CERT-In Annual Report (2015)

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

25 February, 2016

Indian Computer Emergency Response Team (CERT-In)

1. Highlights of 2015

1.1 Summary of major activities

a) In the year 2015, CERT-In handled 49,455 incidents. The types of incidents handled were Website Intrusion & Malware Propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements and Unauthorized Scanning activities. In addition, 61628 spam incidents were also reported to CERT-In. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

b) CERT-In is keeping track on latest cyber threats and vulnerabilities. 16 security alerts, 70 advisories and 316 Vulnerability Notes were issued during the year 2015

c) 25 Training programmes on specialized topics in the area of cyber security were organized for constituency

d) Around 9 million botnet infected systems tracked and notifications sent to Internet Service Providers along with remedial measures.

` 1.2 Achievements & milestones

- 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. 9 such mock drills have been conducted so far.

- CERT-In has initiated actions for setting up of "Botnet Cleaning and Malware Analysis Centre" to detect and enable cleaning of malware infected systems. The project is being implemented in coordination and collaboration with Internet Service Providers (ISPs) and Industry. This would help in enhancing the security of computer systems across the country.

- CERT-In signed a Cooperation Framework with CERT- Australia and MoUs with Cyber Security Malaysia, Singapore Computer Emergency Response Team (SingCERT) and JPCERT/CC, Japan to enable information sharing and collaboration for incident resolution.

2. About CERT-In:

2.1 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 designate d 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

2.2 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.

2.3 Resources

CERT-In has a team of 75 technical members.

2.4 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.

3. Activities and Operations of CERT-In

3.1 Scope and definitions:

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
- Security Quality management services in the form of cyber security audits, promotion of best practices and cyber security exercises/drills

3.2 Incident Handling Reports

The summary of activities carried out by CERT-In during the year 2015 is given in the following table:

Activities	Year 2015
Security Incidents handled	**49455**
Security Alerts issued	**16**
Advisories Published	**70**
Vulnerability Notes Published	**316**
Trainings Organized	**25**
Indian Website Defacements tracked	**26244**
Open Proxy Servers tracked	**1698**
Bot Infected Systems tracked	**9163288**

Table 1. CERT-In Activities during year 2015

3.3 Abuse Statistics

In the year 2015, CERT-In handled 49,455 incidents. The types of incidents handled were Website intrusion & Malware propagation, Malicious Code, Phishing, Distributed Denial of Service attacks, Website Defacements and Unauthorized Scanning activities. In addition, 61628 spam incidents were also reported to CERT-In.

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

Security Incidents	2015
Phishing	**534**
Network Scanning / Probing	**3673**
Virus/ Malicious Code	**9830**
Website Defacements	**26244**
Website Intrusion & Malware Propagation	**961**
Others	**8213**
Total	**49455**

Table 2. Breakup of Security Incidents handled

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

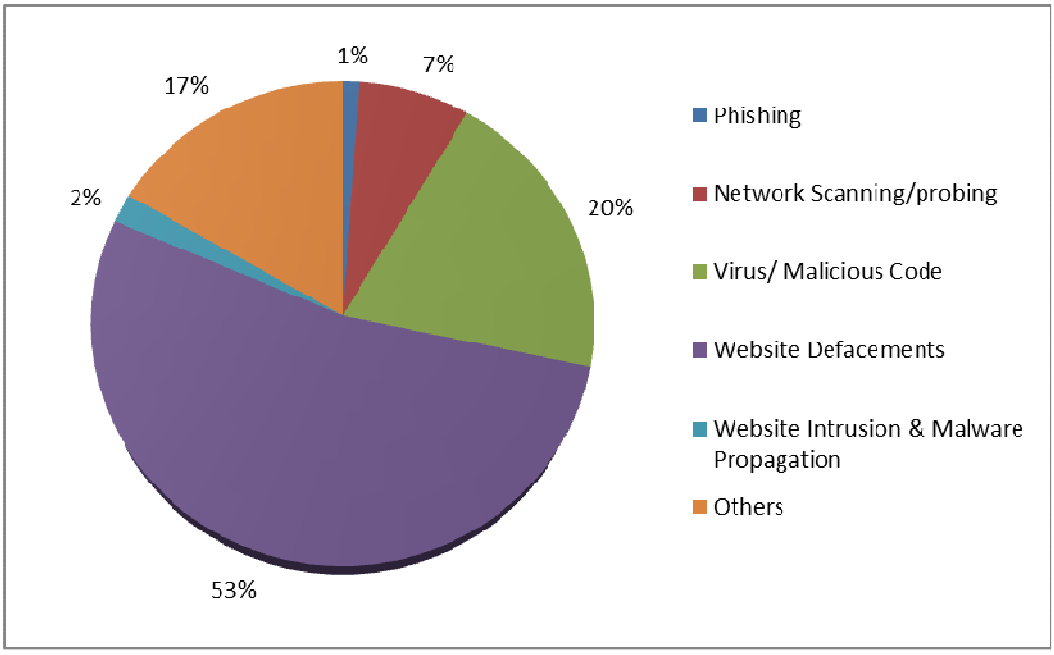
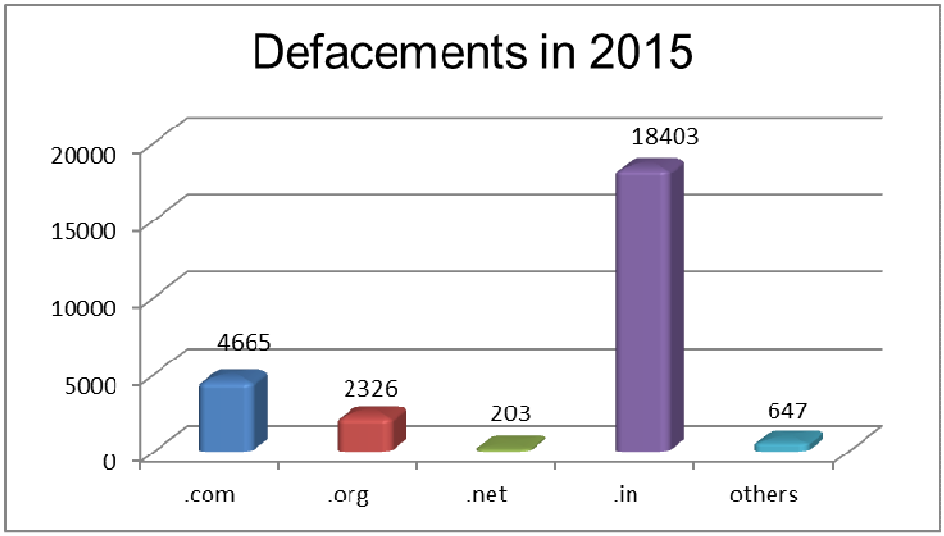


Figure 1. Summary of incidents handled by CERT-In during 2015

3.3.1 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 26244 numbers of defacements have been tracked.



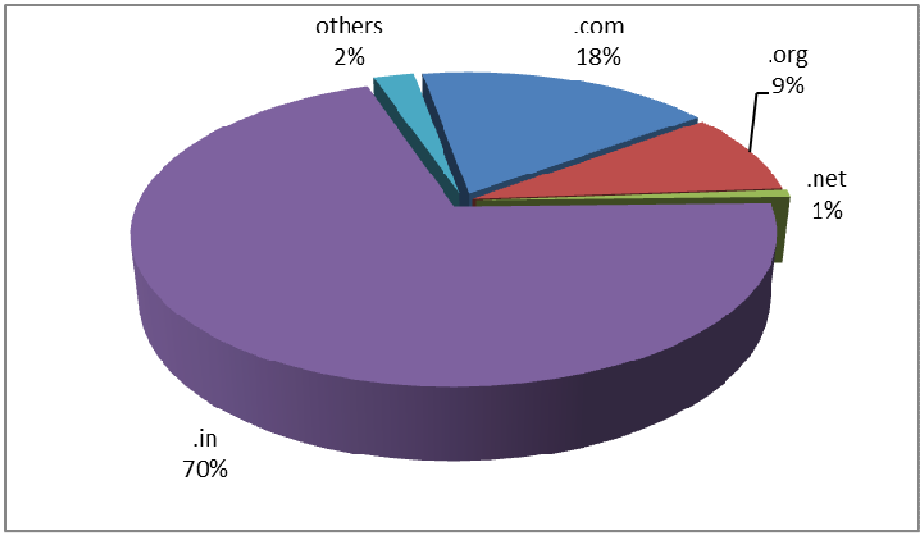


Figure 2 : Domain-wise Breakup of Indian Websites Defaced in 2015

3.3.2 Tracking of Open Proxy Servers

CERT-In is tracking 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 1698 open proxy servers were tracked in the year 2015. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

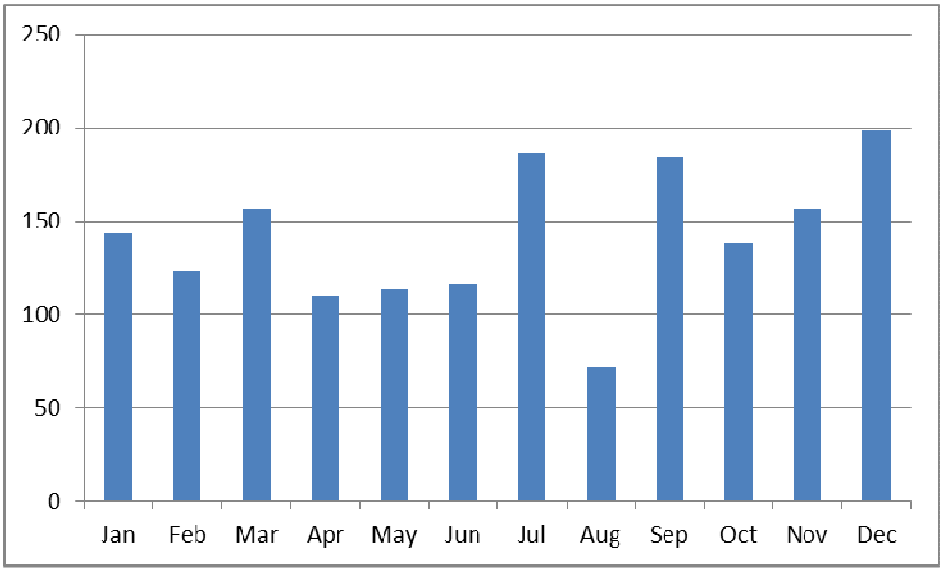


Figure 3. Monthly statistics of Open Proxy Servers in 2015

3.3.3 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 2015.

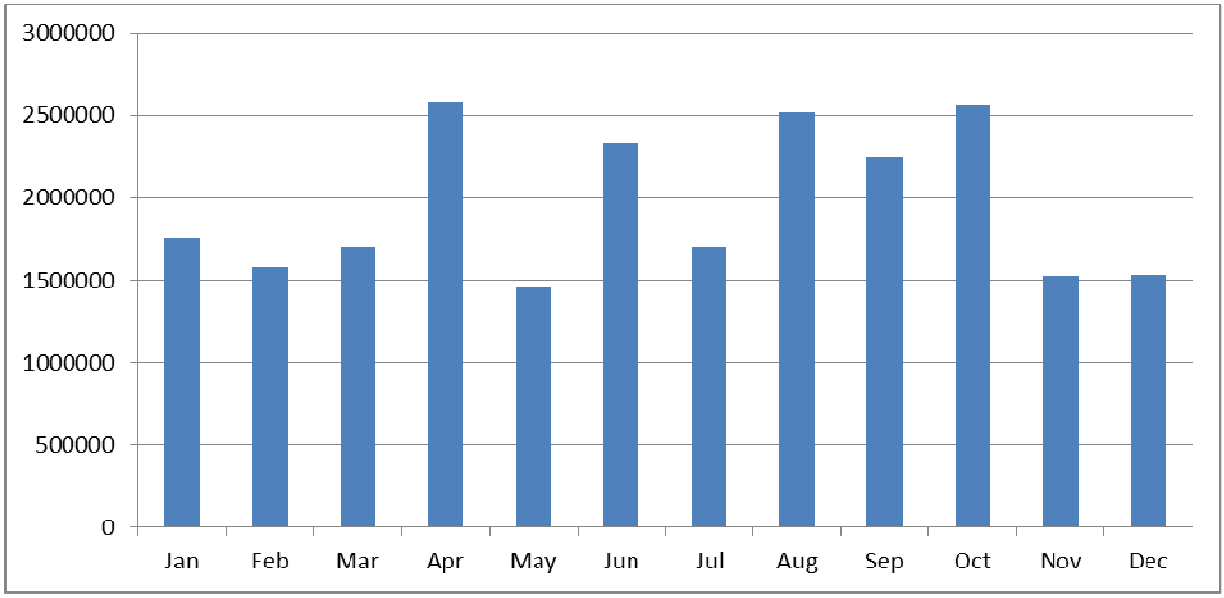


Figure 4. Botnet statistics in 2015

3.4 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.

3.5 New Services

3.5.1 Collaborative Incident resolution

During the year 2015, CERT-In worked in collaboration with security/product vendors and Internet Service Providers in India to detect the botnet infected systems. Botnets such as Sality, ZeroAccess and Dorkbot were tracked through collaborative actions.

3.5.2 Security Profiling, Assurance framework and Audit Services

- CERT-In has provisionally empanelled 57 information security auditing organizations, subject to background verification and clearance of organizations, under the revised process of empanelment for the block 2012-2016, 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.
- 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. Implementation enabling workshops/interactions have been conducted. Services of CERT-In empanelled IT security auditors are being used to verify compliance.
- CERT-In has also carried out episodic security audits of key organizations for enhancing their security posture

3.5.3 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.

4. Events organized/ co-organized

4.1 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 2015:

- Workshop on "Enterprise Architecture & Security" on January 16, 2015
- Workshop on "Endpoint Security" on January 22, 2015
- Workshop on "Trends in Endpoint Security" on January 23, 2015
- Workshop on "Linux Security" on February 09, 2015
- Workshop on "Cyber Crime & Cyber Forensics" on February 26, 2015
- Workshop on "Cyber Security Threats and Mitigation" on March 05, 2015
- Workshop on "Advanced Persistent Threats" on April 10, 2015
- Workshop on "Phishing Attacks and Countermeasures" on April 24, 2015
- Workshop on "Advanced Web Application Security" on May 22, 2015

- Workshop on "Big Data Analytics & Security" on June 25, 2015
- Workshop on "Cyber Security Threats and Countermeasures" on July 30, 2015
- Workshop on "Mobile Forensics" on July 03, 2015
- Workshop on "Cloud Security" on July 17, 2015
- Workshop on "Data Leakage Detection & Prevention" on July 30, 2015
- Workshop on "Advanced Threats Prevention" on August 07, 2015
- Workshop on "Network Security" on August 24, 2015
- Workshop on "Web Application Security" on September 30, 2015
- Workshop on "Auditing and Testing of Windows Active Directory & Domain Controller Environment" on October 16, 2015
- Workshop on "Crisis Management Plan, Compliance & Auditing" on October 26, 2015
- Workshop on "Cyber Security Threats and Mitigation" on November 04, 2015
- Workshop on "Vulnerability Assessment & Penetration Testing" on November 27, 2015
- Workshop on "Latest Cyber Security Threats & Mitigations" on December 11, 2015
- Workshop on "Mobile Security" on December 18, 2015
- Workshop on "Cyber Crime Investigations" on December 21, 2015
- Workshop on "Cyber Crime Investigations" on December 21, 2015

4.2 Drills and exercises

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. 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.

5.0 International collaboration

5.1 International Partnerships and agreements

- CERT-In signed a Cooperation Framework with CERT, Australia and MoUs with Cyber Security Malaysia, Singapore Computer Emergency Response Team (SingCERT) and JPCERT/CC, Japan to enable information sharing and collaboration for incident resolution.
- 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.

5.2 Drills & exercises

CERT-In successfully participated in the ASEAN CERTs Incident Handling Drill (ACID 2015) held in October 2015 and APCERT Drill in March 2015.

6.0 Future Plans

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:

- Setting up of mechanisms to generate necessary situational awareness of existing and potential cyber security threats and enable timely information sharing for proactive, preventive and protective actions by individual entities.
- Creation of facilities to detect and clean the Botnet infected systems in coordination with Industry
- 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

*****

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: 0x2477855F
Fingerprint: 4A8F 0BA9 61B1 91D8 8708 7E61 42A4 4F23 2477 855F
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