

Commtouch : La pornographie, la plus infect e par les malwares

S curit 

Post  par : JPilo

Publi e le : 1/2/2011 15:00:00

Le niveau des spams a recommenc    augment  apr s une baisse significative au cours du quatri me trimestre, mentionne Commtouch dans son rapport trimestriel **Internet Threats Trend Report**, sur les menaces internet.

La moyenne journali re des spams en d cembre  tait de 30% inf rieure   celle de septembre, cependant les activit s li es aux spams ont augment es de 45% juste avant la publication du rapport. Le niveau de spams du quatri me trimestre 2010 correspond en moyenne   83% de tout le trafic de messagerie, en diminution par rapport au trimestre pr c dent qui  tait de 88%. Le nombre de zombies actifs durant le quatri me trimestre  tait en moyenne de 15% inf rieur   celui du trimestre pr c dent.

 « Un r seau de zombie inactif est comme une usine   l arr t pour les spammers, affirme **Asaf Greiner**, vice-pr sident de Commtouch. Nous avons d j  rencontr  des situations o , apr s une accalmie dans la distribution de spams ou de malwares, une nouvelle tactique a  t  introduite. Les experts dans les menaces Internet continuent de suivre les modifications de comportement du r seau afin de bloquer de mani re proactive toutes nouvelles attaques.  »



Parmi les autres points trait s dans ce rapport du quatri me trimestre:

Le niveau trimestriel de spams correspond en moyenne   **142** milliards de messages de type spam/hame sonnage par jour durant le quatri me trimestre alors qu il  tait de au 198 milliards durant le troisi me trimestre.

288,000 zombies en moyenne ont  t  activ s chaque jour, une baisse significative par rapport au 339,000 du troisi me trimestre.

Le sujet le plus populaire des spams ce trimestre est la pharmacie (42% de tous les spams).

Pour le quatri me trimestre cons cutif, les sites cat goris s  «pornographie  » restent la cat gorie web  tre la plus infect e par les malwares.

L Inde garde son titre pour le troisi me trimestre cons cutif, du pays poss dant le plus de zombies (17% du total mondial).

Le domaine du Web 2.0 avec un contenu g n r  par les utilisateurs, ainsi que les divertissements (musique, t l vision, films, critiques, etc.) continuent    tre les th mes le plus populaires des cr ateurs de blogs.

Au cours du quatri me trimestre, les m thodes des attaques de spams traditionnellement ont  t  combin es avec de nouvelles afin d'augmenter leurs efficacit s; achats en ligne plus importants,  hame sonnage   de nouveaux comptes (phishing) ou bien diffusions de malwares. Des polices de caract res petites et cach es ont  t  associ es avec des sujets Twitter et des liens exploitants le service de  cache   de Google. Ce trimestre a  t  le t moins du retour des spams de type art ASCII. Concernant les menaces plus  modernes  , le lien malware Koobface continue de circuler sur Facebook tandis que box.net, qui offre des services de partage de contenu et de synchronisation, a  t  utilis  pour abriter des liens de type spams.

Le rapport trimestriel de Commtouch est bas  sur l'analyse journali re de plus de deux milliards de messages et de transactions Internet arrivant dans ses centres de d tection mondiaux. Avec l'acquisition de la division Command Antivirus d'Authentium (connu aussi sous le nom de SafeCentral), l'infrastructure Data-Cloud  GlobalView   de Commtouch b n ficie des capacit s d'analyse des malwares du laboratoire de Command AV.

Les technologies RPD  (Recurrent Pattern Detection ou D tection de Signatures R currentes), GlobalView  et Command Antivirus multi-couches permettent d'identifier et de bloquer toutes nouvelles agressions de spams, malwares ou attaques de zombies d s leurs d clenchements.

Plus de d information ainsi que des statistiques et des exemples de spams, sont disponibles dans le rapport de Commtouch : [Commtouch Q4 2010 Internet Threats Trend Report](#)

A noter : les niveaux des spams mondiaux sont bas s sur le trafic des courriels mesur    partir des flots de donn es non filtr es et ne comprenant pas le trafic interne des entreprises. De ce fait, les niveaux des spams globaux peuvent  tre diff rents des quantit s re ues dans les bo tes de r ception des utilisateurs, en raison des solutions de filtrage mis en place par les fournisseurs de services Internet.