puis de les exploiter.* Â»

La menace de sÃ©curitÃ© la plus prÃ©occupante observÃ©e cette annÃ©e est Conficker/Downadup, un ver qui permet Ã ses crÃ©ateurs dâ□□installer des logiciels Ã distance sur les machines infectÃ©es. Le ver Conficker est apparu pour la premiÃ¨re fois fin 2008, mais une mise Ã jour datant du 1er avril 2009 lui a confÃ©rÃ© davantage de fonctionnalitÃ©s lui permettant de mieux contourner les moyens de dÃ©tection. Conficker est dâ□□autant plus prÃ©occupant que lâ□□on ne sait toujours pas quelle est lâ□□utilisation prÃ©vue des plus de six millions de machines infectÃ©es Ã ce jour, prÃ©cise le groupe de travail sur Conficker, qui a quand mÃªme minimisÃ© les dÃ©gÃ¢ts potentiels de ce programme malveillant en 2009.

Au premier semestre 2009, la crise du crÃ©dit a servi de prÃ©texte pour de nombreuses nouvelles attaques dites financiÃ¨res, les spammeurs et les criminels cherchant Ã tirer profit de lâ□□incertitude qui rÃ©gnait autour du ralentissement Ã©conomique mondial. En fÃ©vrier, la plupart des premiers spams de la pÃ©riode de rÃ©cession contenaient des liens hypertexte vers plusieurs moteurs de recherche bien connus. En 2009, 90,6 % des spams comportaient une URL, avec une hausse trÃ¨s marquÃ©e au second semestre dâ□□URL raccourcies, facilitant le maquillage du vrai site que lâ□□utilisateur souhaitait visiter et compliquant lâ□□identification de ces messages comme spams par les filtres traditionnels. Des cas frÃ©quents dâ□□utilisation de la technique de raccourcissement dâ□□URL ont Ã©tÃ© constatÃ©s sur les sites de rÃ©seaux sociaux et de micro-blogs. Les cybercriminels apprÃ©cient cette technique du fait de la confiance naturelle des utilisateurs de ces sites les uns envers les autres.

En plus de la crise financiÃ¨re mondiale, beaucoup de spams en 2009 Ã©taient inspirÃ©s de divers autres Ã©vÃ©nements, occasions festives ou encore actualitÃ©s, comme la St. Valentin, la pandÃ©mie de grippe A/H1N1 et le dÃ©cÃ¨s de cÃ©lÃ©britÃ©s comme Michael Jackson ou Patrick Swayze. Les crÃ©ateurs de programmes malveillants et auteurs de campagnes 419 de spams de demande dâ□□avances financiÃ¨res ont rivalisÃ© dâ□□imagination cette annÃ©e. Les premiers exemples autour de Michael Jackson sont apparus quelques jours seulement aprÃ¨s lâ□□annonce de son dÃ©cÃ¨s, dont un cheval de Troie brÃ©silien masquÃ© dans des liens hypertexte malveillants.

Â« *Si les attaques sont de plus en plus innovantes et sophistiquÃ©es, les prÃ©visions jouent un grand rÃ´le dans la lutte quotidienne contre les menaces de sÃ©curitÃ©* Â», dÃ©clare **M. Wood**. Â« *Lâ□□industrie de la sÃ©curitÃ© reconnaÃ®t la recrudescence des attaques thÃ©matiques, comme celles entourant la St Valentin, NoÃ«l ou le dÃ©cÃ¨s de cÃ©lÃ©britÃ©s, mais au vu de leur frÃ©quence et de leurs volumes, il est clair que les cybercriminels obtiennent ce quâ□□ils cherchent ; sans quoi leurs tactiques auraient Ã©voluÃ©. Â»*

Enfin les technologies CAPTCHA (Completely Automated Public Turing test to tell Computer and Humans Apart) ont occupÃ© le devant de la scÃ¨ne cette annÃ©e tandis que des outils de rupture

de CAPTCHA devenaient accessibles sur le marchÃ© souterrain, permettant aux cybercriminels de crÃ©er de trÃ¨s grands nombres de comptes rÃ©els sur les sites de messagerie Ã©lectronique et instantanÃ©e, ainsi que de rÃ©seaux sociaux. On constate Ã©galement un nombre croissant dâ□□entreprises employant de vrais individus 24 heures sur 24 pour crÃ©er de vrais comptes sur les grands sites de messagerie Ã©lectronique. Le poste est souvent prÃ©sentÃ© comme un job de traitement de donnÃ©es, oÃ¹ chaque employÃ© peut prÃ©tendre Ã recevoir deux Ã trois dollars pour 1 000 comptes crÃ©Ã©s ; ces comptes sont ensuite vendus Ã des spammeurs contre 30 Ã 40 dollars. Certains grands sites cherchent des alternatives aux lettres et chiffres distordus. Certains sâ□□intÃ©ressent Ã des grandes bibliothÃ¨ques de photos, qui demandent Ã lâ□□utilisateur une analyse ou une interaction impossible pour un programme informatique.

Les principales tendances en 2009 :

â□¢ SÃ©curitÃ© Web : En 2009, les statistiques montrent une recrudescence des sites Web malveillants, avec 2 465 sites Web interrompus en moyenne chaque jour contre 2 290 en 2008, soit une hausse de 7,6 %. MessageLabs Intelligence a bloquÃ© les sites Web malveillants de 30 000 domaines distincts. 80 % des noms de domaine bloquÃ©s comme malveillants Ã©taient des sites Web lÃ©gitimes ayant Ã©tÃ© corrompus, les 20 % restants Ã©tant de nouveaux domaines crÃ©Ã©s dÃ©libÃ©rÃ©ment avec du contenu malveillant.

â□¢ Spam : En 2009, la proportion des e-mails sâ□□avÃ©rant Ãªtre des spams Ã©tait de 87,7 % (81,2 % en 2008), en augmentation de 6,5 % par rapport Ã lâ□□annÃ©e prÃ©cÃ©dente. Les spams images ont culminÃ© en avril, reprÃ©sentant 56,4 % de tous les spams le 5 avril, alors que la moyenne annuelle Ã©tait de 28,2 %.

â□¢ Virus : En 2009, la proportion des e-mails comportant un virus Ã©tait de 1 pour 286,4 e-mails (0,35 %), soit une baisse de 0,35 % par rapport Ã 2008 oÃ¹ le chiffre Ã©tait de 1 pour 143,8 e-mails (0,70 %). Ce recul sâ□□explique par la tendance Ã dÃ©velopper davantage de variantes (augmentation de 23 % en 2009 par rapport Ã 2008) mais moins dâ□□e-mails malveillants par souche (environ 5 827 e-mails malveillants par souche en 2009 contre 10 436 e-mails par souche en 2008).

â□¢ Phishing : Le nombre dâ□□attaques de phishing Ã©tait de 1 pour 325,2 e-mails (0,31 %) contre 1 pour 244,9 (0,41 %) en 2008. En 2009, il y a eu plus de 161 milliards dâ□□attaques de phishing en circulation.

Le rapport complet MessageLabs Intelligence Report 2009