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	SkullLocker Ransomware
Numéro de Référence	40610603/23
Date de Publication	06 Mars 2023
Risque	Critique
Impact	Critique

Une compagne d'attaque ciblant les systèmes basés sur les systèmes d'exploitation Windows a été observé menée par le ransomware « SkullLocker ».

SkullLocker est une nouvelle variante de la famille des ransomwares Chaos. Le ransomware se propage en utilisant différentes techniques telles que les courriels de spam et les faux sites de torrents. Ce type particulier de ransomware chiffre les fichiers et ajoute une extension ".skull" aux noms de fichiers. Après le processus de cryptage, le ransomware crée une note de rançon dans le fichier "read_it[.]txt". La note de rançon est rédigée en polonais et informe les victimes que leurs fichiers sont verrouillés par le ransomware et demande une rançon pour le décryptage.

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):

Hash :

- e7deceee97a09d539d81eb91f988ece5e2a2ff51
- f4b3ebe7a8076c8a2d0b687f531cd5775f1911d8b90d8660ed97c91d2bf73405

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

- bb5ca9d8de51734dbd14dc081c7c892d819cd14fafd7ccd62849d70f9e679369
- 62e53bc5aa5f2a70a54e328bff51505f
- f34d5f2d4577ed6d9ceec516c1f5a744

Filenames and Extensions:

- .skull
- okok[.]exe