Internet : Les cybercriminels redoublent d'efficacitÃ© dans leur attaque
Internet
PostÃ© par : JulieM
PubliÃ©e le : 19/7/2010 0:00:00

Les cybercriminels redoublent dâefficacitÃ© avec des attaques organisÃ©es en plusieurs Ã©tapes, selon **le rapport de Commtouch** Les activitÃ©s frauduleuses et les spameurs associent Messaging, Web et Â« IngÃ©nierie Sociale Â» pour accroÃ®tre leurs taux de rÃ©ussite

Commtouch publie son rapport sur les menaces Internet : **Internet Threats Trend Report for Q2 2010** et un rÃ©sumÃ© vidÃ©o du rapport : video highlights from the report.

Les cybercriminels ont augmentÃ© lâefficacitÃ© de leurs actions par la crÃ©ation dâattaques en plusieurs Ã©tapes, appelÃ©es aussi Â« attaques enchainÃ©es Â», qui combinent la messagerie Internet et des Ã©lÃ©ments de type Web. **Les cybercriminels utilisent des courriels** ou des rÃ©sultats de moteurs de recherche pour attirer leurs victimes vers des sites hÃ©bergeant des pourriels publicitaires, des malwares ou des phishing (hameÃ§onnage). Le rapport Q2 analyse les diffÃ©rentes mÃ©thodes frauduleuses que les distributeurs de malwares et les spammeurs utilisent pour pousser leurs victimes Ã lâaction, comme lâutilisation de marques reconnues comme Apple et Google ou les jours particuliers du calendrier comme la fÃªte des MÃ¨res ou encore des Ã©vÃ©nements comme la coupe du monde de football.

Durant le second trimestre, Gmail et Yahoo sont restÃ©s en tÃªte pour la diffusion des courriels et ils ont Ã©tÃ© rejoints par Twitter qui se trouve parmi les six premiers. Le nom de domaine Twitter a Ã©tÃ© usurpÃ© et employÃ© dans un envoi en masse de courriels afin de tromper les utilisateurs et pousser ces derniers Ã aller sur une page de rÃ©initialisation de leur mot de passe contenant un malware.

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 ou Â« Data Cloud Â».

. Parmi les autres points traitÃ©s dans ce rapport du second trimestre :

â¢ Le niveau trimestriel de spam correspond en moyenne Ã 82% de tout le trafic de messagerie, avec une baisse allant jusquâÃ 71% au dÃ©but du mois de mai et une hausse atteignant presque 92% Ã la fin juin. Ces chiffres sont un peu plus faibles que ceux du premier trimestre et correspondent Ã une moyenne de 179 milliards de messages de type spam par jour.

â¢ Le niveau de spam dans le domaine de la Pharmacie reste au sommet avec 64% des messages de type spam.

â¢ 307 000 zombies en moyenne ont Ã©tÃ© activÃ©s chaque jour pour effectuer ces missions malveillantes, ce qui reprÃ©sente une lÃ©gÃ¨re augmentation par rapport au trimestre prÃ©cÃ©dent.

â¢ Lâ€™Inde a pris la place du BrÃ©sil pour le titre du pays possÃ©dant le plus de zombies (13% du total mondial).

â¢ Â« TDSS.17 Â» a Ã©tÃ© le courriel porteur de virus le plus diffusÃ©, mais le malware Â« Mal/Bredo Â» a eu le plus de variantes : plus de 1800 (plus du double de variantes que lors du premier trimestre).

â¢ Les sites catÃ©gorisÃ©s Â« Pornographie Â» restent la catÃ©gorie web Ã Ãªtre la plus 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.) sont les thÃ¨mes le plus populaires des crÃ©ateurs de blogs.

Â« *Les cybercriminels ont Ã©tÃ© obligÃ©s de changer leurs techniques pour arriver Ã tromper les nouvelles technologies de dÃ©tection*, affirme **Asaf Greiner**, Vice-PrÃ©sident de Commtouch pour les produits. *Les attaques complexes Ã plusieurs Ã©tapes et une ingÃ©nierie sociale amÃ©liorÃ©e semblent Ãªtre leur technique prÃ©fÃ©rÃ©e.* Â»

Les technologies RPDâ¢ (Recurrent Pattern Detection ou DÃ©tection de Signatures RÃ©currentes) et GlobalViewâ¢ de Commtouch permettent dâidentifier et de bloquer toutes les nouvelles agressions de spams, malwares ou attaques de zombies dÃ¨s leurs dÃ©clenchements. Plus de dÃ©tails, comportant des statistiques et un Ã©chantillonnage, sont disponibles dans le rapport de Commtouch : **Commtouch Q2 2010 Internet Threats Trend Report**, avec **video highlights.**.

A noter : les niveaux des spams mondiaux sont basÃ©s sur le trafic des courriels mesurÃ© Ã partir des flots de donnÃ©es non filtrÃ©s et ne comprenant pas le trafic interne des entreprises. De ce fait, les niveaux des spams globaux peuvent Ãªtre diffÃ©rents des quantitÃ©s reÃ§ues dans les boÃ®tes de rÃ©ception des utilisateurs, en raison des solutions de filtrage mis en place par les fournisseurs de services Internet.