G-Data : croissance soutenue des nouveaux codes nuisibles en 2013
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 17/10/2013 14:00:00

Dans son rapport de sÃ©curitÃ©, le **G Data SecurityLabs** fait un Ã©tat des lieux des risques apparus durant le 1er semestre 2013. Lâ□□Ã©diteur de logiciel de sÃ©curitÃ© allemand constate que la croissance du nombre de nouveaux codes repart Ã la hausse aprÃ¨s une relative accalmie en 2012. Les chevaux de Troie restent les codes prÃ©fÃ©rÃ©s des cybercriminels.

Dans cette famille, la part des chevaux de Troie bancaires a diminuÃ©. Des actions rÃ©alisÃ©es dans diffÃ©rents pays par les autoritÃ©s ont permis de mettre fin Ã certains rÃ©seaux de commandes de ces codes spÃ©cialisÃ©s dans le vol dâ□□argent. Pour contrer cela, les concepteurs de botnet dÃ©veloppent de nouveaux systÃ¨mes de contrÃ´le dÃ©centralisÃ©s.

20 % de hausse de codes malveillants

Durant la premiÃ¨re moitiÃ© de lâ□□annÃ©e 2013, 1 509 934 nouvelles souches de codes malveillants sont apparues, soit en moyenne 8342 par jour. Cela reprÃ©sente une hausse de prÃ¨s de 20 % par rapport au deuxiÃ¨me semestre 2012.

Nouveaux programmes malveillants depuis 2006

AprÃ¨s un relatif ralentissement de la croissance en 2012, la barre des trois millions de nouveaux logiciels malveillants devrait Ãªtre dÃ©passÃ©e cette annÃ©e.

Les chevaux de Troie toujours au top

Nouveaux programmes par catÃ©gorie depuis 2010

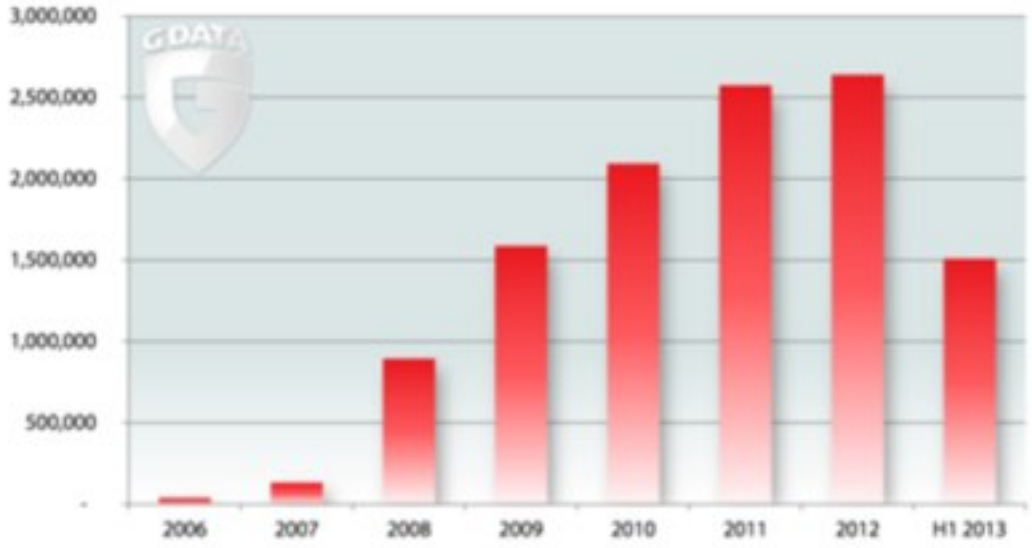
Le nombre de nouveaux programmes malveillants dans la catÃ©gorie des vers a de nouveau augmentÃ© de maniÃ¨re significative, mais reste tout de mÃªme Ã la cinquiÃ¨me position.

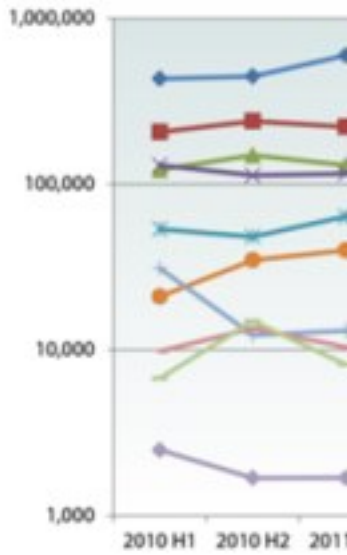
La catÃ©gorie adware a retrouvÃ© son niveau du premier semestre 2012 aprÃ¨s une pÃ©riode moins active au second semestre.

G Data Risk Monitor : Windows toujours leader

Les auteurs de codes nuisibles se concentrent toujours sur Windows. Au 1er semestre 2013, plus de 99,9% de tous les nouveaux programmes malveillants ciblaient Windows !

La famille de logiciels malveillants Sirefef , Ã©galement connu sous le nom ZeroAccess , continue de dominer le top 10. Dâ□□une maniÃ¨re gÃ©nÃ©rale, la fonction principale de la plupart des familles de codes est le gain dâ□□argent. Cela se traduit notamment par la manipulation des rÃ©sultats dans les moteurs de recherche (fraude au clic).





G Data Web Monitor : le porno a la cote

Les sites pornographiques infectÃ©s ont pris une part prÃ©dominante dans le classement des sites dangereux. Leur nombre a doublÃ© et cette catÃ©gorie de sites arrive aujourd'hui Ã la 2e place du classement.

La proportion de sites dangereux liÃ©s Ã des achats a Ã©galement augmentÃ© de maniÃ¨re significative, sautant de la 9e Ã la 4e place.

Les pages infectÃ©es sont de moins en moins concentrÃ©es dans certaines catÃ©gories. Le Top 10 des catÃ©gories reprÃ©sente 74,6% de lâ□□ensemble des sites infectÃ©s. Il a perdu 14% depuis le deuxiÃ¨me semestre 2012.

Les sites Internet malveillants sont encore majoritairement hÃ©bergÃ©s dans des pays fortement Ã©quipÃ©s en infrastructures informatiques.

Chevaux de Troie bancaires : la relative accalmie

Le nombre d'infections impliquant les chevaux de Troie bancaires estrestÃ© Ã un niveau relativement bas au cours du dernier semestre.

Cridex a Ã©tÃ© ajoutÃ© comme une nouvelle famille et câ□□est immÃ©diatement fait un nom compte tenu du nombre Ã©levÃ© d'infections.

Ã□ la fin mai / dÃ©but juin, une grande partie du botnet Citadel botnet a Ã©tÃ© dÃ©truit dans un effort commun de Microsoft et de diverses autoritÃ©s.

Le code source du cheval de Troie Carberp a Ã©tÃ© publiÃ© sur l'Internet et est maintenant disponible gratuitement. Tout ou partie de ce code devrait rÃ©apparaitre dans de nouveaux programmes malveillants.

Les cybercriminels travaillent Ã©galement sur des moyens de communication dÃ©centralisÃ©s pour les botnet. De nouveaux dÃ©veloppements sont attendus dans ce domaine.

Les solutions de sÃ©curitÃ© G Data sont disponibles chez GS2i.