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	" CastleRAT " malware
Numéro de Référence	63780405/26
Date de Publication	04 Mai 2026
Risque	Critique
Impact	Critique

Le malware «CastleRAT» est un cheval de Troie d'accès à distance, conçu pour offrir un contrôle complet d'un système compromis via un serveur C2. Une fois installé, il collecte des informations système (nom de machine, utilisateur, adresse IP, GUID) et les transmet au C2, tout en permettant à l'attaquant d'exécuter des commandes à distance, de télécharger d'autres charges malveillantes et d'établir une persistance via des tâches planifiées.

«CastleRAT» se distingue par ses capacités d'espionnage avancées (keylogging, capture d'écran, accès aux périphériques audio/vidéo) ainsi que par des techniques d'évasion sophistiquées comme le chiffrement RC4 des communications, le détournement du presse-papiers pour exfiltrer des données, ou l'utilisation de processus légitimes pour masquer ses activités.

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 :

- 13a5c1a535c161fd2724423dad1dfa6885c705713569d4ed4f2ebf900df25ed7
- cf202498b85e6f0ae4dffae1a65acbfec78cc39fce71f831d45f916c7dedfa0c
- 7e0d097412ca8c3acdbaaa7c1f79c42cda3a4e50b52c0a8b34d6c75cc764ce42

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: 05 37 57 21 47 – فاكس: 05 37 57 20 53
البريد الإلكتروني contact@macert.gov.ma

- 54942b5bcfc9add448903934fc61f4e02bf2dc6378a65f0aa4af346e858fe9d3
- 7ecf7c1fbcbd0a5cdf683fb1cba2a32d3c999648a3262626345bc044a7f0be4a
- 282fa3476294e2b57aa9a8ab4bc1cc00f334197298e4afb2aae812b77e755207
- a2feb262a667de704e5e08a8a705c69bbcc806e0d52f0f8e3f081a6aa6c8d7b4

Adresses IP:

- 104.225.129.171
- 38.248.95.118
- 139.60.162.100
- 45.11.181.59
- 144.124.225.129
- 45.11.181.63
- 144.172.101.142
- 45.153.34.41
- 144.208.126.50
- 45.156.87.76
- 162.33.177.87
- 5.35.44.176
- 170.130.55.115
- 5.9.230.12
- 172.86.89.253
- 64.23.145.78
- 173.232.146.55
- 67.213.208.9
- 173.239.211.60
- 68.227.235.200
- 185.158.248.31
- 77.238.241.203
- 192.210.150.228
- 89.251.0.115
- 193.143.1.41
- 89.251.0.95
- 193.24.211.84
- 91.215.85.6
- 194.180.191.13
- 94.26.90.106
- 194.76.227.242
- 94.26.90.161

- 212.34.147.218
- 94.26.90.163
- 23.94.145.120
- 94.26.90.64
- 23.94.252.73

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