CERT-In Annual Report (2014)

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

27 February, 2015

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 2014 is given in the following table:

Activities	Year 2014
Security Incidents handled	**130338**
Security Alerts issued	**13**
Advisories Published	**69**
Vulnerability Notes Published	**290**
Trainings Organized	**22**
Indian Website Defacements tracked	**25037**
Open Proxy Servers tracked	**2408**
Bot Infected Systems tracked	**7728408**

Table 1. CERT-In Activities during year 2014

2.2 Abuse Statistics

In the year 2014, CERT-In handled more than 1,30,000 incidents. The types of incidents handled were mostly of Spam, Website intrusion & malware propagation, Malicious Code, Phishing and Network Scanning & Probing.

The summary of various types of incidents handled is given below:

Security Incidents	2014
Phishing	1122
Network Scanning / Probing	3317
Virus/ Malicious Code	4307
Website Defacements	25037
Spam	85659
Website Intrusion & Malware Propagation	7286
Others	3610
Total	130338

Table 2. Breakup of Security Incidents handled

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

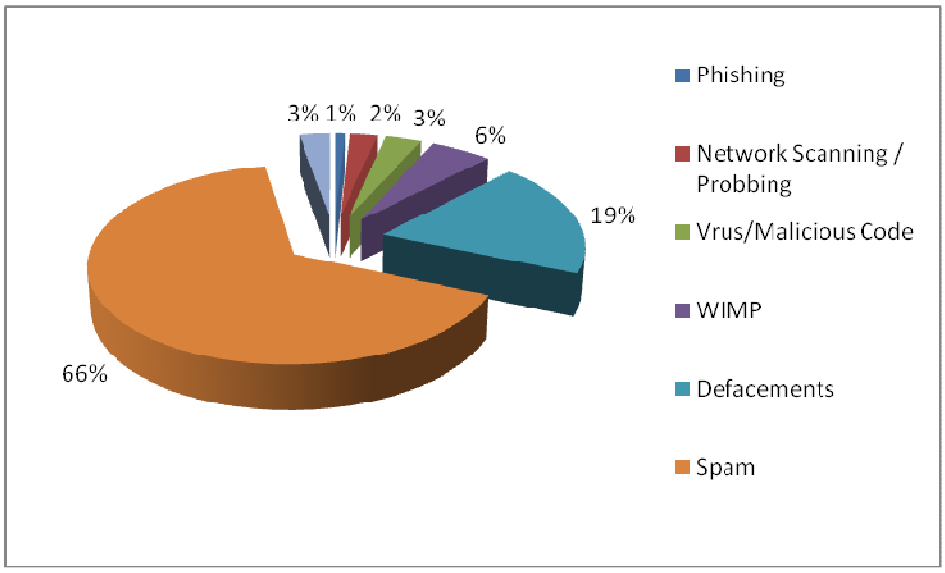

***Figure 1*. Summary of incidents handled by CERT-In during 2014**

2.3 Incident Trends

The trends of incidents reported to and handled by CERT-In and cyber attack trends during the year 2014 are as follows:

- **Exploitation of Drupal Vulnerability in the wild**

  It has been observed that Drupal SQL Injection vulnerability exploitation was wild on the month of October 2014. This vulnerability exists due to insufficient sanitization of data by the database abstraction API. A remote attacker could exploit this vulnerability by sending specially crafted requests, resulting in execution of arbitrary SQL commands. Successful exploitation of this vulnerability could cause attacker to view, add, modify or delete information in the back-end database.

- **D4re|Dev|targeting Mass transit systems and E-Kiosks**

  It has been reported that a new point of sale systems malware, dubbed "D4re|Dev" a.k.a "DareDevil" targeting Mass transit systems is spreading. The malware mainly infect the machines used as public transport ticket vending machines or the interactive Kiosks. The attacker may gain the initial access due to the inadequate internal security policies such as weak passwords along with the use of the POS systems for other activities including web surfing, email accessing, games, accessing social networking sites etc. Once an initial access is gained, then attacker can upload other backdoors using the malware's "Remote File Upload "functionality. These backdoors run under the processes named "hkcmd.exe", "PGTerm.exe" and other legitimate processes of Google Chrome in order to bypass security restrictions and remain undetected. Successful compromise of the infected system gives full access of the infected system to the remote attacker.

- **Havex Malware targeting ICS/SCADA control systems**

  It has been reported that an industrial information stealing malware, dubbed Havex, is targeting ICS based systems by leveraging OPC protocol implementation. OPC is OLE for communication / Open platform communication - a standard for windows applications to communicate to process control hardware and transfer process data between systems from different vendor. The malware reported as performing intelligence gathering by mapping network resources and connected devices information from the

process control network. The HAVEX RAT is reaches the machine via social engineering methods, website redirects, exploit kits or by watering hole.

- **Gameover aka Zeus-P2P malware surge**

  It has been reported that "GameOver" malware aka Zeus-P2P is surging with new tactics techniques and procedures (TTP). GameOver malware is the incarnation of the information stealing banking malware Zeus/ Zbot imbibed with Peer-2-Peer capabilities to communicate with the C2 server, majorly distributed through Cutwail spam bot. The malicious mails used social engineering techniques by impersonating financial institutions and government agencies, with a ".zip" file attached, the compressed archive contains an application titled UPATRE. The application UPATRE is used to download the encrypted file (to evade from perimeter defenses) from compromised websites and decrypt it to extract and execute the GameOver.

- Malware targeting Point of Sale (POS) systems were on the raise. Prominent POS malware reported are Dexter, BrutPOS, BackOff etc.

- Malicous apps affecting the Android Mobile phones are also reported during the year 2014. The android malware families prevalent were OpFake, Android/FakeInst, Android SmsSend, Badaccents etc. Such malicious Apps are capable of performing premium based texting / subscribe the user to expensive services, install backdoors, reading and intercepting SMS'es and send it to remote servers.

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 25037 numbers of defacements have been tracked.

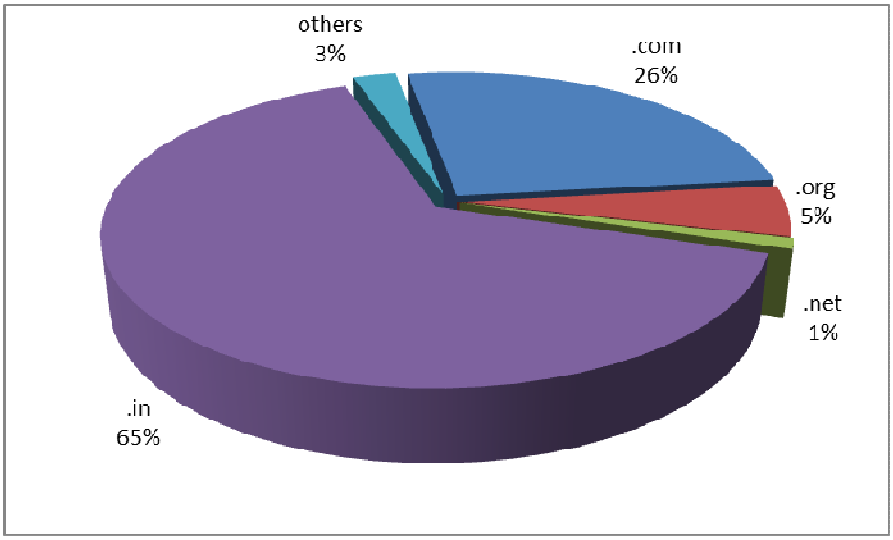

Figure 2 Indian websites defaced during 2014

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 2408 open proxy servers were tracked in the year 2014. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

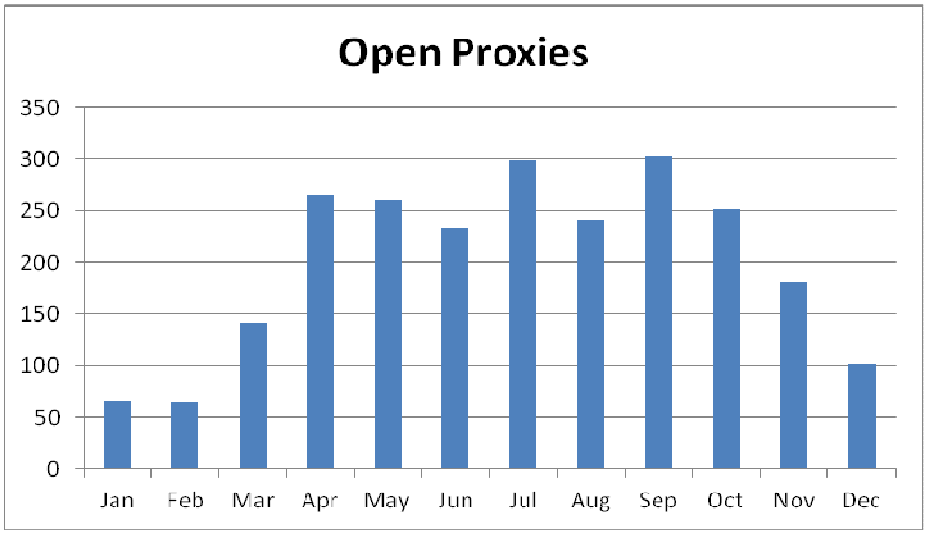

Figure 3. Monthly statistics of Open Proxy Servers in 2014

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 2014.

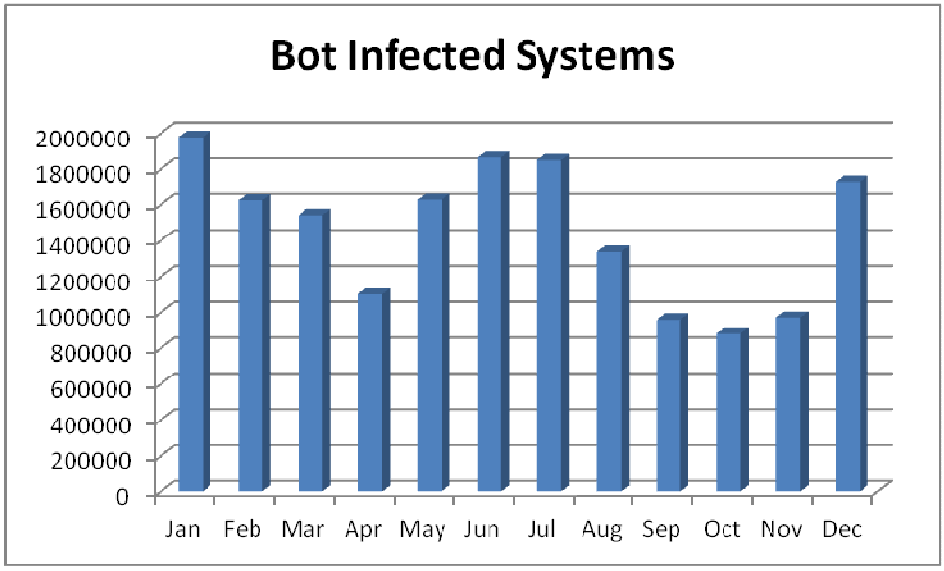

Figure 4. Botnet statistics in 2014

2.7 Collaborative Incident resolution

During the year 2014, CERT-In worked in collaboration with security/product vendors and Internet Service Providers in India to detect the botnet infected systems. Botnets such as Baldabindi, Jenxcus and Gameover/ZeuS P2P 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 45 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 2014:

- Workshop on "Web Application Security" on January 13, 2014
- Workshop on "Linux security" on January 24, 2014
- Workshop on "Critical Infrastructure Security Risk & Compliance" on February 20, 2014
- Workshop on "Data Centre Security" on February 21, 2014
- Workshop on "Cyber Security Threats and Cyber Security Policy" on February 26, 2014
- Workshop on "Cyber Security Threats, Cyber Crime and Cyber Forensics" on March 07, 2014
- Workshop on "Mobile Forensics" on April 16, 2014
- Workshop on "Advanced Web Application Security" on April 21, 2014
- Workshop on "Secure Cloud Computing" on May 30, 2014
- Workshop on "Vulnerability Assessment & Penetration Testing" on June 20, 2014
- Workshop on "Cyber Crime Investigations and Cyber Security Policy" on June 27, 2014
- Workshop on "Targeted Attacks - Trends & Mitigation" on July 25, 2014
- Workshop on "Big Data Analytics & Security" on August 14, 2014
- Workshop on "Windows 8 Security" on August 22, 2014

- Workshop on "Latest Security Trends" on August 27, 2014
- Workshop on "Cyber Security: Threats & Mitigations" on September 17, 2014
- Workshop on "Cyber Security Threats and Cyber Security Policy" on October 15, 2014
- Workshop on "Network Security" on October 17, 2014
- Workshop on "Mobile Forensics" on November 14, 2014
- Workshop on "Wireless Security" on November 26, 2014
- Workshop on "Cyber Security Threats: Advanced Detection & Prevention Techniques" on December 03, 2014
- Workshop on "MS SQL Database Security" on December 17, 2014

3.2 Cyber Security Drills

CERT-In successfully participated in the ASEAN CERTs Incident Handling Drill (ACID 2014) held in September 2014. 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 9 Cyber security drills of different complexities with 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. 9th Cyber Security Mock Drill was conducted on 23rd December 2014.

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.

Summary of Website Defacements depicting break-up of the websites defaced, top defacers and vulnerabilities and suggestions on best practices to secure web applications and web servers is published and circulated to all CISOs on monthly basis.

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, 10 implementation enabling workshops/interactions have been conducted. Services of CERT-In empanelled IT security auditors are being used to verify compliance.
- 45 auditors were empanelled for audit of IT infrastructure after a fresh round of skill assessment in the year 2014.
- 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.
- CERT-In signed a MoU with Korea Internet & Security Agency (KISA) in January, 2014 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