GOVERNMENT OF INDIA
MINISTRY OF HOME AFFAIRS

LOK SABHA
STARRED QUESTION NO.*278

TO BE ANSWERED ON THE 8TH AUGUST, 2023/ SRAVANA 17, 1945 (SAKA)

THREATS EMANATING FROM CYBER CRIMINALS

***278. DR. ALOK KUMAR SUMAN:**

Will the Minister of HOME AFFAIRS be pleased to state:

(a) whether the Government is aware about underlined threats emanating from cyber criminals using the dark net, metaverse, deepfakes, ransomware and toolkit based misinformation for campaign in the country;

(b) if so, the details thereof;

(c) whether it is a fact that cyber criminals are targeting critical information in financial system; and

(d) if so, the details thereof and the measures taken by the Government in this regard to protect the financial system and its other effects in the country?

ANSWER

MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS
(SHRI AJAY KUMAR MISHRA)

(a) to (d): A Statement is laid on the Table of the House.

STATEMENT IN REPLY TO PARTS (a) to (d) OF THE LOK SABHA STARRED QUESTION NO.*278 TO BE ANSWERED ON 08.08.2023.

(a) to (d): The policies of the Government are aimed at ensuring an open, safe, trusted and accountable internet for its users. The Government is fully cognizant of various cyber security threats and has taken various steps to counter such threats. The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication "Crime in India". Specific data in this regard is not maintained by NCRB. Ransomware ecosystem is evolving with wide range of attack campaigns. Cyber threat actors are exploiting known vulnerabilities, compromised credentials of Remote Access services and phishing campaigns for gaining access into the infrastructure of organisations.

The Central Government has taken several cyber security measures which, inter-alia, include the following:

i. **The Government has established the 'Indian Cyber Crime Coordination Centre' (I4C) to provide a framework and eco-system for LEAs to deal with cyber crimes in a comprehensive and coordinated manner.**

ii. The National Cyber Crime Reporting Portal (https://cybercrime.gov.in) has been launched, as a part of the Indian Cyber Crime Coordination Centre (I4C), to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and subsequent action thereon are handled by the State/UT Law Enforcement Agencies (LEAs) concerned as per the provisions of the law.

iii. The Massive Open Online Courses (MOOC) platform, namely 'Cy Train' portal has been developed under the Indian Cyber Crime Coordination Centre (I4C), for capacity building of police officers/judicial officers through online courses on critical aspects of cyber crime investigation, forensics, prosecution etc. along with certification. More than 39,200 Police Officers from States/UTs are registered and more than 19,550 Certificates issued through the portal.

iv. The Government has designated Indian Computer Emergency Response Team (CERT-In) as the national agency for responding to cyber security incidents. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and

sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.

v. The Government has established National Critical Information Infrastructure Protection Centre (NCIIPC) for protection of critical information infrastructure in the country. NCIIPC provides near real-time threat intelligence and situational awareness based on which regular alerts and advisories are sent to Critical Information Infrastructure (CII) / Protected System (PS) entities.

vi. CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate situational awareness regarding existing and potential cyber security threats.

vii. CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

viii. A Cyber Crisis Management Plan is formulated by CERT-In for implementation by all Ministries and Departments of the Central / State Governments and their organisations and critical sectors to help them to counter cyber-attacks.

ix. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers and networks on an ongoing basis.

x. CERT-In is working in coordination with service providers, regulators and Law Enforcement Agencies (LEAs) to track and disable phishing websites and facilitate investigation of fraudulent activities.

xi. CERT-In has published "India Ransomware Report – 2022" in April 2023, covering latest tactics and techniques of ransomware attackers and Incident response and mitigation measures.

xii. CERT-In, through RBI, has advised all authorised entities and banks issuing pre-paid payment instruments in the country to carry out special audit by CERT-In empanelled auditors, close the non-compliances identified in the audit report and ensure implementation of security best practices.

xiii. CERT-In provides leadership for the Computer Security Incident Response Team-Finance Sector (CSIRT-Fin) operations under its umbrella for responding to and containing and mitigating cyber security incidents reported from the financial sector.

xiv. CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same, and to provide cyber security tips and best practices for citizens and organisations.

xv. CERT-In conducts regular training programmes for network and system administrators and the Chief Information Security Officers of Government and critical sector organisations regarding securing the information technology infrastructure and mitigating cyber-attacks. A total of 42 training programmes were conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to June, a total of 627 officials from Government, critical sectors, public and private sector have been trained in 6 training programs in the area of cyber security.

xvi. CERT-In, National Institute of Securities Markets and the Centre for Development of Advanced Computing (C-DAC) conduct a self-paced 60-hour certification Cyber Security Foundation Course for professionals in the financial sector.

xvii. CERT-In and the Reserve Bank of India (RBI) jointly carry out a cyber security awareness campaign on 'beware and be aware of financial frauds' through the Digital India Platform.

*****