Android victime d'une forte hausse du nombre d'adwares

Fort de sa position de numéro 1 mondial des plates-formes mobiles, **Android** attire toujours plus les cybercriminels qui, à l'instar de Windows, y voient une occasion supplémentaire de gagner de l'argent. L'éditeur de sécurité Fortinet rapporte ainsi une hausse des **adwares** sur les smartphones Android au cours de l'été (1er juillet 2012 – 30 septembre 2012).

Rappelons que les adwares, ou publiciels, sont des applications qui intègrent divers outils pour diffuser de la publicité indésirable sur l'écran du téléphone.

Fortinet a constaté l'activité particulièrement virulente de deux variantes d'adware : **Android/NewyearL** et **Android/Plankton**. Elles ont été détectées sur 1 % des systèmes de surveillance de l'éditeur pour les régions EMEA (Europe, Moyen-Orient, Afrique) et Apac (Asie-Pacifique). Un taux qui s'élève à 4 % pour l'Amérique.

Les utilisateurs pistés

Ces bestioles ne se contentent pas d'afficher de la réclame (et faire gagner de l'argent à ses exploitants sous forme de faux programmes d'affiliation publicitaires).

Elles pistent également les utilisateurs à travers leur numéro IMEI (International Mobile Equipment Identity ou identité internationale d'équipement mobile) et demandent l'accès à certaines informations comme l'historique du navigateur, les favoris, le journal des appels et les journaux systèmes.

Autant d'informations inutiles pour une simple application publicitaire trop suspicieuse pour être honnête. *« La forte augmentation des adwares sur Android peut sans doute être imputé aux utilisateurs qui installent sur leurs appareils mobiles des applications légitimes qui contiennent des codes adware embarqués »*, explique **Guillaume Lovet**, responsable senior de l'équipe « Réponses aux Menaces FortiGuard Labs » de Fortinet.

Il recommande à l'utilisateur de bien vérifier les droits d'accès demandés par l'application avant de finaliser son installation. Un homme averti…

Piratage par SMS

Autre constatation inquiétante de l'éditeur, l'apparition de nouvelles versions de Zitmo (Zeus-in-the-mobile) pour Android mais aussi BlackBerry.

Zitmo est le composant mobile du cheval de Troie bancaire Zeus qui contourne l'authentification à deux facteurs en interceptant les codes SMS de confirmation de transaction envoyés par les banques à leurs clients dans le but de pirater les comptes bancaires.

Selon Fortinet, Zitmo s'apparente aujourd'hui à un réseau zombie (ou botnet) qui permet

désormais aux cybercriminels de contrôler le cheval de Troie via les commandes SMS. Autrement dit, envoyer de faux SMS afin de tromper les utilisateurs ainsi invités, par exemple, à installer une application illégitime sur leur terminal.

Zitmo en approche

« La nouvelle version de Zitmo est peut-être déjà dans la nature en Europe et Asie. Bien que nous ne détectons que quelques exemples du logiciel malveillant dans ces régions, cela nous porte à croire que le code est actuellement en train d'être testé par ses auteurs ou déployé pour des attaques ciblées très spécifiques », indique Guillaume Lovet.

L'activité de Zitmo pourrait donc s'intensifier dans les mois qui viennent. Une raison supplémentaire de redoubler de vigilance lors de l'installation d'une application. Surtout si c'est sur invitation d'une banque, ce que ce type d'établissements n'est jamais amené à faire par SMS.

Voir aussi
Quiz Silicon.fr – 4 ans d'Android !