SÃ©curitÃ© : Commtouch averti de la menace du virus Mal-Bredo A
SÃ©curitÃ©
PostÃ© par : JulieM
PubliÃ©e le : 20/1/2010 0:00:00

Les cybercriminels utilisent la confiance qui rÃ¨gne dans les rÃ©seaux sociaux afin de **propager le virus Mal-Bredo A**. Rapport du quatriÃ¨me trimestre : une Ã©volution ininterrompue des menaces Internet

Commtouch publie son rapport sur les menaces Internet : Threats Trend Report for Q4 2009. Les spammers continuent dâ□□Ãªtre Ã la pointe en matiÃ¨re dâ□□innovation Â« marketing Â» profitant cette fois-ci de la rÃ©putation des grandes marques comme UPS, DHL et Facebook pour inciter leurs Â« victimes Â» Ã ouvrir leurs messages.

Pendant ce trimestre, les spammers se sont concentrÃ©s sur la distribution du virus Mal-Bredo A. Bien que le nombre de variantes soit tombÃ© de 10 000 Ã 1 000, comparÃ© au trimestre prÃ©cÃ©dent, Mal-Bredo A a Ã©tÃ© diffusÃ© avec beaucoup plus de virulence.

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 quatriÃ¨me trimestre :

312 000 zombies en moyenne ont Ã©tÃ© activÃ©s chaque jour pour effectuer ces missions malveillantes.

Le niveau trimestriel de spams correspond en moyenne Ã 77% de tout le trafic de messagerie, avec une hausse atteignant 98% en novembre et une baisse allant jusquâ□□Ã 68% Ã la fin du mois de dÃ©cembre.

Les sites reliÃ©s aux thÃ©matiques apparentÃ©es Â« Ordinateurs et technologies Â» ainsi que Â« moteurs de recherche et portails Â» sont en tÃªte des sites de Â« phishing Â» ou dâ□□hameÃ§onnage.

Les sites catÃ©gorisÃ©s Â« Business Â» continuent Ã Ãªtre les plus infectÃ©s par les malwares pour le troisiÃ¨me trimestre consÃ©cutif.

Le pourcentage de spams dans le domaine de la pharmacie est revenu au sommet avec 81%; le trimestre dernier, il rÃ©gnait avec 68%. Les ventes de contrefaÃ§ons (montre, sac Ã main, etc.) restent en seconde place, passant de 19% Ã 5,4%.

Le BrÃ©sil continue de dÃ©velopper le plus grand nombre de zombies et est responsable de 20,4% de ces activitÃ©s Ã lâ□□Ã©chelle mondiale.

Les alertes Ã la contamination du virus H1N1 (grippe porcine) et les escroqueries relatives Ã Halloween continuent de circuler. Les spammers, toujours Ã lâ□□affut de nouvelles escroqueries, ont distribuÃ© des spams dans lesquels les liens Internet frauduleux Ã©taient contenus dans un fichier audio MP3 ou bien encore ont ciblÃ© un Â« public Â» exclusivement fÃ©minin avec des thÃ©matiques dites Â« pharmaceutique Â»

Â« *Lorsque nous passons en revue les menaces Internet pour ce trimestre, nous voyons vraiment lâ□□imagination dont font preuve les cybercriminels pour sâ□□assurer que leurs messages soient bien ouverts*, affirme **Assaf Greiner**, vice-prÃ©sident de Commtouch. *Que cela nous plaise ou non, cette crÃ©ativitÃ© dÃ©montre que les activitÃ©s sociales, comme la participation dans les rÃ©seaux sociaux (Facebook, Twitter, etc.), ont atteint une masse critique et exploitable. Par dÃ©finition, si un spammer a recours Ã une marque spÃ©cifique pour que les consommateurs ouvrent leurs messages, cela signifie que cette marque possÃ¨de une bonne rÃ©putation.* Â»

Les technologies RPDâ□¢ (Recurrent Pattern Detection ou DÃ©tection de Signatures RÃ©currentes) et GlobalViewâ□¢ de Commtouch identifient et bloquent les messages porteurs de virus, les attaques liÃ©es Ã la sÃ©curitÃ© Internet, y compris les agressions de spams, phishing, malwares ou attaques de zombies. Plus de dÃ©tails, comportant des statistiques et un Ã©chantillonnage, sont disponibles dans le rapport de **Commtouch Q3 2009 Internet Threats Trend Report.**

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 mises en place par les fournisseurs de services Internet.