ROYAUME DU MAROC

ADMINISTRATION
DE LA DEFENSE NATIONALE

Direction Générale de la Sécurité des Systèmes d'Information

Centre de Veille de Détection et de Réaction aux Attaques Informatiques

المملكة المغربية

إدارة الدفاع الوطني

المديرية العامة لأمن نظم المعلومات

مركز اليقظة والرصد والتصدي للهجمات المعلوماتية

NOTE DE SECURITE

Titre	Campagne Ransomeware ciblant les serveurs MSSQL
Numéro de Référence	43590509/23
Date de publication	05 Septembre 2023

Des chercheurs en sécurité informatique annoncent l'indentification d'une campagne malicieuse par Ransomware ciblant les entités disposant de serveurs Microsoft SQL.

Le mode opératoire des attaquants consiste à accéder initialement aux systèmes d'information des victimes par une attaque de type « brute force » pour obtenir des identifiants du serveur Microsoft SQL.

Une fois l'accès est garanti, les attaquants utilisent plusieurs techniques et outils pour affaiblir les défenses de la victime, établir leur présence dans le système et accéder à d'autres hôtes du système d'information en utilisant des techniques de mouvements latéraux.

L'attaque s'achève enfin par le déploiement et l'exécution du ransomware « FreeWorld », une variante de « Mimic ransomware ».

Direction Générale de la Sécurité des Systèmes d'Information,
Centre de Veille de Détection et de Réaction aux Attaques Informatiques
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
هاتف: 47 21 57 37 05 – فاكس: 53 20 57 37 05
البريد الإلكتروني contact@macert.gov.ma

Recommandations

Le vecteur d'attaque initial consiste à une attaque « brute force » contre les identifiants du serveur Microsoft SQL. Il est donc recommandé de renforcer la sécurité de ce service par :

- Imposer un politique complexe de mot de passe
- Limiter l'exposition à un internet du service MSSQL
- Limiter l'utilisation de la procédure xp_cmdshell dans les environnements MSSQL
- Surveiller les dossiers les plus utilisés par les malware, spécialement "C:\Windows\Temp" utilisé dans cette campagne d'attaques
- Déployer des outils de journalisation pour les processus, comme « Sysmon » et « Powershell logging »

Références

Rapport de securonix :

- https://www.securonix.com/blog/securonix-threat-labs-security-advisory-threat-actors-target-mssql-servers-in-dbjammer-to-deliver-freeworld-ransomware/