BGD e-GOV CIRT

NATIONAL CYBER SECURITY AGENCY

BANGLADESH COMPUTER COUNCIL
COMPUTER FOR EVERYTHING

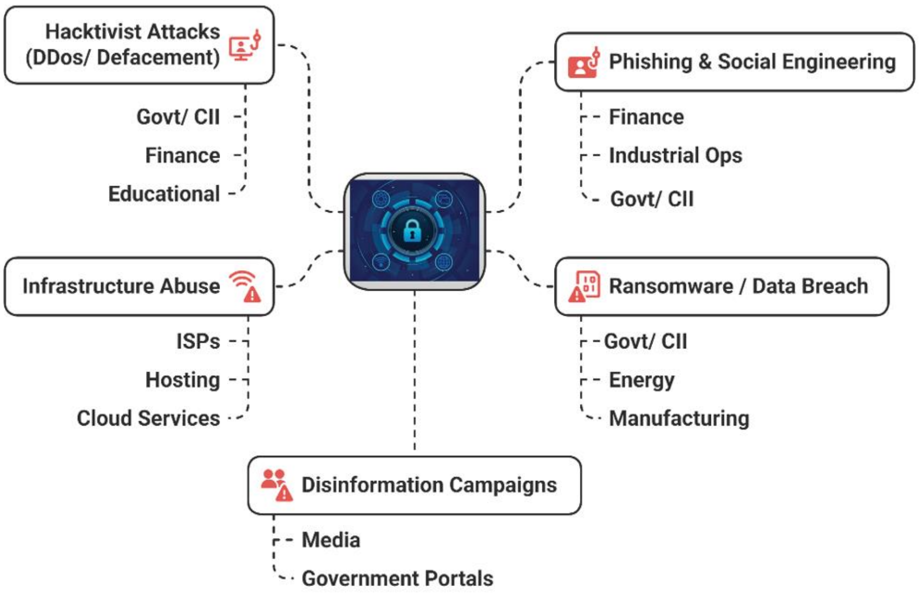
24 July 2025

Guideline for Situational Alert

We would like to inform you that, based on current threat intelligence, there is a potential risk of a large-scale cyberattack targeting Bangladesh's ICT infrastructure in the coming days. Likely targets include Critical Information Infrastructures (CII) and high-impact sectors such as banking, power, and public services. Recent attack patterns indicate a focus on web application exploitation, website defacement, compromised credentials, and Distributed Denial-of-Service (DDoS) attacks, among others.

In light of this, we strongly advise all organizations to enhance 24/7 monitoring of their IT infrastructure, ensure proper logging, and maintain a heightened security posture to detect and respond to any suspicious activities promptly.

Cyber Threats: Emerging Threats and Targets



Recommended Defensive Actions:

- Implement multi-factor authentication (MFA) for all critical systems.
- Immediately review and restrict remote access, VPNs, and privileged accounts.
- Urgently apply latest security patches to internet-facing services, servers, firewalls.
- Review and patch vulnerabilities in web applications and exposed services.
- Disable unused ports and services; enforce least-privilege access.
- Utilize effectively SIEM/NIDS to detect abnormal behavior (e.g., lateral movement, DDoS, data exfiltration).
- Monitor for suspicious logins, unauthorized file changes, and external connections.
- Use EDR or AV with updated threat signatures for detect threat.
- Ensure critical data backups are regular, encrypted, and stored offline.
- Review and update cyber incident response plans.
- Report any IOCs or suspicious activity to National Cyber Security Agency / BGD e-GOV CIRT at notify@ncsa.gov.bd or cti@cirt.gov.bd