

**GOVERNMENT OF INDIA  
COMMUNICATIONS AND INFORMATION TECHNOLOGY  
LOK SABHA**

UNSTARRED QUESTION NO:1135  
ANSWERED ON:11.12.2013  
COMPUTER VIRUS  
Sugumar Shri K.

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

- (a) whether a large number of viruses have been detected affecting the computers;
- (b) if so, the details of the viruses;
- (c) whether India stands 3rd in botnet computer virus infection; and
- (d) if so, the details thereof and the action taken by the Government for preventing the nuisance and protecting the Indian websites from hacking and virus attack?

**Answer**

MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION TECHNOLOGY (SHRI MILIND DEORA)

(a): With the innovation of technology `malicious software` are getting highly sophisticated and complex. Due to proliferation of Information Technology (IT) in all areas worldwide, there is rise in-the virus propagation and malicious activities. With the rise in the number of computers and increase in the broadband connections the same trends are observed in India as well.

(b): As per reports of Antivirus and Cyber Security vendors and incidents of virus propagation tracked by and reported to the Indian Computer Emergency Response Team (CERT-In), prominent viruses affecting Indian cyber space are ZeroAccess botnet, Ramnit, Sality, ZeuS, Reveton, Zortob and Android.Adrd.

(c) : Different Botnets are reported from time to time across the world due to spread of variety of viruses. According to a report of Antivirus vendor Symantec, India is at No. 3 only for specific virus `Zero Access botnet` caused due to infections of multiples variants of `zero access` virus.

(d): As per botnet infections tracked by CERT-In, propagation of `zero access` malware has shown increase during last two months. CERT-In is working in coordination with the Internet Service Providers and Industry to alert users regarding such infections and have suggested remedial measures. Alerts regarding spread of `zero access` botnet are published on website [www.cert-in.org.in](http://www.cert-in.org.in) and measures and removal tools for cleaning infected systems are advised. The specific steps taken by the Government for protecting Indian websites from hacking and virus attacks are :

i) Alerts and advisories about the virus threats are being issued regularly by the Indian Computer Emergency Response Team (CERT-In). Measures to be taken to detect infected systems, dis-infect the same and prevent further propagation are also and being advised regularly to organizations and general users.

ii) Government has released the `National Cyber Security Policy - 2013` for public use and implementation with all relevant stakeholders. The objective of the policy is to create a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country.

iii) The Government has circulated Computer Security Policy and Guidelines to all the Ministries/Departments on taking steps to prevent, detect and mitigate cyber attacks. In addition, all state governments and UTs have been advised to implement appropriate security measures to prevent hacking of websites.

iv) National Informatics Centre (NIC) managing Govt websites is implementing measures to secure the Govt. IT infrastructure from cyber attacks.

v) National Informatics Centre (NIC) is hosting web sites, only after the web sites are audited with respect to cyber security.

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`.