G-Data : Pas de cyber-guerre Ã l'horizon 2013
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 19/12/2012 14:00:00

En cette fin dâ□□annÃ©e, les experts du **G Data SecurityLabs** font lâ□□inventaire sur le domaine de la sÃ©curitÃ© informatique, des attaques et de la cybercriminalitÃ©. En 2012, les cybercriminels se sont focalisÃ©s sur la qualitÃ© plutÃ´t que la quantitÃ© en concevant des logiciels malveillants particuliÃ¨rement intelligents.

G Data s'attend Ã une poursuite de cette tendance l'annÃ©e prochaine. Les auteurs continueront aussi Ã focaliser leurs attaques sur les entreprises et les institutions. Pour cela, lâ□□exploitation des Smartphones privÃ©s ou de lâ□□entreprise constituera un vecteur d'attaque privilÃ©giÃ©.

En 2013, les utilisateurs de Mac devraient aussi Ãªtre plus exposÃ©s aux attaques. Les programmes malveillants pour les SystÃ¨mes Apple ne sont plus en phase de test.

Lâ□□utilisation de kits dâ□□exploits permet de concevoir des attaques en sÃ©rie, sans quâ□□aucune expertise soit nÃ©cessaire. En ce qui concerne la cyberguerre si souvent citÃ©e, G Data souhaite donner un avis clair : espionnage, oui, cyberguerre, non !

Â« *Il y a encore eut une augmentation des attaques ciblÃ©es sur les entreprises et les institutions, et cette tendance ne devrait pas faiblir l'annÃ©e prochaine, car il s'agit d'un modÃ¨le extrÃªmement lucratif. Les auteurs utilisent Ã©galement de nouveaux vecteurs d'attaques, tels que lâ□□infection des appareils mobiles afin de sâ□□introduire dans les entreprises* Â», explique **Ralf BenzmÃ¼ller**, Directeur du G Data SecurityLabs. Â« *Nous assistons aussi Ã un dÃ©veloppement des kits d'exploits. Ceux-ci facilitent les attaques dâ□□ordinateurs, car des paquets entiers prÃªts Ã lâ□□emploi peuvent Ãªtre achetÃ©s sur le marchÃ© noir. Aucune connaissance d'expert nâ□□est nÃ©cessaire pour perpÃ©trer des attaques*. Â»

BaromÃ¨tre de sÃ©curitÃ© pour 2013

Cyberespionnage plutÃ´t que cyberguerre

Le mot cyberguerre a Ã©tÃ© mentionnÃ© Ã plusieurs reprises dans le cadre de Stuxnet, Flame ou Gaus. Mais les experts du G Data Security Labs pensent que parler de cyberguerre est injustifiÃ©. Â« *Ceux qui parlent de cyberguerre font fausse route. Sâ□□il sâ□□agit bien dâ□□activitÃ©s liÃ©es Ã de lâ□□espionnage, utiliser le terme de cyberguerre est une exagÃ©ration* Â», explique **Ralf BenzmÃ¼ller**. Â« *Ce qui est exact, câ□□est que les armÃ©es comptent maintenant dans leurs rangs des forces spÃ©ciales qui veillent Ã la protection des infrastructures informatiques du pays et disposent de moyens de dÃ©fense contre des attaques potentielles.* Â»

Attaques ciblÃ©es dans les PME

Les attaques ciblÃ©es sur les entreprises et les institutions ne vont pas faiblir. Cependant, le spectre des attaques devrait sâ□□Ã©largir. Les grandes entreprises ayant Ã©tÃ© fortement ciblÃ©es en 2012, elles seront sans doute un peu mieux prÃ©parÃ©es en 2013. Les cybercriminels pourraient alors reporter certaines de leurs techniques sur de plus petites structures. La tendance croissante du BYOD facilitera les attaques dans des entreprises oÃ¹ la gestion des flottes de Smartphones nâ□□est pas prise en compte.

Le Mac sous les feux de la rampe

G Data s'attend Ã une plus forte prÃ©sence des programmes malveillants sur le systÃ¨me d'exploitation Apple. Les codes spÃ©cialement destinÃ©s Ã voler de l'argent et espionner les donnÃ©es personnelles, se feront plus nombreux. Â« *La pÃ©riode de test est terminÃ©e, les cybercriminels sont maintenant prÃªts pour l'action* Â», explique **Ralf BenzmÃ¼ller**, qui voit aussi en la prise de conscience du danger limitÃ©e chez les utilisateurs de Mac, un avantage pour les attaquants.

Smart TV : attaque dans le salon

Les ventes de tÃ©lÃ©viseurs connectÃ©s continuent leur forte progression. G Data prÃ©voit lâ□□exploitation des tÃ©lÃ©viseurs connectÃ©s par les cybercriminels. Vol de donnÃ©es, espionnage par la Webcam intÃ©grÃ©e ou le microphone sont des scÃ©narios Ã prendre en

compte. Lâ□□une des possibilitÃ©s dâ□□attaque serait lâ□□infiltration de codes malveillants via des mises Ã jour logicielles (firmware) supposÃ©es officielles.

Les logiciels malveillants mobiles Ã la hausse

L'an prochain, les logiciels malveillants dÃ©veloppÃ©s spÃ©cifiquement pour les tablettes et les Smartphones sous Android vont continuer Ã croÃ®tre. G Data s'attend Ã ce que les vulnÃ©rabilitÃ©s dans les navigateurs soient trouvÃ©es et exploitÃ©es dans des attaques. Ainsi, lâ□□utilisateur pourrait Ãªtre attaquÃ© par simple navigation Web. En outre, les attaquants continueront Ã se concentrer sur l'ingÃ©nierie sociale afin dâ□□infiltrer les appareils mobiles avec des applications malveillantes.

Les failles de sÃ©curitÃ© comme porte dâ□□entrÃ©e

Le nombre d'exploits va continuer Ã croÃ®tre. Ã□ cet Ã©gard, G Data enregistre de plus en plus dâ□□exploits prÃªts Ã lâ□□emploi, mis en vente sur le marchÃ© noir. Les kits dâ□□exploits permettent aux cybercriminels moins expÃ©rimentÃ©s de manipuler des sites Web et de dÃ©livrer ainsi des codes malveillants auprÃ¨s des visiteurs. Les criminels se basent sur des versions de Java pÃ©rimÃ© et des vulnÃ©rabilitÃ©s logicielles. Cette annÃ©e, des failles de sÃ©curitÃ© rÃ©cemment dÃ©couvertes dans les logiciels ont Ã©tÃ© trÃ¨s rapidement adoptÃ©es dans les kits d'exploits.

Les solutions G-Data sont disponible chez GS2i.

Visitez le site de GS2i