

### Une nouvelle donne pour les malware Androïd ?

#### Sécurité

Posté par : JulieM

Publié le : 16/5/2013 11:30:00

**Le dernier Rapport sur les Menaces Mobiles** rapporte une série de nouveaux malware Androïd, qui utilisent par exemple la messagerie en plus des applications pour se propager et infecter les appareils.

**Première conséquence** : le nombre total des menaces continue d'augmenter.

Le premier trimestre 2013 a été marqué par des nouveautés du côté des malware Androïd, qui se veulent de plus en plus complexes. Le Rapport sur les Menaces Mobiles de F-Secure du premier trimestre 2013 présente la première offensive dont la diffusion s'est faite hors des applications, (via des e-mails de Spam), les premières attaques Androïd ciblées, et la première escroquerie prétextant une avance de frais. En parallèle, les revendeurs de malware Androïd se multiplient sur le web.



**Le nombre de familles et variantes de menaces mobiles** est en augmentation de 49 % par rapport au trimestre dernier, passant de 100 à 149. Parmi celles-ci, 136 (soit 91,3% d'entre elles) visaient Androïd et 13 (soit 8,7%), étaient conçues pour Symbian. Pour rappel, 61 familles et variantes de menaces avaient été couvertes au premier trimestre 2012; cette croissance est donc l'image de celle des parts de marché d'Androïd : exponentielle.

« Les nouvelles techniques utilisées par les cybercriminels pour attaquer Androïd sont inquiétantes », déclare **Sean Sullivan**, Security Advisor du Lab F-Secure. « A titre d'exemple : jusqu'à présent, je ne me suis jamais inquiété pour ma mère et son mobile Androïd, car elle n'utilise pas d'applications. Aujourd'hui, j'ai des raisons de

*mâ inqui ter : avec des menaces comme Stels, des malware Android se propagent dans des spams, et ma m re consulte ses e-mails avec son mobile.  .*

**Ce cheval de Troie Android**, plus connu sous le nom de Stels, a commenc    se r pandre via un email falsifi  de        Internal Revenue Services  , transportant un logiciel malveillant vendu sur Internet, con  u pour voler des informations confidentielles pr sentes dans les appareils Android et faire de l  argent en passant des appels   des num ros surtax s. D  apr s Sean Sullivan, cet exemple de banalisation des malware    pourrait changer la donne  .

Le premier trimestre a  t  le th  tre des premi res attaques cibl es utilisant des logiciels malveillants Android. Ainsi, des militants des droits de l  homme Tib tains ont  t  la cible d  emails contenant des pi ces jointes infect es par des malware Android. De m me, et un soi-disant    coupon de r duction   pour une cha ne de caf  tr s populaire a permis de soutirer des informations   des t  phones localis s en Cor e du Sud.

**Des mobiles indiens ont  t  sp cifiquement pris pour cible**, avec ce qui constitue la premi re escroquerie Android pr textant une avance de frais. Dans ce cas, une fausse application Android    d  offres d  emploi   en Inde, informe son utilisateur qu  il est retenu pour un poste au sein de TATA Group, une multinationale indienne. Pour organiser l  entretien d  embauche, l  application demande un d  p t de garantie remboursable.

Le Lab F-Secure met l'accent sur le recensement du nombre de familles et de variantes de malware plut t que sur le nombre d' chantillons uniques. Pour tenter d' viter la d tection de leur malware, les cybercriminels utilisent un syst me automatis , qui fait de l g res modifications au code du malware    en r sultent de nouveaux  chantillons de malware, qui restent dans la m me famille de logiciels malveillants ou autres variantes. Le recensement des familles et des variantes plut t que des  chantillons fournit une mesure plus r aliste du nombre de menaces.