Des malwares pré-installés sur des smartphones Android chinois

Les cybercriminels rivalisent d'ingéniosité pour infecter les terminaux mobiles, ceux sous Android en premier lieu. Après les applications infectieuses téléchargeables depuis des *stores* alternatifs (quand ce n'est pas dans la boutique officielle du système), voici l'heure du **logiciel malveillant directement intégré au terminal en sortie d'usine**.

L'éditeur de solutions de sécurité **G Data** affirme avoir découvert qu'un logiciel espion faisait parti des programmes pré-installés dans un smartphone produit par le fabricant chinois Star. Si **le N9500** doté d'un processeur quadri cœur et d'un design proche de celui des Galaxy S4 de Samsung est disponible en ligne entre 130 et 165 euros, la facture pour l'utilisateur risque d'être bien plus élevée au final.

Des possibilités d'espionnage illimitées

« Les possibilités qu'offre ce programme d'espionnage sont presque illimitées. Les cybercriminels peuvent tout simplement prendre le contrôle du smartphone », estime **Christian Geschkat**, chef produit des solutions de sécurité mobiles de G Data. L'éditeur a en effet découvert que, derrière l'application Google Play d'accès au *store* Android se cachait **le cheval de Troie Android.Trojan.Uupay.D**. Lequel opère en toute invisibilité pour l'utilisateur puisque seul Google Play apparaît dans les processus des tâches en cours quand il est lancé.

Android.Trojan.Uupay.D **communique avec un serveur situé en Chine**, prévient G Data qui n'a néanmoins pas réussi à en déterminer l'exploitant. *« Difficile de savoir qui réceptionne les données et les utilise »*, indique le responsable. Mais la technique ouvre la porte à tous les scénarios possibles pour exploiter le terminal de l'utilisateur en y **installant des applications à son insu** : localisation, écoutes et enregistrements, achats, escroquerie en ligne ou encore envoi de SMS surtaxés, énumère G Data. De plus, la bestiole bloque toutes les mises à jour de l'OS qui pourrait lui nuire.

Quasiment impossible à éliminer

Une présence d'autant plus indésirable que le malware est intégré au firmware et donc **difficilement éliminable** sauf à prendre le contrôle de l'appareil en mode root et installer une nouvelle version du système (en «flashant» une nouvelle ROM). Une opération qui n'est pas accessible au commun des utilisateurs et exige, par la suite, une parfaite maîtrise de l'OS pour assurer la sécurité et les mises à jour.

Il reste néanmoins à déterminer à quel niveau de la chaîne de production provient l'infection du terminal. Car le N9500 de Star ne serait pas le seul smartphone chinois victime du cheval de Troie. Un membre du forum XDA-Developers.com déclare avoir découvert le cheval de Troie Uupay.A macérant dans le Google Play sur son **smartphone iNew i7000** fraîchement reçu. Si cela se confirme, nombre d'autres appareils en provenance de Chine pourraient également embarquer

nativement des malwares. Faut-il désormais bannir les sous-marques des terminaux chinois pour des questions de sécurité ?

Lire également

Le nombre de malwares Android a explosé en 2013

Un milliard de terminaux Android touchés par une faille de sécurité sans précédent