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	DcRat RAT
Numéro de Référence	51290412/24
Date de Publication	04 Décembre 2024
Risque	Critique
Impact	Critique

DcRat est un cheval de Troie d'accès à distance (RAT) identifié principalement en association avec le groupe de menaces RedFoxtrot. DcRat est conçu pour permettre aux attaquants de prendre le contrôle à distance des systèmes infectés et est généralement utilisé pour le vol de données, la surveillance et le déploiement de logiciels malveillants supplémentaires. L'infrastructure du logiciel malveillant a ciblé des secteurs critiques, notamment les télécommunications et la finance. Les certificats associés à DcRat comportent souvent le nom distinctif « DcRat Server » d'une entité nommée « qwqdanchun », ce qui indique une source cohérente de distribution du logiciel malveillant. RedFoxtrot utilise plusieurs méthodes et outils avec DcRat, notamment Cobalt Strike et AsyncRAT, pour l'infiltration et les activités de commande et de contrôle. Les méthodes d'accès initiales impliquent généralement des tactiques d'ingénierie sociale ou l'exploitation des vulnérabilités pour compromettre les systèmes cibles.

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):

Ip :

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

- 103.243.26.65
- 114.4.78.165
- 120.188.39.124
- 120.188.5.65
- 146.70.45.86
- 149.40.62.23
- 149.40.62.24
- 149.40.62.25
- 149.88.25.132
- 159.65.235.56
- 160.178.84.244
- 169.150.196.75
- 172.111.213.73
- 172.56.40.23
- 180.244.132.127
- 198.98.58.93
- 212.47.70.85
- 217.15.160.54
- 223.205.217.176
- 24.88.77.15
- 36.75.65.8
- 45.128.36.146
- 45.128.36.154
- 45.128.36.178
- 45.74.34.32
- 54.193.169.64
- 76.66.229.226
- 89.38.99.82
- 91.187.80.165
- 92.63.205.158
- 94.103.125.116