Annual Report (2011)

Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology
Ministry of Communications & Information Technology
Government of India

24th February, 2012

Indian Computer Emergency Response Team (CERT-In)

1.0 About CERT-In:

1.1 Introduction

CERT-In is a functional organisation of Department of Information Technology, Ministry of Communications and Information Technology, Government of India, with the objective of securing Indian cyber space. CERT-In provides Incident Prevention and Response services as well as Security Quality Management Services.

The Information Technology Act 2000 designated CERT-In to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents
- Such other functions relating to cyber security as may be prescribed

1.1.1 Establishment

CERT-In was operational since January 2004. The constituency of CERT-In is the Indian cyber community. CERT-In works cooperatively with Chief Information Officers and system administrators of various sectoral and organisational networks of its constituency.

1.1.2 Workforce power

CERT-In has 30 member technical staff.

1.1.3 Constituency

The constituency of CERT-In is the Indian cyber community and Indian cyberspace. CERT-In provides services to the organizations in the Govt., Public and Private sectors.

2.0 Activities and Operations of CERT-In

CERT-In provides:

- Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organisations secure their systems and networks
- Reactive services when security incidents occur so as to minimize damage

2.1 Incident handling Reports

The summary of activities carried out by CERT-In during the year 2011 is given in the following table:

Activities	Year 2011
Security Incidents handled	**13301**
Security Alerts issued	**48**
Advisories Published	**81**
Vulnerability Notes Published	**188**
Security Guidelines Published	**4**
White papers/Case Studies Published	**3**
Trainings Organized	**26**
Indian Website Defacements tracked	**17306**
Open Proxy Servers tracked	**3294**
Bot Infected Systems tracked	**6277936**

Table 1. CERT-In Activities during year 2011

2.2 Abuse Statistics

In the year 2011, CERT-In handled more than 13000 incidents. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing.

The year-wise summary of various types of incidents handled is given below:

Security Incidents	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**	**2011**
Phishing	3	101	339	392	604	374	508	674
Network Scanning / Probing	11	40	177	223	265	303	277	1748
Virus / Malicious Code	5	95	19	358	408	596	2817	2765
Spam	-	-	-	-	305	285	181	2480
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344	4394
Others	4	18	17	264	148	160	188	1240
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**

Table 2. Year-wise summary of Security Incidents handled

Various types of incidents handled by CERT-In are given in Figure 1.

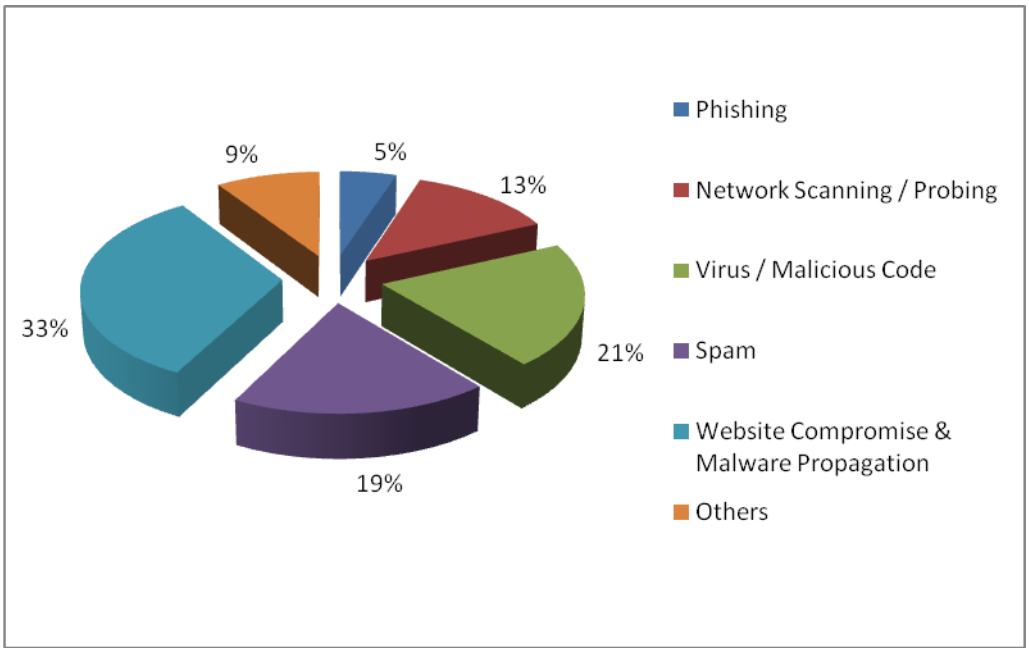

***Figure 1*. Summary of incidents handled by CERT-In during 2011**

2.3 Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends during the year 2011 are as follows:

- Web site intrusions and drive-by-download attacks through compromised websites. Around 4394 malicious URLs were tracked in ".in" space. Most of the attacks were facilitated through attack tool kits such as Techno XPACK, Phoenix Exploit Kit, Neo spolit, Eleonre and Blackhole.
- Prominent client side vulnerabilities exploited in the drive by download attacks were in Adobe PDF, Flash, Java Runtime Environment, Internet Explorer and Mozilla Firefox.
- Malware trends indicate that malware affecting mobile platforms such as Android and Symbian were on the rise.
- Banking Trojans and key logger families were widely propagating. Prominent Trojans observed were ZeuS, Carberp, SpyEye, Torpig, Pushdo etc
- Rougue antivirus programs such as MacDefender, Winwebsec etc. were delivered to users through SEO poisoning

- Malicious Spam and identity theft schemes were leveraging Social networking sites and features therein
- Targeted attacks were on the rise involving exploitation vulnerabilities in Adobe PDF and MS Office.

2.4 Tracking of Indian Website Defacements

CERT-In has been tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. In all 17306 numbers of defacements have been tracked. Most of the defacements were under .in domain, in which a total 9839 .in domain websites were defaced.

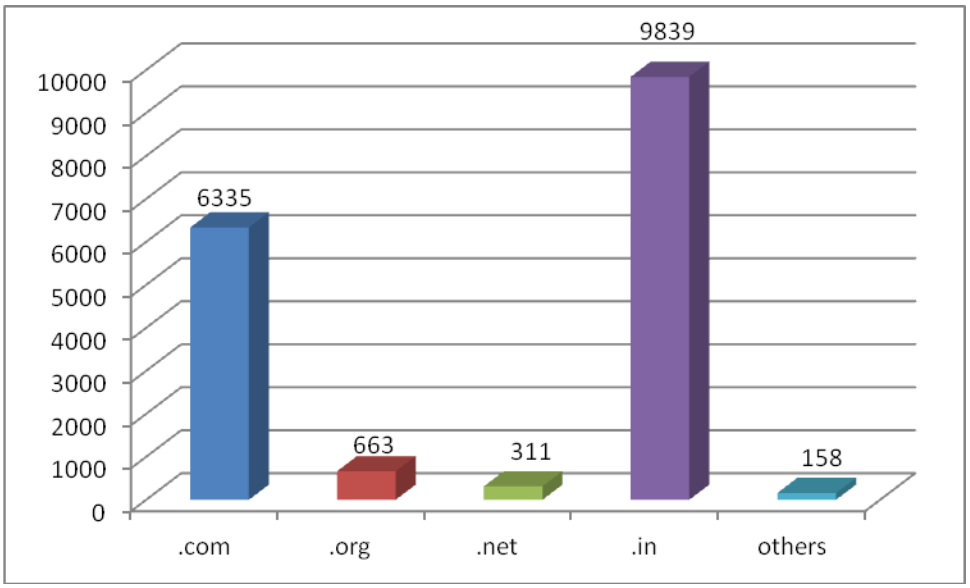

Figure 2. Indian websites defaced during 2011 (Top Level Domains)

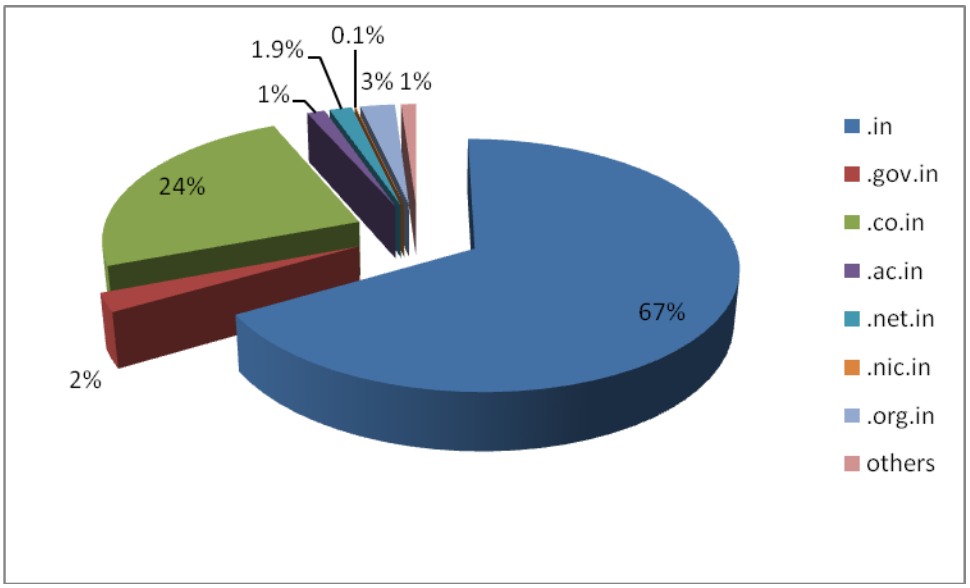

Figure 2.1 .in ccTLD defacements during 2011

2.5 Tracking of Open Proxy Servers

CERT-In is tracking the open proxy servers existing in India and proactively alerting concerned system administrators to properly configure the same in order to reduce spamming and other malicious activities originating from India. In all 3294 open proxy servers were tracked in the year 2011. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

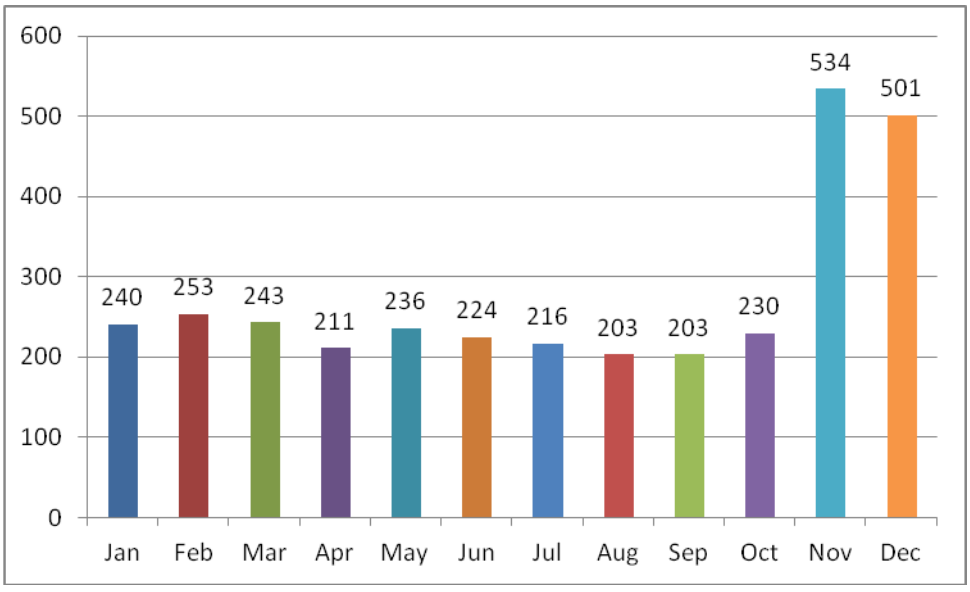

Figure 3. Monthly statistics of Open Proxy Servers in 2011

2.6 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of Command and Control servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2011.

Month	Number of Bot Infected Systems	C&C Servers
January	2005349	11
February	1305033	21
March	1948356	32
April	2439756	33
May	2008282	45
June	2138201	7
July	2098347	7
August	2000925	9
September	2117432	7
October	2011193	4
November	2051836	2
December	1437170	3

Figure 4. Botnet statistics in 2011

2.7 Collaborative Incident resolution

During the year 2011, CERT-In worked in collaboration with Microsoft and Internet Service Providers in India to detect and clean the botnet infected systems, specifically the “Waldec” and “Rustock” Botnets. The outcome was very encouraging.

CERT-In also working in close coordination with cyber security agencies such as Symantec, McAfee and Kaspersky for resolution of incidents of malware such as Stuxnet and Duqu.

2.8 Interaction with Sectoral CERTs

CERT-In plays the role of mother CERT and is regularly interacting with the cyber security officers of Sectoral CERTs in Defense, Finance, Power, Transport and other sectors to advise them in the matters related to cyber security.

2.9 Security Profiling and Audit Services

CERT-In is providing Security Profiling and Audit services to key organizations within the country to identify risks, threats and vulnerabilities in their IT assets and advise appropriate mitigations.

3.0 Events organized/ co-organized

3.1 Education and Training

To create awareness and to enable users to implement best practices, CERT-In is organizing workshops and training programmes on focused topics for targeted audience such as CISOs, financial and banking sector officers, System Administrators, ISPs etc. Experts from industry are delivering lectures in these workshops apart from CERT-In staff. CERT-In has conducted the following training programmes during 2011.

- Workshop on "Secure Cloud Computing" on December 16, 2011
- Workshop on "Windows Security" on December 02, 2011
- Workshop on "Advanced Internet Investigations & Cyber Forensics" on November 18, 2011
- Workshop on "Secure Development Life Cycle" on November 15, 2011
- Workshop on "Targeted Attacks & Mitigation" on November 04, 2011
- Workshop on "Data Centre Security" on October 21, 2011
- Workshop on "Log Management, Compliance & Auditing" on October 17, 2011
- Workshop on "Phishing Attacks and Mitigation" on September 29, 2011
- Workshop on "Web Application Security : Current threats & mitigation" on September 09, 2011
- Workshop on "VoIP Security" on August 24, 2011
- Workshop on "Introduction to Web Application Security" on August 17, 2011

- Workshop on "Advanced Enterprise Security" on July 29, 2011
- Workshop on "Network Penetration Testing" on July 15, 2011
- Workshop on "Data Leakage Detection & Prevention" on June 24, 2011
- Workshop on "Advanced Web Application Security" on June 17, 2011
- Workshop on "Information Security Essentials" on June 10, 2011
- Workshop on "Virtualization Security Challenges" on May 27, 2011
- Workshop on "Advanced Cyber Forensics" on May 05, 2011
- Workshop on "Vulnerability Assessment in Enterprise Networks and Applications" on April 08, 2011
- Workshop on "Web Application Security - Current Trends" on March 18, 2011
- Workshop on "Linux Security" on March 11, 2011
- Workshop on "Network Perimeter Defence" on February 11, 2011
- Workshop on "MySQL Database Server Security" on February 04, 2011
- Workshop on "Introduction to Information Security" on January 28, 2011
- Workshop on "Oracle Server Security" on January 17, 2011
- Workshop on "SQL Server Security" on January 12, 2011

3.2 Drills

CERT-In has successfully participated in ASEAN CERTs Incident Handling Drill (ACID 2011) held in September 2011 and APCERT Incident Handling drill conducted in February 2012.

At national level, CERT-In is carrying out mock drills with key sector organizations for assessing their preparedness in dealing with cyber crisis situation. These drills have helped in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber security incidents, besides increasing the cyber security awareness among the key sector organizations. These drills at present are being carried out once in six months. Till date CERT-In has conducted 5 Cyber security drills of different complexities with 57 organizations covering various sectors of Indian economy i.e. Finance, Defence, Telecom/ISP, Transport, Power, Energy and IT industry.

4.0 Achievements

4.1 Publications

The following were published by CERT-In in the year 2011:

1. **Securing Wireless Access Points/Routers:** The purpose of the guideline is to recommend security practices for implementing Wi-Fi networks in Home and SOHO environments.

2. **Monthly security bulletins**: Monthly security bulletin comprises of Statistics of incidents handled by CERT-In, information on vulnerabilities in various Operating Systems and applications tracked, Cyber intrusion trends and other relevant IT security issues.

4.2 Certifications

Two technical members of CERT-In obtained GIAC Reverse Engineering Malware (GREM) Certification.

5.0 International collaboration

CERT-In has established collaborations with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices. CERT-In is a member of Forum of Incident Response and Security Teams (FIRST), APCERT and Anti-Phishing Working Group (APWG).

5.1 MoU

CERT-In and US-CERT singed MoU to enhance cooperation in the area of cyber security for rapid resolution of and recovery from cyber attacks.

As part of MoU with National Computer Board, Mauritius, CERT-In is providing advice to make CERT, Mauritius fully operational and becoming member of Forum of Incident Response and Security Teams (FIRST).

6.0 Future Plans/Projects

6.1 Future projects

CERT-In has been evolved as the most trusted referral agency in the area of information security in the country. Following are the future plans:

- Regular interaction with CISOs of Critical Infrastructure Organisations and sectorial CERTs to ensure security of the critical systems.
- Development and implementation of a crisis management framework to enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks

- Enhancing collaborations with IT product and security vendors to mitigate the vulnerabilities in various systems and cooperation with international CERTs and security organizations on information sharing and incident response
- Promotion of R&D activities in the areas of attack detection & prevention, Cyber Forensics and malware detection & prevention.
- Creation of framework and facility for collection, correlation and analysis of security events in real time and generating early warning to constituency

Contact Information

Postal Address:

Indian Computer Emergency Response Team (CERT-In)

Department of Electronics & information Technology

Ministry of Communication & information technology

Government of India

Electronic Niketan

6, CGO Complex, Lodhi Road

New Delhi – 110003

India

Incident Response Help Desk:

Phone: +91-11-24368572

+91-1800-11-4949 (Toll Free)

Fax: +91-11-24368546

+91-1800-11-6969 (Toll Free)

PGP Key Details:

User ID: incident@cert-in.org.in

Key ID: 0x9E346D2C

Fingerprint: 4871 0429 EB42 0423 4E6A FAD6 B2D5 5C16 9E34 6D2C

User ID: info@cert-in.org.in

advisory@cert-in.org.in

Key ID: 0x2D85A787

Fingerprint: D1F0 6048 20A9 56B9 5DAA 02A8 0798 04C3 2D85 A787