ROYAUME DU MAROC
ADMINISTRATION
DE LA DEFENSE NATIONALE
Direction Générale de la Sécurité des Systèmes d'Information

المملكة المغربية
إدارة الدفاع الوطني
المديرية العامة لأمن نظم المعلومات

NOTE DE SECURITE

Titre	Le BTMOB RAT
Numéro de Référence	54270505/25
Date de Publication	05 Mai 2025
Risque	Critique
Impact	Critique

Le "BTMOB RAT" est un cheval de Troie d'accès à distance (RAT) qui cible les appareils Android. Découvert pour la première fois en février 2025, ce RAT est principalement distribué via des sites de phishing et des applications malveillantes disponibles sur le Google Play Store. Une caractéristique clé de ce RAT est son exploitation des services d'accessibilité d'Android, qui lui permet d'obtenir des permissions légitimes et de contourner les mécanismes de sécurité du système.

Le "BTMOB RAT" déploie des techniques avancées pour maximiser l'impact de son infection et maintenir un accès persistant à l'appareil compromis. Le principal objectif du "BTMOB RAT" est de collecter des informations sensibles sur l'appareil compromis. Il récupère des données de l'interface utilisateur de l'appareil, ce qui inclut des informations sensibles sur l'écran, telles que des identifiants de connexion, des messages, ou des informations bancaires. Ce RAT surveille également le presse-papiers, permettant de capturer des données qui y sont temporairement stockées, telles que des mots de passe ou des informations de paiement.

Le "BTMOB RAT" tire parti des services d'accessibilité d'Android pour obtenir des permissions légitimes et échapper aux mécanismes de détection des antivirus. Ces services sont conçus pour aider les utilisateurs ayant des besoins spécifiques, mais lorsqu'ils sont mal utilisés par un malware, ils permettent de contourner les restrictions de sécurité. En utilisant

ces services, le RAT peut accéder à des informations sensibles et exécuter des actions en arrière-plan sans être détecté. Il surveille également les comportements des applications légitimes pour éviter les alertes de sécurité, ce qui le rend plus difficile à détecter par les utilisateurs ou les solutions antivirus traditionnelles.

Une caractéristique notable du "BTMOB RAT" est son intégration dans un modèle de Malware-as-a-Service (MaaS). Cela permet à différents attaquants d'acheter ou de louer l'utilisation du "BTMOB RAT" pour mener leurs propres campagnes malveillantes.

Le maCERT recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT en cas de détection d'une activité relative à ce RAT.

Indicateurs de compromission (IOCs):

Hashs :

- b65aa939027363fb64781e51bf0e97add788db1621dd7ade048a8afd2523417b
- 8b292974edd0f6c48c0ebcf4981235c5d375793b716c4d5aeb3af19e77eee76e
- 2b307f11ae418931674156425c47ff1c0645fb0b160290cd358599708ff62668

IPs :

- 206.206.125.203
- 64.233.166.84
- 64.233.184.84
- 66.102.1.84
- 142.250.200.1
- 157.240.221.16
- 142.250.200.2
- 216.58.201.97
- 216.58.212.226
- 172.217.169.33

- 66.102.1.188

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