Commtouch : DÃ©mantÃ¨lement de Rustock, 400 % de spams en plus !
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 13/5/2011 14:30:00

Le nombre de malwares envoyÃ©s par courriels a augmentÃ© de 400 % pendant laÂ derniÃ¨re semaine du mois de mars, mentionne Commtouch dans son rapportÂ trimestriel Internet Threats Trend Report, sur les menaces internet.

Lâaugmentation significative a Ã©tÃ© dÃ©tectÃ©e deux semaines aprÃ¨s le dÃ©mantÃ¨lement du botnet Rustock qui avait eu pour consÃ©quence une diminution de 30% du niveau des spams.

Bien que lâactivitÃ© des spams a diminuÃ© Ã lâapproche de la nouvelle annÃ©e, elle a augmentÃ© de maniÃ¨re significative aprÃ¨s les vacances. De janvier Ã mi-mars, la moyenne journaliÃ¨re des spams Ã©tait de 168 milliards, aprÃ¨s le dÃ©mantÃ¨lement de Rustock, cette moyenne est tombÃ©e Ã 119 milliards. Les activitÃ©s liÃ©es aux zombies ont elles aussi diminuÃ© aprÃ¨s le dÃ©mantÃ¨lement de Rustock. AprÃ¨s une accalmie de quelques semaines seulement, de nouvelles attaques de malwares ont Ã©tÃ© dÃ©clenchÃ©es provoquant Ã la fin du trimestre une forte augmentation du nombre de Â« machines ZombiesÂ».

Â« *Les botnets reprÃ©sentent une part essentielle de lâinfrastructure nÃ©cessaire aux cybercriminels, leur offrant dâÃ©normes ressources informatiques, une bande passante et lâanonymat*, affirme **Asaf Greiner**, Vice-prÃ©sident de Commtouch. *Le dÃ©mantÃ¨lement des botnets est immÃ©diatement suivi par de nombreuses tentatives de reconstruction, afin que les opÃ©rations criminelles puissent se poursuivre.* Â»

Les trois premiers mois de 2011 ont Ã©tÃ© les tÃ©moins dâun large Ã©ventail de tentatives de distribution de malware:

â¢ Les courriels de masse de type Â« suivi dâinformation de colis Â» prÃ©tendant provenir dâUPS et de DHL ont reprÃ©sentÃ© environ 30% de tous les courriels envoyÃ©s pendant le pic de lâattaque

â¢ Les liens URLs envoyÃ©s dans lâapplication Â« chat Â» de Facebook depuis des comptes usurpÃ©s invitant les Internautes Ã ouvrir une page Web de Facebook Â«en apparence Â» et Ã tÃ©lÃ©charger un Â« soi-disant Â» CODEC contenant un code viral

â¢ Des fichiers PDF sous la forme de documents Xerox scannÃ©s contenant des scripts

malveillants

â¢ Le virus Â« Kama Sutra Â» tentant les internautes avec une prÃ©sentation PowerPoint trÃ¨s explicite

â¢ Redirection de la page dâaccueil personnelle crÃ©Ã©e chez T-Online, invitant le visiteur Ã procÃ©der Ã une analyse antivirale locale et tÃ©lÃ©charger un antivirus frauduleux

Parmi les autres points traitÃ©s dans ce rapport du premier trimestre 2011 :

â¢ Le niveau trimestriel de spams correspond en moyenne Ã 149 milliards de messages de type spam/hameÃ§onnage par jour durant le premier trimestre alors quâil Ã©tait de 142 milliards durant le quatriÃ¨me trimestre 2010 et de 198 milliards durant le troisiÃ¨me trimestre 2010.

â¢ 258 000 zombies en moyenne ont Ã©tÃ© activÃ©s chaque jour, une baisse significative par rapport au 288 000 du quatriÃ¨me trimestre 2010 et au 339 000 du troisiÃ¨me trimestre 2010.

â¢ Le sujet le plus populaire des spams ce trimestre est encore la pharmacie, reprÃ©sentant 28% de tous les spams avec une diminution par rapport au 42% du quatriÃ¨me trimestre 2010.

â¢ Lâ€™Inde garde son titre pour le troisiÃ¨me trimestre consÃ©cutif, du pays possÃ©dant le plus de zombies (17% du total mondial).

â¢ Les sites catÃ©gorisÃ©s Â« Parked Domains ou rÃ©servation domaine de noms de domaines / domaines avec trÃ¨s peu de contenuÂ» correspondent Ã la catÃ©gorie web la plus Ã mÃªme dâÃªtre infectÃ©e par les malwares.

â¢ Le domaine du Web 2.0 avec un contenu gÃ©nÃ©rÃ© par les utilisateurs, ainsi que les divertissements (musique, tÃ©lÃ©vision, films, critiques, etc.) continuent Ã Ãªtre les thÃ¨mes les plus populaires des crÃ©ateurs de blogs avec 21% du contenu gÃ©nÃ©rÃ©.

Le report dÃ©crit aussi les tentatives des spammers et des phishers (hameÃ§onneurs) dâÃ©conomiser de lâargent en cachant leur prÃ©sence sur des forums abandonnÃ©s ou en utilisant des services de formulaires en ligne pour rÃ©cupÃ©rer plus facilement les donnÃ©es des utilisateurs hameÃ§onnÃ©s.

Le rapport trimestriel de Commtouch est basÃ© sur lâanalyse journaliÃ¨re de plus de deux milliards de messages et de transactions Internet arrivant dans ses centres de dÃ©tection mondiaux.

Les technologies RPDâ¢ (Recurrent Pattern Detection ou DÃ©tection de Signatures RÃ©currentes), GlobalViewâ¢ et Command Antivirus multi-couches permettent dâidentifier et de bloquer toutes nouvelles agressions de spams, malwares ou attaques de zombies dÃ©s leurs dÃ©clenchements.