G-Data : Croissance rÃ©duite des nouveaux codes malveillants pour 2012
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 2/10/2012 15:00:00

Le rapport de sÃ©curitÃ© semestriel de G Data montre un dÃ©veloppement inattendu sur le domaine des codes malveillants. Lacroissance Ã deux, voire trois chiffres, connue ces derniÃ¨res annÃ©es tend Ã sâ□□essouffler. Avec 3,9 % de croissance constatÃ©e entre les deux derniers semestres, le ralentissement est notable.

Mais ceci nâ□□est pas pour autant signe de crise du secteur cybercriminel. Les nombreuses attaques ciblÃ©es perpÃ©trÃ©es ces derniers mois montrent que les auteurs de malwares ont dÃ©laissÃ© la stratÃ©gie du nombre pour celle du rÃ©sultat. Les codes deviennent plus intelligents et performants. Le rÃ©sultat dâ□□une professionnalisation du cybercrime, initiÃ©e depuis plusieurs annÃ©es.

Au cours des 3 derniÃ¨res annÃ©es, le taux de croissance moyen du nombre de nouveaux codes malveillants Ã©tait de 44,15 % (plus de 180 % sur les 5 derniÃ¨res annÃ©es !). Mais avec seulement 3,9 % de croissance sur les 6 premiers mois de lâ□□annÃ©e, 2012 apparait comme une annÃ©e de rupture. Stabilisation historique encourageante ? Plusieurs Ã©lÃ©ments montrent que la situation reste prÃ©occupante. Ce sont tout dâ□□abord plus de 1,3 millions de nouveaux programmes malveillants qui sont apparus au cours du dernier semestre, soit environ 7200 nouveaux codes par jour. Ensuite, cette stagnation de croissance ne reflÃ¨te pas pour autant une baisse de lâ□□activitÃ© cybercriminel. Durant le dernier semestriel les attaques massives se sont multipliÃ©es sur de nombreuses plateformes (Windows, Android, MacOS). Moins nombreux mais plus intelligents, la professionnalisation du secteur cybercriminel entreprise depuis quelques annÃ©es semble porter ses fruits quant Ã la qualitÃ© des codes crÃ©Ã©s.

Des codes plus intelligents et discrets

Lâ□□automatisation toujours plus poussÃ©e des trojans bancaire est un exemple parlant. Le rapport de sÃ©curitÃ© de G Data explique :

Â« *La plupart des schÃ©mas dâ□□attaque prÃ©cÃ©dents Ã©taient relativement simples : par exemple, lorsquâ□□une victime se connectait Ã son service de banque en ligne, une fenÃªtre lui demandait plusieurs TAN pour sâ□□identifier, donnÃ©es qui Ã©taient immÃ©diatement envoyÃ©es au cybercriminel. [â□¦] Depuis, de nouvelles mÃ©thodes plus sophistiquÃ©es ont Ã©tÃ© employÃ©es : les Automatic Transfer System (ATS). Dans ce scÃ©nario, aucune interaction avec lâ□□utilisateur nâ□□est requise. Les transactions nâ□□apparaissent plus dans la liste et mÃªme le solde du compte est maquillÃ©. Le vol ne peut plus Ãªtre repÃ©rÃ© par la victime.* Â»

Un autre exemple peut Ãªtre trouvÃ© sur la plateforme Android :

Â« *Durant lâ□□annÃ©e 2011, la plupart des malwares sur les plateformes mobiles se concentraient sur lâ□□envoi de SMS et dâ□□appel surtaxÃ©s [â□¦], et Ã©taient cachÃ©s dans des applications distribuÃ©es sur des marchÃ©s parallÃ¨les. 2012 a Ã©tÃ© marquÃ© par lâ□□apparition dâ□□applications complÃ¨tement reprogrammÃ©es ou crÃ©Ã©es de toute piÃ¨ce, apportant certes les fonctionnalitÃ©s indiquÃ©es mais aussi des fonctions malveillantes. Cette stratÃ©gie a permis Ã ces malwares de rester plusieurs jours, voire plusieurs semaines, dans le Play Store de Google avec dâ□□Ãªtre dÃ©couverts.* Â»

La qualitÃ© prÃ©vaut sur la quantitÃ©

En se focalisant sur le dÃ©veloppement de codes malveillants plus Ã©voluÃ©s, les cybercriminels changent la donne. En plus de devenir plus Ã©voluÃ©s et plus discrets, les codes ciblent aussi de nouveaux systÃ¨mes. Le meilleur exemple est lâ□□attaque virale flashback qui a touchÃ© Apple. Eddy Willems, Security Evangelist chez G Data Software commente : Â« Alors que le nombre de nouveaux codes malveillants touchant Apple Ã©tait encore relativement faible, la qualitÃ© du virus Flashback et la faÃ§on dont il Ã©tait propagÃ© (fausse installation flash) a fait toute la diffÃ©rence. Ce code a infectÃ© plus de systÃ¨mes Apple (environ 600 000) quâ□□ils nâ□□en avaient jamais Ã©tÃ© infectÃ©s auparavant. Â»

Quelle Ã©volution ?

Les analystes du G Data SecurityLabs tablent sur une stagnation du nombre de nouveaux codes, mais aussi sur une augmentation de la qualitÃ© et de la puissance de ceux-ci. **Eddy Willems** : Â« *Nous devrions observer entre 2,5 Ã 3 millions de nouveaux codes malveillants par an dans les annÃ©es Ã venir. Mais dans le mÃªme temps, les codes deviendront de plus en plus complexes. Etant optimisme, je me dis que cette situation est aussi le rÃ©sultat dâ□□une meilleure protection des utilisateurs : pour rÃ©ussir Ã infecter le plus grand nombre, les crÃ©ateurs de codes nuisibles doivent passer toujours plus de temps pour trouver des systÃ¨mes capables de contourner la vigilance des protections antivirales et des utilisateurs.* Â»

Les solutions G-Data sont disponible chez GS2i.

Visitez le site de GS2i