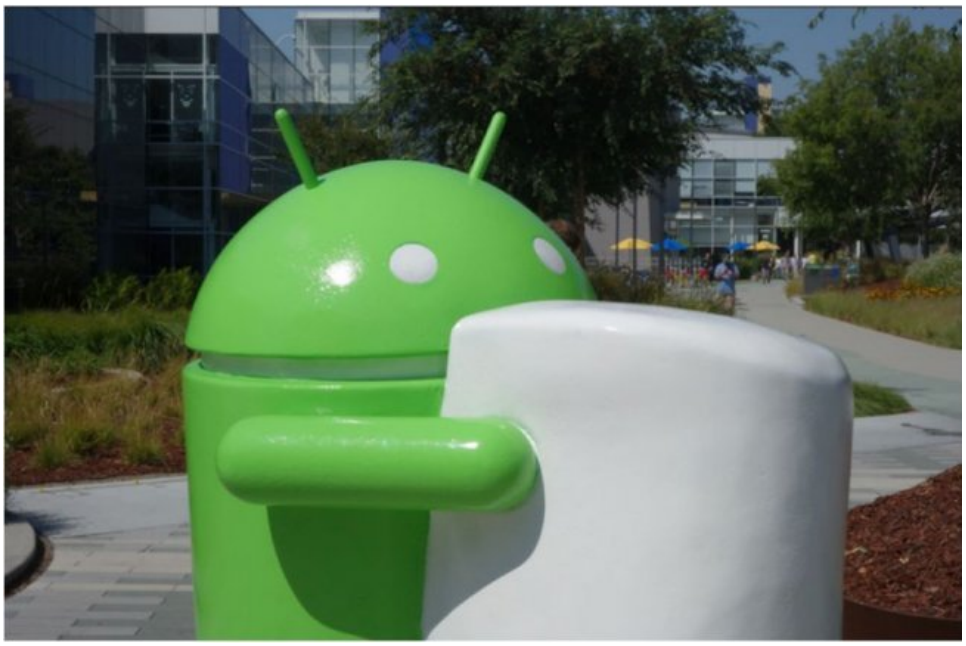
20 000 apps Android détournées dans les boutiques parallèles | Le Net Expert Informatique



20 000 apps Android détournées dans les boutiques parallèles

Sous l'apparence d'applications Android très utilisées comme WhatsApp ou Google Now, des copies malveillantes, proposées sur des boutiques aux critères de sélection moins stricts que Google Play, installent au coeur des terminaux mobiles des adwares extrêmement difficiles à déloger.

Des experts en sécurité de Lookout ont trouvé plus de 20 000 exemples d'apps Android compromises, dont certaines sont des copies d'applications figurant parmi les plus populaires comme Facebook, Google Now, SnapChat, Twitter ou WhatsApp. Elles contiennent du code malveillant et affichent agressivement des publicités sur les terminaux.

Par ailleurs, contrairement aux habituels adwares, ces apps sont installées de telle façon que les utilisateurs ne peuvent pas les supprimer. Elles noyautent les terminaux en accédant aux accès racines permettant de sortir des sandbox restreignant les manipulations et peuvent ainsi prendre le contrôle complet du terminal, de ses applications et de ses données.

Les apps compromises résident sur des boutiques parallèles à Play

Les utilisateurs qui téléchargent leurs apps de façon classique sur la boutique Google Play, ne sont normalement pas concernés car ces applications comportant un cheval de Troie sont principalement distribuées à travers d'autres boutiques d'apps en ligne. Cependant, certains utilisateurs passent par ce type de boutiques car elles proposent souvent des apps que Google Play n'autorise pas, relatives aux jeux en ligne ou pornographiques.

Les pays dans lesquels Lookout a détecté le plus grand nombre d'applications compromises sont les Etats-Unis, l'Allemagne, l'Iran, la Russie, l'Inde, la Jamaïque, le Soudan, le Brésil, le Mexique et l'Indonésie. Les chercheurs de la société spécialisée en sécurité mobile ont distingué trois familles d'apps qui noyautent automatiquement les terminaux à la racine, respectivement dénommées Shedun, Shuanet et ShiftyBug. Les pirates qui les exploitent repackagent les apps les plus populaires de Google Play et les installent sur des boutiques en ligne moins regardantes sur la sécurité. « Nous pensons que ce type d'adware intégrant des chevaux de Troie vont devenir de plus en plus sophistiqués avec le temps et qu'ils pourront mieux dissimuler leur présence sur le terminal », expliquent les chercheurs de Lookout dans un billet.

Source :
http://www.lemondeinformatique.fr/actualites/lire-20-000-apps-android-detournees-dans-les-boutiques-paralleles-62898.html
Article de Lucian Constantin / IDG News Service (adapté par Maryse Gros)