CERT-In Annual Report (2016)

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

3rd March, 2017

Indian Computer Emergency Response Team (CERT-In)

1. Highlights of 2016

1.1 Summary of major activities

a) CERT-In operationalized the Botnet Cleaning and Malware Analysis Centre for common users.

b) In the year 2016, CERT-In handled **50362** 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, 57262 spam incidents were also reported to CERT-In. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.

c) CERT-In is keeping track on latest cyber threats and vulnerabilities. 12 security alerts, 79 advisories and 325 Vulnerability Notes were issued during the year 2016. In addition, 19 Advisories on the use of digital payments channels including DOs and DONTs are issued and circulated among various stakeholders.

d) Cyber security awareness sessions have been conducted for common users regarding security measures to be taken while using digital payment systems under the Government's TV Awareness Campaign.

` 1.2 Achievements & milestones

- Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra - www.cyberswachhtakendra.gov.in) has been established by CERT-In for detection of compromised systems in India and to notify, enable cleaning and securing systems of end users to prevent further malware infections. The centre is working in close coordination and collaboration with Internet Service Providers academia and Industry. Website of the centre was operationalised in December 2016. The centre is providing detection of malicious programs and free tools to remove the same for common users.

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

- In 2016, CERT-In signed MoUs with CERT-UK, Information Security Centre Uzbekistan and Cyber Security Department Vietnam to enable information sharing and collaboration for incident resolution.

2. About CERT-In:

2.1 Introduction

CERT-In is a functional organisation of Ministry of Electronics 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 has been 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 50 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 Government, 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 2016 is given in the following table:

Activities	Year 2016
Security Incidents handled	**50362**
Security Alerts issued	**12**
Advisories Published	**98**
Vulnerability Notes Published	**325**
Trainings Organized	**11**
Indian Website Defacements tracked	**31664**
Bot Infected Systems tracked	**10020947**

Table 1. CERT-In Activities during year 2016

3.3 Abuse Statistics

In the year 2016, CERT-In handled **50362** 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, 57262 spam incidents were also reported to CERT-In.

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

Security Incidents	2016
Phishing	**757**
Network Scanning / Probing	**416**
Virus/ Malicious Code	**13371**
Website Defacements	**31664**
Website Intrusion & Malware Propagation	**1483**
Others	**2671**
Total	**50362**

Table 2. Breakup of Security Incidents handled

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

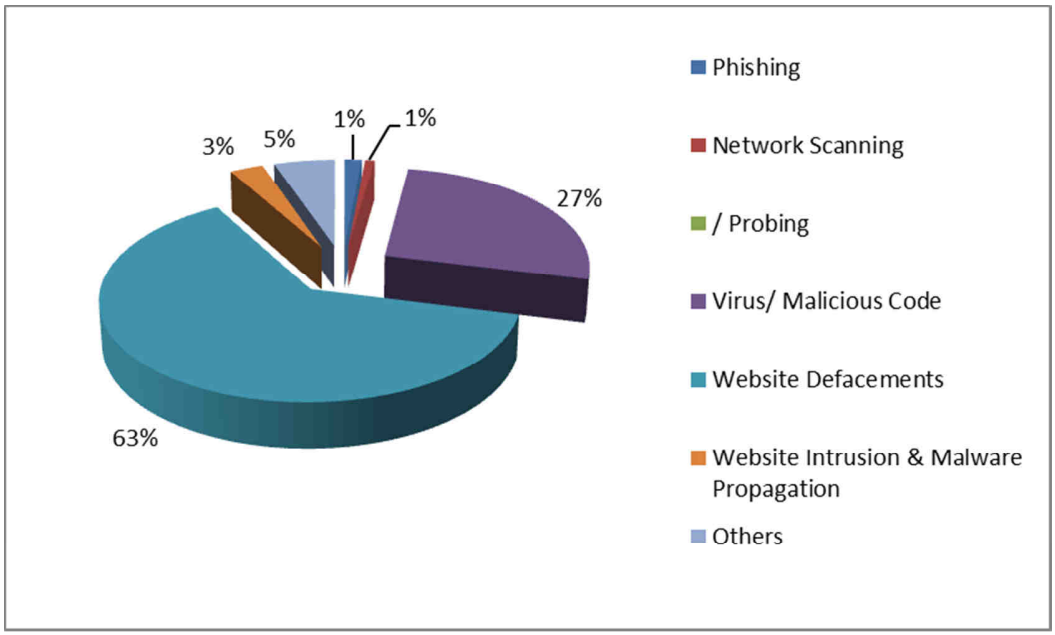
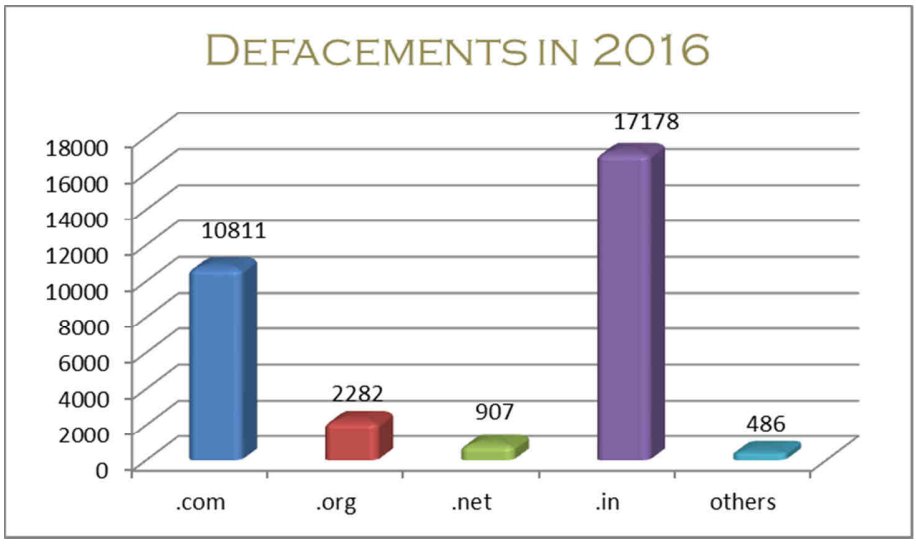


Figure 1. Summary of incidents handled by CERT-In during 2016

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. A total of 31664 numbers of defacements have been tracked.



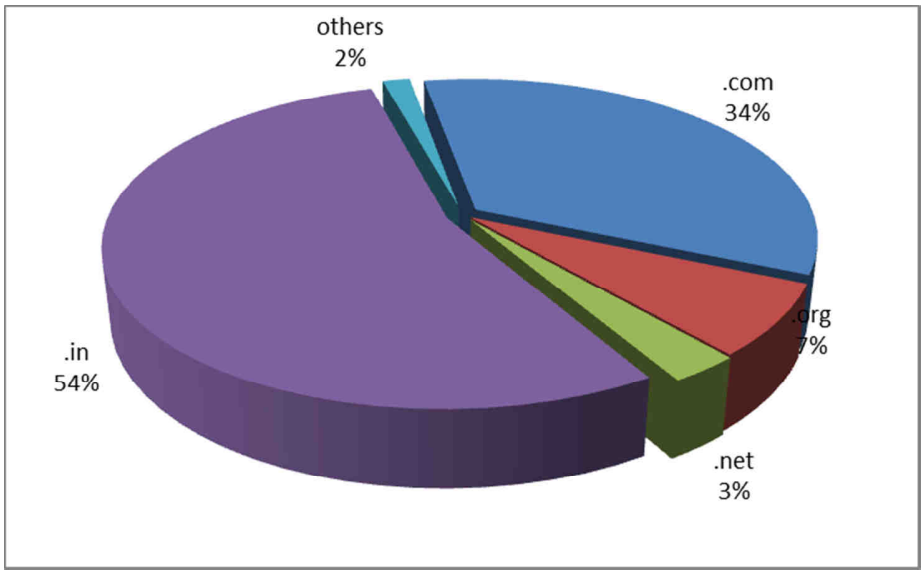
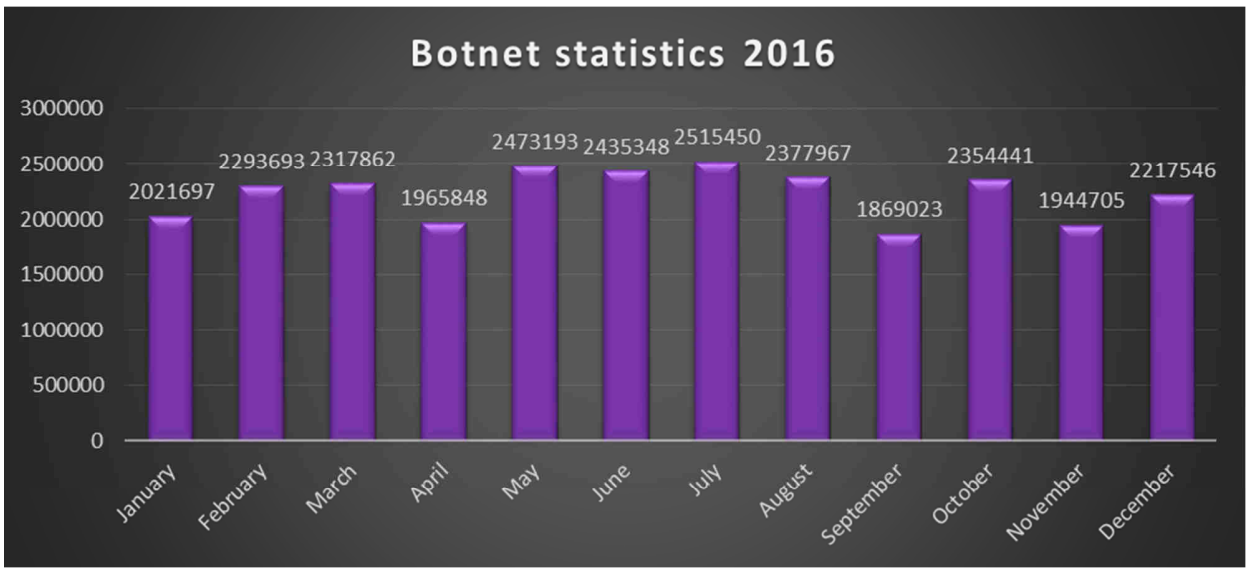


Figure 2 : Domain-wise Breakup of Indian Websites Defaced in 2016

3.3.2 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 2016.



3.5 Services

3.5.1 Security Profiling, Assurance framework and Audit Services

- Under Security Assurance Framework, CERT-In has empanelled 32 auditors to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organizations. 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. Services of CERT-In empanelled IT security auditors are being used to verify compliance.
- 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.

3.5.2 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 captured or scanned. CERT-In is analyzing this network traffic information for providing immediate alerts and 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 2016:

- Workshop on "IPv6 Security" on December 16, 2016
- Workshop on "Secure Coding Practices" on November 18, 2016
- Workshop on "Cyber Security Threats & Cyber Forensics" on October 26, 2016
- Workshop on "Endpoint Security & Secure IT Infrastructure" on October 14, 2016
- Workshop on "Advanced Targeted Attacks" on July 29, 2016
- Workshop on "Cyber Attack Trends and Mitigations" on June 30, 2016
- Workshop on "Cyber Security Threats and Countermeasures" on May 31, 2016
- Workshop on "DDoS Attacks & Mitigation" on February 29, 2016
- Workshop on "Encrypted Traffic & Hidden Threats" on February 25, 2016
- Workshop on "Emerging Cyber Security Threats and Challenges" on January 29, 2016

- Workshop on "Cyber Crisis Management Plan, Compliance & Auditing" on January 22, 2016

4.2 Drills and exercises

Cyber Security Mock Drills are being conducted by the Government to help the organisations to assess their preparedness to withstand cyber attacks. 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 11 Cyber security drills of different complexities with participation from more than 110 organizations covering various sectors of Indian economy i.e. Defence, Paramilitary forces, Space, Atomic Energy, Telecommunications(ISPs), Finance, Power, Oil & Natural Gas, Transportation(Railways & Civil Aviation) , IT/ ITeS/ BPO sectors and Data Centres from Government/Public/ Private. Joint Cyber Security Drill by CERT-In & RBI was successfully conducted on September 30, 2016 for various banks to enable them to assess their emergency incident response preparedness.

5.0 International collaboration

5.1 International Partnerships and agreements

Strengthening International cooperation to effectively deal with cyber security issues has been one of the main focus areas of the Government. As such, this aspect is being dealt with by way of security cooperation arrangements in the form of Memorandum of Understanding (MoU) between Indian Computer Emergency Response Team and its overseas counterpart agencies that are willing to work together and share information in a timely manner for preventing cyber crimes and cyber attacks as well as collaborating for providing swift response to such incidents. In 2016 CERT-In has been signed MoUs with CERT-UK, Information Security Centre Uzbekistan and Cyber Security Department Vietnam. CERT-In is regularly coordinating with leading service providers and product vendors within and outside the country to obtain advance information on latest cyber threats and attack trends and devise appropriate proactive and preventive measures.

5.2 Drills & exercises

CERT-In participated in APCERT Drill 2016 conducted on 16 March 2016 based on the theme “Evolving threat and financial fraud” to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies.

ASEAN CERTs Incident Response Drill (ACID), 2016 was conducted with the objectives of Strengthening cyber security preparedness of ASEAN member states and Dialogue partners in handling cyber incidents and reinforce regional coordination drills to test incident response capabilities. The theme of the drill held in September 2016 was handling incidents of Ransomware, in which CERT-In participated.

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.
- Promotion of R&D activities in the areas of malware prevention.
- 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