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

IP

- 139[.]60[.]161[.]228
- 139[.]60[.]161[.]56
- 91[.]208[.]52[.]149
- 185[.]70[.]184[.]8

MD5

- 6c9ad4e67032301a61a9897377d9cff8
- 6a58b52b184715583cda792b56a0a1ed
- 4fdabe571b66ceec3448939bfb3ffcd1
- bb7c575e798ff5243b5014777253635d
- 5e1575c221f8826ce55ac2696cf1cf0b

SHA-256

- e81a8f8ad804c4d83869d7806a303ff04f31cce376c5df8aada2e9db2c1eeb98
- d0c1662ce239e4d288048c0e3324ec52962f6ddda77da0cb7af9c1d9c2f1e2eb
- 8b9c7d2554fe315199fae656448dc193accbec162d4afff3f204ce2346507a8a
- 572d88c419c6ae75aeb784ceab327d040cb589903d6285bbffa77338111af14b
- 047c2d5a6cf769c33e019c0b576aef702cae77f3418f0aeba0706467be5ba681

SHA-1

- 655979d56e874fbe7561bb1b6e512316c25cbb19
- 3477a173e2c1005a81d042802ab0f22cc12a4d55
- 763499b37aacd317e7d2f512872f9ed719aacae1
- 2146f04728fe93c393a74331b76799ea8fe0269f
- ecf794599c5a813f31f0468aecd5662c5029b5c4

Remediation

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