Le malware Godless prend secrètement la main sur les smartphones Android

Une nouvelle famille de malwares s'étend sur Android. Trend Micro a récemment détecté Godless (ANDROIDOS_GODLESS.HRX). *« Doté de multiples exploits, Godless peut cibler pratiquement tous les appareils Android fonctionnant sur Android 5.1 (Lollipop) ou antérieurs »*, précise l'éditeur de sécurité. Soit environ 90% des smartphones sous Android dans la nature.

850 000 terminaux infectés

Selon Trend Micro, le malware a infecté plus de 850□000 terminaux à ce jour dans le monde. L'Inde est principalement touchée (plus de 46% des terminaux affectés) devant la zone Asie. On notera que la Russie (1,85%) et les Etats-Unis (1,51%) ne sont pas totalement épargnés. La France ne figure pas dans la liste des 10 premiers pays touchés par Godless. Ce qui ne veut pas dire qu'elle n'est pas concernée.

D'autant que cette famille de malwares se retrouve sur les stores alternatifs mais aussi sur le très officiel Google Play. Ennuyeux. Sans grande surprise, ces applications malveillantes prennent souvent la forme d'utilitaires à l'image de Summer Flashlight, ou de copie de jeux populaire. Si les applications malveillantes accessibles depuis Google Play n'embarquent pas le code malicieux, l'utilisateur risque de se faire infecter à la suite d'une mise à jour de cette dernière.

Exploitations de deux vulnérabilités peu connues

Selon Trend Micro, Godless est une réminiscence d'un kit d'exploitation qui s'appuie sur android-rooting-tools, une librairie Open Source pour administrer les appareils sous Android. *« Le dit framework a divers exploits dans son arsenal qui peuvent être utilisés pour 'rooter' divers appareils Android*, explique l'éditeur de sécurité dans son billet de blog. *Les deux vulnérabilités les plus importantes ciblées par ce kit sont CVE-2015-3636 (utilisé par l'exploit PingPongRoot) et CVE-2014-3153 (utilisé par l'exploit Towelroot). »* Des vulnérabilités suffisamment obsolètes et relativement peu connue, y compris dans le monde de la sécurité, dont profitent les cybercriminels pour en tirer profit. Car, au-delà de ces vulnérabilités, l'installation d'un root kit leur permet de prendre la main sur le smartphone victime et de pouvoir y installer n'importe quelle autre application, tant pour diffuser des publicités non voulues que des backdoor à des fin d'espionnage.

Aux yeux de l'expert en sécurité, il n'y a pas grand-chose d'autre à faire que d'être vigilant lors de l'installation d'une application. Vérifier ses notes utilisateurs et la notoriété de l'éditeur peut donner des indices sur sa légitimité et son innocuité. L'autre solution est d'installer une suite de sécurité sur son smartphone comme celle de Trend Micro, bien évidemment.

Lire également

Une centaine d’apps Android infectées par un Trojan
Une horde de Vikings malveillants débarque sur Android
Google fait le point sur les menaces visant Android

crédit photo © Creativa Images – shutterstock