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	Meduza Stealer malware
Numéro de Référence	45372912/23
Date de Publication	29 Décembre 2023
Risque	Critique
Impact	Critique

Medusa, un nouvel malware de vol d'informations lancé en juin, a gagné du terrain sur le dark web en raison de sa compatibilité accrue avec les plates-formes, sa fonctionnalité améliorée d'acquisition de cartes de crédit et de ses mécanismes avancés d'extraction de mots de passe.

Une nouvelle version (2.2) de ce malware a fait surface sur le dark web avec plusieurs nouvelles capacités. Sa capacité d'adaptabilité aux différents environnements lui permet d'extraire des informations sensibles de plusieurs navigateurs, portefeuilles de crypto-monnaies, de diverses applications de messagerie, de gestionnaires de mots de passe et de clients de messagerie. Il peut également s'emparer de fichiers de tout type et récolter des jetons Google, ce qui en fait un outil puissant pour les cybercriminels.

Les créateurs de ce malware proposent des services supplémentaires pour améliorer son efficacité, y compris des options de cryptage pour échapper à la détection et la location de serveurs pour l'infrastructure de commande et de contrôle.

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 cette menace.

Indicateurs de compromission (IOCs):

Hash :

- 005A687909B2CD3B0DC757E696AEDFD3
- 005A687909B2CD3B0DC757E696AEDFD3
- 021B649CE9D11E2CA9C67761953B1408
- 021B649CE9D11E2CA9C67761953B1408
- 02FA600EB8A92D7CE676F87269365CA0
- 02FA600EB8A92D7CE676F87269365CA0
- 05FC2D25B0B1AF9EA058F9B8DB3D5156
- 05FC2D25B0B1AF9EA058F9B8DB3D5156
- 0BB345C489B1D09A276D8AE1409FE28F
- 0BB345C489B1D09A276D8AE1409FE28F
- 14DC11E9386E2AEB9005DC2906F27DD1
- 14DC11E9386E2AEB9005DC2906F27DD1
- 244F76846B82C315F96A6A70BBD4C7DC
- 244F76846B82C315F96A6A70BBD4C7DC
- 2AAA6F1BE965EB98DE80E55286525FF6
- 2AAA6F1BE965EB98DE80E55286525FF6
- 3894A29E43D8847778F0FBB81BB479B9
- 3894A29E43D8847778F0FBB81BB479B9
- 39A083EB4D82950E58CEF105A3C6A9D4
- 39A083EB4D82950E58CEF105A3C6A9D4
- 54BBEBBFEB771DD609FF329099704A6A
- 54BBEBBFEB771DD609FF329099704A6A
- 557BDA3A9CD30126257AE2733DC51738
- 557BDA3A9CD30126257AE2733DC51738
- 5C1E871A99108B68C90F6ADBAC5B190F
- 5C1E871A99108B68C90F6ADBAC5B190F
- 5D9E2C18B4A261519E121754CD682B25
- 6174A343DD4C9A7D4AE7802B3EEA3134

- 6174A343DD4C9A7D4AE7802B3EEA3134
- 6FEF55E48E2392DBE72DF975EEAA5030
- 6FEF55E48E2392DBE72DF975EEAA5030
- 6FEF55E48E2392DBE72DF975EEAA5030
- 6FEF55E48E2392DBE72DF975EEAA5030
- 7264FD364F9DFF44E65DACF23348A29E
- 7264FD364F9DFF44E65DACF23348A29E
- 73070434952F46D1F37F9AB4BB99754F
- 73070434952F46D1F37F9AB4BB99754F
- 74EE6AC5ACEABA962B45D8295DB06823
- 74EE6AC5ACEABA962B45D8295DB06823
- 74EE6AC5ACEABA962B45D8295DB06823
- 74EE6AC5ACEABA962B45D8295DB06823
- 7B9A86691DAE4B913BA8B08F3F2ADFF8
- 7B9A86691DAE4B913BA8B08F3F2ADFF8
- 80136B6C96F8B23F8E938E38E01C58E6
- 80136B6C96F8B23F8E938E38E01C58E6
- 96F38055CAF432E112077AD70663ABD2
- 96F38055CAF432E112077AD70663ABD2
- A77B3786F7A53152D9AE31930D4C7FE4
- A77B3786F7A53152D9AE31930D4C7FE4
- ADC35BB330618A365685B5864E403007
- ADC35BB330618A365685B5864E403007
- B14DA82FD326FB23ADA0B4DF443CDA25
- B14DA82FD326FB23ADA0B4DF443CDA25
- BD1F946D08F9E4747E7DFDEC6823E4F0
- BD1F946D08F9E4747E7DFDEC6823E4F0
- C012CF6D414F3DFFFCE577623D91FD50
- C012CF6D414F3DFFFCE577623D91FD50
- C1824076854ACAC6858177062C1F5493
- C1824076854ACAC6858177062C1F5493

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

- C712A1B8A70FB7D0C7A714E12EFF0E38
- C712A1B8A70FB7D0C7A714E12EFF0E38
- D35ECA43E27128431B427578D7EC4404
- D35ECA43E27128431B427578D7EC4404
- D3A9C85A9155C22F5719D7953BA8F8D6
- D3A9C85A9155C22F5719D7953BA8F8D6
- D8625B338B13C0A1703AE2CD0059540F
- D8625B338B13C0A1703AE2CD0059540F
- DBC8C6622A2E9BE15ADEA1C936340D9E
- DBC8C6622A2E9BE15ADEA1C936340D9E
- E22F9B945371079B09E4E1E562DFC071
- E22F9B945371079B09E4E1E562DFC071
- E7A2BB050F7EC5EC2BA405400170A27D
- E7A2BB050F7EC5EC2BA405400170A27D
- E7C085CD99652B734D208888C91BD249
- E7C085CD99652B734D208888C91BD249
- EA6562FF5BCCA7182EEBC6F4E83DECAA
- EB17C2089CE02C6C9A711DB92751D9E1
- EB17C2089CE02C6C9A711DB92751D9E1
- EB52C4A4BEF2367E721BBE13E89AACF5
- EB52C4A4BEF2367E721BBE13E89AACF5
- EBA71E82CB96780B4711BF898067BA81
- EBA71E82CB96780B4711BF898067BA81
- FA1DED1ED7C11438A9B0385B1E112850
- FA1DED1ED7C11438A9B0385B1E112850
- FA1DED1ED7C11438A9B0385B1E112850
- FA1DED1ED7C11438A9B0385B1E112850
- FBE3D766BC659B28244F5B401D497A1B
- FBE3D766BC659B28244F5B401D497A1B

Référence :

- https://securityaffairs.com/156598/malware/meduza-stealer-released-dark-web.html