FINISHED INTELLIGENCE REPORTS

FBI Releases Indicators of Compromise Associated with Hive Ransomware

TLP:WHITE

Aug 26, 2021

The US Federal Bureau of Investigation (FBI) has released a FLASH advisory reporting technical details and indicators of compromise (IOCs) associated with the Hive ransomware group.

Hive ransomware, which was first observed in June 2021 and likely operates as 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.

Please see the attached FBI Flash for additional insight, technical details, and IOCs.

Report Source(s)	FBI

Release Date
Aug 26, 2021

Sources
AHA: FBI Alerts Organizations to New Ransomware Threat

Threat Indicator(s)

SHA256:
321d0c4f1bbb44c53cd02186107a18b7a44c840a9a5f0a78bdac06868136b72c

MD5:
04FB3AE7F05C8BC333125972BA907398
BEE9BA70F36FF250B31A6FDF7FA8AFEB
b5045d802394f4560280a7404af69263

URL(s):
hXXps://anonfiles[.]com
hXXp://hiveleakdbtnp76ulyhi52eag6c6tyc3xw7ez7iqy6wc34gd2nekazyd[.]onion
hXXps://ufile[.]io
hXXps://mega[.]nz

hXXps://send[.]exploit[.]in
hXXps://www[.]sendspace[.]com

Alert ID 6a09e83c

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags Hive Ransomware, FBI Flash, Ransomware, Remote Desktop Protocol (RDP)

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments Please email us at toc@h-isac.org

FBI The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office or the FBI's 24/7 Cyber Watch (CyWatch). Field office contacts may be identified at www.fbi.gov/contact-us/field. Contact CyWatch by telephone at 855-292-3937 or by email at CyWatch@fbi.gov.

Download Health-ISAC's Information Sharing App.

For more update and alerts, visit: **https://health-isac.cyware.com**