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	Dark Crystal RAT (DCRat)
Numéro de Référence	61690503/26
Date de Publication	05 Mars 2026
Risque	Critique
Impact	Critique

Dark Crystal RAT (DCRat) est un cheval de Troie d'accès à distance utilisé par des cybercriminels pour prendre le contrôle d'une machine infectée et surveiller l'activité de l'utilisateur. Développé principalement en C# sur la plateforme .NET, il cible surtout les systèmes Windows. Une fois installé sur la machine de la victime, le malware établit une connexion avec un serveur C2, permettant à l'attaquant d'envoyer des instructions et de gérer le système compromis à distance.

DCRat est conçu de manière modulaire, ce qui signifie que ses fonctionnalités peuvent être étendues grâce à des plugins ajoutés par l'attaquant. Parmi ses capacités courantes figurent l'enregistrement des frappes clavier (keylogging), la capture d'écran, la collecte des informations sur le système et l'accès aux fichiers de la victime. Le malware peut également récupérer des identifiants stockés dans les navigateurs ou surveiller certaines applications installées sur l'ordinateur.

La propagation de DCRat se fait souvent par phishing ou ingénierie sociale, par exemple via des pièces jointes malveillantes dans des e-mails ou des fichiers malicieux téléchargés depuis Internet. Dans certains cas, l'infection peut être déclenchée par un document contenant des macros ou par l'exécution d'un programme déguisé en fichier légitime.

En raison de sa flexibilité et de son modèle de distribution sur des forums clandestins, DCRat est devenu un outil populaire dans la cybercriminalité. Il peut être utilisé pour

espionner les victimes, voler des données sensibles ou préparer d'autres attaques, comme l'installation de malwares supplémentaires sur le système compromis.

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 :

- 3f5fd4bd45b9126820dce6823bc13665a6f714291dd499be1411da49f9008070
- 277b56d4c86fbe0f3dfdaf937c04a967b9aed4dd21cc7bfe6b9d5cfff51caf3c
- 7a78010786f98d5cd1333094de771c82102ef4507cdfbb15bd283a9d2ff2a7bf
- 8d85569277c57cbc9e8bd34d91cc92d5b8f90500eef8a957c80b593d005c6e50
- ac51a3ab39ce7f3ed0bc6d9751ce703a9441fee4139e3e0f40f52b911a6b73f6
- cba3b3d6e4d09b6085412e9ed837b8d2fba1764b66dddfa48d38eaf27ceda8b5
- 19c778a5e7f9989b0db01e5fe9bc81d942b8b65abf33bd3b53eeb229d4e244bf
- 2977d21fa019b7c51a0b6185544ba8e1aecdf6052baa42a0c7c5f9831ae3d560
- 574e05c6f1930253c79c2f273cb83a887b20ebd34c43f1a92dbfed24908d1bfd
- b5af4f5ba69ba7d5a3bba87a31317443f567d6634fe4ec6fb7082d56e0be95dd
- b4192792413c8cc0fa6f81923619528c252ed630670af08c16db0c66745612de
- 5f8fb7b3ec1ea9b380d255083bd797867c5ffde27092bf4f1e33c4c2cebc0a1e
- a2c85510facfc75315c36bd24c342708c8511ec15ba6171dc5d6e8672a0fd9a9
- 4e12bb2c6c91d0155f37f53f4d03876c85266ee0cb399b154e8c7dc347a33429
- a0085682c3a928c251a87e9299b779a46f79217bab142b8eb71e89478e5045ea
- e6855712dc062c90f5937b5a27aa02109562cf6cfda412348109f43cd1ed263d
- 60ff0d49ad4937bd91cb08ce882330fbd09531a725d06618f5cb3d33e329d0cc
- 7234c2680398141eed2206ed34a2f9f620ba7d6b1c17a50758435e48c375000d
- 979322da68173ae1d4d01e7587eaacbb14fbfd55672e0a8f11f14a6128fe2bd5
- c41cdff672327ed8556a904705fe33bd6e78347280c820ef57812630d7fd14bb
- 866e2db7c12a52486c43dd8d1f1f9d2d7222303d52706519925031346a2ce2f9
- 0226d135bf8420b51e4ea48d29f6d809b666f37e41c61b3c41bdf2d2211d60d2
- 91c81144ae2f995d071cae5f71885cf271a7c719010fc10bd275dbdb853a8cb0
- bfc2b5f62d13eb0be84acc30c539ddb41c357e1d746864a05832fdbbedb5d4a9
- 4db100407d9a45d7611349c6065aa2ad3523447abe7c6ca9f889b2a9cf6e3668
- 2ad866e5f8149ab0346a96cc1641294398979be9b97621741570e8e1629eb31f
- 3fd793205621a1f809968b0df03a72aeb4d2ffd9b105245cf6768e3362239cdd
- b35a3a0fba8aea09936a41f362acb7cb6fdc856950eb634837f2f1ce5ee78e06

- e5b38bfe83cc7d5236cc3e4b7ef5642b1b9b82e5c47e0fabfe896781dced59ab
- 618d49f80e17260217b24c316577d9ca4aaacf79da5bef72a848d4b156288fbf
- 0063a514288a4b440beb7a8940da4ab699df599b3f47659a774e330e5743ea88
- bb4ebfb70f11e593e319d0f922ab49fd22a62868a2e69f850418749aaca38e1a
- 25a628beb05c5b454ad7bd04f6abe3e9b8c442e22c39501db3e0dcfb53f23946
- 0fd63cc7d8ad2b67cb02d56c91584fcde27092bf4f1e33c4c2cebc0a1e
- eee4c2c922bc082e933d8c3a8beea157ccebc7a52c59425bbe682f525d2d4fe4
- 380317a3c5a103a7724abf2ab3726f733e4ff044fbb680155548d41e2613dd80
- 2b1f3a682d2881a5e4c285bbcc98c8d5b6bfa04dd4a64d039734de346681666d
- 0e54c905bfc5607323c4178f0b646b1d0e8d00f8890964b0b5dd4670fd98b6ca
- b048dff568fed582121bb87003539d6e4b8ddf6e0ec37c2dec978ecafd51c7e4
- 389677c14528d6edaf1d6c2a69c6eb0a12941c9e18d96f3d676489dd4947714f
- f2f7e46a79ec3e1c9e2b91be3502a03011e090c750e5474bd0cff98a55501d8d
- 0c1c2659f760ebf2a616a0dd7c88c1bd0e005f759852e97f7edc598db4c65af7
- 5bd32b1ddf67bff424987f7bb2ee7d58c0851b71d2eeb0aa0825fe2546a99c86
- d91e1bc2fe9889e17b4f10f2e5c4187ac8b8fca92b5dccc0cc531ed1ddf18bfd
- 4bfee5921505b680e2938c316280835cc133a8d2f64c289d33407f87c14466ab
- dc8af21b27d5d0a6cd6cc762444ccac0c832f15c2fda71405f66d10f06592f63
- bea014c83ac79d7e0abba71046b3d0009d4ffccce85b8fcac6ebb4c85b98b482
- dc73ce51066fdcd5f0c7c88fd6fdfb9a4a3722ebe3d2def1dc593fbc1af9e467
- 2ddd9be6183767f4d8f5be09fec9372b66290734fc0caf6b8196f1b6625b19f5
- 1973cf3f36dec5cd67d949959e93b2265da651f1c7f0845dbb86d773b89ef515
- 60b25fe0cf4f758c5a20613e10665c301b11384aead7d0f675208604cf1e084e
- d5c2d3b27be8ddc6d84e31a8fbed1910747513a0cbbfb020fa79096dabeb6fb8
- 965d18d43a55c63c2297eaeaecb6417f2136e0bfbed435762c4faf0b894fd5c1
- f60d96d7cf8d811191652427c7ddfd138812c8b6eab8e24404171e20ed32a5c8
- 705fcef1225b54c75b1b9b980c037bf90cde4bc1444734781d88b51b4ac1662a
- 31ec3db789b84a51a3c507130efa8831834c29a06674549072a7bf760155d978
- f01713268126b7c7e10f9e15697ee64817913041e51afe1b29237642d98123c6
- e2a4eb4c6d0d0da0d84e23cdea849d73bffc0e869ce2465b3620fd1c99f427dc
- c0b23c836dd31ea5f7c7b42f3467262c5d85581a0941195b76b118b074fa82ca
- d40d05d96ec1b6cfb6389888befd08d43a762147a9aeeb7cec083b7e96aa9ff5
- bc8cf3d41f67ba93ab6e77c99e6685cc1067c08a5928ff92e7dfb8d90ff394a6
- dae0dac2e4e75007299161ace2987a1107f01098188ec9aaceed7c369b6e13e7
- 3d67bc83003986f92c78b0e42ce7c365cf8802e0ef1b8f15e4e9caf15a71a594
- de9dd2ec67928d3f3c7b6560e54e9f6059ee5b313c5750186dbee6a480bc4341
- 5539212cbdd81f30b979056401d5be95b59c42eab19dd402344f431d4d8a158f
- 8ca3a08051c8f3669b3d418b3b17a19da432824d9e29ff32e8b7fa7f91e16858

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

IP :

158.94.209.58	103.17.185.70	64.7.199.51
108.252.227.16	124.198.132.79	178.16.55.201
191.93.118.254	178.16.53.193	160.187.146.97
203.104.42.92	185.208.156.201	45.133.180.162
154.12.87.24	188.240.81.199	146.70.51.74
94.154.35.114	103.121.92.159	45.133.180.138
181.206.158.190	194.59.30.76	20.52.248.45
45.74.34.32	158.94.211.185	46.246.82.12
94.154.35.160	166.88.99.211	138.2.16.164
103.85.225.63	43.157.1.71	212.64.210.140
193.143.1.216	103.171.34.67	46.246.6.20
80.85.158.49	185.213.25.37	40.66.48.150
12.202.180.102	158.94.211.251	146.235.38.234
144.172.88.250	192.253.245.199	158.94.208.143
188.126.90.11	103.75.190.47	213.171.5.199
158.94.208.135	144.48.180.16	128.90.115.62
158.94.208.109	158.94.211.223	193.233.112.39
91.92.242.165	115.42.60.122	217.60.7.59
103.236.70.158	106.55.135.216	154.36.188.196
103.85.225.40	188.132.165.22	

Domaines:

yearofcolour.com	phishing.barefootblonde.com
barefootblonde.com	v3.barefootblonde.com
malware.trillex.io	data.trillex.io
malware.gmo-compass.org	gmo-compass.org
data.gmo-compass.org	ddos.barefootblonde.com
trillex.io	www.trillex.io
ddos.gmo-compass.org	ddos.yearofcolour.com
quantri.gmo-compass.org	atex.barefootblonde.com
www.gmo-compass.org	malware.yearofcolour.com
quantri.trillex.io	backup.yearofcolour.com
quantri.barefootblonde.com	phishing.trillex.io
quantri.yearofcolour.com	malware.barefootblonde.com
malware.hunewsbaytara23.za.com	hunewsbaytara23.za.com
atex.yearofcolour.com	backup.barefootblonde.com
www.barefootblonde.com	data.yearofcolour.com
v3.trillex.io	v3.yearofcolour.com
v2.yearofcolour.com	atex.trillex.io
v2.trillex.io	backup.trillex.io
phishing.yearofcolour.com	phishing.gmo-compass.org
data.barefootblonde.com	backup.gmo-compass.org
v2.barefootblonde.com	v2.gmo-compass.org

www.yearofcolour.com	v3.gmo-compass.org
ddos.trillex.io	atex.gmo-compass.org

URL / Chaines de connexion

tcp://193.233.112.39:8888/
tcp://128.90.115.62:9999/
tcp://217.60.7.59:8888/
tcp://217.60.7.59:7777/
tcp://46.246.82.12:1963/
tcp://46.246.6.20:2003/
tcp://46.246.6.20:3000/
tcp://213.171.5.199:8888/
tcp://154.36.188.196:65503/