Annual Report
(2013)

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

31st March, 2014

Indian Computer Emergency Response Team (CERT-In)

1.0 About CERT-In:

1.1 Introduction

CERT-In is a functional organisation of Department of Electronics and 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 is operational since January, 2004. The constituency of CERT-In is the Indian cyber community. CERT-In works closely with the Chief Information Security Officers (CISOs) and System Administrators of various sectoral and organisational networks of its constituency.

1.1.2 Workforce power

CERT-In has a team of 75 technical members.

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. In addition, CERT-In provides services to the individuals and home users also.

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 2013 is given in the following table:

Activities	Year 2013
Security Incidents handled	**71780**
Security Alerts issued	**12**
Advisories Published	**92**
Vulnerability Notes Published	**223**
Trainings Organized	**25**
Indian Website Defacements tracked	**24216**
Open Proxy Servers tracked	**2224**
Bot Infected Systems tracked	**7457024**

Table 1. CERT-In Activities during year 2013

2.2 Abuse Statistics

In the year 2013, CERT-In handled more than 71000 incidents. The types of incidents handled were mostly of Spam, Website intrusion & malware propagation, Malicious Code, Phishing 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**	**2012**	**2013**
Phishing	3	101	339	392	604	374	508	674	887	955
Network Scanning / Probing	11	40	177	223	265	303	277	1748	2866	3239
Virus / Malicious Code	5	95	19	358	408	596	2817	2765	3149	4160
Spam	-	-	-	-	305	285	181	2480	8150	54677
Website Intrusion & Malware Propagation	-	-	-	-	835	6548	6344	4394	4591	5265
Others	4	18	17	264	148	160	188	1240	2417	3484
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**	**22060**	**71780**

Table 2. Year-wise summary of Security Incidents handled

2.3 Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends during the year 2013 are as follows:

- **Website Intrusion and Malware Propagations**

  These are website intrusions and drive-by-download attacks through compromised websites. Around 4265 malicious URLs were tracked in the ".in" space. The legitimate web sites which are compromised resulting in redirection of visitors to malicious websites that exploit vulnerabilities in client side applications to deliver malware such as key loggers and information stealers. The malicious websites comprise attack tool kits such as blackhole, RedKit, Nuclear, Darkleech etc. The malicious code on the exploit kits included shellcode and Java scripts besides exploits for vulnerabilities in Internet Explorer, Java SE/SDK, Adobe Flash, Silverlight etc.

- **Vulnerabilites and Malware affecting Android mobile devices**

  Critical vulnerabilities were reported in Android based systems such as "Master key vulnerability", "PRNG initialization vulnerability" etc. Exploitation of master key vulnerability enables attackers to bypass verification process to install malicious files on the affected device.

  The malware affecting Androd mobile platform rose exponentially. Android.Adrd is a trojan horse that arrives bundled with legitimate Android applications and infects Android based smart phones. The malware seems to be created by downloading an application from a marketplace, modifying the legitimate application and then redistributing via marketplace or other separate channels. The Trojan may change mobile device settings and steal device information. Other prominent Android malware reported are Superclean/DroidCleaner, USB cleaver etc.

- **Trojan.Cryptolocker**

  Trojan Cryptolocker is spreading via malicious hyperlinks shared via spam emails, social media, malicious email attachments (fake FedEx and UPS tracking notices), drive-by-download or as a part of dropped file from other malwares. Cryptolocker encrypts files located within local drives, shared network drives, USB drives, external hard drives, network file shares and even some cloud storage drives using RSA public-key cryptography (2048-bit), with the private key stored only on the malware's control servers.

- **ZeroAccess Botnet**

  Win32/Sirefef a.k.a "Zero Access" is a widespread multi-component malware family of rootkits which is affecting the windows operating systems. The threat spreads majorly by exploit kits, use of pirated softwares and other malware downloaders. It uses disk-level hooking to hide itself (hide processes, related files, network activites,) in order to hinder its detection and removal on infected computer. Large number of infected systems are tracked and notifications issued to concerned Internet Service Providers.

- **DDoS attack trends**

  Multiple websites in the Government and Corporate sectors were targeted with Distributed Denial of Service attacks during 2013. It has been observed that vulnerabilities in Content Management Systems (Joomla!, Wordpress, etc.) are being exploited and attack scripts are embedded on compromised websites/servers which utilizes resources of web servers to launch Distributed Denial of Services attacks.

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 24216 numbers of defacements have been tracked. Most of the defacements were under '.in' domain, in which a total 15490 '.in' domain websites were defaced.

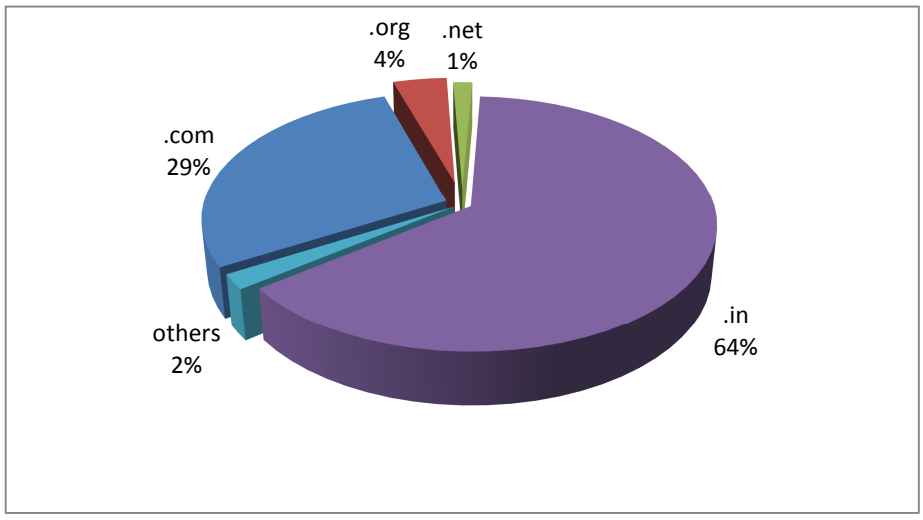

Figure 2. Indian websites defaced during 2013 (Top Level Domains)

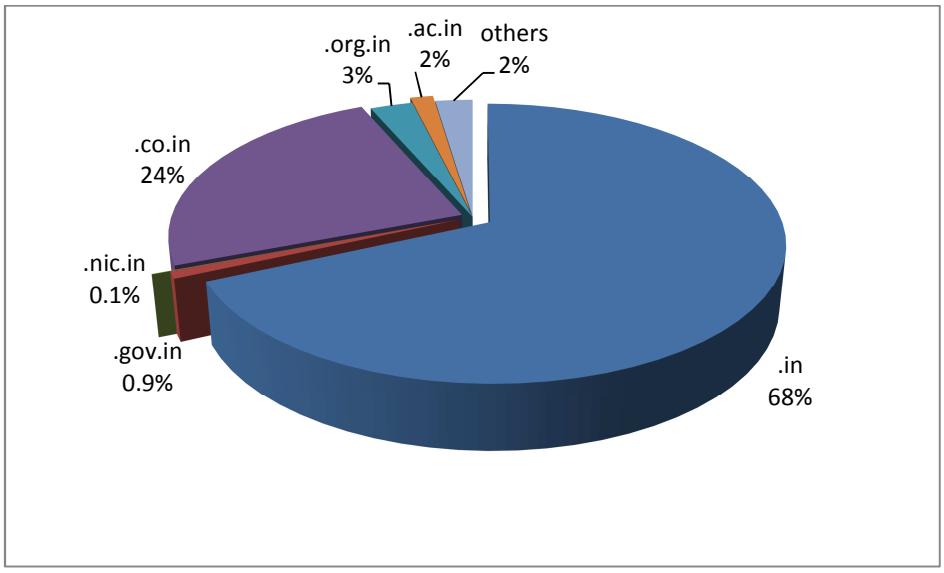

Figure 2.1 .in ccTLD defacements during 2013

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 2224 open proxy servers were tracked in the year 2013. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

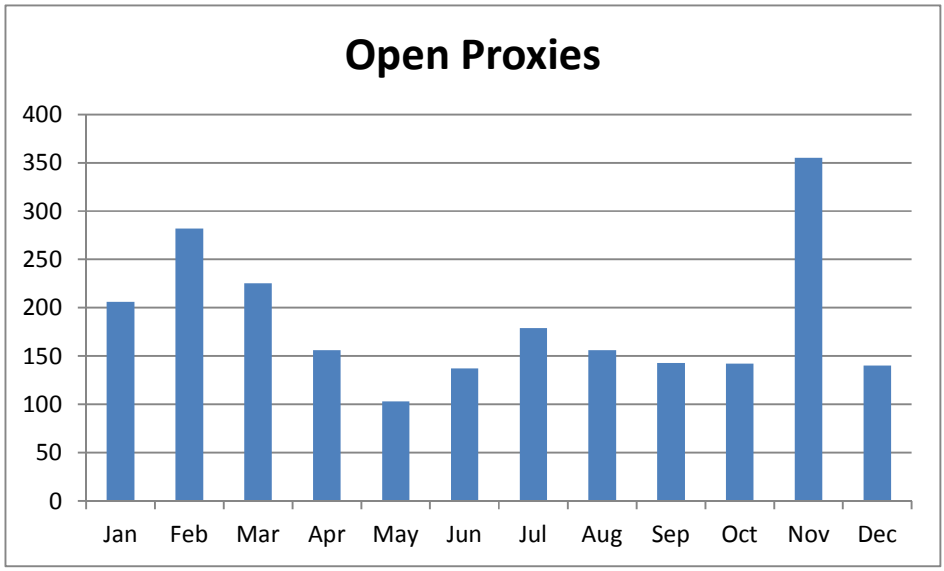

Figure 3. Monthly statistics of Open Proxy Servers in 2013

2.6 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of systems that are part of Botnet, actions are being taken to notify concerned users in coordination with the Internet Service Providers and advise them to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems tracked in 2013.

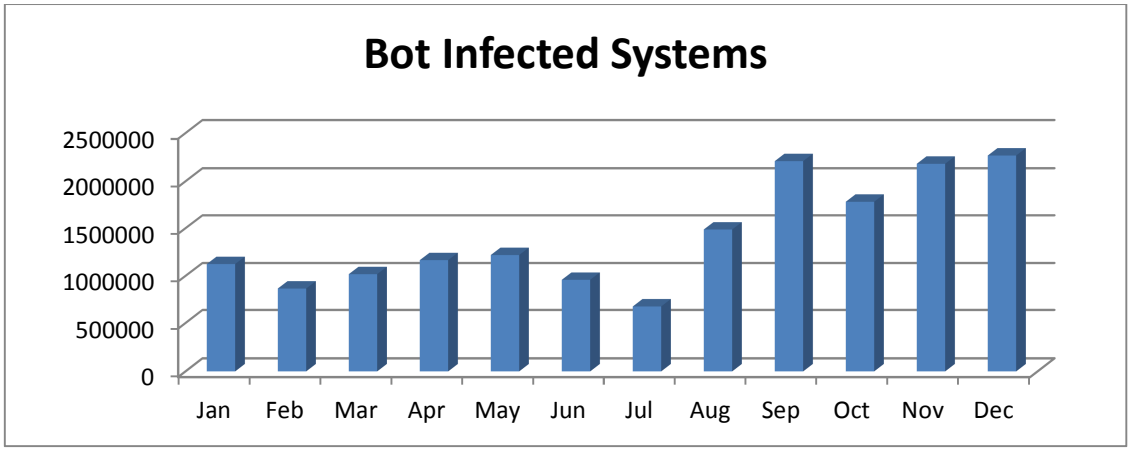

Figure 4. Botnet statistics in 2013

2.7 Collaborative Incident resolution

During the year 2013, CERT-In worked in collaboration with security/product vendors and Internet Service Providers in India to detect the botnet infected systems by tracking the Command & Control servers. Botnets such as Bamital, Citadel and ZeroAccess were tracked through collaborative actions.

2.8 Interaction with Sectoral CERTs

CERT-In plays the role of mother CERT and is regularly interacting with the Chief Information Security Officers (CISOs) 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 has provisionally empanelled 22 information security auditing organizations, subject to background verification and clearance of organizations, under the revised process of empanelment for the block 2012-2015, to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and

critical sector organizations. The technical competency of the empanelled organizations is regularly reviewed by CERT-In with the help of in-house designed practical skill tests.

2.10 Network Traffic Scanning for early warning

CERT-In has set up a facility to gather useful network information from different IT networks across the country for meaningful analysis to detect and predict possibilities of cyber attacks. At present, some organizations are voluntarily providing network traffic information to CERT-In for proactive scanning of their networks. This facility is meant only to scan the network traffic data header information and no content data is either captured or scanned. CERT-In is analyzing this network traffic information for providing immediate alerts, tailored advisories to the participating organizations.

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 2013:

- Workshop on "Data Centre Security " on January 11, 2013
- Workshop on "Linux Security" on January 24, 2013
- Workshop on "Introduction to Cyber Security and Cyber Forensics" on February 18, 2013
- Workshop on "Network Security" on February 22, 2013
- Workshop on "Web Application Security: Current trends" on March 07, 2013
- Workshop on "Mobile Forensics" on March 22, 2013
- Workshop on "Advanced Web Application Security " on April 29, 2013
- Workshop on "Introduction to Cyber Security & Crisis Management Plan(CMP) " on April 30, 2013
- Workshop on "Network Security : Perimeter Defence in Depth" on May 24, 2013
- Workshop on "Virtualisation & Cloud Security " on May 31, 2013
- Workshop on "Cyber Crime Investigation & Cyber Forensics" on June 14, 2013
- Workshop on "Vulnerability Assessment & Penetration Testing " on June 18, 2013
- Workshop on "Cyber Espionage, Infiltration and Combating Techniques" on July 11, 2013
- Workshop on "Windows 8 Security " on August 12, 2013

- Workshop on "Information Security Compliance, Assurance and Crisis Management Plan" on August 27, 2013
- Workshop on "Latest Security Trends " on September 24, 2013
- Workshop on "Cyber Security: Threats & Mitigation" on September 30, 2013
- Workshop on "Cyber Security and Cyber Forensics" on October 14, 2013
- Workshop on "Network Penetration Testing" on October 25, 2013
- Workshop on "Wireless Network Security" on October 31, 2013
- Workshop on "Advanced Persistent Threats" on November 12, 2013
- Workshop on "Cyber Security Policy and Crisis Management Plan" on November 22, 2013
- Workshop on "Advanced Computer Forensics" on December 05, 2013

3.2 Cyber Security Drills

CERT-In successfully participated in the APCERT Incident Handling drill conducted in January 2013 and ASEAN CERTs Incident Handling Drill (ACID 2013) held in October 2013.

Indian Computer Emergency Response Team is carrying out mock drills with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. These drills have helped tremendously in improving the cyber security posture of the information infrastructure and training of manpower to handle cyber 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 8 Cyber security drills of different complexities with 115 organizations covering various sectors of Indian economy i.e. Finance, Defence, Space, Atomic Energy, Telecom/ISP, Transport, Power, Petroleum & Natural Gas, and IT / ITeS / BPO industry. 8th Cyber Security Drill Mock Drill was conducted on 20th December 2013. This time, cyber security drill involved simulated cyber attacks as well as simulated cyber crisis scenarios.

4.0 Achievements

4.1 Publications

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.

Security Tips: Security tips for general users advising best practices to secure Mobile Devices, USB storage, Broadband routers, Desktops etc and secure usage of credit/debit cards online, preventive steps against phishing attacks were published.

4.2 Cyber Security Assurance initiatives

- **National Cyber Security Policy-2013(NCSP-2013)** was released by Government in August 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.
- Government and critical sector organizations are implementing the security best practices in accordance with ISO 27001 standard and as per the advice issued by CERT-In. So far, 9 implementation enabling workshops have been conducted. Services of CERT-In empanelled IT security auditors are being used to verify compliance.
- 21 auditors were empanelled for audit of IT infrastructure after a fresh round of skill assessment in the year 2013, in addition to existing 22 auditors.
- CERT-In has also carried out security audits of some of the organizations in the critical sector.

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).
- Collaborating with overseas CERTs such as US-CERT, for information exchange and Joint cyber exercises.
- MoU is being signed with KISA to enable information sharing and collaboration for incident resolution.

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. The future plans envisaged are:

- Creation of a framework for comprehensive, collaborative and collective response to deal with the issue of cyber security at all levels within the country
- Promotion of R&D activities in the areas of attack detection & prevention, Cyber Forensics and malware detection & prevention.
- 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
- Creation of framework and facility for collection, correlation and analysis of security events in real time and generating early warning to constituency.
- Creation of facilities to detect and clean the Botnet infected systems in coordination with Industry

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