Department of Supervision, Central Office
Cyber Security and IT Risk (CSITE) Group

Alert No: 4/2023 Dated: May 12, 2023

Alerts from Cyber Swachhta Kendra regarding Royal ransomware and ViperSoftX malware

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) of CERT-In has issued alerts regarding Royal ransomware and ViperSoftX malware.

Royal ransomware is targeting multiple crucial infrastructure sectors including manufacturing, communications, healthcare, education, etc. and individuals. The ransomware encrypts the files on a victim's system and attackers ask for ransom payment in bitcoin. Attackers also threaten to leak the data in public domain if denied payment.

ViperSoftX information-stealing malware uses sophisticated encryption methods and anti-analysis techniques such as byte remapping and web browser communication blocking. The threat actors behind the malware deploy carriers in the form of fake software update for multimedia editors, video format converters, or cryptocurrency apps. The Windows malware targets Brave, Google Chrome, Microsoft Edge, Mozilla Firefox, and Opera browsers, and uses several anti-detection, anti-analysis, and stealth-boosting features.

Recommendation

The details regarding the infection mechanism, indicator of compromise, best practices and recommendations regarding the above of the above ransomware / malware are available in the links provided below:

https://www.csk.gov.in/alerts/Vipersoftx.html

https://www.csk.gov.in/alerts/Royal_ransomware.html

Regulated Entities are advised to implement appropriate security measures and leverage this information to take proactive steps to secure the ecosystem.