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 " PseudoManuscrypt "
Numéro de Référence	59592412/25
Date de Publication	24 Décembre 2025
Risque	Critique
Impact	Critique

"PseudoManuscrypt" est un logiciel espion malveillant utilisé dans le cadre d'une campagne d'infection à grande échelle. Le malware est majoritairement diffusé via de faux installateurs de logiciels, souvent présentés comme des versions piratées des programmes populaires et distribués via des réseaux de diffusion malveillants.

Afin d'assurer sa persistance, "PseudoManuscrypt" stocke du code chiffré dans le registre Windows et crée un service système configuré pour s'exécuter automatiquement au démarrage du système. Une fois installé, "PseudoManuscrypt" fonctionne comme un spyware distant, offrant aux attaquants des capacités étendues de surveillance. Il est capable d'effectuer du keylogging, de voler le contenu du presse-papier, de collecter des identifiants sensibles (notamment des credentials VPN), ainsi que des journaux système et des informations détaillées sur l'environnement de la machine infectée. Certaines variantes incluent également des fonctionnalités de capture d'écran, de vol de données issues d'applications de messagerie, de désactivation de logiciels de sécurité et de modification du fichier hosts.

Les données collectées sont ensuite exfiltrées vers des serveurs de commande et de contrôle (C2), principalement via le protocole KCP, un mécanisme de communication qui permet aux opérateurs de maintenir un contrôle à distance de la machine compromise.

L’ensemble de ces capacités fait de "PseudoManuscrypt" une menace sérieuse, adaptée à l’espionnage massif et à la compromission durable des systèmes infectés.

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):

IP :

- 107.172.13.162
- 193.203.203.82
- 51.15.61.114
- 45.9.20.13
- 172.67.166.96
- 104.21.4.208
- 2.18.121.22
- 51.89.23.91
- 104.26.2.46
- 172.67.74.161
- 35.204.181.10
- 3.254.94.185
- 104.18.94.41
- 172.67.19.24
- 140.82.121.4
- 3.33.130.190
- 104.234.118.34
- 123.140.161.243
- 144.76.136.153
- 188.114.96.0

Domains :

- abgtt.com
- ggg-cl.biz

- wetuspost.xyz
- niemannbest.me
- buy-fantasy-football.com.sg
- topniemannpickshop.cc
- mas.to
- all-mobile-pa1ments.com.mx
- staticimg.youtuuee.com
- 360devtracking.com
- a.dowgmua.com
- billpaycanada.online
- connectini.net
- 9twelve-srvcs.zapto.org
- b.dowgmub.com
- api.ipify.org
- www.account-next.com
- toa.mygametoa.com
- tob.mygametob.com
- google.diragame.com
- jom.diregame.live
- email.yg9.me
- google.vrthcobj.com
- diragame.com
- api.2ip.ua
- bukubuka1.net
- bulimu55t.net
- golilopaster.org
- hujukui3.net
- hutnilior.net
- newzelannd66.org
- novanosa5org.org
- potunulit.org

- uaery.top
- j.ffbbjjkk.com

File paths:

- %WinDir%\System32\[0-Z]{10}.tmp e.g. I59RFRLY9J.tmp
- %TEMP%\[0-Z]{10}.tmp e.g. I59RFRLY9J.tmp
- %WinDir%\System32\9cda11af69ab0a2b6a9167f7131e7b93.key

Hashs :

- 77bac9c2a0b042b29d7b7e8553d09d0dcc3fd0977ff2a10402a6d799303a5138
- 59a07e2c448afe8d96a5f79968d7ede52d409d9d36d7a77eaa190c5c70cf3f32
- bbd550a356ad847fbec4080976e7f7d72b3d431d923df772b65880b7a5cc7254
- a759dfe145751752776c392ad2f5dffd1fa7f4e77e3f5daeeb2258baa2271262
- d3e1e0659ff9d7843f91e722d6e94cff0cbf891ab115b7dc23bde7c52a9ead09
- 6aea187ca91ea68222b4e650e2b4baa46ba11252f74763a2d2edec2924a98f10
- 66c50293737f9b121c162073ef894bff11906e8fad9b3c4d0f77f0e49f586d7e
- 7db1175e55e2bc864c8e8f0915b5f4167cb0a49a87a751b3fa429be6dc4a8896
- 1d636ae88bab15613db7d92a33c0bd9d107270d68991faa01c6de1fa06364d92
- 32e60467041b40146d87fc1c8c734f60f7e3763820e0c2a852a801c8afd1c7ab
- eaf978fd469c4acc54a1b4cdaa4298c04b385b0cce10215f96a737b26a27fd30
- c33ecac87bf07fc75b6768b76622daac389e05ef718c457e0393238d646bb130
- ad716b9b395d65dca7a31117215c2adedf392162eab7beee500f8061db4785c0
- 1868f0807fb9ad9be1629bc214b755ede9937036622ef31ae877617aba840080
- 4eeeb2fb37c066baa19b53a02d93d82c40fbedbda7610720b8733c6c1aab555b
- c14dfbc33876ec82c3705cc8cedad7dda10646b4fd9d12c468d786187422bee7
- 343b71456cdcc0f09baf79a2b0f5befe7043f329899f205699ac3ca2424c8282
- d75bdc11107b27e7602f31a93896dbc589dbd313cbb5e76a00d695208218e92a
- 5d0a0c2194f2761cadcc2944ba1397950f120c1e691a8eacd185eba576a36f0d
- 54151922b3a7a1f16e1b10356da10b8293b6ca897fed9d48ffeb3d2eae2685cd
- b261a7995c16bc433bd714b2830e519c40c3b8bd60ad6a6239ce27e672dc6650
- 6dbddba630ea7382f81f01ede022be530fae7f1ba7a369c7808fd67a2457523c

- ea40d05c81d27ac61843cabdbaf45a81347ae058d1229300313a17b6143f35e3
- 0a5d832f3594465625f855e63075362cf73ef323fc32964e73327aa6a1030584
- 4ca6df75008045a45e441869a4389b4ef620df9f89cd5f05fd329d0f9987c822
- b9a81253d85a5da410ec8cf345c2444ec09739e5c9842e4031195209bacbf8ab
- 5b0708551a5c3cf9932c8aea5e890e3f2abe7b7b5911cefebc6155d20692e365
- 9a8d4f6c8f24d96d32ef8974ba8c96cc02d4fca7d46c3d1edf7e70d6027805f5
- 9d6f720f4d9bd455371b863ce479c490ebb437ff53c1635fe7befd5eff30af10
- 248cc9a72ef0f0740bd05bf10b56345530e820a2179ccf295722cd85667ee8c1
- 2aa80995de6dce2c7590be4937c9e53b8f56a515f6699c3818c19000cd0a6bb0
- 867a7eaf299f034c5acc0ba7bd662d7336a3c443a51de629eb07392a0173f5b1
- 0f8957164a9652a11ebdc564de062475ab11f8b4ff0cf7394a317f8460ca059f
- 1600297e9fc5e9d1fd05e5cfb3d2650ad4d5d2a0767803076355bddc6dae8f57
- 0763a57785eb147b7b22f433f07ea905f27ac6d44bf0f041f235199065da1d48
- 9b3bf352cba2cd6fd814ff336a0bb2d2192d07b4404f22d99192ec17012ebae4
- 807badc86df04d85f8c977ac586daab5101072d145d2e654f4f80c1d1b04f214
- 4b8e47b3073b1193b5cd0bc2c12016754683a09213d1299415ec40088b4a9290
- ccf4b97d104da5adad77300a8af26faf23868c86b0c273d644112b3d62a51ddc
- 721c6344039504a039421662f0c681147aa140f3ee5598ce17491ec60cd21dab
- 2658e2d285ffb7dbc4d084728bcb65a537fefe900eeb07a10b42f3c61291ce2c
- b70c3586d51a5d1b230051cc0a004ea1340f837066ecc6bc13bc88c11c88add0
- 77a7949f1c2511971c674037e762400557453371346fc8ea1cc04e0d8a67e968
- e7bded553dd053da75e9c1247a24b16344028de8c8100324b8f6852daf5078c4
- b266486b81e48f59ef21b02c6151f26fe2aa77d0e1cce73718342a4e0e703cc7
- 99c1e9b26ff369764907dd0576d3ac4d9aa4db2f8a85fea23a6dd22ff6df1922
- e6a503c99e5afadde39a9927346470a6476458682ed8f536c95d79feb3896f90
- ea00e7aba317832fe7ee630e343d633389da5e1c1b08b4c1e41e77d2c80e242a
- 0452d0d3b5f5899e4f16810c4cfd5ecdd572222640f7383f7a1c32cdcdc5abf7
- a16e2ada8d8b81b0204ed70a8a32ce2c602f145b3af841d7e6c8b6ecc908126e
- c33623c100b142d0e571d6d8a27daf50da9f31801b85711581db01b267c14368
- 0471d54ab6711ddd815b40600aaf220d4ae06fad64c5e2d026885c6a56354bc7
- 21c58e9daa884fe0792c045ef5dcd797c14541f0445153d58a91c3e82c233cba

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

- 7986eafbcfa7145edadcbc2b9d82e9f07985ec73154e8b2123cb1eac0c6688c1
- 6304025b1257897362538a402ecb3fc47af94868332ff843d5f2075a9d58d81e
- b95d3f837860a9458844193b1eb148f16865728200f62c2671ebf37644f57dff
- cebf4c9af84506f3b683d5d4867b739244b6ba595772d583b3455781c4d91b74
- da374bf0e3e22b934b4f6d0e355887e836a3ddac2a1ded8a186559de69894289
- e2ffb8aeeb869fbb3de97b95b0c5c9cf2234d85612ba111115a938c89e4d94f6

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