HC3: Alert

December 02, 2022 TLP:CLEAR Report: 202212021700

Cuba Ransomware Alert

Executive Summary

The FBI and CISA have released a joint security advisory to disseminate known Indicators of Compromise (IOC) and Tactics, Techniques, and Procedures (TTPs) that have been associated with the Cuba Ransomware actor. The new advisory is an update to the December 2021 FBI Flash: Indicators of Compromise Associated with Cuba Ransomware. Over the past year, the group has doubled the number of American victims, infecting at least 65 organizations in critical infrastructures. Due to the nature of the threat actors targets, they pose a threat to the Healthcare and Public Healthcare (HPH) sectors.

Report

#StopRansomware: Cuba Ransomware
https://www.cisa.gov/uscert/ncas/current-activity/2022/12/01/stopransomware-cuba-ransomware

Impact to HPH Sector

Currently, the full impact to the HPH sector is unknown. The group has been targeting several critical infrastructure organizations, including the HPH sector, financial services, government, manufacturing, and information technology. The threat actor has continued to compromise their victims through a variety of software vulnerabilities, phishing, stolen credentials, and legitimate remote desktop protocols. The group also threatens to publicly release the exfiltrated data if a payment is not made. According to the Palo Alto Networks Unit 42, Cuban Ransomware actors have been seen exploiting CVE-2022-24521 and CVE-2020-1472. The FBI and CISA are encouraging all defenders to implement the reported mitigations to defend their system from Cuba Ransomware. Due to the historical nature of their targeting and the frequency with which ransomware gangs victimize the greater healthcare community, organizations should maintain awareness of the threat group's activity.

Contact Information

If you have any additional questions, we encourage you to contact us at HC3@hhs.gov.

We want to know how satisfied you are with the resources HC3 provides. Your answers will be anonymous, and we will use the responses to improve all future updates, features, and distributions. Share Your Feedback