FINISHED INTELLIGENCE REPORTS

HC3 Joint Sector Alert: Rhysida Ransomware

TLP:WHITE

Aug 04, 2023

On August 04, 2023, the Health Sector Cybersecurity Coordination Center (HC3) released a sector alert regarding a ransomware variant and threat group, identified as Rhysida Ransomware.

Rhysida is a new ransomware-as-a-service (RaaS) group that has emerged since May 2023. The group drops an eponymous ransomware via phishing attacks and Cobalt Strike to breach targets networks and deploy their payloads. The group threatens to publicly distribute the exfiltrated data if the ransom is not paid. Rhysida is still in early stages of development, as indicated by the lack of advanced features and the program name Rhysida-0.1. The ransomware also leaves PDF notes on the affected folders, instructing the victims to contact the group via their portal and pay in Bitcoin. Its victims are distributed throughout several countries across Western Europe, North and South America, and Australia. They primarily attack education, government, manufacturing, and technology and managed service provider sectors; however, there has been recent attacks against the Healthcare and Public Health (HPH) sector.

For additional details, please see the attached report.

Report Source(s)	HC3

Release Date
1691207999

Alert ID 111ceee1

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 Rhysida

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

Download Health-ISAC's Information Sharing App.

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