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	Campagne de cyber espionnage attribuée au groupe "MuddyWater"
Numéro de Référence	57742310/25
Date de Publication	23 Octobre 2025
Risque	Critique
Impact	Critique

Une campagne de cyber espionnage attribuée au groupe "MuddyWater", a récemment été identifiée, ciblant des entités sensibles à savoir (des organismes gouvernementaux, des entreprises de télécommunications et des infrastructures critiques) en Afrique du Nord, au Moyen-Orient, en Europe et aux États-Unis.

"MuddyWater" s'appuie sur des campagnes de phishing utilisant des comptes compromis, des emails piégés, des documents infectés et des applications Android malveillantes, afin de collecter des informations sensibles ou pour diffuser des malwares comme « Phoenix, FakeUpdate, StealthCache et Chromium_Stealer ».

Les infrastructures de commande et de contrôle (C2) de "MuddyWater" utilisent une combinaison de services cloud tels que (AWS et Cloudflare), permettant de masquer la véritable origine du trafic et de rendre la détection plus complexe.

Le maCERT/DGSSI recommande d'appliquer les mesures préventives ci-dessous et de l'alerter en cas de détection d'une activité relative à ce groupe via « incident@macert.gov.ma ».

Mesures préventives :

- Intégrer les indicateurs de compromission (IOCs) ci-dessous au niveau des moyens de détection.

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

- Surveiller le trafic sortant HTTP/HTTPS vers des domaines ou IP inconnus hébergés sur (AWS/Cloudflare) pour détecter d'éventuelles communications C2.
- Appliquer l'authentification multifacteur (MFA) sur toutes les messageries et VPN.
- Limiter l'installation et l'utilisation des outils de surveillance et gestion à distance (RMM) aux administrateurs autorisés.
- Mettre à jour les solutions EDR/AV avec les dernières signatures.
- Surveiller les indicateurs liés à (Phoenix, FakeUpdate, Chromium_Stealer et StealthCache).
- Analyser les logs d'authentification pour repérer toute activité anormale depuis des comptes compromis.

Indicateurs de compromission (IOCs):

IP adresses:

- 165.227.82.147
- 192.3.95.152
- 198.46.178.135

Domain Name:

- my-sharepoint-inc.com
- googl-165a0.web.app
- cloud-233f9.web.app
- cloud-ed980.web.app
- cloud-233f9.firebaseapp.com
- googl-6c11f.web.app
- my2cloudlive.com
- cloud-ed980.firebaseapp.com
- googl-6c11f.firebaseapp.com
- my1cloudlive.com
- web-16fe.app

Hash:

- d4715827692a248f1fbeecd60f9a99b7bd639198e64c2f400710c52503eba1f8
- f359f20dbd4b1cb578d521052a1b0e9f
- 2cddc7a31ea289e8c1e5469f094e975a
- 23dda825f91be93f5de415886f17ad4a
- 0aa883cd659ef9957fded2516b70c341

- 5325de5231458543349152f0ea1cc3df
- 7ddc947ce8999c8a4a36ac170dcd7505
- 4ab1a1d13496803ea594bd1d22269fe92084b754b3d41493b7cd9ae7a7ef4b1c
- 24b6b5b8be0b6640539cd7f5458a9d2a2bee05f9260aff905da9d06f4de9c726
- 7bf78e2191152afd4e805b5665f3ca51d58f1aa6355bbff723f198fed660be2d
- 911d0bf57d4d1168c9fa40ad4fb3e681b35625183bf7cc52f83caeb98bb071a5
- dc55fa2bb0bdb3f126148b1bb5acca88508147b320655eb864c195e2df2e3c51
- 8055f1c450d3d680a2a3ce5ad534034d2fb5b49a8c2ac39039f460a0491be5e6
- 5272187ff64ac4830f326ff7a73639af15112e0fa8b96f9f33766a748c6aeb21
- 9cb4eb5f3af54c0600b9e7c9ca7c127a6648c832f7589347ce56b31fcc3a0ca0
- 82047cb3e292b39da99b3ed821d9ada223ebfe05f36706980a414c8b1bcd8697
- 09a5b7e448ffa0f2c2390ec7f01b1eb8faeca081f4dbfafeb0fcbaa0190e7079
- c2d4decf232858f70bdb83e9ce52c31c37e73ece568ec58fb1599dc51b99b055
- d3c2058203ff511a4c83b1d0a9a3c4613563581fa78450ab51c55b1247ba48ba
- 9b64044c15cbe74316804a05ba11ede94f308cc40acc62adbba86f7834228c36
- 476593e5222cc396c4852761aa580a89d60a955c7fbbd90f0d101b4cc35c30fe
- 4c479f2f3ea71b51dedc9bb84cf4dfdedec057b82bdad7ae0f3304c905659491
- 6c163bee10e7a3b0c3ca2174f9875841fe26815c52d63cdfc4553ef422493d98
- 5785ebf2b3947f2c9490a3aa1b5efbde8a9762cb11261a35d91c819e21833114
- b8363d36701b3a635ce001132768a8383d7584b1080eab3859b8fcb839298e47
- 934abcdf300f5601ee6bc225920a59003a6ea558ad2ce4ca8a0fc21bab40306a
- 21c7e8b0fa1b8c5a8b3a9ece0b2b6ec4fe940d98289bdad2f36e31ca8916b1f8
- 134a896fb7252b21691838eb53f6f96e6ac8f36003775e384d786e3a44ef1ca1
- 114d29dfb63b29c803a3e743808ca285e95b380b1378321dca2dff5742423246
- 76e289ec5b947d7d79543c389d2a2bea067cc19d77cbfa4add81c988c1835a4e
- f0269becabc7ac8356de24d36a9fe0b03e708da26d5062bf94b8ab8073462702
- a4f7d54fa2a8b5748519d20fd65745ece3fc0ecd8685b48791acbf4e967d9727
- 430b70e01fbcbd7a9bc603e708d94c45dbff0ffbe7d49fe77fc7e27651d788e3
- 96336ed4f840c241ed216e7682d91ed9a4cc76dd56087956200fb88f4781ae9c
- 956e562808a1da1908cb475e3cbaaa81319809835b33327949d20db0b5d0b1ef
- 6df263204ae5a0fa24825d78a280cabbc7c3f5288281b6ac770465807f22946f

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

- 5a60de044c16784f219f6c5500c105ef06bdc00975a1518a5a73f90ca2bdc68a
- 3dcb61c8530dca57db103b359bfeef325b3495166ceff0c68449d597c4aa77ba
- 1decc5cefbd3f7aaabbc916d509a8e6a16fdeb73f7dbb30bc0f02d33851d78c1
- dcba6db4d94eaa0caff01673d47930c53d3ccd4fe793c09e12547ac5d53b2d0a
- 219908bd5651065041fc2333d2d77a5b7eaddeaaa6a103038b69ad6c4952a873
- 1666f3571f20bd83257e3525a05d141977ce18d0b30f0dfd9bd348498bc513bb
- f3c37e7f065b4a9ec6d9d6b05313b8027e13097a4ebec04f5e140a8d76f788cc
- cfc6be807622eee92d19f4c79fbea4b8df263211c719ed828dfb0e28e5a13ae0
- bde3aeaa908777766d7a105789ea0af25c21a445f3092e574917f7b9b4d8e936
- ad1a6487ec0d6e97c223d55cdb6cf93f08897afce06034fd5699ba1479e8035c
- a9379eb4a91d9f04a767d45d65435df1dd021c17ea802c69de3b3509b93a22f3
- 5cdfb7506671b54ba2aa06ca79ed345b0f7454dc8376673c6928cbaa09d98243
- 1c3b60712c5fae9fb4ebb0b3bd05514d4d02727d65826f3f56d9aeaa74d50690
- 195c8edd53b0bead92afcf59d84011f774471c10f1456242296eac55a40fca76
- ebd6e7a18412487ccec4124f22d008ac12208b6293cfeda0f5b0f9c44b04da4f
- bd0a37c5aa2b7964e1946343a95ae4e9edf06638ec63af058f198059868779a9
- bcb6b071f96c578d2262fc1559b8ee534fecfb47e9cee3096b3cde7576de99da
- bca59991c29615f5bc0dae618df88f3e5f2823f39fb9193b30b6cf9884a73127
- 0920dc44442e04d196db33657904fa09414b02c767c56ef06b17d6a5ef2d5f53
- 3a7e74024c233663dc9b627117a4df291f5a413cc829b5282f090941254365ee
- 14d4d556cf7a47c9a5ca72e20e9cc33266958077cc417215579d4a7b7d69452e
- fe7164552d0745762dd0194ca0b33c7198da914db047a595e0c7a83a66ea7ece
- a75d66c55204c841dc76f24be92b8d631a4018f3a6503da5692b21ac7081ae2d
- 0bbe4dd2c3c71ac981b7c57111fb893504ef21e8a47248f50a6cd719e4abbad4
- c22a6dee941346ad89b2de52d7c9a0ee57c0f414a062395abf64dc30f59debde
- c56085f7a62b696b939392eb3f71a2867fd80ed6a269325df81e2720f2527b6b

Référence:

- https://www.darkreading.com/cyberattacks-data-breaches/muddywater-100-gov-entites-mea-phoenix-backdoor