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 Vidar « Update »
Numéro de Référence	60690402/26
Date de Publication	04 Février 2026
Risque	Critique
Impact	Critique

Vidar est un malware de type infostealer conçu pour exfiltrer des données sensibles, notamment des identifiants (bancaires, connexion…) ainsi que des informations liées à la navigation des victimes. Il se distingue par son mode de communication avec son serveur de commande et de contrôle (C2), dont l'adresse est obtenue de manière indirecte via des plate-formes légitimes ou des réseaux sociaux tels que Telegram ou Steam. Ce malware a fait l'objet d'une note de sécurité publiée par le maCERT/DGSSI sous la référence 40610203/23.

Étant donné que ce malware est très actif à l'échelle mondiale, et particulièrement présent en Afrique du Nord, le maCERT a procédé à une mise à jour des indicateurs de compromission (IOC) afin d'améliorer la détection des nouvelles mutations et variantes de Vidar.

Indicateurs de compromission (IOCs):

IP :

95.217.16.127	77.42.48.194	159.69.3.93	37.27.21.37	193.233.198.76
157.90.148.112	65.109.242.126	95.217.25.219	77.42.83.33	5.75.217.179
116.203.6.107	77.42.49.41	78.46.234.189	77.42.42.202	95.216.180.148
116.203.6.107	77.42.48.196	84.234.29.122	135.181.14.71	116.203.8.88

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

138.226.237.24	77.42.49.169	77.42.48.195	159.69.25.30	91.244.71.42
193.221.201.197	77.42.48.199	37.27.63.113	95.217.24.39	5.75.222.189
46.62.168.52	138.226.236.178	138.226.236.224	5.75.216.229	138.226.237.75
135.181.14.65	95.216.181.234	138.226.237.12	95.217.242.12	65.108.121.254
95.217.27.206	77.42.49.175	138.226.236.2	94.141.122.199	77.42.82.203
138.226.237.167	95.217.25.135	94.141.122.173	95.216.178.83	185.112.59.194
37.27.92.232	138.226.236.233	77.42.49.168	77.42.49.39	49.13.36.101
135.181.14.66	95.85.230.160	45.136.49.229	194.87.77.26	116.203.123.136
95.85.230.162	89.125.48.8	192.177.26.143	77.42.48.197	95.217.28.115
141.11.164.188	77.42.48.192	91.184.243.129	95.217.245.163	95.217.246.140
77.42.48.198	78.47.190.106	5.75.220.143	95.217.27.5	49.13.33.221
95.217.245.117	77.42.49.170	49.13.35.111	135.181.14.67	49.13.51.73
77.42.49.172	138.226.236.53	135.181.14.69	138.226.237.77	77.42.49.174
138.226.236.14	138.226.236.252	95.217.241.93	77.42.49.171	65.109.242.146
95.217.29.133	65.109.187.78	95.217.243.117	94.103.1.193	65.109.242.146
94.141.122.203	95.217.240.165	192.177.26.249	138.226.237.105	85.192.63.15
77.42.49.40	185.112.59.195	95.217.243.215	138.226.236.182	49.13.36.49
77.42.49.173	77.42.48.193	135.181.14.70	91.99.131.54	138.226.236.164
138.226.236.164	213.165.74.206	95.216.180.153	45.84.1.88	103.125.190.248

Hash :

- 307ecca772115edacfffdf5b9c8ade78ca95fa005021ed86a7a17bce928e57f9
- 813d7404f015b94fa9b2e5966823a80c7df8e09c73e1967226b8e597d9808272
- 21a2a73efbb58e827757dd73c8224f875bded71ad82accd3581fa6502e894c97
- 631d063862424092569a127aa502dae1dddc6336bd1d0b78623e90be5b808810
- ab11f502c7432b22132e21229abd81196720eaad0c1b6a83f5371eea64f5be25
- 660da1824c143de666903c2b3983df605a3494a9ddaa7b65919e1263b095e343
- 5fef7a3e3534a2d5ea0edbbdb6cf639c9249c9e948f54e837f064431dee58d04
- 081d7b8be9bbc400d5598227399acfa7ec024acc6098742b1270330bb6c7fe50
- defc1bcc113f1ebd1ae086569126075d11a953a8f8be6cbc1caf81300c8dafdc
- a923e82009a0b929cfeaa99c6c73fd08ced463bdd69c2cc91ab00fe285e8fcbb
- 166195cb65782ad68d424cd92a05c3f3ab1fd413d37d156688dd2028fd7f6c87
- 4ed8567ea2048af98c1a36219e521df92a9fbba4e1229a3a7d850bd5b6682bbb
- 0c82c872b3a66cb680b2244ec6a8f8ff9c5dc4d49b67ec4e83994bad9deab5c2
- 10759f171472d621a113aff74591ff0f61c67bbbf32b50121c941b3ac026f840
- 9d413d9cb8d392df809b1990232b11c756e033835906941c20ba16d640f74fd0

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

- 2015f45ddbeb48b12498c7885a70820c16edf22f6b81325219f79b991294202c
- 7641c1234ea497a045129e5b1998a189d66abc85336d5b696c2769a58e8e9d7f
- 1ed5f85a3ba4f909241079be6eef79d5c0adb2081176c9f6b6cb8d43e74e7419
- eb31641a82f6df9ff00cec64d912b336b15deff08dd3c375a7ef74445719ac99
- 323023f093410b48ce3484b1145f5523183eeb25d3880c0fe527e51684d47b72
- ad848546ad8796f472e439e5aaeefa3bf114b27a471ea19ee893d1fce6ae0b0b
- 73703b4f00c42c9df1ae5cd8bed844cd892606117a59b105cea23f572bed9694
- 1475a3bb4ec2d699b19fcc965c7a133dd253fa1e7aa1aed1eb85604315f34882
- 84dd73a6745210692de384877251dec92bd1af255601327d1d5732e08a79f643
- e14e998a41b779eac31f6ccdcf5de297a079d67fdc55e790587400e25351ca15
- dd2bfe36d8908d2dcaeb41521e9eb0bdd9741162cd3819bcf5fc96f6b95a2f1e
- aee03d2d68c96f700260f5411ffc86c8b2c0a28016823fd2f09fa8190d8ee93b

Domain :

- https://t.me/litlebey
- https://steamcommunity.com/profiles/76561199472399815
- http://www.tiktok.com/@user6068972597711
- https://t.me/mantarlars
- hxxp://www.ultimate-guitar.com/u/smbfupkuhrgc1
- https://t.me/larsenup
- tiny.cc
- ip-api.com
- l3monrat.com
- notepadplusplus.site
- download-notepad-plus-plus.duckdns.org
- download-obsstudio.duckdns.org
- dowbload-notepadd.duckdns.org
- dowbload-notepad1.duckdns.org
- download-davinci.duckdns.org
- download-sqlite.duckdns.org
- download-davinci17.duckdns.org

- download-rufus.duckdns.org
- download-kritapaint.duckdns.org

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