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	"Remcos" malware
Numéro de Référence	63311704/26
Date de Publication	17 Avril 2026
Risque	Critique
Impact	Critique

"Remcos" est un Remote Access Trojan (RAT) implémentant un backdoor persistant permettant le contrôle distant d'une machine compromis. Il est délivré via des vecteurs d'infection tels que les spams ou les fichiers joints malicieux.

À l'exécution, le loader met en œuvre des techniques d'obfuscation, puis déploie le payload directement en mémoire afin de réduire la surface de détection. Sur le plan opérationnel, "Remcos" exploite des techniques avancées d'injection de code, telles que le process injection et le process hollowing, pour s'insérer dans des processus légitimes et contourner les mécanismes EDR basés sur le comportement. Il assure également sa persistance via différentes méthodes, notamment l'ajout de clés de registre, la création de tâches planifiées ou son installation en tant que service Windows. Par ailleurs, des techniques d'évasion comme la désactivation de l'UAC (User Account Control), l'anti-debugging et l'anti-VM sont intégrées afin de compliquer davantage l'analyse et la détection.

L'infrastructure de commande repose sur un serveur C2 centralisé. Les communications sont chiffrées (RC4 ou AES) et transitent via TCP. Pour rester discret et résilient, le malware peut utiliser des services DDNS, des ports non standards ou des techniques de tunneling afin d'échapper à la détection par les systèmes de sécurité (IDS/IPS).

"Remcos" dispose de nombreuses capacités malveillantes : enregistrement des frappes (keylogging), captures d'écran, enregistrement audio via le microphone, vol d'identifiants et exfiltration de données. Il permet aussi d'exécuter des commandes à dis-

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

tance, de déployer d'autres charges malveillantes et de se propager au sein d'un réseau 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 :

- 26cf235fa16ac73b07f8be193dabbfb57726a5f66f0e3c47e69c88e957f98550
- a82a1dc134b509de477082f809f6e2fc5370db6b3624e4377ebe136bb33090d1
- 06f611d4425e5f423826aaa8ee1d7031f14990de2ecd0cfdb7f8e60300fafec9
- 242fa6fe46dba02d3638c2a4907fd19d6de540daf9a3c690603eb316ce1f0d02
- 4ca26fdb091c72e253aa4345b0e9cb6f895b61ca1e99e42ee5d0883c1c776f65
- 56277772f8b42caf9646df9d45f85386d4d3adcab604f151d65ed44ca2dcb3d1
- 970fb432d18a2c6792851c437c7364b4a3a4775d65fcfbb79a49024fd1f489e5
- cac09b5f11f1b298ceaa8cf43117bcdf3b39c884ad95365d42c79a2a66a0f7ae
- f6f64ab3d29a0f5edc7a151b99b97d9bed3d1695b52e7a827cb452b6dfafaee7
- 00beb0f758918bbe3282cc7f2411eca831ec74b2de18ccc17111c7efbbeced21
- 1316cc8f353f8fb54766ae2a5b7226e7e5e0d9c2c444cea12bac2592e3d2d6a4
- 135d1368fd695d271faa5cfd9e7c23ed9e1fdb7a5ad7039fcfb6269dbdd9a45d
- 1b845fa5723e939d914acda442623277711c416b8dc2437fac3e3303c7e76314
- 1c96b0da7ac411c2f8b1ce5eac76691b4c74a5ea5a0e62098e1265da4f763fb2
- 33b4f8cefa68f2b66edbe43dfc6c1a86a985a077e8006ddf60e8523bde92e87c
- 340af80fff1f26c4c4f559dd1866db3adef7f568a61938f51e8e736bf5fa9e8a
- 390c6ace5bf980c6f7fdf11635188bd01efd9d592e03692f67f5ca7ee6848851
- 3c2bcd878348b18289f4d983583d395f6c2346342040389336319cdfade1b25f
- 40a48d608f8e0a28548175d252f333b7f9a0e5e75e11fd8a492d0314e4f52836
- 42bce6327fbcbd9b42edabe4f64b5f9dbb13c0a969cac2daa087154c2a79ef6d
- 45d2774e85ef19ded1b6a9dfcae50c06274ae0c387a7c36933816287437c5d62
- 475402ec2bfe62c990f967853b6c42b8ac2314412303ed2ad8bb853409f7f340
- 4f025783d12931cc6c983d92ac89ebcc3f59b9d7d6f743b01b2a70c53411d2ed
- 51bae4fffb3b491f5ecd2a9d6ccae7bb72f53940894fcfb60673cc3968c55109
- 553eea14198b799907b1e6c5927d2288b5676ce407c36da69f6b5791f93682b2
- 5ae5eb4f03ab3b12226afd215a29618e5748859e8c2f05e5031355d777e407a1
- 664ebfc0787033e3ad6ac7b882f82d3fb97bb7e406cdec7ca0f686aa710f67af

- 6704f3399019eb291d806c7364748012ae8da38a40cabadaa11d0b2e7fc42e67
- 74c8146e7915ea8e3039f0af7fe119dce47b88d8bef93d73593a2a3c3c9ff25e
- 7b293cdd5280060fa6c9e30d218900aba6f233d2f631d11997db58978c1856d4
- 7c65435bc572ecf2a56e3d19d0e1d5de3caa56cf6d281b194bc74b59fad48247
- 7ec30279c0e0ef051ebce0ffaf3c85cdf8fefd693a2cc350eb8ab9ececc841ca
- 936739a9c70db7faaf4002bc638b3c518ad6045ce7a2dd1174e1b8c3e3497b57
- 9c7dcf8a256b10d41729c58f9361618a957c6b9691bcf4eb3f9148112940ca27
- 9ccfeffcf7e83ba612badeb68ff7bfe03fa3173a6c8398189bc3b533154ef142
- 9fcfb8fedef7253c3dcae7bced4e966e6877ebf454a861351e6bf8e969ba7f3b
- a7370bbf86ef6787e8f33df762d142f037e2d267b513474b21346c664d10ec43
- aed0ad989cbf7a7fa14e2c2f66da5c9ccf265b4a5c83a294df4aed27136155b1
- b4e80f7bb2c6048f0918b039aa8ad5d54d27d0771cf844c30b60e1ca797f2dc0
- b7866e43dc081330aeb9a9333f66649ffda5bcbba6045760c4f9280b316bed77
- b7dd3bce3ebfbc2d5e3a9f00d47f27cb6a5895c4618c878e314e573a7c216df1
- b9a802c93e7893f84102c6725ddf95aecd84fb77ed03084ba9638325b32e73c2
- be3a771339a0be2cd91f4620a63d9012432b1633918384e02643c275528057fd
- c03a18c05e44860700a6e948df27ff49ae8e938991aa925e7ccf6e3d56faf562
- c6119b42ef13c2c1a72825e98b91f8337f531da08c00e6703547bbf89d57e2ed
- c77c661d14fe00389cd5dd3ed3aea6069044ebb10e4666544b7364f8f6a04f0b
- d2c9f87fd8247cf131dff929e6709c5d2a06422f347d8e8f1bb27025ee53b117
- d467253bb0445c55667adf61ab995ee45df96af2250d86ba43927760e5ae81ea
- d9e2c3d64a11c1695a0e4414a272bf72f0926d76cdb0de51220664592f740ccf
- dd092b872728c53fd6934e40a0c8d8116ef132d177813b3eff6feaeae47f0ea5
- e44dde9bfcf394fc66dd24ad790f9020e8c0017dd3a4e018aa53e62fa2b1daf7
- e593ffd815b0bca8197d065d0175e82843bc46f0ef84e0435f70562932312519
- ecb8ad001b1e4cf9e79d00aa036cf6f24d1127a63dcd2985e3a60520cdc2d57f
- f4dc1bb82425b6031ffdab1333d3de5ff46d8d7c772a50fd998e953370ad99ad

IP:

- 91.92.242.227
- 178.16.52.221
- 130.12.181.40
- 84.32.5.105
- 38.102.9.247
- 155.103.71.232
- 82.102.23.131
- 212.118.56.95
- 104.37.174.154

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

- 78.142.18.62
- 89.31.121.220
- 104.249.10.200
- 38.242.144.218
- 167.88.160.135
- 151.243.109.130
- 209.145.53.103
- 142.171.178.189
- 148.113.165.11
- 194.180.48.18
- 198.135.55.193
- 213.152.187.220
- 193.142.146.203
- 173.211.106.171
- 54.37.128.55
- 154.26.154.57
- 213.183.58.19
- 172.245.4.221
- 104.250.161.126
- 185.140.53.140
- 135.125.188.227
- 45.74.19.149
- 37.221.65.44
- 66.70.181.72
- 146.19.24.131
- 185.161.208.123
- 192.210.150.26
- 67.213.113.231
- 178.16.53.54
- 107.172.31.107
- 207.174.0.178
- 154.216.18.45
- 81.19.131.36

Domains:

- tcp://185.167.61.11:14600/
- tcp://178.16.52.88:37609/
- tcp://192.227.135.240:3000/

- tcp://178.16.52.88:63093/
- tcp://209.54.101.159:5003/
- tcp://185.185.69.14:2404/
- tcp://185.208.158.210:20000/
- tcp://45.74.48.72:5671/
- tcp://185.208.158.210:28730/
- tcp://45.83.31.52:5000/
- tcp://185.208.158.210:37609/
- tcp://51.210.60.123:2404/
- tcp://185.208.158.210:47640/
- http://172.245.95.28/11/goodthingswithbestspeakforme.hta
- https://aumri.ae/img_053925.png
- https://aumri.ae/rump1_MSI.png
- https://gitlab.com/sudo_mom/sostsenrer2/-/raw/main/hold.txt
- “Remcos”s.onmypc.org
- fastroute661.duckdns.org
- newaddressrmc.duckdns.org
- 5junio2023.webredirect.org
- grantadistciaret.com
- payday27.duckdns.org
- 9.tcp.ngrok.io
- www.fahrzeugshaus-mueller.de
- angeliscamebacktotheearthwithblessgoodfo.duckdns.org