HC3: Alert

February 07, 2022 TLP: White Report: 202202071700

Indicators of Compromise Associated with LockBit 2.0 Ransomware and Additional Mitigations

Executive Summary

LockBit 2.0 operates as an affiliate-based Ransomware-as-a-Service (RaaS) and employs a wide variety of tactics, techniques, and procedures, creating significant challenges for defense and mitigation. The indicators of compromise (IOCs) and malware characteristics outlined in this Report were derived from field analysis and are current as of February 2022.

Report

Indicators of Compromise Associated with LockBit 2.0 Ransomware
https://www.ic3.gov/Media/News/2022/220204.pdf

Impact to HPH Sector

Although the LockBit 2.0 cybercrime gang claims to not attack healthcare organizations, all ransomware continues to act as a major cyber threat against the U.S. Healthcare and Public Health (HPH) Sector. It is extremely important to both know AND apply the information included in this FLASH.

Reducing your organization's attack surface to the greatest extent possible is the primary goal, and this FLASH provides several ways to do that. Notably:

- Utilize the included IOCs in your threat hunting and detection programs.
- Use multi-factor authentication and strong passwords.
- Establish a robust data backup program.
- Consider signing up for CISA's cyber hygiene services.

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office at http://www.fbi.gov/contact-us/field-offices.

References

Stop Ransomware
https://www.cisa.gov/stopransomware

CISA Ransomware Readiness Assessment (RRA)
https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr

Contact Information

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

We want to know how satisfied you are with our products. Your answers will be anonymous, and we will use the responses to improve all our future updates, features, and new products. Share Your Feedback