**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** | Atomic Stealer |
| **Numéro de Référence** | 62221903/26 |
| **Date de Publication** | 19 Mars 2026 |
| **Risque** | Critique |
| **Impact** | Critique |

Atomic Stealer, également connu sous le nom d'AMOS (Atomic macOS Stealer), est un malware de type infostealer spécifiquement conçu pour cibler les systèmes macOS. Il s'inscrit dans une tendance récente marquée par l'augmentation des menaces visant les utilisateurs Apple. Proposé selon un modèle de Malware-as-a-Service (MaaS), il est mis à disposition de cybercriminels via abonnement, ce qui facilite sa diffusion et son adoption à grande échelle.

Ce malware a pour objectif principal de collecter et d'exfiltrer des informations sensibles depuis les machines compromises. Il est capable de récupérer des mots de passe stockés dans les navigateurs et le trousseau macOS (Keychain), des cookies de session, les portefeuilles de cryptomonnaies ainsi que divers fichiers présents sur le système, ce qui en fait un outil particulièrement lucratif pour les attaquants. Les données volées sont ensuite envoyées vers des serveurs C2.

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 :

- 04dd02068b04bfb91198085c56e181bfbb8be9d77ad9f2e6087c8cee890771b3

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

- 1821556d7cb2b1e9016ea21e19d0a5e58b81d9a29770d85bf9cc13e628c138d4
- 1b652f8e4419e3adb6a43d1d981c5b98cef5c68402f9e1965e1272134acd61f7
- 2b790c4d3eeddee410bb8f666759030e7f037e407144706931e0e68ccff976d2
- 47eb748d6c673614a1d88a104a9927c0c0fe0fb29abe3d671e60547a6dd86548
- 558b33f175ae32bef836f8ddcc092b032ac15203c251d0239b5ed6b4e0984438
- 5f59761d501363a4fe359e75b245eacefaedfeb679c8a239a3991fa40d77d51a
- 75d67ad34b3ffa0b0932d29d1c2647bd126cf042e0d7313a41c8fe1a06d3d751
- 79811749a4199bc2ba4f4abe9d9bc0586ff2b2e74622bebac91bce4e236cb3b2
- 998c38b430097479b015a68d9435dc5b98684119739572a4dff11e085881187e
- a9f0c4a27c0142460d9d9733283519d638774185ae3e8d08f23e77ee6bf79ce4
- ae6dce47f2570e84df9045d9a237d45e59ce015c4f638693d64b61061eb518f5
- c0676ba7726e6b4b836c2a07aacb92e41efd9eea7cbc31bbf1a7f9f9556dd4cb
- c8613819cb4978591f4d98edd56bf3fdcc9f52245778416406d5b1e582a7024b
- cdfd9a1d53e6164ce5d2ad530e536ed20ade512b1e632051526ce9154d02a137
- d874054687ce5bf99ac4c83791e6f60c7b00db67091de6fe08985d7d56f7a8d2
- e33b432676455014c350eb392a0a65552419ebc04c522fb6f46fb717d4326a12
- f0507fbad9f699e964659adf1cee12dc9950ea6f99a02a760d1521c4cd9984c3
- f2cb9de40cb8b7e13e7d2b0b3e426f8503781a35d8bba3715395430e9b5eeb38

IP:

- 144.172.92.231
- 145.249.109.155
- 185.11.61.84
- 213.209.159.175
- 77.91.100.96
- 91.103.252.233
- 91.92.242.30

URL:

- http://144.172.92.231/Hisefuhu
- http://145.249.109.155/bullnecked.php
- http://91.92.242.30/dx2w5j5bka6qkwxi
- http://www.antimalwarehub.com/Hisefuhu
- https://gutando.com/cleaner
- tcp://145.249.109.155/
- tcp://185.11.61.84/
- tcp://213.209.159.175/
- tcp://77.91.100.96/