

GOVERNMENT OF INDIA  
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY  
**RAJYA SABHA**  
**UNSTARRED QUESTION NO. 1546**  
TO BE ANSWERED ON: 28.07.2017

**RANSOMWARE ATTACK ON GOVERNMENT COMPUTERS**

**1546 SHRI SANJAY RAUT:**

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

- (a) the effect of the ransomware attack on Government computers;
- (b) whether any sensitive data was stolen;
- (a) the overall extent of the damage;
- (b) the measures taken to reduce the effect of the attack and to ensure quick elimination; and
- (c) the corrective action being taken to increase security and to protect information in case of a similar attack in the future?

**ANSWER**

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

(a),(b) and (c): 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, thus rendering them unusable till recovery/cleaning is performed.

As on date, 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.

(d) : The following measures are taken to mitigate 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 Wannacrypt 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) Free tools for detection and removal of Wannacrypt and Petya ransomware were provided on the website of Cyber Swachhta Kendra ([www.cyberswachhtakendra.gov.in](http://www.cyberswachhtakendra.gov.in)).

(e) : The following measures are taken to mitigate recent ransomware attacks and enhance cyber security in the country, namely:-

- (i) 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 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 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.

\*\*\*\*\*