GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 1541
TO BE ANSWERED ON: 28.07.2017

GOVERNMENT NETWORK AFFECTED BY RANSOMWARE ATTACKS

1541 SHRI NARAYAN LAL PANCHARIYA:
SHRI SANJIV KUMAR:

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

(a) whether any IT network of Government of India or any State Government or any Government body has been affected by the recent Ransomware attacks, if so, the details thereof;
(b) whether the quantum of damage by the said attack has been evaluated, if so, the details thereof; and
(c) the steps being taken to strengthen the security of online data being held by Government agencies?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI P.P. CHAUDHARY)

(a) and (b): 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. Ransomware is a type of malicious software that infects a computer and restricts users' access to affected files by encrypting them until a ransom is paid to unlock it.

4 incidents from Central Government Departments and 4 incidents from state Government Departments have been reported to the Indian Computer Emergency Response Team (CERT-In) regarding infections of Wannacry ransomware. As reported to CERT-In, operations of one sea-port were partially affected by the Petya ransomware. Remedial measures to contain damage and prevent such incidents have been advised by CERT-In.

(c): The following measures are taken to strengthen security of government departments and prevent 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 Wannacrypt and Petya ransomware alongwith remedial measures.

(iii) CERT-In informed various key organisations across different sectors in the country regarding the ransomware threat and advised measures to be taken to prevent the same. A webcast was also conducted in this regard for organisations and users.

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

(v) CERT-In regularly issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect systems and mobile devices.

(vi) 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

(vii) 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.

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

(ix) 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.

****