Centre de Veille de Détection et
de Réaction aux Attaques
Informatiques

مركز اليقظة والرصد
والتصدي للهجمات المعلوماتية

Note d'information

Titre : **Le malware RottenSys affecte des millions de smartphones**

Numéro de Référence : 15841603/18

Un nouveau malware nommé ***RottenSys*** a été découvert sur des millions de nouveaux smartphones fabriqués par Honor, Huawei, Xiaomi, OPPO, Vivo, Samsung et GIONEE. Ce malware se cache en un service «System Wi-Fi» sans fournir aucun service lié au Wi-Fi. Il dispose de presque toutes les autorisations Android sensibles pour activer ses activités malveillantes.

RottenSys a été conçu pour communiquer avec ses serveurs de commande et de contrôle afin d'obtenir la liste des composants requis, qui contiennent le code malveillant réel.

En ce moment, les propriétaires du logiciel malveillant pousse un composant publicitaire sur tous les appareils infectés qui affichent agressivement des publicités sur l'écran d'accueil de l'appareil, comme des fenêtres pop-up ou des publicités plein écran pour générer des revenus publicitaires frauduleux.

Étant donné que RottenSys a été conçu pour télécharger et installer de nouveaux composants à partir de son serveur C & C, les attaquants peuvent facilement manipuler ou contrôler totalement des millions de périphériques infectés.

Recommandations:

Pour vérifier si votre appareil est infecté par ce logiciel malveillant, accédez aux paramètres du système Android → Gestionnaire d'applications, puis recherchez les noms de package de logiciels malveillants suivants:

- com.android.yellowcalendarz
- com.changmi.launcher
- com.android.services.securewifi
- com.system.service.zdsgt

Références :

- https://research.checkpoint.com/rottensys-not-secure-wi-fi-service/
- http://securityaffairs.co/wordpress/70299/malware/rottensys-botnet.html
- https://www.theinquirer.net/inquirer/news/3028610/rottensys-aggressive-malware-found-pre-installed-on-five-million-android-devices
- https://thehackernews.com/2018/03/android-botnet-malware.html

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques, Méchouar Saïd,
B.P. 1048 Rabat – Tél : 05 37 57 21 47 – Fax : 05 37 57 20 53
Email : contact@macert.gov.ma

المديرية العامة لأمن نظم المعلومات ,مديرية تدبير مركز اليقظة والرصد والتصدي للهجمات المعلوماتية ، المشور السعيد، ص.ب. 1048 الرباط
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma