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	Nouvelle compagne d'attaque par le malware « Vidar »
Numéro de Référence	40610203 /23
Date de Publication	02 Mars 2023
Risque	Critique
Impact	Critique

Vidar est un malware de vol d'informations écrit en C++ qui permet aux acteurs malveillants de collecter les éléments suivants à partir des machines compromises : détails du navigateur (cookies, URL de sites Web et noms d'utilisateur de comptes avec mots de passe), porte-feuilles de crypto-monnaies, données de paiement, fichiers et historique des sites Web.

Les caractéristiques du malware-as-a-service (MaaS) comprennent un stockage et un télé-chargement faciles des données récoltées, des notifications de mise à jour, des capacités d'étiquetage et des méthodes de tri personnalisées. Vidar est généralement distribué par le biais des mails spam ou des versions piratées de logiciels commerciaux, notamment Win-dows. Les serveurs de commande et de contrôle (C2) et les logiciels de ciblage de Vidar changent constamment, ce qui aide les attaquants à éviter la détection.

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):

IP :

- 179.43.162.94

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

- 94.131.99.185
- 45.87.153.50
- 194.87.31.146
- 185.143.223.136
- 65.109.131.183
- 185.149.120.9

Hash :

- 1e09d04c793205661d88d6993cb3e0ef5e5a37a8660f504c1d36b0d8562e63a2
- 77d6f1914af6caf909fa2a246fcec05f500f79dd56e5d0d466d55924695c702d
- 87f18bd70353e44aa74d3c2fda27a2ae5dd6e7d238c3d875f6240283bc909ba6

Domain :

- http://146.70.161.51/273d9c8034a95cb4.php
- http://162.0.238.10/752e382b4dcf5e3f.php
- http://666palm.com/bca98681abf8e1ab.php
- http://94.142.138.48/f9f76ae4bb7811d9.php
- http://176.124.192.200/bef7fb05c9ef6540.php
- http://777palm.com/bef7fb05c9ef6540.php
- http://185.5.248.95/api.php
- http://179.43.162.2/d8ab11e9f7bc9c13.php