HC3: Alert

August 25, 2021 TLP: White Report: 202108261600

Indicators of Compromise Associated with Hive Ransomware

Executive Summary

The FBI shared indicators of compromise (IOCs) associated with the Hive ransomware, which they believe "likely operates as an affiliate-based ransomware." While Hive uses multiple methods to comprise victims' networks, the FBI highlighted "phishing emails with malicious attachments." Once a victim's network is compromised Hive provides "two to six days" for payment of the ransom by the victim. If the ransom is not paid, Hive leaks their victim's data to their Tor website, HiveLeaks.

Because Hive uses legitimate applications to further their compromise of a victim's network, "the FBI recommends removing any application not deemed necessary for day-to-day operations."

Report

FBI – Flash Alert (MU-000150-MW) Indicators of Compromise Associated with Hive Ransomware
https://www.ic3.gov/Media/News/2021/210825.pdf

Impact to HPH Sector

As recently as August 2021, Hive has victimized entities in the Healthcare and Public Health (HPH) Sector. Sector entities targeted by ransomware could have some or all of their data leaked if a ransom is not paid and experience disruptions to services provided to their patients and customers.

References

CISA - Alert (AA20-245A) Technical Approaches to Uncovering and Remediating Malicious Activity
https://us-cert.cisa.gov/ncas/alerts/aa20-245a

CISA - Additional Resources Related to the Prevention and Mitigation of Ransomware
https://www.stopransomware.gov

Contact Information

If you have any additional questions, please contact us at HC3@hhs.gov.