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 "M0yv"
Numéro de Référence	59522212/25
Date de Publication	22 Décembre 2025
Risque	Critique
Impact	Critique

Le maCERT a détecté une activité malveillante liée au malware "M0yv". "M0yv" est un malware de type virus infecteur de fichiers ciblant les fichiers exécutables Windows au format PE (Portable Executable). Il se distingue par sa capacité à s'infiltrer directement dans des programmes légitimes sans en perturber immédiatement le fonctionnement, ce qui complique sa détection par les solutions de sécurité traditionnelles.

Lorsqu'un fichier infecté est exécuté, "M0yv" charge son propre code en mémoire, puis procède à l'infection d'autres exécutables présents sur la machine compromise ou accessibles via le réseau. Ce mécanisme permet au malware de se propager efficacement, notamment au sein des réseaux internes, favorisant une propagation latérale rapide.

Au-delà de son rôle de virus, "M0yv" peut également agir comme un dropper et un RAT (Remote Access Trojan). Il est ainsi capable d'ouvrir une porte dérobée, offrant à un attaquant un accès distant au système infecté. Grâce à sa structure modulaire, le malware peut injecter des payloads supplémentaires telles que des keyloggers ou des outils de vol d'informations (infostealers), étendant considérablement son impact.

L'accès initial se fait généralement par des campagnes de phishing, des téléchargements malveillants ou l'exploitation de réseaux déjà compromis. Une fois exécuté, "M0yv"

analyse le système à la recherche d'autres fichiers exécutables à infecter, assurant ainsi sa persistance et sa dissémination.

Les conséquences d'une infection par "M0yv" peuvent être graves. Sa capacité à se propager sur l'ensemble d'un réseau peut entraîner des interruptions d'activité significatives. De plus, le malware peut servir de plateforme pour des attaques secondaires, notamment le déploiement de ransomwares, exposant les organisations à des pertes financières importantes. Enfin, la compromission des systèmes peut conduire à l'exfiltration de données sensibles, facilitant le vol d'identité, la fuite d'informations confidentielles ou des activités d'espionnage industriel.

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 botnet.

Actions recommandées :

- Déployer et maintenir à jour des solutions antivirus reconnues capables de détecter les infections de type file-infector.
- Isoler immédiatement tout système suspect afin de bloquer la propagation latérale.
- Effectuer des analyses complètes et approfondies des systèmes et du réseau.
- Mettre en place des sauvegardes régulières hors ligne ou dans le cloud sécurisé pour garantir une restauration rapide des données.
- Sensibiliser les utilisateurs aux bonnes pratiques de cybersécurité :
    - Prudence face aux pièces jointes et liens inconnus,
    - Téléchargement uniquement depuis des sources fiables,
    - Signalement rapide des comportements anormaux.

Indicateurs de compromission (IOCs):

IP :

- 5.79.71.225
- 44.244.22.128

- 50.16.27.236
- 3.229.117.57
- 176.100.243.135

Domains :

- http://pywolwnvd.biz/uuep
- att-106696.weeblysite.com
- att-102856.weeblysite.com
- att-support-100433-104385.square.site
- att-105221.weeblysite.com
- att-service-106541-103143.weeblysite.com
- att-101145-105177.weeblysite.com
- att-yahoo-mail-netmailcurrentlynetworkfix.square.site
- att-102160.weeblysite.com
- lpuegx.biz
- http://pywolwnvd.biz/axbsmawbla
- http://cvgrf.biz/kqpcfsxvxw
- http://npukfztj.biz/ahsbuipdgcyx
- http://knjghuig.biz/cqrjy

Hashs :

- 03428fe5c6161e6f512514d5f1827baa24617611fd068d98e0a8be94fc8030bc
- 09e46d987078b47591635650daeda7b8c4b6d5c3fec95d4373ae044007cb819d
- 0b3ad575168e0457905f19bb5304a8ea8cce461d7b1ebd0964d1171374271e47
- 0ea246c52245f5dd919aead5707821080a13b70af25218973a14f373a4691ec3
- 1273e390eab2f69aa5ed380f296a7cd6c8ff01142367fe5dd76eae5f515947e2
- 222a73ccace7821334a969f5837f9d179c6f0259fe9791b61d857f036b456fee
- 2a60ca525c89948993b31e2e086a88455e71363863cfc7f835a47c1b657ea4a5
- 301dc94eb5d63a0fcd4a53c6b378d5d20ae42d0e56e0a5ab584f0baa59b5c8d6
- 38f9926ddf5c8c04566dafb0da2bdba633cf6578f3de13d1cf9c6e7502d54345
- 39c3b1276f2519a918613c7c33662a21ed9453482d40692b872b36c40933ffe3
- 3ca1c11c2d4173581e8007b955c912dd1d6abdb1bafe03924aca8cba437df745

- 434100ebc74ef000ce28edc1b388174cc57a7a708a92899e0c18fa6af946cb83
- 452d7f2afb6fbb3afa307419983194bd68e9a577fb47a02f6ba36c881f13c10d
- 463a99c4d82f346dd9cb1236df6c6acd9dc5f5df50467848efa167b59c635120
- 47982e52404153480451980cf1589b7416f031afcf5bf0f23b247cf54273bf1b
- 4aa2ea3cc55b48f3f6e54c75d383592a6fd4fa449908adbc019c3fb676dd5285
- 51bde105a641629948c300d04aecece518f2e96913c48463dcc508a026768120
- 5201e83114e993d01d950075620061d04d15acc5dccd2693ae7242a229b6b038
- 593d89afb5fddfe947207dc69f93816c665e480ecd2a78c9eaab108b9799691e
- 5a1e020c5c5ad435e9bb8cd1d76d10a88f9312f2622ddcaf4b4b559e37e8a992
- 5ae86c1b231a95b8eaa105ca9214589dea3d22efd601cd2018f7a5e6c474ddca
- 5f0d6bb3445ed0c410b2dd8874cf7fc7b1c4e06cc2e620790eb782f2c339c796
- 6ae76ecc053bd375adaf3e8ac072a82a
- 76efda6c81b51a09ca94c5aa645cf08d2bf876cc0ead4855ba57582bb32bcb2d
- 77fff1c59aace50f9bbb9184b1086cccb57df0cb5d3b10589a9b6b91283aa719
- 8ddfda62decd6de3185b1ec3bebe067a20a124a39f8483afa9bbc47b3f3d0c09
- 95075ecbdcd1ff294433ceeb45d7bb3d24e94857620dba98b5f6b08250cff811
- 9733092223c428fc0e44a90b01c7f77a97bb1205def8be1224ac68969182638e
- 99ad2350970b462018fed5a0912ba5bd73976a4058d7f96596f08851b823b025
- a36f4ee96ff62eee2a503838850d7dce90aabc36a704b742b6814f187618f3c1
- abb727416ce1cbf43185b9f0e01ea2d5dedb7dbc1d8d262fc382219ca4120e2a
- b10016211f6c0ad5738fa25a9c742291a7a92ed2c0f383ef30c356fff04f6bcc
- b43b109b61b1ca610d50e10a4ede95e54263a792a2a9ef8b96312bda0c416994
- b4b9d129ba597a083715e91c4c65d3a3a2d8fe80fbbc8839e0943a14055b2f6f
- bdcf8029051a0fe59cfadc08d3d012f79cc7ff2d
- c15bc74ee0c5a67c433ba8ca227c8fce74dfebf5e8abbe4d77b573309e259d9c
- c259979b6ab2cd0383f1f92ebc968db0fdbcc4a5238bead0e420b3421aee7724
- c4e8d830f31b61906d6c839ccb66c14838a0c58c90a14116d721a2cba2ba57ae
- c680cab3467b411214b7515a76da90610a3748c87ae884f27df878f8f5016479
- cc1f3c519bd416933caf5b073a01a673c9ae9d3ff6dcb34a5525526dceaa6245
- cc6318bd74051fc086d861b2ae5aafd66dee62a2b5cf8069041d96582df2e7e6
- df3a33660b34cdc059d867704dc9d3f49799ba431243b0db3e66843fd584ceb3

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

- dff12e1840c3265f14378662e2dbd2e1cad4aa31027ff29056a42964adda27c6
- ec01b76e956bceeec02a2bf5004ec837639562729f5ea4fd61f2f9f1ea0e803f
- ed0b66043d5223c79f2206468bd12d369d933e0db2234508702ce7402579835f
- f2392e04e5ffb9bcee95ce763a7686322a9abd7210af28ef3f653402515a6013
- f7883b978863cc7d5d5b53d3a4192936
- f8f75d4ece048062d8a86f3a60a7f4c2e44e99a0
- f9d78174d15fee469beb09ad3a07fb4a87333cd00477b8dc934568edcb959738
- fbf1e50a03434dc9800dbd8f24a9e2cc5e623138c487b69560b0251b58f04ad9
- fced488bab6f8793e1ca19858cf208ebc5c2b0ee18087489a2a35eb7fee803af
- fdc56663b329b0db2769462b363f4658e4087030934f8858da8119f7f3b44c3d
- ff3bcc4bc70f9e6724fcc0fb36c4f57cc5956136850bd39c9581413f7c4688a9

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