G-Data : Smartphones et transactions bancaires, cibles des cybercriminels
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 7/3/2012 13:00:00

Les cybercriminels ont Ã©lu domicile sur les appareils mobiles â□□ câ□□est le bilan qui ressort du nouveau rapport de sÃ©curitÃ© de G Data Software.**Le G Data SecurityLabs** constate que le nombre de nouveaux logiciels malveillants ciblant les smartphones et les tablettes a Ã©tÃ© multipliÃ© par 2,5 fois durant la seconde moitiÃ© de lâ□□annÃ©e 2011.

Sur le systÃ¨me Android, les attaques ont Ã©tÃ© multipliÃ©es par 8 durant cette mÃªme pÃ©riode. CÃ´tÃ© PC, le rapport fait Ã©tat dâ□□une recrudescence des chevaux de Troie bancaire. Variantes trÃ¨s frÃ©quentes et cycles de vie moyens de 27 heures, ces codes tentent de contourner les mÃ©canismes de dÃ©fense rÃ©actifs des antivirus. Au total, lâ□□annÃ©e 2011 aura connu un nombre record de 2,5 millions de nouveaux codes malveillants.

Â« *Les cybercriminels privilÃ©gient la rentabilitÃ©. Il n'est donc pas surprenant que les auteurs de logiciels malveillants se concentrent de plus en plus sur les smartphones et les tablettes. Sur ces appareils peu protÃ©gÃ©s par des solutions de sÃ©curitÃ©, les attaquants nâ□□ont pas de difficultÃ© Ã voler des donnÃ©es personnelles et professionnelles* Â», explique **Ralf BenzmÃ¼ller,** Directeur du G Data Security Labs.

Â« *La recherche de gains rapides est aussi une des explications de la croissance des chevaux de Troie bancaires. Ces codes nuisibles utilisent des techniques Ã mÃªme de contourner les protections antivirales classiques. Une nouvelle menace Ã laquelle nous avons rÃ©pondu avec lâ□□intÃ©gration de nouvelles protections dites immÃ©diates dans nos solutions.* Â»

Inondation de logiciels malveillants

Au cours de lâ□□annÃ©e 2011, le G Data SecurityLabs a comptabilisÃ© un total de 2,575 millions de nouveaux codes malveillants. Dans la seconde moitiÃ© de l'annÃ©e, 1 330 146 nouveaux malwares ont Ã©tÃ© dÃ©tectÃ©s.

Par rapport Ã l'annÃ©e 2010, les codes nuisibles ont augmentÃ© de 23 %. Les chevaux de Troie sont toujours la catÃ©gorie de logiciels malveillants dominante. Les experts G Data relÃ¨vent aussi une forte augmentation du nombre d'adwares et de programmes-espions. Cela montre que l'affichage de publicitÃ©s et l'espionnage des donnÃ©es personnelles sont particuliÃ¨rement rentables pour les cybercriminels.

Malware mobile toujours en hausse

Les cybercriminels se concentrent de plus en plus sur les smartphones et les tablettes Ã©quipÃ©s du systÃ¨me d'exploitation Android. Le nombre de codes visant les mobiles a augmentÃ© de 2,5 fois au cours de la seconde moitiÃ© de l'annÃ©e. Par rapport Ã 2010, ce nombre a Ã©tÃ© multipliÃ© par plus de dix durant lâ□□annÃ©e 2011.

Les auteurs utilisent des applications manipulÃ©es qui sont diffusÃ©es comme des programmes inoffensifs. Les cybercriminels peuvent alors faire envoyer des SMS payants aux utilisateurs infectÃ©s, ou rÃ©cupÃ©rer contacts et numÃ©ros de tÃ©lÃ©phone stockÃ©s dans le carnet dâ□□adresses.

Les hacktivistes ont aussi dÃ©couvert les smartphones et les tablettes comme outils pour la diffusion de messages Ã caractÃ¨re politique. Le cheval de Troie Android.Trojan.Arspam.A envoie des messages provenant de forums traitant du Moyen-Orient Ã tous les contacts du carnet d'adresses de la victime.

Dans le passÃ©, les applications malveillantes restaient cantonnÃ©es aux pays ciblÃ©s. Mais ces derniers temps, les auteurs modifient les codes pour Ã©tendre les effets des logiciels malveillants mobiles sur un plus grand nombre de pays (localisation des langues, insertion de numÃ©ros surtaxÃ©s en fonction du pays, etc.)

Services bancaires en ligne dans le viseur

La banque en ligne est un service de plus en plus populaire. Selon lâ□□Observatoire 2011 de lâ□□opinion sur lâ□□image des banques â□□ IFOP de Juin 2011, 80 % des internautes franÃ§ais consultent leur compte bancaire en ligne. La forte utilisation de ce service le rend Ã©galement trÃ¨s attrayant pour les cybercriminels.

Ils utilisent des chevaux de Troie bancaires spÃ©ciaux pour manipuler les transactions bancaires en ligne, par exemple pour transfÃ©rer certaines sommes d'argent vers d'autres comptes.

Selon les experts du G Data SecurityLabs, seulement quelques familles de chevaux de Troie

bancaires existent, mais elles sont utilisÃ©es comme base pour la crÃ©ation de variantes aux cycles de vie trÃ¨s courts. Ainsi, le cycle de vie moyen de ces fichiers serait d'environ 27 heures. Le cheval de Troie le plus frÃ©quemment utilisÃ© est Sinowal, qui se caractÃ©rise par le changement frÃ©quent de ses mÃ©canismes d'infection.

Vous trouverez les solutions G-Data chez GS2i.