Annual Report
(2017)

Indian Computer Emergency Response Team (CERT-In)

Ministry of Electronics & Information Technology

Government of India

9th April, 2018

Indian Computer Emergency Response Team (CERT-In)

1. Highlights of 2017

1.1. Summary of major activities

a) *CERT-In under the aegis of Ministry of Electronics & Information Technology hosted the Asia Pacific CERT (APCERT) Annual General Meeting and Conference 2017 during 12-15 November 2017 in New Delhi, India.*

b) *CERT-In was elected as an APCERT Steering Committee Member.*

c) *CERT-In to lead two new working groups across APCERT, namely IoT Security and Secure Digital Payments.*

d) *In the year 2017, CERT-In handled* **53081** *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,* **53692** *spam incidents were also reported to CERT-In. Remedial measures for handling incidents were suggested and implemented in coordination with relevant stakeholders.*

e) *CERT-In is keeping track on latest cyber threats and vulnerabilities.* **19** *security alerts,* **66** *advisories and* **191** *Vulnerability Notes were issued during the year 2017 including* **7** *Advisories on the secure use of digital payments channels including DOs and DONTs are issued and circulated among various stakeholders.*

f) *Cyber security awareness sessions were conducted for common users regarding security measures to be taken while using digital payment systems under the Government's TV Awareness Campaign and also a Webcast on Wannacry Threats and Countermeasures was carried out.*

g) *CERT-In published key Roles and Responsibilities of Chief Information Security Officers (CISOs) in Ministries/Departments and Organisations managing ICT operations on Ministry of Electronics & IT website.*

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 a public private partnership model in close coordination and collaboration with Internet Service Providers, academia and Industry. The centre was launched on 21st February 2017. 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 cyber security exercises comprising of table top exercises, crisis management plan mock drills and joint cyber security exercises with organizations from key sectors to enable participating organizations to assess their preparedness in dealing with cyber crisis situations. Total 12 such exercises have been conducted in 2017.*
- *In 2017, CERT-In has signed two MoUs with United States Computer Emergency Readiness Team (US-CERT), Department of Homeland Security, United States of America and The Bangladesh Government Computer Incident Response Team (BGD e-Gov CIRT), Bangladesh Computer Council of Information and Communication Technology Division, Ministry of Posts, Telecommunication and IT, People's Republic of Bangladesh respectively 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 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*

2.2. Establishment

CERT-In has been operational since January, 2004.

2.3. Resources

CERT-In has a team of 70 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 & Operations

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 2017 is given in the following table:

Activities	Year 2017
Security Incidents handled	**53081**
Security Alerts issued	**19**
Advisories Published	**66**
Vulnerability Notes Published	**191**
Trainings Organized	**22**

Table 1: CERT-In Activities during year 2017

3.3. Abuse statistics

In the year 2017, CERT-In handled **53081** *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,* **53692** *spam incidents were also reported to CERT-In.*

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

Security Incidents	2017
Phishing	**552**
Network Scanning / Probing	**9383**
Virus/ Malicious Code	*9750*
Website Defacements	**29518**
Website Intrusion & Malware Propagation	**563**
Others	**3315**
Total	**53081**

Table 2: Breakup of Security Incidents handled

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

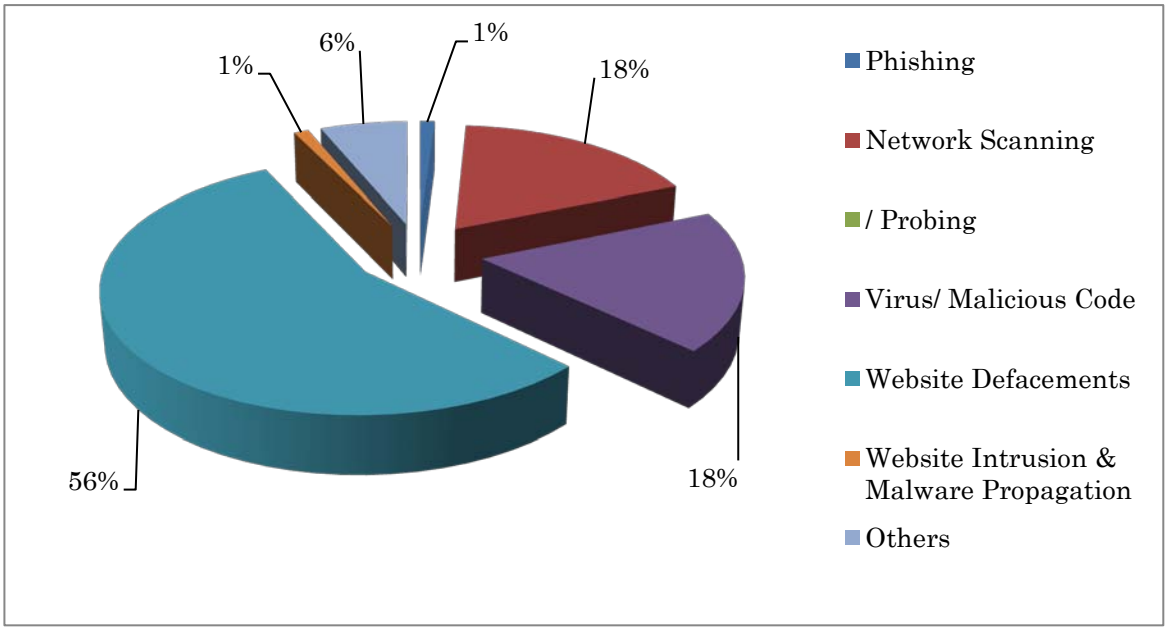

Figure 1: Summary of incidents handled by CERT-In during 2017

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 **29518** *numbers of defacements have been tracked.*

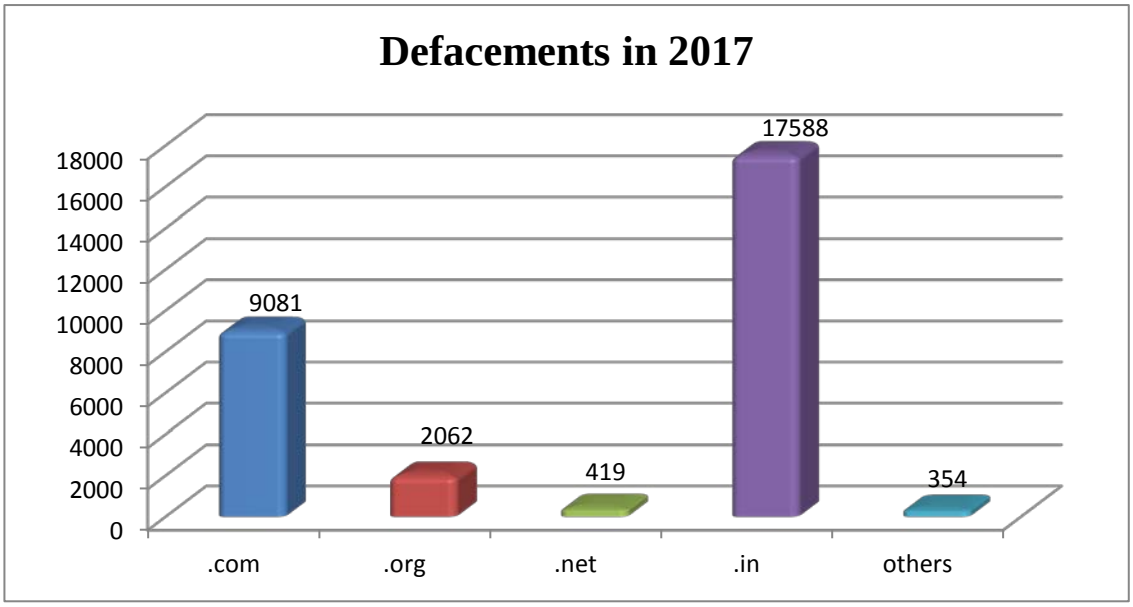

Figure 2: Indian Website Defacements tracked by CERT-In during 2017

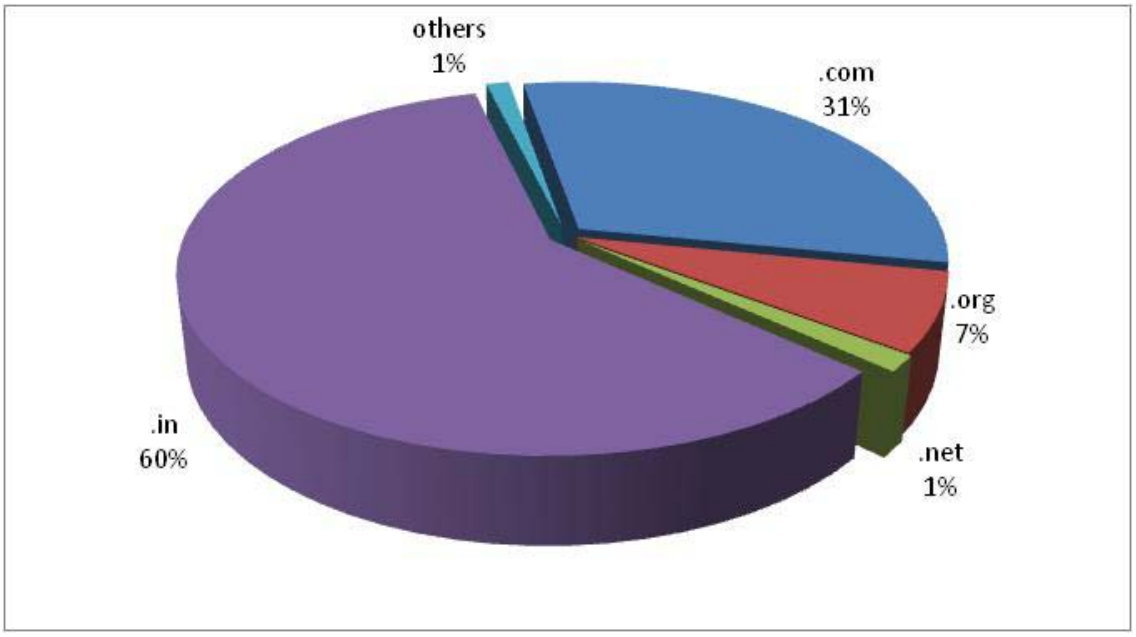

Figure 3: Domain-wise Breakup of Indian Websites Defaced in 2017

3.3.2.Botnet Cleaning Initiatives

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra - www.cyberswachhtakendra.gov.in) has been established by CERT-In for detection of compromised devices 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.

Botnets events processed by Botnet Cleaning and Malware Analysis centre (Cyber Swachhta Kentra) during 2017.

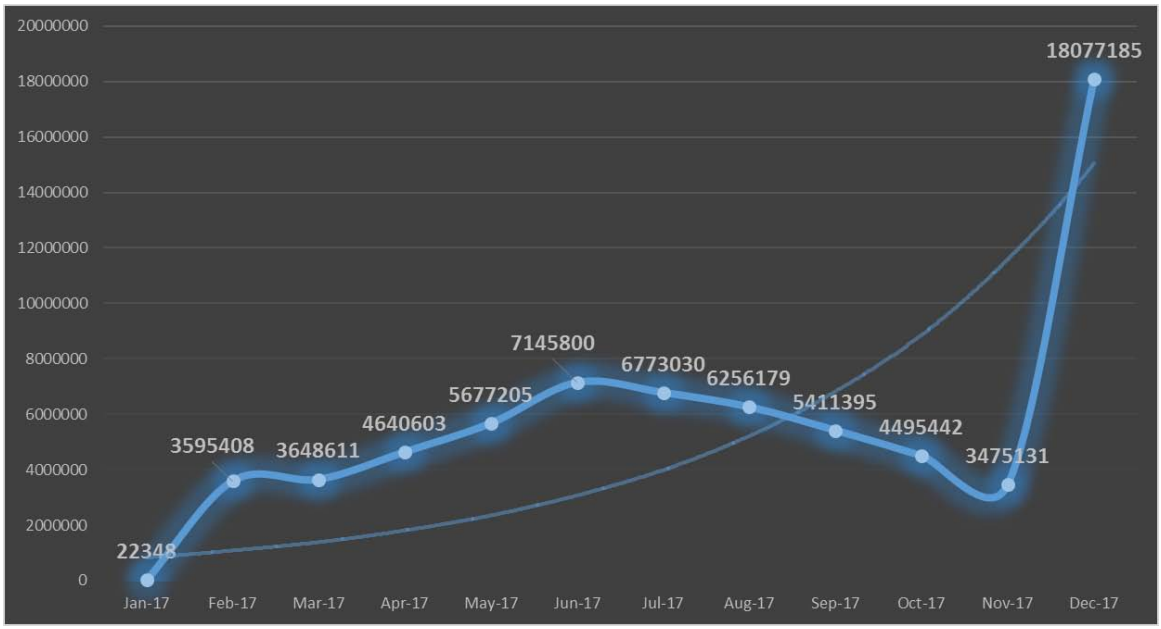

Figure 4: Botnet events tracked by Botnet Cleaning and Malware Analysis Centre

3.3.3. Security Profiling, Assurance framework and Audit Services

- *Under Security Assurance Framework, CERT-In has empanelled 67 technical IT security 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 technical 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 technical 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.*

4. Events organized / hosted

4.1. Security awareness, skill development and training

In order to create security awareness within the Government, Public and Critical Sector organisations, CERT-In regularly conducts trainings / workshops to train officials of Government, critical sector, public sector industry, financial & banking sector on various contemporary and focused topics of Cyber Security. In 2017, CERT-In has conducted 22 trainings on various specialized topics of cyber security. A total of 610 officers including

system/Network Administrators, Database Administrators, Application Developers, IT Managers, Chief Information Security Officers (CISOs)/ Chief information officers (CIOs), and IT Security professional have been trained. CERT-In carried out a specific training session only for women IT professionals.

CERT-In has conducted the following training programmes in 2017:

- *Workshop on "Cyber Crisis Management Plan" on February 17, 2017*
- *Workshop on "Embedded Software Safety & Security of National Critical Infrastructure" on February 27, 2017*
- *Workshop on "Proactive Automated Cloud Security" on February 28, 2017*
- *Workshop on "Cyber Crisis Management Plan" on March 17, 2017*
- *Workshop on "Cyber Threats Trends" on March 20, 2017*
- *Workshop on "Contours of DevOps" on March 23, 2017*
- *Workshop on "Secure Digital Payments" on March 30, 2017*
- *Workshop on "Cyber Crisis Management Plan" April 19, 2017*
- *Workshop on "Endpoint Security & Security of IT Infrastructure" on April 26, 2017*
- *Workshop on "Cyber Crisis Management Plan" on MaY 16, 2017*
- *Workshop on ""Cloud Data Governance & Security" on May 26, 2017*
- *Workshop on "Cyber Threats and Countermeasures" on May 30, 2017 ((Exclusively for Women IT Professionals)*
- *Workshop on "Cyber Crisis Management Plan" on June 22, 2017*
- *Workshop on "Cyber Security Threats & Mitigations" on July 5, 2017*
- *Workshop on "Desktop & Mobile Devices Security" on July 11, 2017*
- *Workshop on "Cloud Security & DDoS Mitigations" on July 13, 2017*
- *Workshop on "Ransomware & Malware Threats" on July 14, 2017*
- *Workshop on "Cyber Crisis Management Plan" on August 8, 2017*
- *Workshop on "Cyber Crisis Management Plan" on August 30, 2017*
- *Workshop on "Cyber Forensics" on October 11, 2017*
- *Workshop on "The Hidden Threats & Economics of Cyber Attacks" on October 25, 2017*
- *Workshop on "Cyber Threats & Cyber Forensics" on November 1, 2017*

4.2. **Cyber Security Exercises**

Cyber security exercises are being conducted by the Government to help the organizations to assess their preparedness to withstand cyber attacks. These exercises 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. CERT-In has conducted 12 exercises in 2017 including 3 joint cyber security exercises conducted with Finance, aviation and

shipping sector organizations.

4.3 Cyber Forensics

CERT-In is equipped with the tools and equipment to carry out retrieval and analysis of the data extracted from the digital data storage devices using computer forensics and mobile device forensic techniques. CERT-In's facility for Digital Forensics data extraction and analysis is being utilised in investigation of the cases of cyber security incidents, submitted by central and state government ministries, departments, public sector organizations, law enforcement agencies, etc. CERT-In imparts training through workshops organised by CERT-In on computer forensics and mobile device forensics through lectures, demonstrations and hands on practical sessions, which covers seizing, preservation, imaging and analysis of the data retrieved from the digital data storage devices. CERT-In also provides support to the other training institutes in imparting training by delivering lectures with demonstrations on various aspects of cyber forensics.

5. 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 incidents and cyber attacks as well as collaborating for providing swift response to such incidents. In 2017 CERT-In signed MoUs with United States Computer Emergency Readiness Team (US-CERT), Department of Homeland Security, United States of America and The Bangladesh Government Computer Incident Response Team (BGD e-Gov CIRT), Bangladesh Computer Council of Information and Communication Technology Division, Ministry of Posts, Telecommunication and IT, People's Republic of Bangladesh. 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 2017 conducted in March 2017 based on the theme "Emergence of a New DDoS Threat" to test the response capability of leading Computer Security Incident Response Teams (CSIRT) from the Asia Pacific economies. *The objective was to enables CERTs to review, practice and strengthen computer security incident handling mechanism and exercise coordination with multiple parties (internal and external) when*

handling computer security incidents.

CERT-In participated in the ASEAN CERTs Incident Response Drill (ACID) in September 2017 wherein the objective was strengthening cyber security preparedness of ASEAN member states and Dialogue partners in handling cyber incidents and reinforce regional coordination to test incident response capabilities. The theme of the drill was handling incidents of Ransomware.

CERT-In participated in The Organisation of The Islamic Cooperation – Computer Emergency Response Teams (OIC-CERT) drill in September 2017. The theme of the drill was Encountering Cyber Terrorism and Human Trafficking.

5.3. **Other international activities**

- *CERT-In under the aegis of Ministry of Electronics & Information Technology hosted the Asia Pacific CERT (APCERT) Annual General Meeting and Conference 2017 during 12-15 November 2017 in New Delhi India.*
- *CERT-In participated in the Global Conference on Cyber Space (GCCS) 2017 during 23 – 24 November 2017 in New Delhi.*
- *CERT-In participated in the FIRST AGM & Conference during 11 – 16 June 2017 at San Juan, Puerto Rico.*

6. Future Plans

6.1. **Future projects**

CERT-In has 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.*
- *Strengthening of auditor empanelment skill assessment infrastructure.*
- *Setting up of an automated Threat Information sharing platform.*

6.2. **Working Groups**

- *IoT Security Working Group*
  - *To ensure the secure usage of IoT devices in priority sectors and build trust in secure usage of IoT Ecosystem*

- *Secure Digital Payments Working Group*
  - *Build trust in secure usage of digital payments so as to ensure economic stability.*

*****

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