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	«3AM » ransomware
Numéro de Référence	43851909/23
Date de Publication	19 Septembre 2023
Risque	Critique
Impact	Critique

Le ransomware 3AM est une nouvelle variante de logiciel malveillant qui a été découverte récemment. Il a été identifié pour la première fois lorsque des acteurs de la menace l'ont utilisé comme solution de repli après l'échec d'une tentative de déploiement du ransomware LockBit. Le ransomware 3AM chiffre exclusivement les fichiers qui répondent à des critères prédéfinis et ajoute l'extension ".threeamtime" aux noms de fichiers compromis. Il tente d'arrêter les services de sécurité et de sauvegarde avant de chiffrer les fichiers et de supprimer les originaux. Le logiciel malveillant tente également de supprimer les copies du Volume Shadow et laisse une note de rançon dans chaque dossier analysé, menaçant de vendre les données volées si la rançon n'est pas payée.

Le ransomware 3AM est un exécutable 64 bits écrit en Rust, ce qui en fait une toute nouvelle famille de logiciels malveillants. Il utilise diverses méthodes pour échapper aux mesures de sécurité et aux systèmes de sauvegarde, ce qui indique un certain niveau de sophistication de la part de ses créateurs. Le logiciel malveillant utilise des commandes de reconnaissance spécifiques telles que "whoami", "netstat", "quser" et "net share" après avoir exploité des systèmes à l'aide de Cobalt Strike, ce qui laisse supposer des activités post-exploitation pour un mouvement latéral.

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

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:

- 185.202.0.111
- 212.18.104.6
- 85.159.229.62

Hash :

- 320c539fdee1096e07c8e000b90605a9
- 4d64b85e83ef5ba016b3cadb95eb6d7e30791422
- 079b99f6601f0f6258f4220438de4e175eb4853649c2d34ada72cce6b1702e22
- 307a1217aac33c4b7a9cd923162439c19483e952c2ceb15aa82a98b46ff8942e
- 680677e14e50f526cced739890ed02fc01da275f9db59482d96b96fbc092d2f4
- 991ee9548b55e5c815cc877af970542312cff79b3ba01a04a469b645c5d880af
- ecbdb9cb442a2c712c6fb8aee0ae68758bc79fa064251bab53b62f9e7156febc

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