Une seconde backdoor chinoise nichée dans les terminaux Android

Les smartphones chinois ont le vent en poupe en Europe où le marché de la téléphonie mobile s'intéresse aux terminaux à prix abordables. Mais la semaine dernière, première alerte, les chercheurs de Kryptowire avaient déniché une porte dérobée au sein d'un firmware de l'éditeur chinois, Adups Technology. Ce logiciel sert en principe pour le support client des constructeurs, mais l'analyse de Kryptowire montre qu'il transmet beaucoup de données personnelles comme les messages, la liste des contacts, l'historique des appels et des identifiants des terminaux comme l'International Mobile Subscriber Identity (IMSI) et l'International Mobile Equipment Identity (IMEI). Pour expliquer la présence de backdoor, Adups Technology a expliqué que ce code avait été installé par « inadvertance » sur les terminaux.

D'autres spécialistes en sécurité d'Anubis Network ont découvert un autre firmware présent sur plus de 2,8 millions de smartphones Android et comprenant une backdoor. L'éditeur, lui aussi chinois, se nomme Ragentek Group. Le firmware utilise une procédure de mise à jour OTA (Over The Air) non chiffrée. Cette absence de communication sécurisée avec les serveurs distants expose le micro-programme à une attaque de type « *homme du milieu* », afin d'envoyer des fausses données aux serveurs et des commandes malveillantes au terminal.

Un code pour cacher le firmware à Android

Ce risque est connu, mais les experts en mobilité ont trouvé plus surprenant. Le firmware comprend un code pour masquer sa présence à Android. Ainsi, un développeur analysant les processus actifs sur Android ne s'apercevrait pas de l'exécution d'une mise à jour sur le téléphone. Comme les mises à jour en mode OTA fonctionnent en mode root sur l'appareil et en l'absence de protection SSL, le firmware devient une porte dérobée.

Tout comme Kryptowire, les chercheurs d'Anubis Group ont découvert le pot aux roses dans des smartphones de la marque BLU. Mais d'autres fournisseurs sont touchés comme Infinix, Doogee, Leagoo, Iku, Beeline et Xolo. Anubis a travaillé avec Google, BLU et le CERT américain sur ce sujet. Les agences américaines de renseignements prennent très au sérieux la présence de backdoor sur des terminaux chinois vendus dans les grandes enseignes comme Best Buy.

A lire aussi :

La faille Rowhammer assomme les smartphones Android

Fuites de données : les apps iOS plus percées que celles d'Android

Photo credit: Stratageme.com via Visualhunt