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	Revenge RAT
Numéro de Référence	58742611/25
Date de Publication	26 Novembre 2025
Risque	Critique
Impact	Critique

RevengeRAT (souvent appelé Revenge Remote Administration Tool) est un cheval de Troie d'accès à distance (RAT) utilisé par des cybercriminels pour prendre le contrôle complet d'un ordinateur infecté. C'est un malware Windows, souvent distribué par phishing, pièces jointes infectées ou téléchargements piégés pour exécuter des scripts Visual Basic ou PowerShell afin d'installer Revenge RAT.

Revenge RAT dispose de plusieurs plugins permettant l'enregistrement des frappes clavier, l'extraction des identifiants du système d'exploitation, l'accès RDP, la capture d'écran, la capture audio et la communication avec un serveur de commande et contrôle (C2). Le malware peut également récupérer les noms des utilisateurs présents sur la machine et a la capacité d'accéder à la webcam du système

Le maCERT/DGSSI recommande d'intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection et d'alerter le maCERT/DGSSI en cas de détection d'une activité relative à ce malware.

Indicateurs de compromission (IOCs):

Domain:

- nextboss.ddns.net

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

- h0pe1759.ddns.net
- kimjoy007.dyndns.org
- monthending.duckdns.org
- vemvemserver.duckdns.org
- hoc2021.ddns.net
- 4success.zapto.org
- cdt2021.zapto.org
- cdtmaster.com.br
- generic.ml
- housecommand.duckdns.org
- adobe.myactivedirectory.com
- brasilnativopousada.com.br
- bodmas01.zapto.org
- n0ahark2021.ddns.net
- cdtpitbull.hopto.org
- quedabesouro.ddns.net
- qcpanel.hackcrack.io
- 8970.ddns.net
- loading8992.bounceme.net
- kimjoy.ddns.net
- frankent2021.ddns.net
- e29rava.ddns.net
- exchangexe2021.ddns.net
- success20.hopto.org
- shugardaddy.ddns.net
- builtx.ddns.net
- reserverem.duckdns.org
- queda212.duckdns.org
- franco.ddns.net
- kingslanddomain.ddns.net
- hypemediardf.com.pl

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

- unimed-corporated.com
- 111234cdt.ddns.net
- asin8988.ddns.net
- asin8989.ddns.net
- 3030pp.hopto.org
- akconsult.linkpc.net
- asin8990.ddns.net
- www.unimed-corporated.com
- alamdarhardware.com
- jorigt95.ddns.net
- alice2019.myftp.biz
- msin.hopto.org

Ip :

- 103.171.35.26
- 154.91.34.165
- 192.169.69.26
- 149.154.167.220
- 208.95.112.1
- 34.41.139.193
- 13.107.246.64
- 172.67.177.134
- 104.21.67.152
- 212.102.46.118
- 172.67.219.235
- 154.23.184.57
- 185.121.177.177
- 185.156.72.2
- 13.107.213.51
- 20.42.73.25
- 132.226.8.169
- 132.226.247.73
- 158.101.44.242
- 193.122.6.168
- 150.171.27.10
- 150.171.28.10
- 200.87.164.69
- 139.99.85.213
- 172.67.70.203

- 176.65.144.23
- 13.107.246.51
- 13.107.253.51
- 4.153.57.10
- 13.107.213.64
- 13.107.246.41
- 20.42.65.93
- 20.189.173.12
- 51.105.71.137
- 52.182.143.211
- 104.208.16.89
- 190.186.45.170
- 200.119.204.12
- 116.203.169.158
- 18.238.238.40
- 104.26.9.83
- 3.163.165.83
- 18.238.238.49
- 104.26.8.83
- 108.138.94.51
- 108.138.94.77
- 4.153.29.52
- 13.91.96.185
- 20.25.227.174
- 23.213.53.34
- 63.140.36.131
- 94.156.179.222
- 108.138.94.58
- 108.138.94.63
- 108.138.94.99
- 108.138.94.115
- 184.30.42.173
- 3.163.165.45
- 3.165.160.26
- 13.107.213.41
- 18.65.229.36
- 23.213.53.33
- 52.168.117.174
- 63.140.36.26
- 63.140.36.107
- 63.140.36.165
- 63.140.37.103
- 74.120.9.89
- 74.120.9.90
- 104.40.82.182
- 104.208.16.92

Hashs :

- 3755718db9d33f4aba2563de454d4530a308b41b1096c904102d08e2101f2020
- 42167454c380a6c730937ae036ba3ca72816d9d9a485363942a4003f53d13eaa
- 4ca6303c84e4134a7cf6399ec541bd82860be09d7c2a38a27affa51cd98e19e1
- 70145527219a5d9dc828243f645d9112e81e62d564a3ac2c263b55af749c8131
- f45f543fea980cd31c4dd4688b9a2a825571c74679f317965b14b3fc65c9ecf5
- fe8c931cec42b96e6d65a9c012b2252f3ffff509d191f798efa2ce3238d68564
- 06152caff6146d423b82800f152b60447ee9e620636369e2d3b0ec61066981f3
- 0b6610924d611b5f7416e7287b473759494b62b3c8777a04fcbe14ba02b01be4
- 0c41e3a88c1b00ff761810a78b7c1435bcca8b820d944a9b0008bca8168d9e7d
- 0dacb4ed834faff5cbfe8ab0d91cd122fd45537a1cce04f82c6546b7c5e8cc02
- 1b01116d6654b6ee69344766bf93e2dbcedeeb216e21ec136fd86e5e00cc7021
- 1e0b1a196791a8ec7a0b959587348f739dde93e1ff6c18a924d3b64a40f04769
- 255a46f6846c2d5d1905fb674610c437c7eda4f003a0971ae2ba22aa09aac0d8
- 26183f2ecc0150b3f4a86497cf02261317acd015b8d2a1d2b9e7035ed35c0c80
- 2b6d56470bb226fae6e0e082b4157a3a4a0c6e21c711f030c1ca9184735a7d5c
- 2f3dd23d44b0404bede4516fa6696ed06aefc5b6bdf58772ec1fb27e697da38d
- 37c767c9c67551d7912070f31a2b2bc4ef6360fa71ff4461097bda77cc7ecb7d
- 37e78f2264e34a3e12b36e9f2a2bbbfb8dcc03291f3052cef5f8606b23ebcc08
- 3bccede4f35680000b063a5596ab9cd36279fcd13f1157937ffeb48dc378a4b1
- 3cbe23fc9fe898bb33622838577d75903c27e668a4d28c14ac23e07062b86122
- 448a687d05f8c5d9d66c4c095174b0882138d904c273f69fed563e8c54452653
- 46d7e215c2f5acaf3156efa1131cee996edfa9d9af764a8f87df52f74cbbd405
- 4726d9f0ae5190a2282076bd42516678ac5383a5df6f90c3f8b004ff2ec84745
- 4a343e3456daddfec95cd05d57235cdcf248f2526d62ae33e09cee131ad3e1cb
- 4ab39deb8e65a8e8e7635585d6970043a072e6634c16592458c48d7d585cc1a9
- 4d2dfafda25c29615f20ade0b78ad841fd63115e5a84227a003eddf07c2c4e2f
- 513fd1b6da4990818480bfe41803ccb601fd2102799e9b5fde0111a5512a8866
- 5773b8fce0b2bc98a9a547ad2880d95e374315e943722f34e94c4cf40d6492c0
- 5927c4f148bf707f8f7afa2a11119db602907add108394230cbaa78243020f79
- 59704f756fb842bb9a6f5af14c72da4afc8f0fdff55621627be03a1015f6ed52

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

- 5b4306579963a2cff27a6729b8338f4922b289f23f598a35043378340634c831
- 5bfe2005b8ea01e579b2b8467b89b594d4bc27b072634e584d034eea44b41abf
- 5f715b4c0666330e8714a317a1ab66bb5db1aa06de8120d86cdcc4508b165328
- 617224c8fe5ccc1b48301b11090960cbd123734f7c6f8abd30ca7ac3407f59d2
- 641ac47beaa6b0e5f429562531b89a497efcbabcaed50fe8430acbb574670f20
- 6538b29b833d393a5484f31eb2e90703d17483f053cbed043439365b69a26bf5
- 6630a0ea265395b22d4410967aca6dcc6838b6bdb03615d866b6f2e803a4b220
- 66d15cfcbacd6e33b8c31cedc82c28bb7845f7ebdcbaf4363a1d65cb3df8da7d
- 6bdd45ce099e479382de52af5494fdfe70f675d6b1e490b1c635bee3a77e8027
- 6e9acedd0a0258568362606478abc7a9ca674406338bcc13a376e012d2d1bf3b
- 6f51c166742bcd213dd2714fcdb49d2986f15d449367b5f5974cf0e1693ad5c2
- 73be82793d3bfe2bcc26a2dab2ce55c99a97f3b4d79959dd111b820e3820f2f2
- 79a07b8e89571c19903d53cfd89779bee1866f757948f732bb6ba98d951b6dd0
- 7ae597f7ce6509c69b18ac49ba61dbb58859f69d31c28a1e65c96312ef87ab9c
- 7bd16db500f710258e1329c6c1b29cdbe1c7c74595b97c0aac7279bc23b83a27
- 7c35eb99c94cab09781a78938a70fa790723a4c978f1b017c231e4a8e98025be
- 7e12481fb7627111458434b60d1846ec501870282758d77acf94cc16358c429b
- 8403fb27a3f2ac792591fd7131332ba8fd5e7e863b5ff3e10f8c9899d8da1110
- 85596d86879503a3f7cf53ccb597e78efdf9ce1d154a0901c31ba521535a895c
- 855a30abeef87888edbfc4c8804f0e9d8fec3f9974167e8dcf1d8bce62dcff31
- 86fa3bb79ae2428b34d2f2a7004b88e383b7763cf2c7e82548f50d70e064812c
- 8ee513c5be3fe709175b3d16afe063b8c8a6fe0f613c780fa55586de1768aa9f
- 90f01e221df2af7ff16d961e0ecb397e4e6f30d0e9986ab99c9035dfa82d0f61
- 9410a0718172a5ba53a68f3708c313d1542ac4b89ec9245183f245e9f20eb9df
- 94d46d103ee5fbf0f8b52076574e88081fac70c17dad02b5621a079874327d0c
- 99c9edcba469f497b87c5d2a51f2e4e03cfce680cc16f9d705c17d138b7f2068
- 9a2c9e022964112762ab46c0399242cd9552b57d832fb44f1f94ac8d6a003e25
- 9b49b3a898f9f88d67b2e58fc7749491d8ce19b30262248e7da93bec50c5e840
- 9cce3910815081665746fb9787bf6f2aeeff00d1b4689f6c011cd4ebf833147b
- 9d507366027764c74fc1e211123f5762c6e6c76fe0d5717c8b184b87c18c0311
- 9f6552b2a1470e3c6439cbafe050c358470cbbd6712125fe08f818bd2e487bbc

- 9fdf0f05481f8bb15d5aabf4b91a3167f4ae9e3b2c9a2027abfa3f54eae5c7b0
- a0dca4250c95161c1a0ddc85c93c722ef7975bab1350acea82e54ee89447df56
- a4778ca1fa269566c1f57d71025d56e2e2ab74b749cb31c1f9f869738830b5a6
- a96271d7122685c4531bde11295ee6fb4a5795283d74e0a786bafa06bad81010
- ad2f07c33843d11334b3567ca11239f4aab4df1023c563c07a5842ad9fe98f8a
- b3229a43f0f1ac228129ff94da393c2c2d588f6b667eb8985da21f49ef18d6ab
- b458b1275049940eb2a1b89b69f0be5c3948045541dfe66c1a6d554f7c0313fd
- b652a8795e21d9e5ebdeec8dd23a60e0c43c8507a17560a286de35ad8ec0e8bf
- bc5dc412145d5f91b8bbc9c6dcbba9800520fe1748e75429c5f2079111545c54
- c18338ed31a1ce1bc568344dda4f82b024c8c34d2c175400b857eab94ff37eb4
- c3e5bac625d071c247445124b6b3bcee80ea4a6ff17f3be1b928ec5d4dcd1105
- c4b659dc6fe72bfdc38bf2f5237eadc39793f546610ab46e3ce1bcfd108e1a45
- c795d7b89add2db5ca161647c0ecd6eb8f3b14ef2972585a31fd3904b3e6f2d1
- cc6dcb5e979027de11aba402cd57e16598013a109b14aff157f608e27fa33174
- cd01b7649306a03afee26ce2afa8122b93878c712e7034270113681b4f807ab8
- dd8985f756a48a32fec9f9166de32365b386c09a452dffbf0803c369530aa40f
- e70fda551745c0abcc8c8c1c5fdcc71d12c76c723a23e273d4e7398803914efa
- ea1113fd102b68e27045cc2a395f7073bc9b52c3437afe76758ec9abf99fd85e
- efc5693b7560702eb583989ebbe717158f0274cd5b93df8c7650999b157c786e
- f43d0a09c138d88eb69f8725d9f8093e1b2e7dd0d6b9a7a6669388049a0a698b
- f458db8cdae95897a5fd4f790d4f91170cc14a4995415c7bed997601c0f43464
- f45a5fd61aa37346b7667a7d7828abbd55a83d2b494b585792d33dba85a4d55d
- f5c4dcc09b063c9cf130b410a5fa6a2502a85236ae7ebb44300781ba1f49de91
- fb7fd279fda77be1ba00309913327ae3901ca7bfea6d8bf1f523691ea17d0879
- fc6ef1c7ca7550e9eb80df34fc1889230860d9e4df16c5bfe0f19f58deae937d
- ff49d89ce3f18b23052a0f1c3d9b63246e240870dc3085e9fcdb9b1e7600b9a2

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