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	RisePro Stealer
Numéro de Référence	61791003/26
Date de Publication	10 Mars 2026
Risque	Critique
Impact	Critique

" RisePro " est un malware de type « infostealer » conçu pour collecter des données sensibles sur les systèmes infectés. Il vole notamment des identifiants, des informations financières et d'autres données confidentielles, puis les transmet aux serveurs contrôlés par les attaquants.

Ce malware cible principalement Windows et se propage souvent via phishing, téléchargements malveillants ou logiciels piratés. Une fois installé, il peut utiliser des techniques comme l'injection de processus pour éviter la détection et exfiltrer les données volées vers une infrastructure de commande et contrôle.

" RisePro " est fréquemment proposé sous forme de Malware-as-a-Service sur des forums clandestins, ce qui permet à différents cybercriminels de l'utiliser dans leurs campagnes d'attaque.

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):

Hashs :

- 000aea032ebf3dc8f4c1d461f6952e17cfc7cf26b03684cfffca4a433272a8a6
- 17afa3442e08b3cc2046f4dfde32f42516d0113d9449e0234424921f792e005a

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

- 1aea8173dccb016cc71d481353659328be2531316d76e3106a21a523306cd3e1
- 1fea6b7eff1a51f2beacf0cfae24c3c13f05dbdc706bc057a010a170a1a4d72d
- 22013778de2350e844beadb3c3cd9a57a31ac84ad4b40053fecd74999a0b7284
- 27d7d26b1ac998711a102740891006c29d3582623936c274c935dc55ad552884
- 30bc9626e4f7894d2021559919ab3136be2ccb444af4eed1f27e24e334b79c3f
- 32859f8a093bb8f2fec51f7c2ca2e23d54c9692dc091e3e7a01f33d78b2b6133
- 342a1bff72a3d0ce70980914152a4ad6a0ee98436bb54f08e0ea3b89cae4a71d
- 3c1160845edcd0773cbe829fcd31eea101dfc5750439e32c69b03fd1e63638eb
- 4507f93d3da896b0974b3b86d4f28229616a06fdc41254d23c7e45813846f7db
- 51d22dd0a8258395d7ab7b1d11e1ad847b0deafe14755d7b9b30dac032d350c1
- 57810a126a160b8660165d5c29a021abf3c5e3afcc0d0d34f5d3b6e131393edb
- 5b503890d01ba5682f55c8f4be872816a5779fa16c5740b6f88bdf2a98d77ce6
- 61df14737e49cc0df77e47cae135d1c40a8799b776211746b09a960268872256
- 61f2afc649d58e5f581e2eb06cd0fbe8a9e104aa62e6b6dab8edbff515640ac5
- 6292b1c6ec75fb42a901b28fe202a08adf39a76d1b01bff75ec7844356b5ed3d
- 6862a91cf983ab56a51c9dd188e86770b210da2c1b36d33d36ecd0db48e0aaf6
- 6fe32dd5209722767a77931e4ce85a832df280cc3a46ee5aa2421402d676445b
- 7426899934d65d48c0c55488aca8d89a7fdb05870667f57e97cdd7469791d0ce
- aebfcc549a0a0d258532f7c996ea42c7f56547ed391b0eba3859ff5cac744198
- b482f0259f3298bb09557a29b1bc6e78238491ddfed4a796ae1fa4c4303379b3
- bd3e210be56907a71f709debfed04444dc415188dc70f55035a2b21ff233f2aa
- c34533f233218569e959521ce8e6373a14b03f1e3b084fb7cf398a8a0bbbaf58
- c716ed2e2ee154d35cffc4230369bbf58da8b8b352897f616e53067d5860ba3c
- d3a10a526f44aa4d8d1e58fd5d71d9793c03c5046de4ca736a66abe8aa8a1d2b
- d7b87cc18e6ff4e87671612ffab1ade7933d6a5f0ab1553d1ca53a5951b7bc14
- e714413584046ccf9431cca84b16b4659a37fd1590badce790a8f3830ae6fe9f
- edb870b4444c3912f57c0c221856d53ca0ee55f2d7b5e004a89aab2b1727f60b
- f2ec401b3541c38eb1aa44c63434eff2d70a8348045aeb06861a06a6813dc451
- f855bcaa0c2dd25a6ef311f8bd035fb07482a7a5c8e3577258a91a6c6d4e5a76

IP :

193.233.132.51	194.169.175.128
194.169.175.220	194.49.94.152

Signatures Malware :

HEUR/QVM19.1.DCB9.Malware.Gen	Win.Malware.Doina-10010822-0
Trojan.PWS.RedLineNET.9	Trojan.PWS.Siggen3.31554

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

Win.Packed.Stealerc-10017072-0	Trojan.Win32.RisePro.1p!c
Trojan-Spy.Agent	Trojan.Win32.Autoit
Trojan.Win32.VirLock.4!c	Trojan.PWS.Stealer.37852
Trojan.MSIL.PSW	Trojan.PSW.RisePro.v
Riskware.Win32.Autoit.kfumrt	Gene.Win.Harmlet.1097-57
Win32/Trojan.Sdum.HxMB1EkA	Backdoor.Mokes.huc
Win32/TrojanDropper.Generic.HxMB1EkA	Trojan.Win32.Azorult
Win32/Heur.Generic.HxMB2Z4A	Trojan.Win32.RisePro.kboxxd
Trojan.Win32.Graftor.kfgajc	Trojan.Win32.Risepro
TrojanSpy.Stealer.ajzf	Win.Packer.pkr_ce1a-9980177-0
PUA.Protected.Enigma	Trojan.Win32.SmokeLoader.4!c
Virus.Generic.AI.1!c	win/malicious
Trojan.Win32.Graftor.kfgepv	Trojan.Win32.SmokeLoader
Trojan.PWS.RisePro.180	Win32/TrojanPSW.RisePro.HgIAUCYA
Trojan.PWS.Siggen3.33223	Win32/Ransom.Sarento.HxMB1EkA
Win32/Trojan.Generic.HgIAUCUA	Trojan.PSW.RisePro.x
Trojan.Win32.Generic.4!c	Trojan.Win32.Dacic.i!c
Trojan.PSW.RisePro.f	Malicious
Trojan.Win32.RisePro.jykilf	Win32/Trojan.Generic.HgIAUA0A
Gene.Win.Harmlet.3640-0	Virus.Win32.Virlock
Trojan.Win32.Enigma.i!c	HEUR/QVM10.1.D4FD.Malware.Gen
Win32/TrojanPSW.RisePro.HwMB0B4B	Trojan.Win32.Redline
Trojan.PWS.Stealer.36160	Trojan.PSW.MSIL.eyax
Win32/Trojan.Generic.HxMB0x0A	Trojan-PSW.RisePro
Win.Malware.Ursu-9794593-0	HEUR/QVM03.0.D99E.Malware.Gen
Win32/Trojan.Generic.HxMB0B4B	Win.Dropper.Tinba-9943147-2
Win32/TrojanPSW.RisePro.HgIAUCUA	TrojanSpy.Windigo.avc
Trojan.PWS.RedLineNET.6	Win.Malware.Zard-10015589-0
Gene.Win.Harmlet.86847-3963	Trojan.Win32.Mint.kedzcw
Trojan.PSW.MSIL.ewpt	Trojan.Win32.RisePro.kfgjqx
Win32/Trojan.Generic.HxMB1EkA	Win32/TrojanPSW.RisePro.HwMB1EkA
Trojan.PSW.RisePro.i	Win32/Trojan.Generic.HwoC0B4B
Trojan.StartPage1.62992	Win32/Trojan.Generic.HwoC1EkA
Trojan.Siggen21.33991	Trojan.Generic.hrxdp
Hacktool.Win32.Autoit.3!c	

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