GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
STARRED QUESTION NO. *244
TO BE ANSWERED ON: 02.08.2017

RANSOMWARE ATTACK

***244 SHRI HARISH MEENA:**
DR. THOKCHOM MEINYA:

Will the Minister of Electronics & Information Technology be pleased to state:-

(a) whether the Government has made estimation of the losses incurred/data lost due to attack of ransomware virus across the country;

(b) if so, the details thereof and if not, the reasons therefor along with the number of virus attacks that have been reported across the country during each of the last three years and the current year including the attack of Jawaharlal Nehru Port Trust, Mumbai;

(c) whether the Indian cyber experts have successfully restored the data attacked / encrypted by the said virus in the country and if so, the details thereof;

(d) whether any cooperation has been extended by the developed countries to Indian cyber experts to fight against the ransomware virus and if so, the details thereof along with the level of preparedness to counter cyber attacks caused by Ransomware, WannaCry, Petya, etc.; and

(e) the other steps taken/being taken by the Government to protect data of the country from such virus attacks in future?

ANSWER

MINISTER FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAVI SHANKAR PRASAD)

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

STATEMENT REFERED TO IN REPLY TO LOK SABHA STARRED QUESTION *244 FOR 02.08.2017 REGARDING RANSOMWARE ATTACK

……..

(a) and (b): As per the information reported to Indian Computer Emergency Response Team (CERT-In), a total no. of Nil, 2, 26 and 37 incidents involving ransomware were reported during the years 2014, 2015, 2016 and 2017 (till June) respectively. The details of financial impact of these incidents is not reported to CERT-In as CERT-In provides technical support and remediation.

Propagation of ransomware called WannaCry / WannaCrypt has been reported in many countries around the world including India since 12 May 2017. Propagation of another ransomware called Petya was also reported since 27 June 2017.

34 incidents have been reported to CERT-In from organisations and individuals regarding infections of Wannacry and Petya ransomware. Operations of Jawaharlal Nehru Port Trust (JNPT) Mumbai were partially affected by the Petya ransomware.

(c): Decryption tools for some of the ransomware are available which allows users to decrypt their unusable/encrypted files. The information regarding such decryption tools is published on the website of the CERT-In (www.cert-in.org.in) and of the Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in).

With regards to WannaCry Ransomware, decryption tools have limited capability at present and hence have not been very successful. With regards to the new variant of Petya ransomware, there is no decryption tool publicly available.

For all ransomware attacks, data affected could be restored from a data backup, if available, thereby minimizing the impact of the said attacks.

(d): CERT-In is regularly interacting with its counterparts in other countries and antivirus / technology companies to obtain updated information and remedial measures regarding the emerging ransomware threats. Specific information to prevent and detect the ransomware threats is published on the website of CERT-In and Cyber Swachhta Kendra. This information is also shared with key organisations on regular basis.

The following measures are taken to enhance preparedness of organisations to counter recent ransomware attacks:

(i) CERT-In issued an advisory regarding detection and prevention of Wannacry ransomware on its website on 13 May 2017. Advisory regarding detection and prevention of Petya ransomware was issued by CERT-In on 27 June 2017.

(ii) CERT-In had issued a vulnerability note on its website with a severity rating of “high” on March 15, 2017 providing information regarding vulnerabilities in Microsoft Windows systems which have been exploited by Wannacry and Petya ransomware alongwith remedial measures.

(iii) CERT-In informed various key organisations across sectors in the country regarding the ransomware threat and advised measures to be taken to prevent the same.

(iv) CERT-In conducted a live webcast for citizens at large on the WannaCry attack to explain the issue, impact, its modus operandi, preventive measures and best practices. CERT-In also communicated the advisory through social media.

(v) Free tools for detection and removal of Wannacry and Petya ransomware were provided on the website of Cyber Swachhta Kendra (www.cyberswachhtakendra.gov.in).

(e): The following measures are taken to prevent virus / ransomware attacks and enhance cyber security in the country:

(i) The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect systems and mobile devices.

(ii) Security tips are published for users to secure their Desktops and mobile/smart phones.

(iii) Government has launched the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre). The centre is providing detection of malicious programs and free tools to remove the same for banks as well as common users.

(iv) Government has formulated Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors

(v) Cyber security mock drills are being conducted regularly to enable assessment of cyber security posture and preparedness of organizations in Government and critical sectors. 15 such drills have so far been conducted by CERT-In where 148 organisations from different States and sectors such as Finance, Defence, Power, Telecom, Transport, Energy, Space, IT/ITeS, etc participated. 4 such drills have been conducted in June 2017 specifically for ransomware scenarios to enable preparedness of organisations for such threats.

(vi) Government has empanelled 54 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) Government is setting up the National Cyber Coordination Centre (NCCC) to continuously scan the cyberspace in the country at metadata level and generate near real time situational awareness for macroscopic views of the cyber security threats in the country.

(viii) Government has published Guidelines for Chief Information Security Officers (CISOs) for Secure Applications and Infrastructure. Government has also specified key roles and responsibilities of CISOs in Ministries/Departments and Organisations managing ICT operations.

(ix) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. 14 training programs covering 431 participants and 13 training programs covering 329 participants were conducted during 2016 and 2017 (till June).

(x) Two workshops on Cyber Security Threats & Countermeasures were conducted exclusively for Women by CERT-In.

(xi) Ministry of Electronics and Information Technology is implementing the Information Security Education and Awareness (ISEA) project which aims to generate 1.14 lakhs qualified professionals at various levels in period of 5 years. A total of 52 institutions in various categories across the country are participating in the project. Besides, National Institute of Electronics and Information Technology (NIELIT) is conducting certification courses for creation of cyber security professionals.

(xii) Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI), Ghaziabad to impart basic and advanced training in cyber forensics and investigation of cybercrimes to police officers. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of law enforcement personnel and Judiciary in these States.

(xiii) MeitY in collaboration with Data Security Council of India (DSCI) has trained 28000 Police (including 447 Judiciary).

(xiv) Ministry of Electronics & Information Technology (MEITY) regularly conducts programs to generate information security awareness. Specific book, videos and online materials are developed for children, parents and general users about information security which are disseminated through Portals like "http://infosecawareness.in/" and "www.cyberswachhtakendra.gov.in"

(xv) MeitY has developed course content for safe and secure use of Internet for school children and has provided it to Ministry of Human Resource Development for use in schools books.

****