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	Abyss Locker Ransomware
Numéro de Référence	52501002/25
Date de Publication	10 Février 2025
Risque	Critique
Impact	Critique

« Abyss Locker » est une famille de rançongiciels détectée pour la première fois en juillet 2023, ciblant à la fois les systèmes Windows, Linux et les équipements réseau critiques, notamment les serveurs VMware ESXi. Dérivé du code source du ransomware « HelloKitty », il utilise la technique de la double extorsion, en volant des données sensibles avant de chiffrer les fichiers avec l'extension ".abyss" sur Windows, et ".crypt" sur Linux.

La technique utilisée pour la distribution de ce ransomware est souvent via des campagnes de phishing, incitant les victimes à télécharger des pièces jointes malveillantes ou à cliquer sur des liens infectés. Abyss Locker a été impliqué dans plusieurs attaques touchant des secteurs variés comme la santé, l'éducation et l'industrie.

Ce ransomware utilise une infrastructure comprenant un site sur le réseau TOR pour les négociations de rançons, reflétant un haut niveau de sophistication. Deux nouvelles versions ont été publiées début 2024, confirmant une activité de développement continue au sein de ce groupe malveillant.

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.

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

Indicateurs de compromission (IOCs):

Hashs :

- 362a16c5e86f13700bdf2d58f6c0ab26e289b6a5c10ad2769f3412ec0b2da711
- 2e42b9ded573e97c095e45dad0bdd2a2d6a0a99e4f7242695054217e2bba6829
- 0763e887924f6c7afad58e7675ecfe34ab615f4bd8f569759b1c33f0b6d08c64
- e6537d30d66727c5a306dc291f02ceb9d2b48bffe89dd5eff7aa2d22e28b6d7c
- b524773160f3cb3bfb96e7704ef31a986a179395d40a578edce8257862cafe5f
- 72310e31280b7e90ebc9a32cb33674060a3587663c0334daef76c2ae2cc2a462
- 9243bdcbe30fbd430a841a623e9e1bcc894e4fdc136d46e702a94dad4b10dfdc
- 1a31b8e23ccc7933c442d88523210c89cebd2c199d9ebb88b3d16eacbefe4120
- dee2af08e1f5bb89e7bad79fae5c39c71ff089083d65da1c03c7a4c051fabae0
- 25ce2fec4cd164a93dee5d00ab547ebe47a4b713cced567ab9aca4a7080afcb7
- 056220ff4204783d8cc8e596b3fc463a2e6b130db08ec923f17c9a78aa2032da
- 3fd080ef4cc5fbf8bf0e8736af00af973d5e41c105b4cd69