

Sécurité : BadNews pour Android

Lookout, éditeur de solutions de protections pour terminaux mobiles, [notamment Android](#), a repéré **BadNews**, un nid à *malwares*, présent dans 32 applications distribuées sur le Play Store officiel de Google (on en trouvera la liste en bas d'article).

Présenté comme un réseau publicitaire à l'allure innocente, le SDK BadNews s'avère très intrusif. « *Il a la capacité d'envoyer de faux messages à caractère informatif qui invitent les utilisateurs à installer les applications et à envoyer des informations sensibles telles que le numéro du téléphone et l'identifiant de l'appareil à son serveur C&C (Command and Control). BadNews exploite sa capacité à afficher de faux messages dans le but de diffuser des programmes malveillants de monétisation et de pousser des applications affiliées,* » détaille l'éditeur de sécurité.

Leurrer les systèmes de traque

BadNews pousse notamment l'installation d'AlphaSMS, une application qui envoie des SMS surtaxés, sur les terminaux infectés. Lesquels toucheraient surtout les échanges de texto issus de Russie, d'Ukraine, de Biélorussie, d'Arménie et du Kazakhstan. La moitié des applications repérées par Lookout se trouve d'ailleurs en Russie.

Par ailleurs, BadNews innove dans sa capacité à infecter en toute discrétion un grand nombre de terminaux. La plate-forme peu recommandable se diffuse largement, mais ses activités nocives ne se déclenchent que dans un second temps. « *Un bon moyen de leurrer les systèmes de traque d'applications malveillantes, qui après avoir jaugé le nouveau venu estiment qu'il est sans danger* », note Lookout.

Entre 2 et 9 millions de téléchargements

L'éditeur déclare avoir prévenu Google qui a immédiatement retiré les applications infectieuses de son catalogue et fermé les comptes des quatre développeurs associés. Il est néanmoins difficile de savoir si leur intention était de propager l'agent malveillant ou bien s'ils ont été victimes de manipulation. Mais les applications malveillantes auraient été téléchargées entre 2 et 9 millions de fois, estime Lookout sur la base des statistiques de Google Play.

Lookout en profite pour rappeler qu'il est préférable de ne pas autoriser le système à installer des applications de sources inconnues (en décochant la case correspondante depuis le menu Sécurité des paramètres Système). La base même de l'intégrité de l'OS mobile de Google.

Voilà néanmoins qui ne va pas arranger la réputation d'Android en tant que plate-forme sécurisée (même si la plupart des infections sont le fait des utilisateurs peu regardant sur l'intégrité des applications qu'ils installent). Récemment, le fournisseur de services NQ Mobile estimait à [33 millions le nombre de smartphones Android infectés](#).

Voir aussi

[Quiz Silicon.fr – 4 ans d'Android !](#)