Indian Computer Emergency Response Team (CERT-In)

Annual Report (2006)

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

31st March 2007

Indian Computer Emergency Response Team (CERT-In)

About CERT-In:

CERT-In is a functional organisation of Department of 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.

Activities 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

The summary of activities carried out by CERT-In during the year 2006 is given in the following table:

Activities	Year 2006
Security Incidents handled	552
Security Alerts issued	48
Advisories Published	50
Vulnerability Notes Published	138
Security Guidelines Published	1
White Papers Published	2
Trainings Organized	7
Indian Website Defacements tracked	5211
Open Proxy Servers tracked	1837

Table 1. CERT-In Activities during year 2006

Summary of Computer Security Incidents handled by CERT-In during 2006

In the year 2006, CERT-In handled more than 550 incidents. The types of incidents handled were mostly of Phishing and Network Scanning & Probing. Among the malicious code incidents, significant numbers of incidents were reported in February, 2006 due to spreading of Nyxem (Kamasutra) worm, targeting Indian users. CERT-In published alert regarding spreading of this

worm well in advance and suggested suitable countermeasures and disinfection tools thereby containing wide spread damage in the country.

The most widespread phishing attacks reported in 2006 are carried out against E-Commerce sector. It is accounting for 76%. The second most targeted sector is Financial Services which accounts for 24% for the total number of incidents reported in the year 2006. Of the total phishing incidents handled in 2006, the cases in which Indian Financial Institutions were involved were about 2% and rest belonging to outside India.

The summary of various types of incidents handled during 2006 and previous years is given below:

Security Incidents	**2004**	**2005**	**2006**
Phishing	3	101	339
Network Scanning / Probing	11	40	177
Virus / Malicious Code	5	95	19
Email Spoofing	3	8	7
Others	1	10	10
Total	**23**	**254**	**552**

Table 2. Security Incidents handled yearly trend

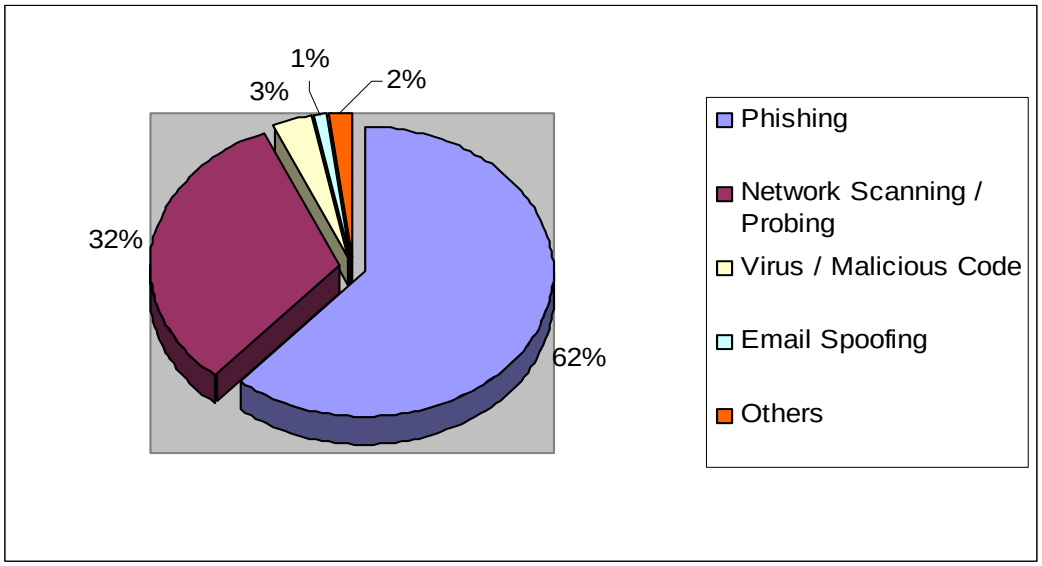

Figure 1. Summary of incidents handled by CERT-In during 2006

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 5211 numbers of defacements have been tracked. Most of the defacements were done for the websites under ***.com*** domain. In total 1226 ***.in*** domain websites were defaced.

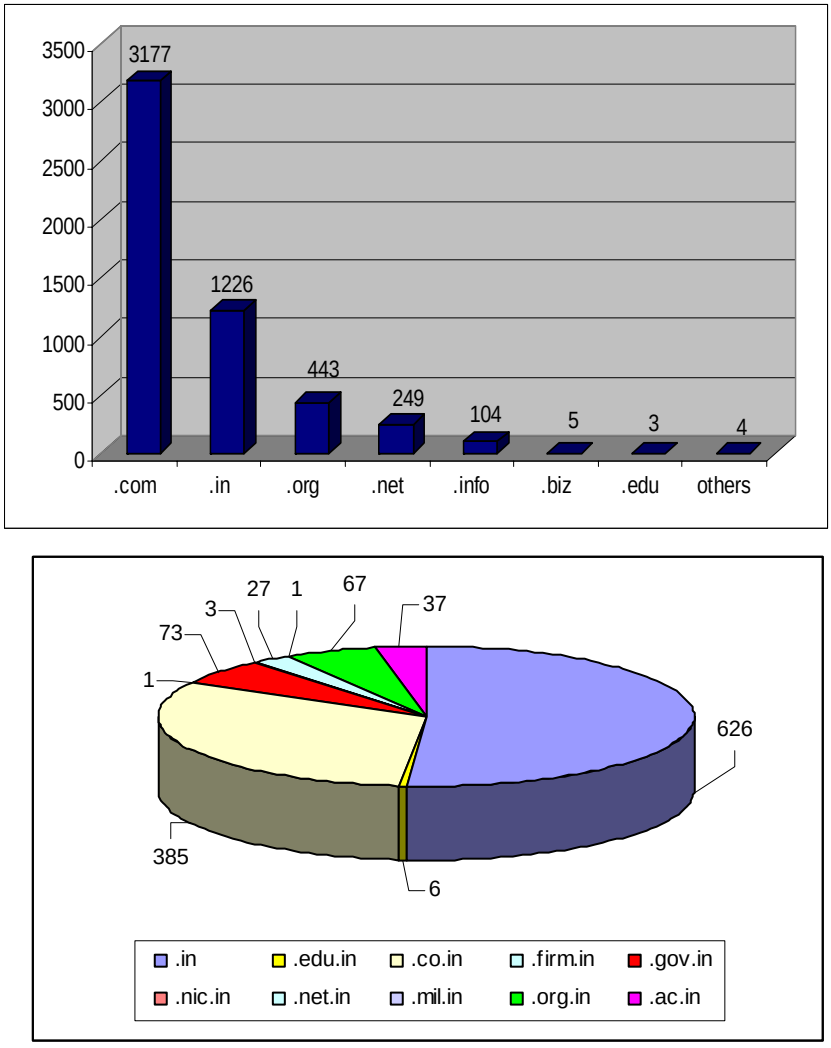

Figure 2.1 .in ccTLD defacements during 2006

The following figure shows the month wise comparison of the Indian website defacements in year 2005 and 2006. In the month of August unusual increase has been noticed in the year 2005 as well as in the year 2006. In the year 2006 total 1311 defacements were tracked on Indian websites during the month of August.

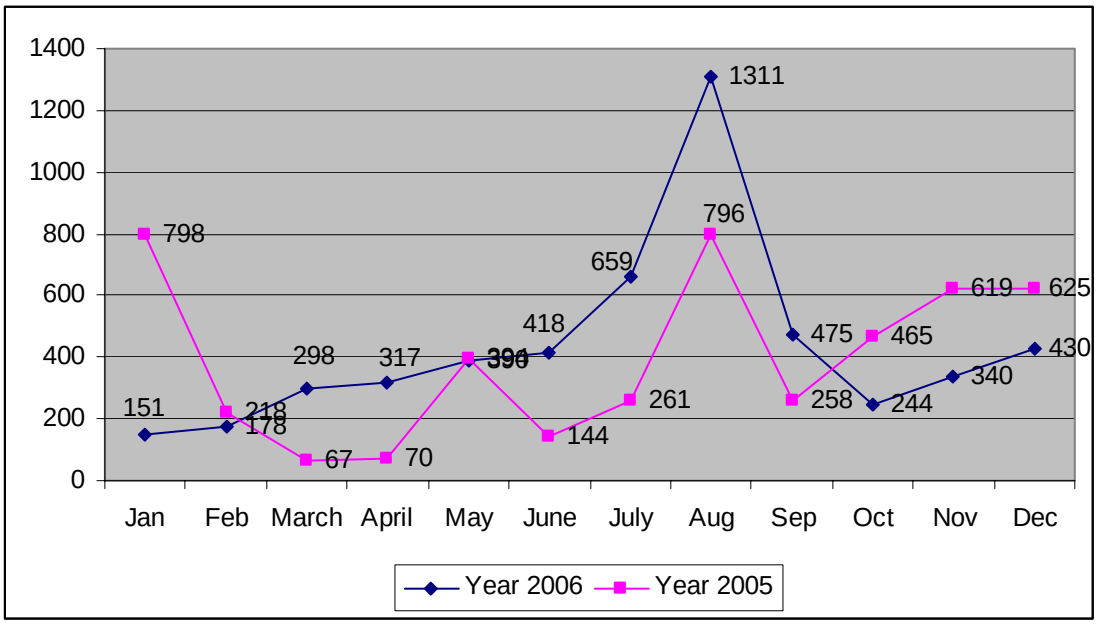

Figure 3. Monthly comparison of the Indian Website Defacements (2005 -2006)

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 1837 open proxy servers were tracked in the year 2006. As compared to previous year the number of open proxy have increased, 1156 open proxy were reported last year. A bar chart of open proxy servers tracked during this year is shown in the figure.

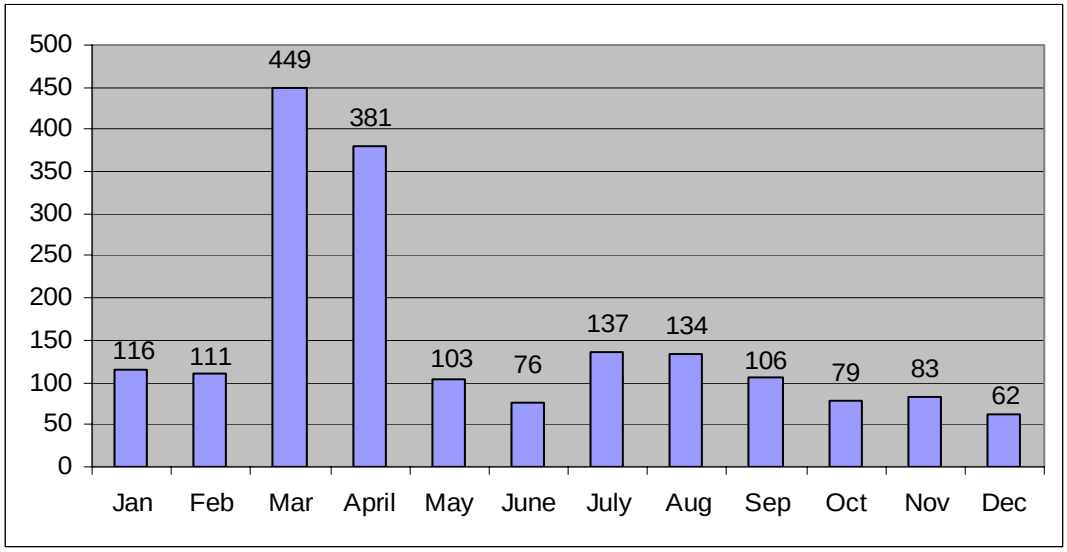

Figure 4. Monthly statistics of Open Proxy Servers in 2006

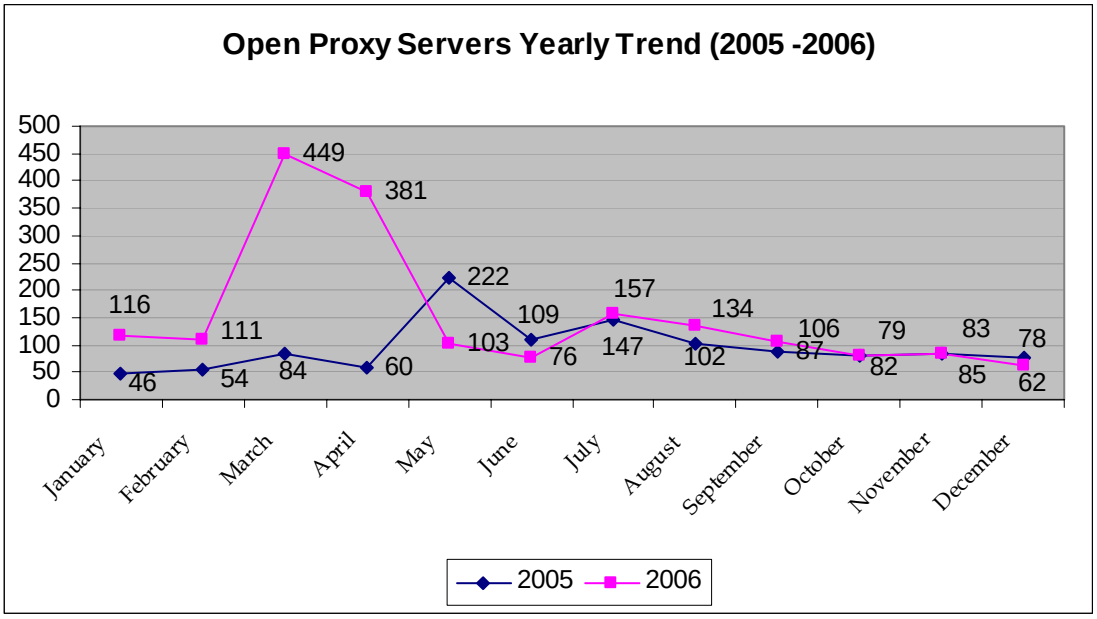

Figure 4.1 Monthly comparisons of Open Proxy Servers (2005 -2006)

Education and Training

To create awareness and to enable users to implement best practices, CERT-In is organising workshops and training programmes on focused topics for targeted audience such as CIOs, financial and banking sector officers, System Administrators, ISPs etc. Experts from industry are delivering lectures in these workshops apart from CERT-In. CERT-In has conducted the following training programmes for CIOs and System Administrators during 2006.

1. Workshop on "Protection against Phishing Scams" on 15th February, 2006
2. Workshop on "DNS DDoS Amplification Attacks and Mitigation" on 1st May, 2006
3. Workshop on “Information Security for CIOs” on 16th May 2006
4. Workshop on “Information Systems Security” for System Administrators of ASEAN Countries, 28-30 August 2006
5. ASEAN Regional Forum(ARF) Workshop on “Cyber Security”, 6-8 September 2006
6. CERT-In & eBay joint workshop on "E-Commerce Security" on 26th September, 2006
7. Workshop for Points-of-Contact from critical sectors on “Cyber Security” on 31st October, 2006

Cyber Security Assurance Framework

CERT-In is establishing the National Cyber Security Assurance Framework for protection of Critical Information Infrastructure. As part of this, CERT-In has empanelled 57 ‘Security Auditors’ for auditing, including vulnerability assessment & penetration testing of computer systems and networks of various organisations of the government, critical infrastructure

organisations and those in other sectors of the Indian economy. CERT-In plays the role of mother CERT in the country and helping formulation of sectoral CERTs in critical sectors.

Collaboration with Vendors

To facilitate its tasks, CERT-In has initiated steps to collaborate with IT product vendors and security vendors in the country. Some of the vendors collaborating with CERT-In for cyber security assurance are *Microsoft, RedHat, Cisco, Computer Associates, eBay, EMC*^{2}*, McAfee, Symantec, Trend Micro* etc.

International Collaboration

CERT-In is collaborating with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices.

- CERT-In became general member of ***Asia Pacific CERT (APCERT)*** in March 2006.
- CERT-In has organised a workshop on "Information Systems Security for System Administrators of ***ASEAN Countries***" from 28th to 30th August 2006 at Manesar, Haryana , India in coordination with International Cooperation Division of Department of Information Technology and Ministry of External Affairs, Government of India. In all 21 participants including two members of ASEAN Secretariat have participated in the workshop.
- CERT-In has organised the ***ASEAN Regional Forum (ARF)*** Workshop on "Cyber Security" under the guidance of Department of Information Technology and Ministry of External Affairs in New Delhi during 6th -8th September 2006 . In all 58 delegates from 20 ARF participating countries and representatives of *ASEAN Secretariat* and private sectors participated in the workshop. There were 13 country presentations and 4 industry presentations were made during the workshop. The topics of discussion included Threat of Cyber Terrorism – National Perspective, Government Initiatives on Cyber Security and Protection of Critical Information Infrastructure, Cyber Security - Trends and Protection Strategies and Strategy to Counter Cyber Terrorism and Areas of Cooperation.
- CERT-In participated in the ***APCERT International Incident Handling Drill 2006*** coordinated by KrCERT. As part of the drill, the malicious websites were successfully brought down. Local ISPs and security vendors from India also participated in the Drill.
- CERT-In became Full Member of ***Forum of Incident Response and Security Teams (FIRST)*** in December 2006.

Future Outlook

The thrust is to make CERT-In the most trusted referral agency in the area of information security in the country. CERT-In is focusing on building a network of CIOs of Critical Infrastructure Organisations and interacting with them to ensure security of the critical systems, collaboration with IT product and security vendors to mitigate the vulnerabilities in various systems, providing guidance for developing and augmenting sectoral CERTs, cooperation with international CERTs and security organizations on information sharing and incident response,

promote R&D activities in the areas of Artifact analysis and Cyber Forensics and security training and awareness. CERT-In is developing a mechanism to issue advance warnings and alerts on cyber attacks and provide countermeasures by analyzing Internet traffic pattern.
CERT-In is also developing separate security web portal for Government & Critical information infrastructure organisations and home users. This web portal will publish information on latest threats & their countermeasures alongwith security best practices.

Contact Information

Incident Response Help Desk

Phone: +91-11-24368551
+91-1800-11-4949
Fax : +91-11-24368546
+91-1800-11-6969

PGP key details:

User ID: incident@cert-in.org.in
Key ID: 0x35DC5287
Fingerprint: 2E68 2FB6 0438 E77D 2F65 0F35 BB03 3855 35DC 5287

User ID: info@cert-in.org.in, advisory@cert-in.org.in
Key ID: 0x6CA13DF4
Fingerprint: A1FF 5956 36EC 25D7 1D76 635C 7597 7983 6CA1 3DF4

Postal Address:

Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology
Ministry of Communications & Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India