LEADERSHIP FOR IT SECURITY & PRIVACY ACROSS HHS
HHS CYBERSECURITY PROGRAM
OFFICE OF INFORMATION SECURITY

HC3: Alert

April 26, 2022 TLP: WHITE Report: 202204260900

BlackCat/ALPHV Ransomware Indicators of Compromise

Executive Summary

As of March 2022, BlackCat/ALPHV ransomware as a service (RaaS) had compromised at least 60 entities worldwide and is the first ransomware group to do so successfully using RUST, considered to be a more secure programming language that offers improved performance and reliable concurrent processing. BlackCat-affiliated threat actors typically request ransom payments of several million dollars in Bitcoin and Monero but have accepted ransom payments below the initial ransom demand amount.

Report

FBI FLASH - BlackCat/ALPHV Ransomware Indicators of Compromise
https://www.ic3.gov/Media/News/2022/220420.pdf

Impact to HPH Sector

Many of the developers and money launderers for BlackCat/ALPHV are linked to Darkside/Blackmatter, indicating they have extensive networks and experience with ransomware operations. HC3 has noted at least two attacks on the Healthcare and Public Health Sector by this actor since December 2021.

Among the mitigations the FBI recommends are to:

- Review domain controllers, servers, workstations, and active directories for new or unrecognized user accounts.
- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (e.g., hard drive, storage device, the cloud).
- Use multifactor authentication where possible.

All organizations should immediately report incidents to a local FBI Field Office, CISA at https://us-cert.cisa.gov/report, or U.S. Secret Service Field Office. CISA also offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

References

FBI: BlackCat ransomware breached at least 60 entities worldwide
https://www.bleepingcomputer.com/news/security/fbi-blackcat-ransomware-breached-at-least-60-entities-worldwide/

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