Skygofree: un audacieux spyware sévit sur Android selon Kaspersky

Une nouvelle menace baptisée **Skygofree** plane sur les terminaux mobiles Android.

Le fournisseur russe de logiciels antivirus **Kaspersky** vient de détecter un « puissant » logiciel de surveillance (« spyware » en anglais).

S'il est passé sous les radars jusqu'à présent, ce logiciel espion très avancé serait en service depuis 2014 et a évolué depuis suivant plusieurs versions.

Au gré de 48 commandes différentes dans sa déclinaison la plus récente, le malware semble avoir en effet bénéficié d'un développement soutenu et continu depuis sa création.

Les pirates derrière Skygofree (en référence à un mot utilisé dans l'un de ses domaines) ont cherché à l'exploiter en passant sous les radars de surveillance et de détection des éditeurs de sécurité IT.

La plupart des attaques semblent remonter à 2015 mais Kaspersky a repéré des preuves d'activité plus récentes de l'espiogiciel (avec des signaux remontant à octobre 2017).

Le spyware exploite cinq failles distinctes pour obtenir un accès root à l'appareil qui lui permet de contourner les mesures de sécurité clés d'Android.

Skygofree intègre des fonctionnalités furtives inédites, telles que l'enregistrement audio qui s'active suivant la géolocalisation.

A l'insu du propriétaire de l'appareil, Skygofree peut aussi prendre des photos, filmer et saisir des enregistrements d'appels, des messages texte, des données, des événements de calendrier et des informations commerciales stockées dans la mémoire de l'appareil.

Autre exploitation malveillante : le malware permet de dérober des messages WhatsApp en abusant du service d'accessibilité Android. Initialement, celui-ci est conçu pour aider les personnes handicapées ou temporairement incapables d'interagir pleinement avec un appareil.

Skygofree inclut aussi la possibilité d'enregistrer automatiquement les conversations et le bruit lorsqu'un périphérique infecté est localisée dans une zone spécifique.

Méfiez-vous des connexions sans fil impromptues : le malware permet aussi de connecter les périphériques infectés à des réseaux Wi-Fi exploités en sous main par des pirates.

Voici typiquement le genre de menace sur terminaux mobiles auquel le lanceur d'alertes Edward Snowden veut s'attaquer à travers l'application Haven.

La piste italienne

Selon Kaspersky, la technique de contamination de Skygofree consiste à leurrer le mobinaute via de fausses pages Web imitant celles de grands opérateurs mobiles.

Les différentes déclinaisons de Skygofree examinées par Kaspersky Lab contiennent plusieurs éléments précieux pour déterminer son origine.

Les traces comprennent ainsi le nom de domaine h3g.co, qui a été enregistré par Negg International du nom d'une société informatique italienne.

« Les éléments que nous avons découverts dans le code malveillant et notre analyse de l'infrastructure nous portent à croire avec un haut degré de certitude que les auteurs des implants Skygofree travaillent par une société informatique italienne proposant des solutions de surveillance, à la manière de HackingTeam « , évoque Alexey Firsh, chercheur spécialisé dans les attaques ciblées au sein de Kaspersky Lab.

Dans sa contribution blog en date du 16 janvier pour évoquer ce sujet, l'éditeur russe invite les utilisateurs de terminaux Android à prêter une attention particulière aux adresses de sites Web qu'ils visitent et à installer des logiciels uniquement dans les boutiques d'applications officielles (marketplace).

Tout en recommandant chaudement l'installation d'une solution antivirus sur son mobile, comme Kaspersky Security for Mobile. On n'est jamais mieux servi que par soi-même.