FalseGuide terrorise déjà 2 millions de smartphones Android

Google a beau renforcer l'intégrité de Play, les malwares parviennent toujours à passer les filtres de sécurité de son magasin d'applications mobiles. Le dernier en date se nomme FalseGuide. Repérée par Check Point, la bestiole se fait passer pour un guide de jeux populaires comme Pokemon Go, Fifa Mobile, Super Mario ou encore Ninjago Tournament. L'éditeur de sécurité a dénombré 45 faux guides de ce type sur le store de Google.

Visiblement, le malware développé par Анатолий Хмеленко a su se montrer discret jusqu'alors. Dans un premier rapport daté du 24 avril, Check Point pointait son arrivée dans le store applicatif au 14 février 2017 et dénombrait 600□000 infections de terminaux. Depuis, l'éditeur a mis à jour ses données après avoir finalement constaté que les premières traces de FalseGuide remontaient à novembre 2016. Ce qui l'amène à revoir le volume d'infections à quasiment 2 millions de terminaux touchés.

Créer un botnet

Quels risques encourent ceux qui ont installé FalseGuide□? Selon Check Point, le malware chercherait notamment à créer un botnet à l'issue d'un certain nombre d'étapes. Concrètement, après son installation, qui nécessite d'accorder les droits administrateur (pour empêcher l'utilisateur de supprimer l'application ultérieurement), l'agent malveillant s'enregistre sous le nom de l'application dans Firebase Cloud Messaging (FCM), la solution qui permet au développeur d'envoyer des notifications à ses utilisateurs. Dans le cas de FalseGuide, FCM est détourné pour envoyer des messages contenant des liens vers des modules additionnels qui viennent s'installer sur le terminal vérolé.

« Après une longue attente, nous avons pu recevoir un tel module et déterminer que le botnet est utilisé pour afficher des pop-up illégitimes hors contexte, en utilisant un service en arrière-plan qui commence à s'exécuter dès le démarrage de l'appareil, relatent les chercheurs Oren Koriat, Andrey Polkovnichenko et Bogdan Melnykov de Check Point sur le blog de l'entreprise. *Selon les objectifs des attaquants, ces modules peuvent contenir un code hautement malveillant destiné rooter le périphérique, à mener une attaque DDoS ou même à pénétrer dans des réseaux privés. »*

La sécurité de Google Play facilement contournable

Alerté, Google a naturellement retiré le malware de son magasin d'applications mobiles. Mais après Viking Hord et DressCode, deux autres malwares qui avaient passé les barrages de sécurité de Google Play en 2016, FalseGuide montre une nouvelle fois la fragilité du modèle de distribution des applications en ligne. Dans son cas, les cyber-criminels ont profité du caractère non infectieux du premier niveau de l'application pour s'installer légitimement sur le store de Google avant, ensuite, de télécharger les charges malveillantes. Qui plus est, les pirates ont ciblé des applications populaires, des guides de jeux, pour espérer obtenir une large propagation de leur malware. Avec 2

millions de terminaux touchés, on peut penser que l'objectif est largement atteint.

Lire également
Le malware Gooligan terrorise des millions de terminaux Android
Des fausses antennes radio diffusent des malwares Android en Chine
Switcher, le malware Android qui s'attaque aux réseaux Wifi