**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** | Aurora Stealer |
| **Numéro de Référence** | 62392503/26 |
| **Date de Publication** | 25 Mars 2026 |
| **Risque** | Critique |
| **Impact** | Critique |

" Aurora Stealer " est un malware de type infostealer, initialement développé comme botnet avant d'évoluer vers un modèle de Malware-as-a-Service (MaaS) largement diffusé sur des forums cybercriminels.

Ce malware a pour fonction principale de voler des informations sensibles sur les machines compromises. Il cible notamment les données des navigateurs (mots de passe, cookies, historiques, cartes bancaires), les comptes Telegram ainsi que de nombreux porte-feuilles de cryptomonnaies. Une fois collectées, ces données sont regroupées, encodées puis exfiltrées vers des serveurs C2, permettant leur exploitation ou revente.

" Aurora Stealer " se distingue également par ses capacités supplémentaires, notamment la possibilité de télécharger et d'exécuter des charges malveillantes additionnelles, agissant ainsi comme un loader. Lors de l'infection, il réalise des actions comme l'identification du système, la capture d'écran du poste et l'exploration des fichiers locaux afin de maximiser la collecte d'informations.

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 malware.

## Indicateurs de compromission (IOCs):

Hashs :

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

- 03eb03dad424be63868872a75064d87e1475b3102e73fce5d1068e68d6754803
- 073f4e0fd6c50ca8c10cb69bf299f8caaa43b3507be50cad1e908e864f4c6eb9
- 166826098c8e3a2141ba33e148c36cb49a4d60db3297303d71b826b351739b17
- 176651546ec8a3c7ce8a979b0660804bced83a3f405bf42cba10d6617db13b5f
- 18514c44291329fb7adb9ffe307b123f026ea0dce3cf37e7de9ae9e63dacd70e
- 18613fd1fc3560a37917714a4803bf5c50d77f69a242862566c484f71c4bf669
- 2654fbfb9dbb1e04765fcc9caf198d0ac31a1bcd464d5d87e3d2a5c6d510aff9
- 2c116b7cce59dc84b06dfed3a661ade3fa4e7dafd5005ab1bae1c403c57113fe
- 31cde950f7b0bea068e88429b4f83b143333af9002bca24778ba2e7e25bbe256
- 3f99287fc34fa3f9d97cc63f810dc00d391c073dde79b0e1c2c6fe0174020602

IP:

- 103.195.103.54
- 45.137.65.190
- 104.248.91.138
- 45.15.156.172
- 107.182.129.73
- 45.15.156.210
- 138.201.198.8
- 45.15.157.130
- 157.245.55.151
- 45.15.157.142
- 185.106.93.132
- 49.12.222.119
- 195.123.218.52
- 65.109.216.5
- 45.128.234.60
- 79.137.206.138
- 94.142.138.71
- 82.115.223.77
- 94.142.138.93
- 94.142.138.18
- 94.142.138.94
- 94.142.138.34