GOVERNMENT OF INDIA
COMMUNICATIONS AND INFORMATION TECHNOLOGY
LOK SABHA

UNSTARRED QUESTION NO:1398
ANSWERED ON:04.03.2015
WORM VIRUS
Khuba Shri Bhagwanth

Will the Minister of COMMUNICATIONS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether the Government is aware of the 'Worm' virus that steals login secrets and password of an individual;

(b) if so, the details thereof and the reaction of the Government thereto;

(c) the losses incurred to individuals in the last three years and current year; and

(d) the steps taken by the Government in this regard?

Answer

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

(a): With the advances and proliferation of Information Technology (IT) in all areas worldwide, there is rise in the virus propagation and malicious activities. Malicious codes that propagate in the networks are generally called "Worms". There are different categories or types of "worms". Recently one type of worm called "Cridex" has been reported to be spreading in the cyber space globally.

(b): This type of "worm" propagates through removable disk drives and injects fake web pages and redirects users to fake banking sites. In this way this "worm" tricks users to divulge online login credentials.

Incidents of malware infections in Indian cyber space are reported to and tracked by the Indian Computer Emergency Response Team (CERT-In). CERT-In works with Internet Service Providers to identify the infected systems and organisations. Remedial measures to dis-infect such infected systems and prevent further infections are suggested to the users and organisations owning such infected systems. Besides, alerts and advisories about the virus threats are being issued regularly by CERT-In on its website www.cert-in. org.in.

CERT-In, Department of Electronics & Information Technology (DEITY) has initiated action with active participation of Service Providers and Industry to set up a centre for detection of computer systems infected by malware and to notify, enable cleaning and securing systems of end users to prevent further malware infections.

(c): Several cyber attack techniques are used in combination while committing cyber frauds. Losses are normally computed as a whole with respect to each category of cyber crimes reported in area of operation such as ATM/Debit cards, credit cards, Internet Banking etc. Segregation of losses with respect to each cyber attack technique such as malware becomes difficult. However, As per the information provided by the Reserve Bank of India (RBI) , 10048, 8765, 9500 and 9362 cyber fraud cases and losses of Rs. 38 Crores, Rs. 67 Crores, Rs. 78 crores and Rs. 60 crores have been reported to the RBI during 2011-12, 2012-13, 2013-14, and April to December 2014 respectively.

(d): Government has taken following steps to prevent cyber crimes in the country:

i) CERT-In is working in coordination with Reserve Bank of India and banks to track and disable phishing websites.

ii) Banks have implemented Two-factor authentication to mitigate risks due to theft of online credentials. Besides, SMS alerts are sent to users intimating details of transactions involving amounts above specified threshold.

iii) Steps have been taken to monitor and prevent financial frauds through phishing attacks, Credit / Debit card frauds, money laundering schemes etc.

iv) The Information Technology Act, 2000, provides legal framework to address various types of prevalent cyber crimes and security breaches of information technology infrastructure.

v) 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 and Judiciary in these States.

vi) Cyber Crime Cells have been set up in all States and Union Territories for reporting and investigation of Cyber Crime cases.

vii) Academia like National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.

viii) More than 26000 Police Officers and 600 judicial officers have so far been trained in the Training Labs established by the Government.

ix) It is proposed to set up two National Centres of Excellence in the area of Investigation of Cyber Crimes and Digital Evidence.

x) Number of Cyber forensics tools for collection, analysis, presentation of the digital evidence have been developed and are being used by Law Enforcement Agencies.

xi) Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

xii) Government has formulated a set of investigation manuals with procedures for Search, Seizure Analysis and Presentation of digital evidence in courts. The manuals have been circulated to Law Enforcement Agencies in all States.

xiii) Department of Electronics & Information Technology (DEITY) is conducting 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 "secureyourpc.in" and "www.secureyourelectronics.in".