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	Malware " PlugX "
Numéro de Référence	60111901/26
Date de Publication	19 Janvier 2026
Risque	Critique
Impact	Critique

PlugX est un malware utilisé dans des attaques cyber ciblées.. Il appartient à la catégorie des chevaux de Troie d'accès à distance (RAT) et sert de porte dérobée permettant aux attaquants de prendre le contrôle complet des systèmes Windows compromis.

Une fois déployé, PlugX permet l'exécution à distance de commandes et l'ouverture des sessions interactives sur la machine infectée avec des fonctionnalités avancées de surveillance et de collecte d'informations sur l'activité de l'utilisateur.

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 :

- 085ba6fd93badd8db832822ac9d2c66c52e7c7f0bbd5d993fe7558dfefb90f85
- 0c6f794c372d1298388473b9a3ce87d7f8f03be61b0d804fab9c22b7188e664f
- 26015fea3c8dfa90d7d660cad4bc4de38e23f1e245e6ec2a9437d5f6e3176fae
- 4f4dba176858dd6f60114de4de180066a30e5a280136e980ad623883abb49785
- 6df2f0135c3d5892360557e244b440679dfceada50b7f964c13e8b5c9afbfd9e
- 90520957e251bf845cefd5a8b018d02406bb7cb1c06812939f25e76cf91f2785
- 9e0c7216dff5be4dc620e79788cf0e4d61b542c1e7d3fc7487d0fc5750ea9f4a
- b0a59478a990b42c64418fc14737e8a029f0adcd9af466345c6f61a041724c08

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

- f937efdd57d710e48ca391fdeb9ef6251cfdad836f7c46bd92920b5e3d66a4c8
- 0103073e028279dfc352b44cc65f6c0ba35c925216ba9f762d79466b27025aa4
- 787014513eeaaf0c6992b25476a1df30fc52a21e785d17e35a6eb2a8dccdef27
- 859a79c8fc9679da7597acf00176bdcb0cf8f6ef1ddaa41f35bd309d1fcc4dda
- 8fdb6e1fc50b4e729f7007e9f4c6d9830fd694cada5b444dc058a908e50d19c9
- a2898af691137f2a0a353e984a99dc0373f04b1f31b37c764e73ab8ef8cc3bf8
- a4c08d6f0c190a26b43cd545c9e6c13150fd4804581242d4f72829ba02090436
- cbfb079a24896534ad3c478bca64098e53004a38d686d5c61f62f485fe581c08
- eef5c4cb080dacba76e0dfcb21c2d8842eb96887344c13f9c9aee56702e62f1d
- 273f0dec1ffeddeac5555378959dcb4cf7d1349b90d1187d9c6eff0269384b1d
- 7fc8e350ec735791d058b3cc3812592f9ed6930c6c2782c9beefc348019414ba
- 8cdee2431860113a6c60ee0a0f7aadfda6dd3b63765b52d4926aad7455250d11
- d6933507cff7df6c171fbda9e4a69414e36ba4f85ef76ab8d65391f8a000314d
- dafbe2b475d39d59e1d6f297c10da8c0a3cc4c5767d6780005211cd1590cc4dc
- e8a9ca27b4480df0209ab8e2a60a82021f4eaebc2fcf1bc764996a7329059fb1
- f4e9599dfdc3209e6147c5bb4884f78ea0a20da6f7019a267054fd39f7c66356
- 05cc9dbb6d09407f7abb25a137a3fb522389cfca6688ce272147f9b1bfd075cd
- 2ada64caa86bb02aa3886ab792b6638c16eb2787f478bed6298afdd101c40237
- 3f4fe9c060ecaa4008d81675747b804324ade5667569f4420cb1e74b85a704b0
- eaa4689ae42a576248ed589e21aa455712277ad5894298df1c8e66fa94eb98a7
- 387135f4a63ea284fd0c0a17b5e98c0971c8d13bf0dfc85791a0b5baeb723a09
- 6113385c8c6bbe5f08408b023cf157f44e4e52c1f7a1fedb6a22647960ff1015
- 844e5a3dec0a1d1cc59950ac5a03cff87e2af0d280f2cfa208a6dc3ee568b5c7
- 9aabd59a316e675565b8b58dbfad5e075acbe788e0db879aa17a556a8a06c228
- aab4df03d311ec24f84883aa26c27b2c36b17895cf3271fc904f14fd23e81156
- c658e2e4bfb37a4d30417c677dca9563ccfcbcd6ffc1e5da4cd2e19f0b1b76d9
- 44d75e5351ddb0db02ea4096ae4e7148800fa546758ce349807c67e215428771
- 6bad739942c38819635fcb6ef9f977d4c87c628a2540f7961c8f42c84c835f03
- 85ad4581dc2557fc99de7e6f9dd39d02b85ce7097d067dd1e0d731c855976558
- 9be00f9128a52aa0d1f9c2b7c9670af2dceabc7a242ff0057252b26ca006b0f2
- d18768e42971ceb006fe6b10f2ba38feef80e6696fb97f8eaf469b0ff9d695e3
- f01477aae43f0148158c8abb5e902a5c425031cd17f71281c1ad8badbe65f408
- 54633710f29180a4af09fe1c5090c297c29f0a958026073d4bef3465aa98451f
- 10d6911a1c96a7f2e7db84652da863b085da2ccbc8730cb3f6f4f5039d8c0947
- 529f28d62bbbacb8c8ba96b5d0c069063417d1d8949974d454da4611a4081120
- 5ef61d2e0346d02f5f83029bfe0f57091e8d5d4f3cd6a233d8f6f95fc63ea5ae

IP:

- 103.238.225.248
- 103.27.109.117
- 108.165.100.65
- 139.84.227.139
- 140.82.55.149
- 149.104.2.7
- 154.213.178.185
- 154.31.218.222

- 166.88.77.210
- 180.178.47.18
- 180.178.47.19
- 180.178.47.20
- 180.178.47.21
- 180.178.47.22
- 195.245.242.234
- 198.20.155.142
- 208.85.16.182
- 208.85.19.80
- 223.254.129.212
- 23.133.4.5
- 23.133.4.6
- 38.147.172.12
- 45.115.38.119
- 45.147.26.117
- 45.32.148.180
- 47.75.177.15
- 5.188.190.39
- 63.141.237.208
- 64.176.6.235
- 64.176.65.165

Malware Signature:

- Backdoor.Win32.Plugx
- Gene.Win.Harmlet.1493-19
- Gene.Win.Harmlet.1685-25
- Gene.Win.Harmlet.18768-0
- Gene.Win.Harmlet.5142-0
- Gene.Win.Harmlet.61488-6
- HEUR/QVM11.1.5FDD.Malware.Gen
- HEUR/QVM11.1.6814.Malware.Gen
- HEUR/QVM11.1.6B1D.Malware.Gen
- HEUR/QVM11.1.B131.Malware.Gen
- HEUR/QVM11.1.B305.Malware.Gen
- HEUR/QVM11.1.B338.Malware.Gen
- HEUR/QVM11.1.B341.Malware.Gen
- HEUR/QVM11.1.B34D.Malware.Gen
- HEUR/QVM11.1.B35C.Malware.Gen
- HEUR/QVM11.1.B37A.Malware.Gen
- HEUR/QVM11.1.B911.Malware.Gen
- HEUR/QVM11.1.B92F.Malware.Gen
- HEUR/QVM11.1.BDDF.Malware.Gen
- HEUR/QVM11.1.BE18.Malware.Gen
- Trojan.Crypt.ico

- Trojan.DOMG.nozn
- Trojan.Generic.cdptq
- Trojan.Heur.dxd
- Trojan.Packed.18626
- Trojan.Siggen2.50583
- Trojan.Win32.Cospet.lpX7
- Trojan.Win32.Gen.tqIl
- Trojan.Win32.Generic.4!c
- Trojan.Win32.Lethic.fcmfps
- Trojan.Win32.Plugx
- Trojan.Win32.VBKrypt.lvtJ
- Trojan.Win32.Vilsel.cqkyek
- Trojan.Win32.Vilsel.tpQK
- Trojan.GenericML.xnet.yzmj
- Trojan.GenericML.xnet.kdlw
- Win.Malware.Genpack-6989317-0
- Win.Trojan.Plugx-9938343-0
- Win32.Outbreak
- Win32/Virus.Synares.HykCud0A
- Win32/Worm.Mau.HwsBs5sA
- Win32/Worm.Mau.HwsBSSAA
- Win32/Worm.Mau.HwsBX90A
- Win32/Worm.Mau.HwsBXUwA

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