Une backdoor chinoise planquée dans des smartphones Android

Y a-t-il un espion dans plus de 700 millions de smartphones Android ? Oui, selon les chercheurs de la société Kryptowire, une start-up de sécurité soutenue par la DARPA et le Département américain de la sécurité intérieure, qui vient de rendre public ses travaux mettant en cause un firmware (un FOTA, soit Firmware Over The Air, capable de se mettre à jour à distance), édité par 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). *In fine*, l'ensemble des informations pour surveiller et suivre les traces d'un individu.

Des envois bien cadencés et bien renseignés

Les chercheurs ont réussi à découvrir que la transmission des messages et des journaux d'appels se déroule toutes les 72 heures ; les autres informations personnelles étant envoyées toutes les 24 heures. La communication avec les serveurs est assurée par deux applications systèmes : com.adups.fota.sysoper et com.adups.fota. Elles transfèrent les données vers 4 serveurs : bigdata.adups.com (adresse primaire), bigdata.adsunflower.com, bigdata.adfuture.cn, bigdata.advmob.cn. Ils sont tous rattachés à la même adresse IP, 221.228.214.101, qui appartient à Adups. Les experts ont ensuite décortiqué les fichiers JSON envoyés aux serveurs et les ont compilés dans un tableau (cf ci-dessous). Les descriptions sont assez éloquentes.

Files	Description
DcApp.json	App's that the user has installed on the device.
DcAppOp.json	Android App Ops data
DcMobileStatus.json	Diagnostic data
DcRootInfo.json	A listing of files in the /system/bin and /system/xbin directories
DcTellMessage.json	The user's call log (and numbers people the user has texted)
dc_app_flow.json	The order in which a user uses apps
dc_msg_key.json	The content of the user's text messages

La société chinoise, originaire de Shanghai, ne semble pas de prime abord affiliée au gouvernement chinois. Mais la découverte de la backdoor est prise très au sérieux par le gouvernement américain, car le firmware incriminé ne publie pas ses fonctionnalités et il est pré-installé par défaut sur de nombreux terminaux.

Un aspirateur à données placé par inadvertance

De son côté, Adups Technology dément les accusions de Kryptowire sur la collecte d'informations personnelles et la transmission aux autorités chinoises. Dans son communiqué, la société explique

que ce micro-programme avait été installé par accident pour filtrer les messages et les appels indésirables des utilisateurs dans les smartphones de la marque Blu.

C'est sur ce type d'appareil que les experts de Kryptowire ont découvert la porte dérobée, mais elle touche aussi plusieurs autres terminaux Android. Adups a comme clients Huawei et ZTE et fournit son firmware à plus de 400 partenaires dans la mobilité (semi-conducteur, wearable, mobile, etc.). La firme chinoise a indiqué avoir suspendu cette fonctionnalité de filtrage et précise « *qu'aucune information comme les messages, les contacts et le journal des appels n'a été transmis à d'autres* ». En tous cas, cette transmission de données se faisait sans le consentement de l'utilisateur et les explications d'Adups laissent pour l'heure perplexes et contribuent à entretenir le doute.

A lire aussi

La faille Rowhammer assomme les smartphones Android

Foxconn laisse des backdoor trainer dans des smartphones Android

Photo credit: edowoo via VisualHunt / CC BY-SA