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	« Lumma Stealer » Malware (Update)
Numéro de Référence	60911002/26
Date de Publication	10 Février 2026
Risque	Critique
Impact	Critique

LummaStealer est une famille de malware de type infostealer activement utilisée dans des campagnes à grande échelle, dont la propagation repose notamment sur des campagnes de phishing et des techniques d'ingénierie sociale. Il est principalement conçu pour collecter des informations sensibles sur les systèmes compromis, telles que des identifiants, des données de navigation, des portefeuilles de cryptomonnaies et d'autres informations confidentielles. Sa distribution s'appuie sur des droppers spécialisés, comme CountLoader, qui assurent l'infection initiale et le déploiement furtif du malware.

Ce malware, très actif à l'échelle mondiale et particulièrement présent en Afrique du Nord, a déjà fait l'objet d'une note de sécurité référencée par « n° 47320905/24 ». Dans ce contexte, le maCERT a procédé à une mise à jour des indicateurs de compromission (IOC) afin d'améliorer la détection des nouvelles mutations et variantes associées à LummaStealer.

Indicateurs de compromission (IOCs):

Hash :

- 0086fd1e22cb00c3d4082b57813f9dc4eb119da6cdf69285d07c58bde96d3a78
- 53b6d03df06aa6291e07f865a571cc69a32c8b05b538f9b103445bf3fc7f6407
- 26c256fe3377e5877c880a7b6e960bd3261b97080d2c3bf061d96d1d367ebfb8
- b22d9619b0ec298a06181f22008ef2ae9d2b71982fb171caa9eec80e22d59df2
- 9e7ae536e206ab841cfc4aee52cfd99eaf293ddf8b1a832b6e5f7b158907821a
- df210ae22dabca82ddb5c5fa569cf7383f6f52496ea077067ce1903fe0ecf43a
- f5e0444bff54c830d6ba041d8ef5ea88969d9a8c55eb56e521e71f6e1c4dd367
- a38711de86becce770cf135e1ce898cc805fac1eb66b57634f51da9225d06e9b

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

- 657e6262f72446c54a793adef2bff23971c7d4a5fd876616fb5831de34589656
- ae4a678995bc06afe6bdfff6fd07b8e2d2423e1cebb7c4d61d770880cbd32674
- 62133eedda392ea99db303cf9e893b339cece05ab880185230a45d6cb1f0c60f
- c18228e68a73567bbed21eb70f43fc363fe5264373c464a11aab5e73aea41256
- 5d064a2d1abba51d8340472e56850599cc9e519ca4fdd0c3f2831bc1658d634d
- 490f7acc0dff183f3e4ad5cb378967ca185972aec0cfdae363a42884500e9a2e
- 75336d07bd7dd7e99de625d314548d7d4a73b031784709655032fd16214047d4
- cf2966ce96e73a222097322ec962e81b42cf3c1f14af0b8c7e728ab669162efd
- 3071915771ee7c1c0daeb01ae44919678926fe354157b4e4e7db5e2b7e204d5e
- 2ff2fc4f2a0d09d2bd799b9c0ac63e6e583dbb07cfefc1498999f801539ee687
- 5a0a1324e1d34c61edb622767867019299cc86b036a623013745fd44ca670e22
- 385b377b07431f3c4497c4b8b5415fdce58abf9ab8c78931d56144fccdab9435
- c4af13b412f67e7a1818e76d163f5701d7c58ff6a0347004c570f882b7a061ba
- 36077a7c73cb97dc5f0c92e4b6e1771766c8739721bb3c8fee55683d2bcd0551
- 4e5cc8cb98584335400d00f0a0803c3e0202761f3fbe50bcab3858a80df255e1
- f2928bd0f20020d3e6f793e0d388f76bbe0eae430a4fad5abdd232412a352f8c
- 051604b65cd8f54ad438c24fa3220c943080f113a15075424b34f2d410030ac6
- 830c439720bf2ad811b102b1842c8ed42b2bb115547407e617c117f8aabe56f2
- 53bc9125ed216a0704e8ae3ea6f2966b30ba2d0b68037bcf98462a2c00ab1891
- 16876037c49ec1a61d9075b775c7ef271a22eb1ad156fcb7ba6c9ed41026c5fd
- d6e5b47c0235fc147206127f1f4e7b1acbdb680e31024a5650cb9da78cf31723
- ff3cfcd05ce33fbf35e2853c2d0edac5a0de099e6baf4ad2cfd1abccbc98e9b0
- e0840404856dacdfc5e22a7ba96bd5d54f5efa330c6ca82a0e1a2d37be356d22
- 278130ea5339ba07b75c9b8a8c9ea22c51dce0edddacafde195c65f928a8e1a3
- f0fac6b6cf2f51d8336981fab80df48d5050fa13596e9e746c99ef7689aa1b66
- 3ac9859d4561fcaf4b2eb109fb473d9c5659aa41a7aefe70b6ad8f468164603d
- 0e6dd2f45a78b0981e6e5d440830508d9da61292c71b46d121a1eed7220c0ce3
- 443556999ce1bb88ece9f11f0a2c1a3fd3ba601f261591aeaa6edf35e3e88766
- ebfafa3bbd0ff07f5d96b38ebb9e5faeec2f5fd05fe4c0bedf032b01f5d0c337
- 226fe5dd27a8de7fa9cbcd8b876235a8e3f5e0ef42712e5dd0a8f1ff5a4cb8d8
- 29452bc71d81b8e611a97fa38ade52ae3c808bbe920b6896c95a149c721667c4

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

- a5f838f5c752bd39f2a094af5c2d4cc8f62b7a2154b629e4802a85b847a3fd3b
- 5147a678aaaf1e396faae37d72d97b9450b3a1adf1a3517f6fadcd8c296549f7
- b42ec65282f43a7c6cfc464bd9389c3c3d3c2f23a74016a2a6d82ee98c4c3280
- 30fdbe09f9eed23e3716097c7052ff30e5a2b00025b9aec2d6ccfb3e9db511b9
- 8a69cb647f5890008aacb0c535914d32272b7f1731ca00df20d0be77efa60a7a

Domaines C2::

- lacevcnt.cyou
- carpoba.cyou
- tribadu.cyou
- dutchfj.cyou
- tasselg.cyou
- homuncloud.su
- underpt.cyou
- manufao.cyou
- cheship.cyou
- troyouc.cyou
- ebonizz.cyou
- dinglev.cyou
- broguenko.su
- scarfkn.cyou
- sponges.cyou
- swedisc.cyou
- oculusr.cyou
- inconsk.cyou
- molewyn.cyou
- whitepepper.su
- dreamlm.cyou
- enjoyag.cyou
- belloww.cyou
- marktwx.cyou
- eldesty.cyou
- genusgp.cyou
- limulit.cyou
- killnnk.cyou
- whooptm.cyou
- verbala.cyou
- pepperz.cyou
- capitaf.cyou
- ulmacea.cyou
- editorr.cyou
- thoughg.cyou
- theengn.cyou
- backsan.cyou
- judicis.cyou
- dameagm.cyou
- trainen.cyou
- saudiab.cyou

Malware Signature:

- Suspicious:Packed.Krap.ag.ohja.mg
- Win32/Backdoor.Simda.HxQBKDIA
- Trojan.Win32.Inject.lVIb
- Win32/Backdoor.Simda.HxQBNDgA
- HEUR/QVM20.1.3B3D.Malware.Gen
- Trojan.Win32.Badur.m8MH
- Trojan.Win32.Themida.4!c
- Win32/Trojan.Inject.HgAASScA
- HEUR/QVM20.1.2D96.Malware.Gen
- Trojan.Win32.LummaStealer
- HEUR/QVM20.1.2F61.Malware.Gen
- Win.Virus.Neshta-7101689-0
- Win32/Backdoor.Simda.HxQBL4sA
- Trojan.Win32.InstallMonster.exjplz
- HEUR/QVM20.1.FA51.Malware.Gen
- Trojan.InstallMonster.2560
- Trojan.Packed.20771
- Win32/Trojan.Generic.HxMBGDkA
- Win32/Backdoor.Simda.HxQBD2kA
- Trojan.Win32.Inject.ewmwty
- Win32/Backdoor.Simda.HxQB49EA
- Win32/Backdoor.Simda.HxQB9tkA
- Trojan.Inject.ahycf.vkne
- Gene.Win.Harmlet.1333-39
- Trojan.InstallMonster.2517
- Win32/Backdoor.Simda.HxQBfqkA
- Gene.Win.Harmlet.613-0
- Win32/Backdoor.Simda.HxQBHXkA
- win/malicious
- HEUR/QVM20.1.2B89.Malware.Gen
- Trojan.Win32.InstallMonster.4!c
- Malicious
- Win32/Backdoor.Simda.HxQBkAUA
- Win32/Backdoor.Simda.HxQBAlEC
- Trojan.Inject.aifbc.dxov
- Trojan.Inject.adln

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.Win32.InstallMonster.evrlju
- Backdoor.Win32.Shiz
- Trojan.Inject.alsh
- PUA.InstallMonstr.Up
- HEUR/QVM20.1.DE31.Malware.Gen
- Backdoor/Shiz.apd
- Win.Packed.Generic-9795615-0
- Trojan.Win32.Shiz.tsF1
- Trojan.DownLoader26.9861
- HEUR/QVM20.1.3516.Malware.Gen
- Win32/Backdoor.Simda.HxQBK4kA
- HEUR/QVM20.1.3AFE.Malware.Gen
- HEUR/QVM20.1.3339.Malware.Gen
- Trojan.Win32.Shiz.kncajv
- Trojan.Inject.admg

IP:

- 109.104.153.203
- 37.77.150.171

Référence :

Bulletin de sécurité maCERT Numéro de Référence 47320905/24 du 09 Mai 2024**.**

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