SÃ©curitÃ© : Commtouch, Les piÃ¨ces jointes en HTML, vecteur de Phishing
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 3/11/2010 13:30:00

Lâutilisation de courriels avec des fichiers joints aux formats HTML a considÃ©rablement augmentÃ© mentionne Commtouch dans son rapport du troisiÃ¨me trimestre sur les menaces Internet : Â« Third quarter Internet Threats Trend Report Â». **Les piÃ¨ces jointes au format HTML affichent des pages dâhameÃ§onnage** (Phishing) sur lâordinateur de lâutilisateur ou renvoient les internautes vers des sites comportant des malwares ou des spams.

Le rapport du troisiÃ¨me trimestre dÃ©taille la mÃ©thodologie des attaques combinÃ©es, comme le ver âHere You Haveâ, qui a Ã©tÃ© largement diffusÃ© au mois de septembre Ã travers lâutilisation des listes de contacts dâOutlook des ordinateurs infectÃ©s. Aussi bien le message âHere You Haveâ que les invitations falsifiÃ©es de LinkedIn, sont basÃ©es sur une combinaison de piratage psychologique et dâhyperliens masquÃ©s pour amener les utilisateurs vers des sites web possÃ©dant des scripts malveillants.

Pendant le troisiÃ¨me trimestre, les marques PayPal, LinkedIn, CraigsList, Bell Canada, NewEgg et Amazon ont Ã©tÃ© utilisÃ©es par les spammeurs afin de pousser les consommateurs Ã agir. Le rapport nous informe Ã©galement sur des attaques de spams assez peu habituelles, basÃ©es sur la solidaritÃ© avec plusieurs cÃ©lÃ©britÃ©s et politiciens europÃ©ens en proposant sur la mÃªme page des slogans publicitaires vantant les mÃ©rites de produits pharmaceutiques.

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. Avec lâacquisition de la division Command Antivirus dâAuthentium (connu aussi sous le nom de SafeCentral), lâinfrastructure Data-Cloud Â« GlobalView Â» de Commtouch bÃ©nÃ©ficie des capacitÃ©s dâanalyse des malwares du laboratoire de Command AV.

Parmi les autres points traitÃ©s dans ce rapport du troisiÃ¨me trimestre:

Le niveau trimestriel de spams correspond en moyenne Ã 88% de tout le trafic de messagerie, une hausse atteignant presque 95% Ã mi-septembre avec 198 milliards de messages de type spam/hameÃ§onnage par jour. Ces chiffres sont un peu plus Ã©levÃ©s que ceux du second trimestre, avec une moyenne de 80% de tout le trafic de messagerie et avec 179 milliards de messages de type spam par jour.

339 000 zombies en moyenne ont Ã©tÃ© activÃ©s chaque jour, presque 30 000 de plus par jour que dans le trimestre prÃ©cÃ©dent.

Le sujet le plus populaire des spams ce trimestre est la pharmacie, avec 59% de tous les spams.

Pour le troisiÃ¨me trimestre consÃ©cutif, les sites catÃ©gorisÃ©s Â«pornographie Â» restent la catÃ©gorie web Ã Ãªtre la plus infectÃ©e par les malwares.

Lâ□□Inde garde son titre pour le second trimestre consÃ©cutif, du pays possÃ©dant le plus de zombies (14% du total mondial).

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.) continue Ã Ãªtre les thÃ¨mes le plus populaires des crÃ©ateurs de blogs.

Â« *Lâ□□utilisation croissante des piÃ¨ces jointes HTML montre la proÃ©minence des attaques Ã plusieurs Ã©tapes ou attaques enchaÃ®nÃ©es*, affirme Assaf Greiner, vice-prÃ©sident de Commtouch. *La nature de ces activitÃ©s malveillantes souligne encore plus le besoin dâ□□une offre sÃ©curitÃ© intÃ©grÃ©e permettant de bloquer les spams et les courriels malveillants, de dÃ©truire les fichiers infectÃ©s et scripts auto-exÃ©cutables tout en empÃªchant les internautes de visiter les sites malveillants*Â»

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

Plus de dâ□□information ainsi que des statistiques et des exemples de spams, sont disponibles dans le rapport de Commtouch : **Commtouch Q3 2010 Internet Threats Trend Report**

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.