Une horde de Vikings malveillants débarque sur Android

Une nouvelle vague d'applications malveillantes menace les utilisateurs de smartphones et tablettes sous Android. Selon les chercheurs de Check Point, au moins 5 instances de «Viking Horde» ont réussi à contourner les filtres de sécurité de Google Play. Téléchargées, Viking Jump, Parrot Copter, WiFi Plus, Memory Booster et Simple 2048 ne se contentent pas de générer des faux clics publicitaires depuis le terminal. Elles peuvent aussi être utilisées dans le cadre d'attaques DDoS et de campagnes de spam, notamment. Check Point a alerté Google le 5 mai.

« Sur tous les appareils – en mode root ou non -, Viking Horde crée un botnet qui utilise des adresses IP derrière un proxy afin de déguiser des clics sur des annonces, ce qui génère des revenus pour l'attaquant, explique l'éditeur de sécurité sur son blog. *Sur les terminaux rootés (qui donnent ainsi accès aux droits administrateur, NDLR), Viking Horde distribue des malwares supplémentaires qui peuvent exécuter un code à distance, ce qui pourrait compromettre la sécurité des données sur le périphérique. Il tire également parti des privilèges d'accès pour rendre sa suppression à la main difficile, voire impossible. »*

La France épargnée par les Vikings d'Android

Dans son article publié le 9 mai, Check Point ne précise pas depuis quand opèrent les instances de Viking Horde. Ni le nombre de victimes potentielles. Sur la base des données collectées à partir des nombreux serveurs de contrôle utilisés par les botnets, celles-ci se concentrent principalement en Russie (44%), en Espagne (12%), au Liban (10%), aux Etats-Unis et au Mexique (8% chacun), ainsi qu'en Arabie Saoudite (4%). La France semble pour l'heure épargnée.

Malgré les outils installés par Google pour vérifier l'intégrité des applications distribuées dans son Play Store, les apps malveillantes prolifèrent sur la plate-forme mobile de Mountain View. Qui fait évidement le ménage… mais souvent une fois le mal fait. La semaine dernière, l'éditeur russe Docteur Web alertait les équipes californiennes de l'infection de 190 applications du store par le Troyen Android.Click.95. Des logiciels infectieux distribués par les développeurs allnidiv, malnu3a, mulache, Lohari, Kisjhka, et PolkaPola. *« A ce jour, au moins 140 000 utilisateurs ont déjà installé ces applis malveillantes »*, indique Docteur Web dans un billet du 4 mai. Google en a évidemment été informé. Et a supprimé les malwares en question. Jusqu'à la prochaine vague.

Lire également :

Une vulnérabilité vieille de 5 ans menace des millions de terminaux Android
Une centaine d'apps Android infectées par un Trojan
Google fait le point sur les menaces visant Android

crédit photo © Khosro – shutterstock