

GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
LOK SABHA
UNSTARRED QUESTION NO.3921
TO BE ANSWERED ON: 18.03.2020

MALWARE THREAT TO ANDROID OPERATING SYSTEM

3921. SHRI V.K. SREEKANDAN:

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

- (a) whether the Government has sent an alert to all States warning them about the vulnerability of the Android Operating System to a bug called Strand Hogg that allows real time malware applications to pose as genuine applications and access user's data of all kind;
- (b) if so, the details thereof and if not, the reasons therefor along with other steps taken by the Government in this regard;
- (c) whether the Government has also sent a detailed list of the modus operandi of the hackers and latest trends in cyber attacks for appropriate action by the States; and
- (d) if so, the details thereof and the response received by the Government from the States in this regard?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI SANJAY DHOTRE)

(a) and (b): A vulnerability which has been named "StrandHogg" has been reported in the Android operating system. The vulnerability allows a malicious application to masquerade as genuine mobile app and steal information.

The Indian Computer Emergency Response Team (CERT-In) has published a vulnerability note on this issue on 9th December 2019 and alerted the users regarding precautionary measures to be taken.

Government has taken following measures to check malicious apps and enable users to protect their mobile phones:

- (i) Alerts and advisories about the threats, vulnerabilities and malware affecting mobile phones along with countermeasures are being issued regularly by CERT-In.
- (ii) Government has operationalised the Cyber Swachhta Kendra to enable detection and cleaning of malicious code including from mobile / smart phones.
- (iii) Ministry of Electronics & Information Technology (MeitY) regularly conducts programs to generate information security awareness. Tips for users about information security including securing mobile phones are disseminated through websites like "<https://infosecawareness.in>", "<https://www.cert-in.org.in>" and "<https://www.cyberswachhtakendra.gov.in>".

(c) and (d): The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis.

Further, Government has formulated guidelines on 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.
