Insolite : Les noms de domaines cÃ©lÃ¨bres, lÃ©gitimitÃ© trompeuse pour le spam
Insolite
PostÃ© par : JerryG
PubliÃ©e le : 19/4/2010 15:00:00

Les noms de domaines cÃ©lÃ¨bres de lâ□□Internet donnent aux spams une lÃ©gitimitÃ© trompeuse, selon le nouveau rapport de **Commtouch.**

Comment les spammeurs utilisent les notions familiÃ¨res pour provoquer la chute de leurs victimes. Commtouch publie aujourdâ□□hui son rapport sur les menaces Internet : Internet Threats Trend Report for Q1 2010.

Les spammeurs sont devenus des experts dans lâ□□utilisation de noms de domaines les plus cÃ©lÃ¨bres de lâ□□Internet ceci afin de donner une lÃ©gitimitÃ© trompeuse aux milliards de courriels qu'ils envoient. Par exemple, entre cinq Ã dix pour cent de tous les spams Â« semblent Â» provenir de comptes Gmail. Ce rapport trimestriel analyse le pourcentage de spams qui Ã©mane effectivement de comptes Google. Le Â« style Â» des messages de Gmail, ainsi que ceux de PayPal et Facebook, est frÃ©quemment utilisÃ© par les spammeurs et spÃ©cialistes dâ□□attaques de phishing comme structures de leurs courriels.

Ce trimestre, une attaque de phishing visant les utilisateurs de Google et les blogueurs reposait sur un modÃ¨le utilisant des techniques qui permettent de minimiser la nature frauduleuse et suspecte du message.

Une autre attaque de spams dÃ©crite dans le rapport prÃ©sente une arnaque au Â« travail Ã domicile Â» utilisant comme point dâ□□entrÃ©e le site Internet de la CNN.

Le rapport trimestriel de Commtouch est basÃ© sur lâ□□analyse 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 premier trimestre :

Le niveau trimestriel de spams correspond en moyenne Ã 83% de tout le trafic de messagerie, avec une hausse atteignant 92% fin mars et une baisse allant jusquâ□□Ã 75% au dÃ©but de lâ□□annÃ©e.

Le niveau de spam dans le domaine de la Pharmacie reste au sommet avec 81% des messages de

type spam, conservant ainsi la moyenne du trimestre prÃ©cÃ©dent. Les ventes de contrefaÃ§ons se maintiennent Ã une moyenne de 5.4% des messages de type spam et restent le sujet numÃ©ro 2 le plus abordÃ©.

305 000 zombies en moyenne ont Ã©tÃ© activÃ©s chaque jour pour effectuer ces missions malveillantes.

Bien que le BrÃ©sil continue de dÃ©velopper le plus grand nombre de zombies, les chiffres ont diminuÃ© dans le premier trimestre. Au dernier trimestre de 2009, le BrÃ©sil Ã©tait responsable de 20.4% de ces activitÃ©s Ã lâ□□Ã©chelle mondiale. Au premier trimestre 2010, ce nombre est tombÃ© Ã 14%.

Les malwares Mal/Bredo ont Ã©tÃ© distribuÃ©s Ã plus de 838 variantes ce trimestre.

Les sites reliÃ©s aux thÃ©matiques de lâ□□Ã©ducation sexuelle et des jeux sont en tÃªte des sites manipulÃ©s, Â« phishing Â» ou hameÃ§onnage.

Les sites catÃ©gorisÃ©s Â« Pornographie Â» ont remplacÃ© les sites de type Â« Business Â» comme la catÃ©gorie web Ã Ãªtre la plus infectÃ©e par les malwares.

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 Spammeurs et les cybercriminels font continuellement des expÃ©riences afin dâ□□atteindre leurs objectifs*, affirme **Assaf Greiner** Vice PrÃ©sident de Commtouch. *Ils ont toujours testÃ© de nouvelles techniques pour attirer leurs victimes vers leurs supercheries; formats de courriels populaires, noms de domaines plÃ©biscitÃ©s, crÃ©ations de procÃ©dures dÃ©tournÃ©es, etc. tout ceci afin de mener Ã bien leurs opÃ©rations malveillantes*. Â»

Les technologies RPDâ□¢ (Recurrent Pattern Detection ou DÃ©tection de Signatures RÃ©currentes) et GlobalViewâ□¢ de Commtouch permettent dâ□□identifier 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 Q1 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.