

Subject: - Cyber Security Advisory – WinRAR Critical Vulnerability Exploitation via Phishing Emails (Advisory No. 52)

Reportedly, hackers are targeting users with improvised phishing email containing attachments of password protected WinRAR zip files. Upon unzipping the rare files, malware automatically executes by exploiting WinRAR remote code execution vulnerability (CVE-2023-40477) on victim's system. The exploitation may result in attacks such as ransomware, data extraction and data wiping etc.

2. Above in view, users are advised for following:
 - a. Do not open and download any suspicious email attachment especially password protected WinRAR/WinZip files.
 - b. WinRAR users are advised to update to latest version 6.23 or above.
3. Kindly disseminate the above information to all concerned in your organizations, all attached/affiliated departments and ensure necessary protective measures.