



NOTE DE SECURITE

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

Des chercheurs en sécurité informatique annoncent l'identification 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 ».

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 une 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/>