Weaxor: Rebranded Mallox Ransomware with a Unique Payload Delivery Method

Shrutirupa Banerjiee
Seqrite, Pune, Maharashtra, India

Rayapati Lakshmi Prasanna Sai
Seqrite, Pune, Maharashtra, India

Niraj Lazarus Makasare
Seqrite, Pune, Maharashtra, India

Abstract:

The rise of Mallox ransomware in 2023 marked a surge in attacks on unsecured Microsoft SQL (MSSQL) servers, leveraging dictionary attacks to gain unauthorized access and deploy its payload. By late 2024, Weaxor ransomware emerged as a rebranded variant of Mallox, maintaining key similarities in its targeting strategies and executable structure while introducing a more sophisticated payload delivery mechanism. Unlike its predecessor, Weaxor employs multi-layered obfuscation in its initial-stage loaders and utilizes an advanced payload to deliver the final malware. Attackers compromise exposed or vulnerable MSSQL instances through weak credentials, known vulnerabilities, and unpatched systems, deploying obfuscated loaders that perform process injection and establish communication with a command-and-control (C2) server. The injected code acts as a Beacon, ultimately delivering Weaxor ransomware as the final payload. This paper dissects Weaxor's infection chain, evasion techniques, and advanced delivery methods, providing critical insights for cybersecurity professionals to detect and mitigate this evolving ransomware threat.