RAMSOMWARE ATTACK
MODUS OPERANDI AND REMEDIAL MEASURES

1. Background:

It has been observed that "Ransomware malware" attacks are on rise affecting financial institutions, businesses and academic institutions in the country. Ransomware are type of malicious software (malware) that scramble the contents of a computer or server (associated network shares and removable media) and demands payment/ransom to unlock it, usually in the form of anonymous decentralized virtual currency like Bitcoin.

2. Modus Operandi of Ransomware Attacks:

Ransomware is typically spread through spear phishing emails that contain malicious attachments in the form of archived content (zip/rar) containing a JavaScript file. Upon visiting such infected/compromised websites or web links, a piece of malware is dropped on victim's machine, which executes itself without user's knowledge and encrypts the contends of a computer or server.

3. Best Practices and Remedial Measures:

Users and administrators are advised to take the following preventive measures to protect their computer networks from ransomware infection/ attacks:

- Perform regular backups of all critical information to limit the impact of data or system loss and to help expedite the recovery process. Ideally, this data should be kept on a separate device, and backups should be stored offline.
- Check regularly for the integrity of the information stored in the databases.
- Regularly check the contents of backup files of databases for any unauthorized encrypted contents of data records or external elements, (backdoors /malicious scripts.)
- Ensure integrity of the codes /scripts being used in database, authentication and sensitive systems
- Keep the operating system third party applications (MS office, browsers, browser Plugins) up-to-date with the latest patches.
- Maintain updated Antivirus software and Active Directory on all systems
- Don't open attachments in unsolicited e-mails, even if they come from people in your contact list, and never click on a URL contained in an unsolicited e-mail, even if the link seems genuine. In cases of genuine URLs close out the e-mail and go to the organization's website directly through browser
- Disable remote Desktop Connections, employ least-privileged accounts. Limit users who can log in using Remote Desktop, set an account lockout policy. Ensure proper RDP logging and configuration.
- Enable personal firewalls on workstations.
- Implement strict External Device (USB drive) usage policy.
- Employ data-at-rest and data-in-transit encryption.
- Carry out vulnerability Assessment and Penetration Testing (VAPT) and information security audit of critical networks/systems, especially database servers from CERT-IN empanelled auditors. Repeat audits at regular intervals.

***