Severity

High

Analysis Summary

Hive ransomware, which was first observed in June 2021 and likely operates as an affiliate-based ransomware, employs a wide variety of tactics, techniques, and procedures (TTPs), creating significant challenges for defense and mitigation. Hive ransomware uses multiple mechanisms to compromise business networks, including phishing emails with malicious attachments to gain access and Remote Desktop Protocol (RDP) to move laterally once on the network. After compromising a victim network, Hive ransomware actors exfiltrate data and encrypt files on the network. The actors leave a ransom note in each affected directory within a victim's system, which provides instructions on how to purchase the decryption software. The ransom note also threatens to leak exfiltrated victim data on the Tor site, "HiveLeaks."

Impact

- Unauthorized Access
- Data Exfiltration
- File Encryption

Indicators of Compromise

MD5

- 036539c87a839b419424c8d535252185

SHA-256

- f4a39820dbff47fa1b68f83f575bc98ed33858b02341c5c0464a49be4e6c76d3

SHA-1

- cedb0c1dcb83aacd19a6bec04f7f1c4d875034c0

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.