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 " Pykspa "
Numéro de Référence	62181803/26
Date de Publication	18 Mars 2026
Risque	Critique
Impact	Critique

" Pykspa " est un malware qui se propage principalement via des messages malveillants envoyés sur des plateformes de messagerie instantanée. Il incite les victimes à cliquer sur des liens infectés menant au téléchargement du malware.

Une fois installé, " Pykspa " permet aux attaquants de prendre le contrôle à distance des systèmes compromis, d'exfiltrer des données personnelles et de télécharger d'autres charges malveillantes. Il communique avec ses serveurs de commande et contrôle (C2) en utilisant des techniques avancées comme le Domain Generation Algorithm (DGA) afin d'échapper à la détection.

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 :

- 02f32cd32cddb07c1aa19790791a962f355a844c2511e8d4bd2f307bff243524
- 24bcecb93f2e6721ddf0e1450a64c123b5aaab2b2ceb5d67ab1569fc9ae45ebb
- 744ddb5c1098b84f006029a287b695dbf804870a86e663da447c9cb3478d79ec

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

- 750b60f5636c326ccbbff7046e92c9724ea0874e099b7c5565b33438fa5fd592
- 96bdb784656c14e1736e1dc2fa2811fb3c0725f8bb94f8c97c990745ae4fc85a
- c10b0aa8086c4510e750520dfd1f8ad78c9a3b3cce91ed36eb4c2dd4e8b3c45a
- 01a66f5c79f9116c4cdff0a900973760cf36b31e7e46e31c78037e690e1a38d1
- 02c16396e9206f729380d4cf00bd2f8a818d320dacf0150ba3baf56e7c8e22b9
- 046d1bc01d6d5b8b8a5496b9390e415c4edeb639d95fc8177f2aa0bb2afc1fc7
- 0558d0e5290a5588d3d4fc5ac10e84a6cd917456d270c60372155b6eee1349cd
- 05c929b9faae0bd39fb5ce83456e7bd72d911c52596b4240ad0768b1d3765c59
- 077edf6e854cc4bc20e43d65d206b09604973259fd653d9873c5086c7a7d2769
- 0a4e18cfbe99a70af750ebf675009e4dbb6736c1a9ff002b5ecff04ca32945d6
- 0b40ec53e16274dfd81d7b7ba189e2da34f4aa2ed56a82e325782288755e2002
- 0c5dfef296e118812c3ab038416edf0c90ac1ecd4965cf398220b4e1acff506d
- 0d1cf1b91229a9f1d321b1f2596700771f3604b648e743243766a14ba1ff955a
- 0d5dedb84942ba8de42c3cf82be74c1167b696f807511bd51f9fd7f543e0b8eb
- 114dae28a6be216f564bd1bb4add692176d07721e50a801963c879727f8f7468
- 125ad197395a6272b67ae8d2f6756fba7bac0593b3bf105b9c121d4b5f5cc453
- 12af269c1f5e32c14ea2208a60ebe5869b94220f441e7c947cfb1896f7e85ede
- 1325d504c6ac00bed8d55dbc7842fdef3d6edd338c1ddd70c434a0730cf64fef
- 1347c61fd51519fb584b3310a4a9fe95bd2f45685d4091e3c905f08ef491cbe2
- 13a717dce4b901d719c60323f2627d9d69caad35ef766599eb4f39c953d4afe3
- 1509b93450d737876c3124be368dd0424bd04294396b5e7f879a022bbb7883b2
- 1645679eb0f988b9d0dff5d7d8ef4deff0028c6b2f8f2fab8bb6f2a017282ff6
- 19c5e6aac915bcdfb415cc57dcee6f0392203597521c96136f20c7ec729d5367
- 1bf6dd3b052fe5a0b9b49862c99cedf0ba309f99719b82be52492269aaf6312e
- 1d0f4c2b21debb8b4e7d192479ad82157f98c38f618e106598e36625f94fd6bb
- 1e4c299eee15f4b4aa348f6f62000ce22ac5012ea2e983049d1a752763cb4442
- 1f7ccdaacf29a789db678a8baded1c922d69dd93d62af6ed6a1fe3e370a284b8
- 20c0e1275ec38f9b96183f58568e5fa8a07fb5a8afdd68ba041993907d501e40
- 21608c5f0ae526a963973684876bbf4d1ac7fcfd13f528d22e15560a1e3bcb13
- 23ec1255b5931798db5298582f22710b402784fc86e859bf337703e34e705778
- 266ef133ac5f36c29273c07eb29c520021deed5d4b69e15d23417434f4dd5b6b
- 2690a9fa5e442650ff34289ecd2f59d062a3702c8dd0dd2b05b36b1e7b6b3a45
- 26cb155e596db0fc7ca44f8d9b2640cb4eca9edf8e81b52a80793d95792b2e4e
- 29bdc32a9d8ff97ebd7a4a6b3809b79fb67e077b1d896133d2bf9725859e7712
- 2a180de2e75b865e793c68b6216d517e45f2536c176eb3ac785f2822ad113590
- 2adf894ab669c233d77e379f8c7ce702db4d27c445ad6b0d104ced25130569e5
- 2b6a58a530026f826dfb4db7f4fe819fe12e20ed91fb0d44090da9772d871a84
- 2c6824d9367940bda6737d68e1db0846226b276aaf86f7c9bfd9a1cce562ca26
- 2ee5b201a8e9a0f3972720cc7cd722518ba272c6bb53551628855e57def2536f

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

- 2f1dbf75abc85da67db1c4b6427f3b2f20099c8f78de4e60becb208e4ddf8480
- 2f2f8a2ca2d4f3acf08d60c3f7122a46cd0c5e4e444e118ef71552e255464406
- 308a5ce6032619867b59fcf451ae257b855b61591cf900730e32cfd2bcf86400
- 32f83d5c6cb2a9bc33089830f4c11817b672c5e136394e2a558b1c820df35b87
- 3317db8605c427d2a9aec046fe26c09ab90b2326d92d1f0499fbac5c66461c14
- 352f5cb02288b4b5f89713fd9d8a6dfd8bad5d89bd330eb9e448b34f8b83252e
- 38c38c13341f7941cb028883c93fddf982d2ae8cb0064f66334212371bb0ff7c
- 3efe98fc7b4742ada118d5b1a300dcd73b7f0bd344f730149740b7cc96b2ae64
- 3f1ce0254da3787ad0402770154e32184e3e220586a754701f599f9c12e66895
- 4265b6acdf179d5d8cd4e43e50d75e4a2d3a1be8a751ecd3b169294335f5e6f4
- 49fb173ed290b37fade6f2077dde1b1f634b3d37257d98bc79c43ca16de10ef4
- 4c6d0db43154a74db864ffe1e20b996c8b34dafd11fb749894504e73668fd566
- 4fc7f020f4b98fafafd3d84e9b369a7a23b199f1c6956de4b458c87ac2a64907
- 500916fd0e5f1454c565e1a46096c0d4eb1edf7712defaffaf33a7817051dcc0
- 50e076571fc01eb1ab8f7da4cbf46d9c2d8e5966ae46754dc4be383c24c0a204
- 5172f7b53181ba90f62d574ea7326dec67cb7cc3a49d35afe366d410c49eeef9
- 542165f94a4cbb2e738a590d226ae3835762c101d21a5d108c455d8ec6ae698b
- 54a081678612ee9dd3347899e315227499cb21a3d1bbd429f27c13da9362456b
- 552c45c836d3aca7021686a387ed754b2c2ca0d5a2b3b9f9a94d7538545de112
- 55fe719d1fe5d72bc94e5e2e330060de395d41513a5a8a3fe95bc9b4dff82faf
- 5c44a8fe6c3c0bc6667868c436b7bca695fe1c15fc384248f3fb1c78e8e14cbe
- 60f75de894676ff03fbc8516496da4b6ea057bb50343374af69eb54e2dbd1163
- 611b5fed7bd1b951b21aaab910d31acd9ee84bb1298d99c1ed5307d394e927cb
- 62d15f89e3a05d615b2056cc26377511fd38e094e3ae8d4751cc5867e9df6b59
- 634f20bf29bec4efa842994faa0e4471a063ce7030598dc395cdedf93b01e4d9
- 63574202b93c3bcca893dd8c8d5efc8446e462c4668298616f133ecc6cc4c18e
- 640583e4914082fe2e045483628088de0cd05c056d5ca41cb7b383243935c4d8
- 64a53634bf904224cff5589e6fc08cd3a28a22cd09c8ddc387b4196d9e2df5ab
- 673facb61446df7546fdd7d9414a6d777881d463d2a7face0324bf0afa007cea
- 68dd7c53600c825491eeddffe24be7ac166a4eefa0e02bd29d74fa8a39493a30
- 6988e61d401fb3533258e8b236bf08d86e991df09c1d847d5f6bb7fef563848b
- 6a759e53515bcd770ebd76ef225f7f70fc37f5d1e89ba48a4fa2767769b5738b
- 6ad458c52af1c71f3889b57b7d3a97f13ed18620b8a56d26d66f472a3a4c2c5d
- 6ba469bee619c2e363f3584f3e0a5fa18fd8abeb94070d27cc43ab9651a90e3e
- 6c5cdaaff51cca0bfe640a8d363af793b364b904666576330ab735bd4482c0e5
- 6d1488c78620947e40a8e1362e9db6c113a5bd2cef33811b80fc4d814a4b7c5e
- 6de9ebaae2585e0fa03bedf329062bb592e82d6f56dcc95fc1816d232c48444a
- 708a2e764c8d92f064a253c8326ff21416be3c3a49d124a1f73d89ab3a0c4257
- 70e69ffc6f8ba839440087ff7838f7790b8b0be99b96486918e6b4999e9e0774

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

- 71663686fa39deffc863b71cd25ff05fd5b04d1b2c2ec6ce96e8d987fdd31352
- 72820654a1d390777e8104e2f0a02c5a32e4dc669a5979ffcc84ffc1d66728e9
- 734f186e6b32ee063ba9c336aefba84bb4dbed279584ff2746e7228a2ef6b948
- 759acc6be3afd8605d82599b3cf03bd0cf3df6358a3d9a352dca11cf4e20550e
- 75adbc11eb9093a2c217f4e76de57ff5042ca48c531ba83894788e333f0b5123
- 76dc6cc95c1fb4a5ab1142ce465bcc98139861dbbd7b74be24d6e9d6e60848f0
- 79980bfadb285a98d834e236b799d146301a41c525b7adb8b522def74b72e4fa
- 7a5e9e2acfff61c00373018f3a43a5a559f5833479b73dedeac316278ce54406
- 7ccb46c91706de7c7d409a9a8b8f44adcee8c693fc2db8799ca0db4eaba6e329
- 7d87407f49c5b03c1ee23ecf3e0e8ec1cfda7300cd92fe61c4b0d51f3c10cbdd
- 80b730f9a0fed5fb62e0ff5a4c54dc19f6014842e50c5bc6d49f61ee5def7a19
- 835a53b41c4303249764a91c00156f4f90d44c18b09860cba91a4ae1ef16883c
- 83af4162c17d7778b5bcd22a5d4a31aef190a0f71e8a1ba7ee448224874eeb07
- 84fe4ffa7adc8002a0aa9a4da536dbf34f647339e1e5d1b6ef58ae841094381c
- 8550465f4c1d834e91216ba2578da0bd71fc45b629199f99a12c1101076c4d29
- 894a2c9cfb5ed4c8893566f681b87407a470713daf81479462b234a820bfe856
- 8caa82e00d550d8cfc9094361611b365213f4b385fd32622dc5b17d32d39b47e
- 8d095a7966490bc8c0d1a10155b8bddec5b7862367c9c6f2623f58860e47f775
- 8d3fe294af52d9fb86b4a45571c4d22e9b6ad5e8a4b1628cfe447ae8abab918e

Malware Signature:

- Trojan.Siggen6.13363
- Trojan.MulDrop4.63862
- Trojan.Vilsel.pvi.qdpa
- Win32/Worm.Pykspa.HwgAEYcA
- Worm.Win32.Agent.A
- Win32/Backdoor.Zepfod.HwgAEpsA
- Win32/Worm.Pykspa.HwgAt94A
- Trojan.Win32.Vilsel.bqgox
- Trojan.Vilsel.ofn.yyjy
- Gene.Win.Harmlet.11819-0
- Trojan.Kypes.18
- Trojan.Vilsel.ofn.foml
- Suspicious:W32.AutoRun.Agent.TG.spvj.mg
- Trojan.Win32.KillAV.X
- Win32/Worm.Pykspa.HwgABYcC
- Win32/Worm.Pykspa.HwgAAAoC
- Trojan.Win32.KillAV.Y

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

- Trojan.MulDrop4.60762
- Win32/Worm.Pykspa.HwgAAGQC
- Win32/Worm.Pykspa.HwgA9r0A
- Win.Malware.Pykspa-6747516-0
- Win32/Worm.Pykspa.HwgA93EA
- Trojan.AntiAV.pin.obkj
- Trojan/Blocker.lhz
- Trojan.MulDrop.46689
- Trojan.Win32.Agent.ctkmgw
- Trojan.Win32.Zepfod.bdqfn
- Trojan.AntiAV.enq.kbqv
- Trojan.AntiAV.epf.ljtr
- Trojan.Win32.Drop.ihult
- Virus.Win32.Nimnul.lse3
- HEUR/QVM08.0.001D.Malware.Gen
- Trojan.Vilsel.ofm.aerg
- Win.Trojan.Zepfod-6828577-0
- Backdoor.Zepfod.a.shyx
- Trojan.Vilsel.moz.muux
- Trojan Agent
- Trojan.Vilsel.ofm.gnny
- Trojan.Chydo.clr.jkff
- Win32/Worm.Pykspa.HwgAAb0C
- Win32/Worm.Pykspa.HwgA7pYA
- Trojan.Chydo.ckl.qkrx
- Gene.Win.Harmlet.5241-0
- Win.Trojan.Zepfod-10029379-0
- Trojan.Chydo.clr.xdfl
- Win32/Worm.Pykspa.HwgAEpsA
- Trojan.Vilsel.ss.iwhb
- HEUR/QVM08.0.EF3D.Malware.Gen
- Worm.Win32.Pykse.A
- Trojan/Vilsel.bgc

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