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	Le RAT Remcos
Numéro de Référence	51622312/24
Date de Publication	23 Décembre 2024
Risque	Critique
Impact	Critique

Le RAT Remcos (Remote Control & Surveillance) est un logiciel malveillant principalement distribué par le biais de campagnes de phishing impliquant des fichiers Microsoft Office malveillants qui exploitent des vulnérabilités connues telles que CVE-2017-0199 et CVE-2017-11882 permettant l'exécution de code arbitraire. Les attaquants exploitant ses capacités pour un accès à distance persistant et le vol de données. Une fois exécuté, le logiciel malveillant utilise diverses techniques d'obscurcissement et des chaînes d'infection en plusieurs étapes, commençant généralement par des scripts visual basic qui téléchargent des payloads et injectent Remcos dans la mémoire de processus légitimes tels que RegAsm.exe. Des rapports récents ont mis en évidence sa capacité à contourner les mesures de sécurité, y compris le cryptage lié à l'application Chrome pour le vol de cookies.

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 cette menace.

Indicateurs de compromission (IOCs):

Hash :

- 017bb90012dfa9fd9a6a05efd01d1d929e411039
- 0cc54ffd005b4d3d048e72f6d66bcc1ac5a7a511ab9ecf59dc1d2ece72c69e85
- 10c9b7a2f71f61c44df8b277fb2b7921

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

- 1b48e7513cdc33036bc7172bcefbc8b197bb698ca51066d28f15c8478c9592fd
- 1c5fd7bf511885054464124142f793501ab2c6e987b203c1a5f4b3bdcccb1fa1
- 1d466b66435f85871baf84e16bf476be7622dbb5
- 1e2a74e19754bc8f438fed42e3794cc44af3f949db9658c29ee6862c5adcbc09
- 20d412f4c2d2cf23a735109ee712e5df0c03e7ed6b16c0d9f61cff2f4be77549
- 2677b8022e9fd3c18334dd672e16f457
- 3a1b13e80cfd6e053f5a605e531c17a936a33fc5c5467e40be5a8845a2d2dbcb
- 3fffd142a944ee842b2b1f7b6d1446e6
- 4c39cdd2bfb2c7dde761a6e5b8c01321
- 4ef3a6703abc6b2b8e2cac3031c1e5b86fe8b377fde92737349ee52bd2604379
- 4ef9133773d596d1c888b0ffe36287a810042172b0af0dfad8c2b0c9875d1c65
- 55233743d7c15b0a417233becc07dcb4
- 5572ffd080ba92dc24bd703be1d53d5b4bcad05ae87bf74c175f9cb03ac7c09a
- 67c8e554be1e02a42b6d4d7568917e69f346b7f13caed52c5d9ee5b469f4cde2
- 683eb38c67e70e0cf2b9f5b2cb2ecb80dd91abd50539e216de7568512d5087c9
- 69ffd7a475c64517c9c1c0282fd90c47597e3d4650320158cfb8c189d591db8c
- 6b816d84accc3e1ebce3ef55b64b0c5e0485228790df903e68466690e58b5009
- 6d9ae2b15c6995be94b84f2a1d86fc8945594215678711318c88a447263a201e
- 71d8f6d5dc35517275bc38ebcc815f9f
- 7bf7dfc7534aec7b5ca71d147205d2b8a3ce113e5254bb342d9f9b69828cf8ee
- 8eab0679cfb78fe905758bed258de9f454d6a65e
- 9124d7696d2b94e7959933c3f7a8f68e61a5ce29cd5934a4d0379c2193b126be
- 92af4545d62a5b2af0dd493c5270a03ae5d9163b3fbda51b4dcb81996e5ee94f
- 93946883de3d4074ac4baed60abcc3f2d0c57c8ef6e41ceaedbc5ca0de55dc30
- 93dd445822c1c5b30270fc5552a71a02eab536a80ba51e345632d2be18aded49
- 9c176196e1ea1061400ed75a74b16784aa58e87710f516eb363f296d0f909fb0
- a6b930401417a341092dbfd48399c92b
- a782a89d736b8151f153373731479184
- aed52a2c473bbe5272636d738b2e214c601b3079
- bd3f44153b618109f79fcd79ddc856b6
- c1ad7328fcf745c1656f3a541c66608da754ed92

- c202d352895b4977494c10d2942e3f5800a55d84
- c44506fe6e1ede5a104008755abf5b6ace51f1a84ad656a2dccc7f2c39c0eca2
- ca408a4f313a8dc8afe42b490e74b345d758bc319c0b5b251f03fed84e8deb0e
- ca93ad9d9887663ed1afc2197b775268
- cae4e8c730de5a01d30aabeb3e5cb2136090ed8d
- d79593a6fb6c636a50334085b9d6018b
- da8b178b2f11d5a0e08c08395dbe484b
- e256b7c4d8310c13da7e56740f635ef935b6898b
- ee42511075de43ee5be1f719b9d821f3
- f048985cc8229b16b5fbb282ece05980
- f0ec86f6992b1424390d89d3fcfad1a7f3e78bd6461cfb6581c7e9dcebeba2bb
- fb090bb6f92f0ad0f0ab27cdf57db31e
- fb73a819b37523126c7708a1d06f3b8825fa60c926154ab2d511ba668f49dc4b
- fbedc42f24b70fe064a49f5486276c8f
- fc0f6892d07214ae5e43d997c38ca393491d5aba
- fdc8fddeb50b8dd709e3580c0eac02613406602eff4ccbd2903722b7157ef30b

URL:

- tcp://185.208.156.182:2404/
- tcp://186.169.95.181:8888/
- tcp://192.210.150.35:2560/
- tcp://46.246.14.9:2404/
- tcp://92.255.85.63:5002/
- http://212.162.149.39/wqYLnyQAkdh155.bin
- tcp://192.227.228.36:2404/
- tcp://172.94.127.3:5290/
- tcp://79.116.68.10:2404/
- tcp://172.111.139.12:2405/
- tcp://185.241.208.44:2000/
- tcp://207.189.164.112:5471/
- tcp://46.246.12.11:2404/
- tcp://5.230.77.102:2404/
- https://evesecret.ma/WCtwqryUQxCLDR152.bin

- http://evesecret.ma/WCtwqryUQxCLDR152.bin
- tcp://80.66.76.99:2404/
- tcp://172.94.9.164:2404/
- tcp://217.76.57.196:2426/
- tcp://195.211.99.96:2404/
- tcp://94.156.177.165:2404/
- tcp://45.32.129.178:2404/
- http://212.162.149.39/CNWvHQWa203.bin
- tcp://194.59.31.143:4444/
- tcp://185.196.10.242:7736/

Malware Signature:

- Trojan.Win32.Stealer.12!c
- Trojan-Dropper.MSIL.Agent
- Trojan.PWS.Stealer.13052
- Trojan.Win32.BypassUAC.m!c
- Backdoor.Remcos
- Trojan.Siggen8.11083
- Trojan.Win32.Agent.Y!c
- Win.Malware.LuminosityLink-9954241-1
- Win32/Backdoor.Generic.HwMBKJwA
- Trojan.Win32.Rescoms.flybtw
- Trojan.Win32.Remcos
- Trojan.4303FED9D1365C17
- Trojan.64E80D10B2134CDB
- Trojan.MSIL.Crypt
- Trojan.Inject3.11217
- Trojan-Downloader.MSIL.Agent
- Win32/TrojanDropper.Generic.HwMBDJQA
- Win.Malware.Ulise-9768992-0
- Gene.Win.Harmlet.27283-0
- Win.Trojan.Remcos-9763891-0
- Trojan.Win32.Salgorea.m!c

- Win32/Backdoor.Generic.HwMBDJQA
- Win.Malware.Razy-9865942-0
- Trojan.MSIL.Inject
- win/malicious
- Suspicious:Trojan.55545D@2FF0000@32.mg
- Trojan.Win32.Inject3.icemau
- Trojan.Win32.Remcos.m!c
- BackDoor.AgentTeslaNET.20
- Win32/Trojan.Salgorea.HxQBIZ0A
- Trojan.Inject4.16717

IP:

- 101.99.91.158
- 107.173.4.16
- 107.175.31.187
- 128.90.108.132
- 135.181.170.169
- 185.92.239.14
- 191.93.114.27
- 192.210.201.57
- 192.3.220.22
- 213.5.130.58
- 216.38.7.245
- 37.1.206.16
- 66.63.162.155
- 79.134.225.69
- 80.66.75.51
- 94.131.99.153
- 94.131.99.156
- 94.131.99.56
- 94.131.99.89