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 " StealC"
Numéro de Référence	60282301/26
Date de Publication	23 Janvier 2026
Risque	Critique
Impact	Critique

StealC est un malware de type info-stealer apparu en 2023, diffusé via un modèle de malware-as-a-service. Il cible principalement les systèmes Windows et a pour objectif le vol de données sensibles, en particulier celles stockées par les navigateurs web. Sa spécialité réside dans le vol de cookies de session, permettant aux attaquants de contourner l'authentification, y compris le MFA, et d'accéder directement aux comptes des victimes.

Le malware collecte également des identifiants, des informations système, des données liées aux portefeuilles de cryptomonnaies et peut agir comme downloader, en récupérant d'autres charges malveillantes. Son code est obfusqué et ses communications avec le serveur de commande et contrôle sont discrètes, ce qui complique sa détection.

StealC V2, apparu en 2025, marque une évolution notable. Cette version introduit un nouveau protocole C2 plus structuré et chiffré, ainsi qu'un support étendu des payloads, incluant des fichiers MSI et des scripts PowerShell. Elle s'accompagne d'un panneau de contrôle plus avancé, permettant un ciblage précis des victimes et des fonctionnalités supplémentaires comme la capture d'écran.

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.

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

Indicateurs de compromission (IOCs):

Hashs :

- 43c9efe2914b7613e36eb50512e1a4c0a5fdfcdd42bc9207fd235cffdca7a1d1
- 62571d78ec2b682c600689772860b56f2ddcf39faea4cffcc3db9e66acf865c7
- 8066b7569459b883d019e60b445516e7bc3878e06bc087a0469ae7ed503a5628
- e0251b228c16680ae4aa66c812969eeac49e47fabb992714687f3f413a1584e8
- d607111a93224dfdf0ab58a8529c6b4db88e7647bde13532ce23c81bf156ab04
- 961046a740359060c7963ebfe5f64443e4bb74efa589c8334a50aac00ae12005
- 7b91275ed2b10e99e589b8de6646717756544720864416b07f59024a5a509614
- 2ee1b24c13d898260160fd79dc60b443fba4d6ed7971479c08c817bd95038f71
- 630b82b7e4012a7fcdda4260d09507068bf30840d3f68279a5962666dc779cea
- b554667949dc3847c3f04642b6c7b8d24948b72d5d3f0ee4ac656aa34a3dc8ed
- 887e25373ff825154b7a6ed86a9cdcceed320d48039a50621da661e1356d6339
- 65ba3988d38f83b9ee1f31cafa5bd37dc6b72279f5618aac94d71a904efa0cac
- 6d97acf787fc0571e81d0c82c301f91005523246319a2b17eb9db765e754ad89
- 4e5cc8cb98584335400d00f0a0803c3e0202761f3fbe50bcab3858a80df255e1
- 700c02cd565612e925e01d055b7363b6a9677defcb496914c0957100ec2f8507
- 465da9a3f2f36ba40fdf1d7bc998171f470c43bfccb51aab6425dae0ae5c443e
- 2fcad226b17131da4274e1b9f8f31359bdd325c9568665f08fd1f6c5d06a23ce
- 0b586f16ba08538d8779a08b19004993f2bad1aa936ef2e75899c24133309357
- 24eee62bd862f60a36a4167243c972bb0a7b9537087e9da48b37c74039b03b3b
- a6f1351894fb6f5976c2783da33335b56a31921feb8380a6903de45088d255c6
- 3ded7bd3ffd671ab7dc7cd5779623fb650f0a0dbfd8bcfd305a0cff3ebff8b46
- 789f9c1df69d10ae09c7f5dfe66ab8bb542b909b3311e1362a0b8167b96ebfdf
- 9b5a5c4b0f2fbb96698f76bb460eaa61cd7d49ebb1323fb149b54988c80ed725
- 5f6293d390f112155b66b3e3e68f848c6200a6b5f4922f42a4fc53b46835787e
- ac768aed44d1fb0ea06f3c726806cc517f7566d4260686133a82063e911465f8
- 12b78f63fd3358c9cf5184a6a4af662cc7e9e8706a25c864e423827564186 55f
- 943ce8ed3c64064357b5f67ab798cb53df3ed5a5a42be5ab7d777c361dea5fc2
- 32ea0428ac0ec4157e97779a7e0bc872b120a3ae28234856828e4fe04b73801a
- 426f6769de44ebf2c3066cbe28a016eee69eef44ef6a60eaaa2691210bed748c
- c0a30be7bd1025d36ac3712fb3cfaa0aa027cd0951e06eb20d1de58c3f0248f2
- 769aac8954481363c5783e562bf8862698ade1f73be6d5e4c1add5887af1fd41
- 1819dd98ca99ff72ca4d734b189cd513c78ccb83b60acf0bd92c53143513d49d
- fab38fc0d5f4d14895c4c450be0f1a8dc74ee07bd950e93b865660b1d82a6ae8
- fe33c0f159c8d2f37c694215f63a95f55b498da024863b87f7f5601e0c6c42b9

IP :

- 209.38.69.155
- 217.156.66.49
- 144.124.251.175
- 45.93.20.198
- 107.189.20.142
- 141.98.6.181
- 77.105.161.133
- 198.251.89.171
- 77.110.114.11
- 147.45.60.45
- 172.86.66.132
- 196.251.107.23
- 138.124.108.212
- 45.83.28.99
- 178.16.54.175
- 77.110.102.149
- 77.110.102.154
- 77.42.83.71
- 138.226.237.196
- 173.214.162.172
- 91.214.78.60
- 91.212.150.246
- 91.244.70.130
- 104.164.55.54
- 193.233.112.44
- 91.208.162.22
- 159.198.75.187
- 213.176.72.194
- 116.202.213.222
- 91.92.240.18
- 5.182.86.73
- 62.164.177.35
- 213.176.73.149
- 45.93.20.34
- 138.124.89.194
- 196.251.107.104
- 138.124.79.35
- 146.103.104.108
- 91.107.87.85
- 94.183.183.156
- 194.164.34.182
- 163.5.112.94
- 85.209.129.159
- 91.92.240.190
- 64.188.91.237
- 5.8.18.106
- 69.5.189.119
- 65.87.7.251
- 45.93.20.64
- 103.101.85.56
- 45.93.20.61
- 89.110.69.65
- 204.13.232.123
- 198.251.84.61
- 193.233.198.199
- 81.19.131.77
- 23.94.252.171
- 91.92.243.147

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

Signature Malware :

- Win32/Trojan.Loader.HxQBZrkA
- Trojan.DownLoader49.24217
- Trojan-Spy.Win32.Agent
- Trojan.PWS.StealC.456
- Win64/Trojan.Loader.H8oA190A
- Trojan.Win64.Spy
- Trojan.Win64.Crypt
- Win64/Trojan.Loader.H8oA3tYA
- Win64/TrojanPSW.Generic.H8oAsH0A
- win/malicious
- Trojan-Dropper.Win32.Agent
- Win64/Trojan.Loader.H8oAY9kA
- Win64/Trojan.Loader.H8oAiGkA
- Win64/Trojan.Loader.H8oAgFwA
- Trojan.Win32.Stealc.i!c
- Win64/Trojan.Loader.H8oA2JEA
- Gene.Win.Harmlet.10611-0
- Trojan.Win32.Generic.4!c
- Trojan.Win32.StealC.tsZY
- Trojan.PWS.StealC.393
- Win32/Trojan.Loader.HxQB3x4A
- Win64/Trojan.Loader.H8oAYAkB
- Safe
- Gene.Win.Harmlet.4-15
- Win64/Trojan.Loader.H8oAr8kA
- Trojan.Win32.StealC.tt0r
- Win64/Trojan.Loader.H8oA2vsA
- Win.Malware.Msilperseus-9811767-0
- Trojan.Win32.Reflo.4!c
- Win64/Trojan.Loader.HgEATBkB
- Trojan.Win32.Cryptagent.4!c
- Win64/Trojan.Loader.H8oAttQA
- Malicious
- Trojan.Win32.Loader.i!c
- Win64/Trojan.Generic.H8oASTEA
- Win.Malware.Marte-10045369-0
- Trojan.Win64.Agent
- Win64/TrojanPSW.Generic.H8oAyAkB
- Win64/Trojan.Loader.H8oA3jEA
- Win.Malware.Phil-10045361-0
- Win64/Trojan.Loader.HggATBYB
- Trojan.Win32.Stealc.4!c
- Gene.Win.Harmlet.1638-573
- Win32/Trojan.Loader.HxQByAkB

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