Annual Report
(2012)

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

1st March, 2013

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 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 2012 is given in the following table:

Activities	Year 2012
Security Incidents handled	**22060**
Security Alerts issued	**10**
Advisories Published	**56**
Vulnerability Notes Published	**122**
Security Guidelines Published	**1**
White papers/Case Studies Published	**5**
Trainings Organized	**26**
Indian Website Defacements tracked	**23014**
Open Proxy Servers tracked	**2759**
Bot Infected Systems tracked	**6494717**

Table 1. CERT-In Activities during year 2012

2.2 Abuse Statistics

In the year 2012, CERT-In handled more than 22000 incidents. The types of incidents handled were mostly of Spam, Website compromise & 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
Phishing	3	101	339	392	604	374	508	674	887
Network Scanning / Probing	11	40	177	223	265	303	277	1748	2866
Virus / Malicious Code	5	95	19	358	408	596	2817	2765	3149
Spam	-	-	-	-	305	285	181	2480	8150
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344	4394	4591
Others	4	18	17	264	148	160	188	1240	2417
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**	**13301**	**22060**

Table 2. Year-wise summary of Security Incidents handled

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

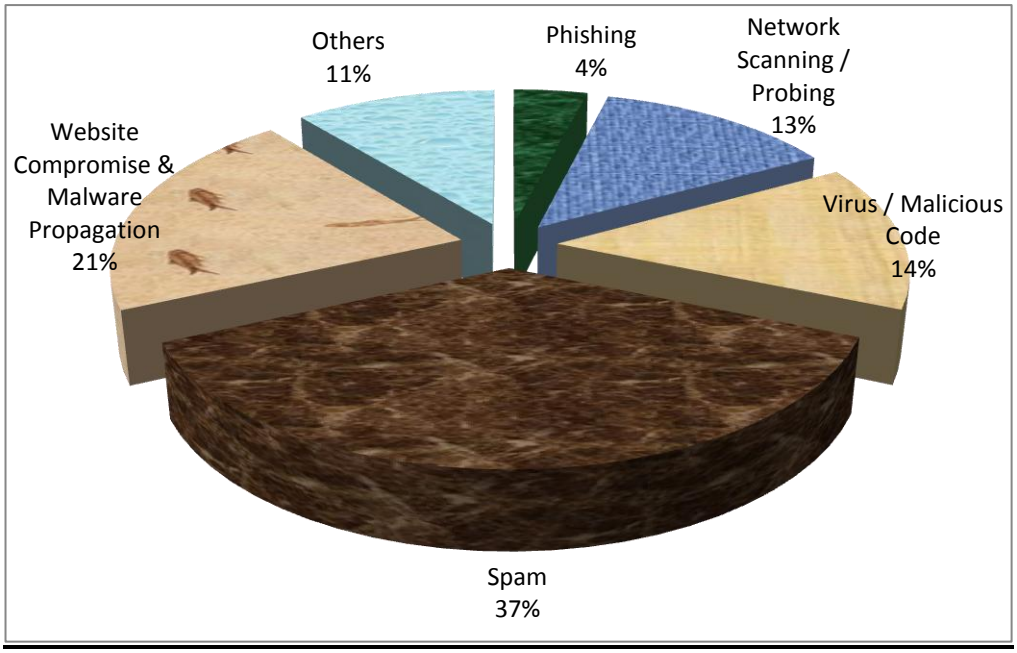

***Figure 1*. Summary of incidents handled by CERT-In during 2012**

2.3 Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends during the year 2012 are as follows:

- **Website compromise and Malware Propagations**

  These are website intrusions and drive-by-download attacks through compromised websites. Around 4591 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 end-systems to deliver malware such as key loggers and information stealers. The attackers targeted web browser plug-ins lavishly to deliver malicious contents. The code injected into the websites are heavily obfuscated and polymorphic making them harder to detect.

- **Surge of Exploit Kits**

  Significant increase in the exploit tool kits were observed in this year. An exploit kit/ exploit pack, is a toolkit that facilitates the automation of client-side vulnerability exploitation. The modus operandi normally revolves around targeting browsers and programs that a website can invoke through the browser. The exploit kits are typically concealed with client side software vulnerabilities in Adobe reader, JRE, Adobe flash Player, Media Players etc.(non-exhaustive list).

- **Persistent and complex PC malware**

  The major and notable malware families observed were Autorun, dorkbot, Nitol, Ramnit, Sality(new variants), Vobfus, Win32/CplLnk , Conficker, Rimecud,

- **Information and Banking Trojans - New trends and methods in the arsenal**

  The most notable information stealer Trojans were Zeus and Spyeye, which among other capacities, are able to inject code onto the webpages returned from the banking sites and also having immense stealth mechanisms. Three derivates of Zeus have been reported such as Citadel, Ice IX, P2P version. Additionally threats into the banking malware family, Carberp and Tinba were observed.

- **DNS Changer**

  The malware initially infects the Windows or Apple computers and subsequently gain access to routers connected to those systems to exploit weakness like default factory

configurations, easily guessable passwords etc. Once exploited or accessed, changes the DNS settings in the said computers and devices and make them point to rouge foreign DNS servers, which are forced to connect to the rogue network rather than to legitimate Internet Service Providers (ISPs). Users surfing the Web on infected computers would be redirected from legitimate sites to fraudulent or malicious ones.

- **Mobile malware and Mobile Botnets**

  Malware trends indicate that malware affecting mobile platforms largely Android was on the rise due to the high prevalence of Android enabled mobile devices. The android malware families prevalent were Opfake, Android Kungfu, Plangton, FakeInst, SMSreg, GAMEX, RootSmart, Lotoor capable of performing premium based texting/subscribe the user to expensive services, install backdoors, exfiltrated confidential data, reading and intercepting SMSs and send it to remote servers and wait for the command from cybercriminals and effectively becoming part of botnets.

- **Mobile Botnets**

  Botnet that targets mobile devices such as smart phones, attempting to gain complete access to the device and its contents as well as providing control to the botnet creator. Mobile botnets take advantage of unpatched exploits to provide hackers with root permissions over the compromised mobile device, enabling hackers to send e-mail or text messages, make phone calls, access contacts and photos, and more. Most mobile botnets go undetected and are able to spread by sending copies of themselves from compromised devices to other devices via text messages or e-mail messages.

- **Malicious Spam and identity theft schemes were leveraging Social networking sites**.

  Several campaigns hit the deck spreading virally such as clickjacking, LIKE jacking. Additionally series of malware attacks creates pandemonium on the SNS sites such as My Webcam Thingy (Twitter), FireFoxed (click jacking intrusions), Dislike Scam(Facebook), Over The rainbow(Twitter).

- **Distributed Denial of Service (DDoS) Attacks**

  A no. of websites in the Government and Corporate sectors were targeted with Distributed Denial of Service attacks during May - June, 2012. These attacks were carried out by the well known hacktivist group 'Anonymous'.

- **Other Trends observed in 2012**

CERT-In has observed that Content Management System vulnerabilities(especially Joomla! and Wordpress) were widely getting exploited for Wesbsite Defacements and launching Distributed Denial of Services attacks. Sophisticated tools(web versions also) capable of launching flood attacks have been used for Denial of Service attacks against Govt., Financial and private sector organizations. There has been a rise in the spamming incidents targeting genuine users for financial frauds.

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 23014 numbers of defacements have been tracked. Most of the defacements were under '.in' domain, in which a total 11304 '.in' domain websites were defaced.

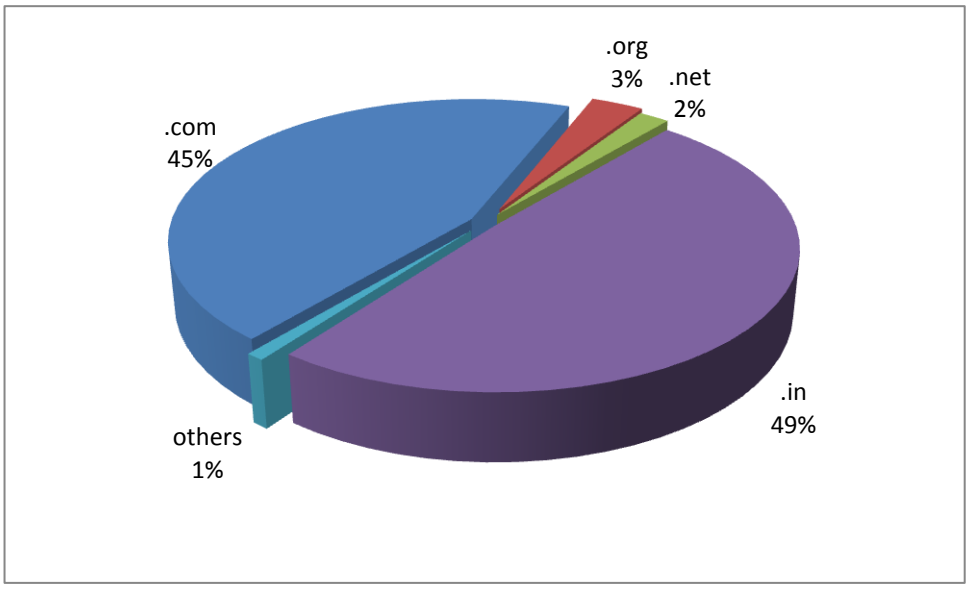

Figure 2. Indian websites defaced during 2012 (Top Level Domains)

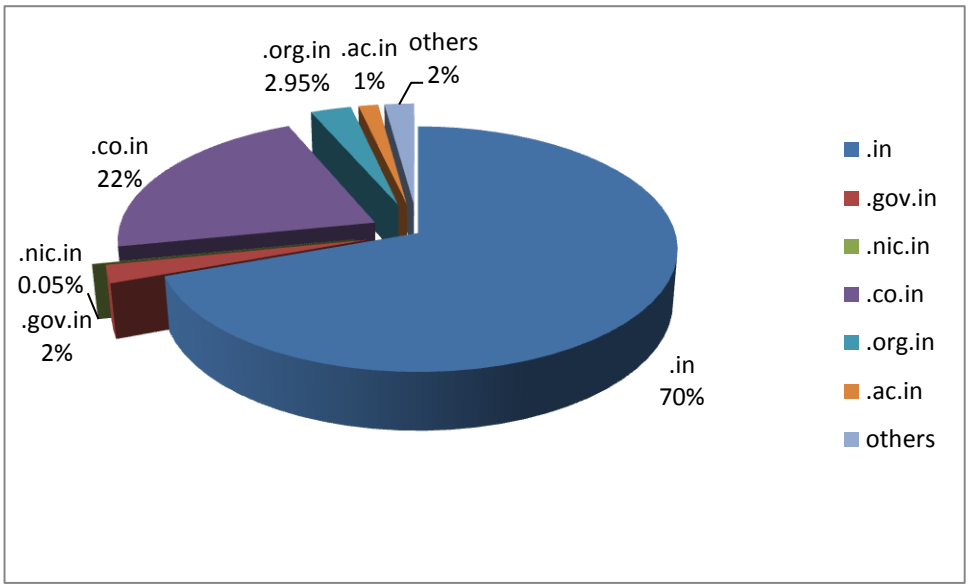

Figure 2.1 .in ccTLD defacements during 2012

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 2759 open proxy servers were tracked in the year 2012. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

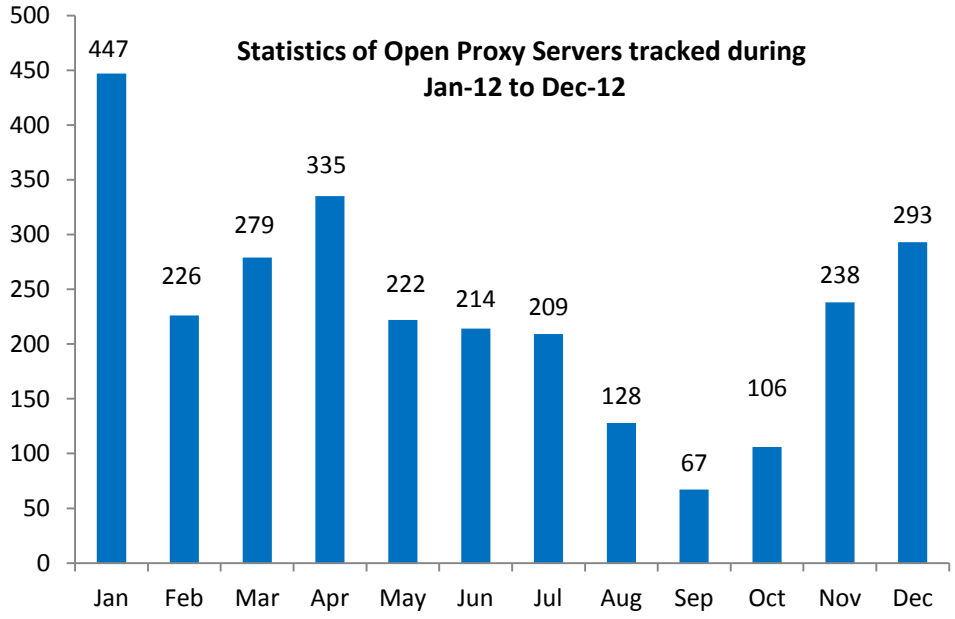

Figure 3. Monthly statistics of Open Proxy Servers in 2012

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 2012.

Month	Number of Bot Infected Systems	C&C Servers
January	977043	3
February	809164	1
March	835255	6
April	725003	4
May	779566	5
June	555274	5
July	485776	2
August	705660	1
September	1234512	5
October	1261631	4
November	3188652	6
December	2907292	6

Figure 4. Botnet statistics in 2012

2.7 Collaborative Incident resolution

During the year 2012, CERT-In worked in collaboration with Microsoft and Internet Service Providers in India to detect and clean the botnet infected systems, specifically the ZeuS variants and Nitol Botnet. The outcome was very encouraging.

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.

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 2012:

- Workshop on "Identity and Access Management" on January 06, 2012
- Workshop on "Network Perimeter Defence in Depth" on January 20, 2012
- Workshop on "Linux Security" on February 03, 2012
- Workshop on "Current Security Trends" on February 09, 2012
- Workshop on "Intrusion Detection in Depth" on March 02, 2012
- Workshop on "Mobile Forensics" on March 23, 2012
- Workshop on "Cyber crime & Computer Forensics" on April 26, 2012
- Workshop on "Network Penetration Testing" on April 30, 2012
- Workshop on "Cyber Espionage, Infiltration & Combating techniques" on May 09, 2012
- Workshop on "Information Security for Railway officers" on May 14, 2012
- Workshop on " IPv6 Essentials, Implementation and Security" on June 11, 2012
- Workshop on "Virtualization & Cloud Security" on July 18, 2012

- Workshop on "Cyber Forensics" on July 19, 2012
- Workshop on "Web Application Security & Penetration Testing Basics" on July 31, 2012
- Workshop on "Securing Critical Information Infrastructure" on August 06, 2012
- Workshop on "Advanced Information Security" on August 24, 2012
- Workshop on "DDoS Attacks & Mitigation" on August 28, 2012
- Workshop on "Threat & Vulnerability Management" on September 21, 2012
- Workshop on "Windows Security" on September 28, 2012
- Workshop on "Wireless Security" on October 17, 2012
- Workshop on "Advanced Application Security" on October 30, 2012
- Workshop on "Information Security Policy, Compliance and Auditing" on November 09, 2012
- Workshop on "MS SQL Database Security" on November 27, 2012
- Workshop on "ORACLE Database Security" on December 07, 2012
- Workshop on "MySQL Database Security" on December 14, 2012

3.2 Cyber Security Drills

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

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 7 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. 7th Cyber Security Drill Mock Drill was conducted on 19th and 20th December 2012. This time, cyber security drill involved simulated cyber attacks as well as simulated cyber crisis scenarios.

4.0 Achievements

4.1 Publications

The following were published by CERT-In in the year 2012:

1. **Enterprise Wireless Fidelity Implementations Using Port Based Network Access Control (IEEE 802.1X)** - International Journal of Computer Science and Telecommunications [Volume 3, Issue 7, July 2012] - Noorul Ameen, Vincy Salam and Anil Sagar
2. **Integrated approach to prevent SQL injection attack and reflected cross site scripting attack**, International Journal of System Assurance Engineering and Management, December 2012, Volume 3, Issue 4, pp 343-351 - Pankaj Sharma, Rahul Johari, S. S. Sarma,
3. **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.

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).

India-US Joint Cyber Security Exercise (CSE) was conducted for first time between CERT-In, India and National Cyber Security Division (NCSD), Department of Homeland Security(DHS), USA on 11th, 12th and 17th September 2012 in order to build increased operational collaboration between CERTs as part of the MoU. Indian Computer Emergency Response Team (CERT-In), United States Computer Emergency Response Team (US-CERT) and Industrial Control CERT-US (ICS-CERT) were the participants of Joint CSE. The exercise was appreciated highly by both sides to build a workable path forward for joint cyber security cooperation between USA and India.

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.

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