Indian Computer Emergency Response Team (CERT-In)

Annual Report (2007)

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

18th March 2008

Indian Computer Emergency Response Team (CERT-In)

1.0 About CERT-In:

1.1 Introduction

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.

1.2 Establishment and Constituency

CERT-In was operational since January 2004. The constituency of CERT-In is the Indian cyber community. CERT-In works cooperatively with Chief Information Officers and system administrators of various sectoral and organisational networks of its constituency.

2.0 Activities and Operations of CERT-In

2.1 Services and Activities

CERT-In provides:

- Proactive services in the nature of Advisories, Security Alerts, Vulnerability Notes, and Security Guidelines to help organizations to 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 2007 is given in the following table:

Activities	Year-2007
Security Incidents handled	1237
Security Alerts issued	44
Advisories Published	66
Vulnerability Notes Published	163
Security Guidelines Published	1
White papers Published	2
Trainings Organised	6
Indian Website Defacements tracked	5863
Open Proxy Servers tracked	1805
Bot Infected Systems tracked	25915

Table 1. CERT-In Activities during year 2007

2.2 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 76 '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. These audits enable CERT-In to assess the vulnerabilities in Critical Information Infrastructure systems and device suitable corrective actions and response capabilities. Implementation of security measures as per ISO 27001 has been mandated for all government organisations. A comprehensive database of Chief Information Security Officers (CISO) of Critical Infrastructure organisations is being maintained and training programs have been conducted to form a network of CISOs and encourage them to implement best practices to secure their systems. CERT-In is providing early warning on emerging threats to CISOs so as to enable them to take suitable actions to mitigate the risk.

To facilitate its tasks, CERT-In has initiated steps to collaborate with industry and security vendors in the country. Some of the vendors collaborating with CERT-In for cyber security assurance are Cisco, Computer Associates, eBay, EMC2, McAfee, Microsoft, RedHat, Symantec, Trend Micro, Quickheal etc.

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.

2.3 Incident Handling Reports

2.3.1 Summary of Computer Security Incidents handled by CERT-In during 2007

In the year 2007, CERT-In handled 1237 incidents. The types of incidents handled were mostly of Phishing, Malicious Code propagation and Network Scanning & Probing.

The year-wise summary of various types of incidents handled is given below:

Security Incidents	2004	2005	2006	2007
Phishing	3	101	339	392
Network Scanning / Probing	11	40	177	223
Virus / Malicious Code	5	95	19	358
Others	4	18	17	264
Total	**23**	**254**	**552**	**1237**

Table 2. Year-wise summary of Security Incidents handled

2.3.2 Incident Statistics

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

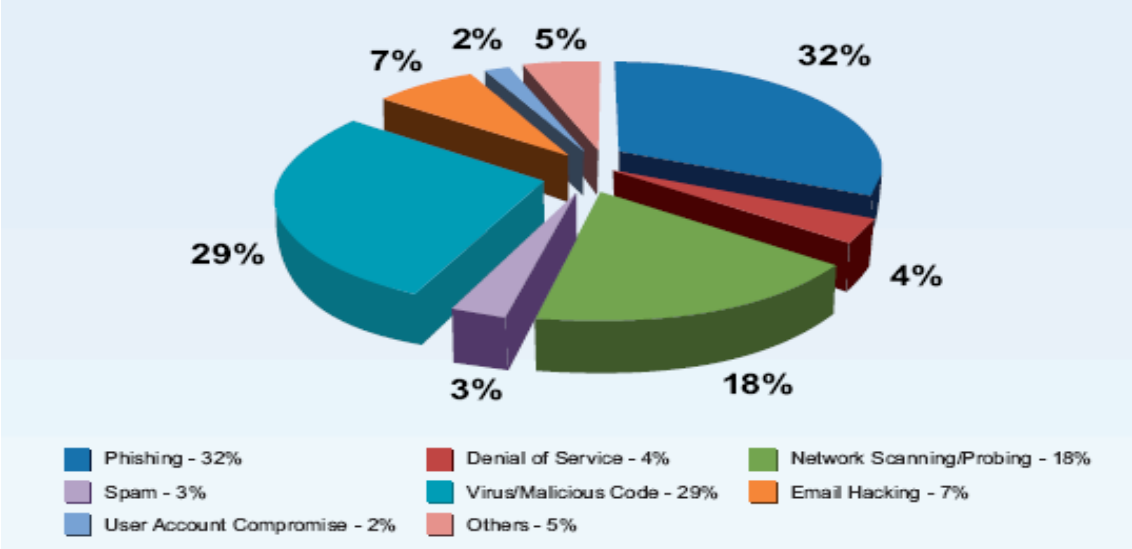

Figure 1. Summary of incidents handled by CERT-In during 2007

The phishing attacks reported in 2007 were primarily carried out against e-commerce sector and Financial services. While phishing attacks on E-commerce sector account for 51% of the total phishing attacks, the second most targeted sector is financial services which accounts for 47% of the total number. The phishing incidents affecting Indian Financial Institutions were around 12 % of total phishing incidents reported, while remaining incidents were affecting brands of other countries.

2.3.3 Incident Trends

In the year 2007 automated infection toolkits such as MPack and "Random JS Toolkit" used i-Frame injection and JavaScript injections to infect the websites and propagate malware.

Incidents of Phishing using toolkits such as Metaphisher were observed. Phishing websites were hosted on Fast-Flux DNS using Botnet such as Storm. Phishing Incidents using Rock-Phish and Fast-Flux techniques were on the rise.

CERT-In handled various cases of information stealing Trojans such as Clampi, Bzub and Nethell, affecting users of online transactions. These Trojans used key logging features to capture information that is fed to web forms and sent this captured information to the remote systems.

Storm worm, transpired in January 2007, used the spam to propagate using different social engineering techniques based on current events. Storm botnet spread to thousands of systems and used P2P network for Command & Control operations. This botnet was used for malicious purposes such as spam and phishing.

An increase in XSS attacks and website defacements exploiting vulnerabilities in PHP were observed in year 2007.

2.4 Proactive Services

2.4.1 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 organisations. In all 5863 numbers of defacements have been tracked. Most of the defacements were done for the websites under ***.com*** domain. In total 1693 ***.in*** domain websites were defaced.

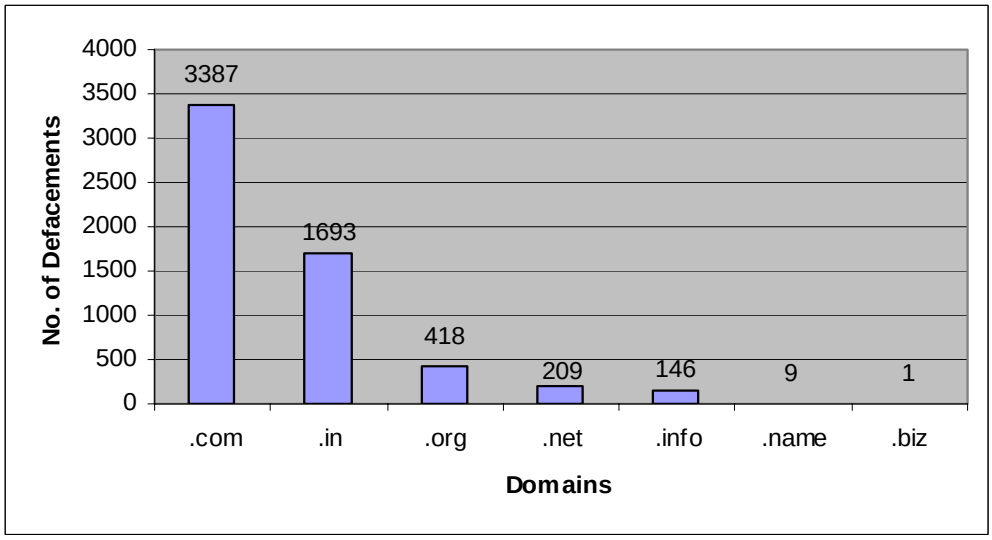

Figure 2. Indian websites defaced during 2007 (Top level domains)

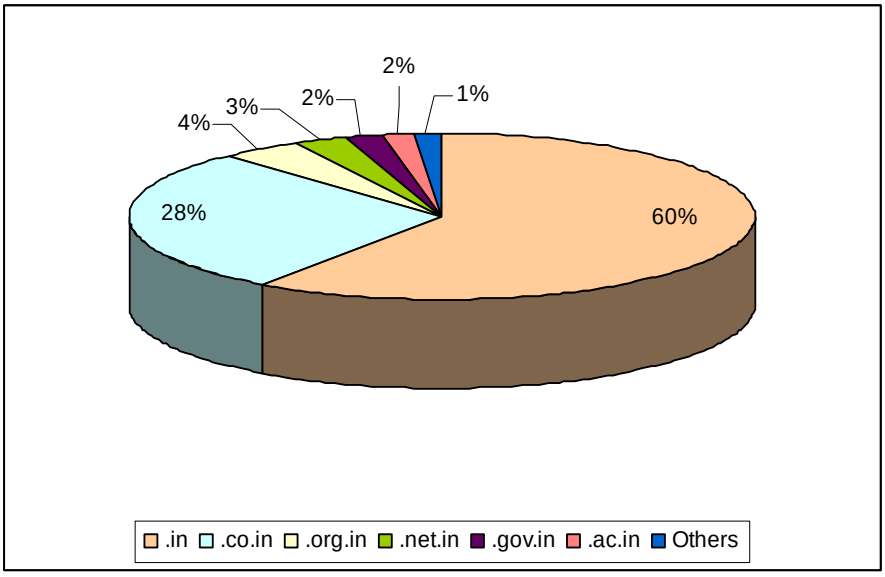

Figure 2.1 .in ccTLD defacements during 2007

2.4.2 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 1805 open proxy servers were tracked in the year 2007. As compared to previous year the number of open proxy servers has decreased, 1837 open proxy were reported last year. The month-wise distribution of open proxy servers tracked during this year is shown in the figure.

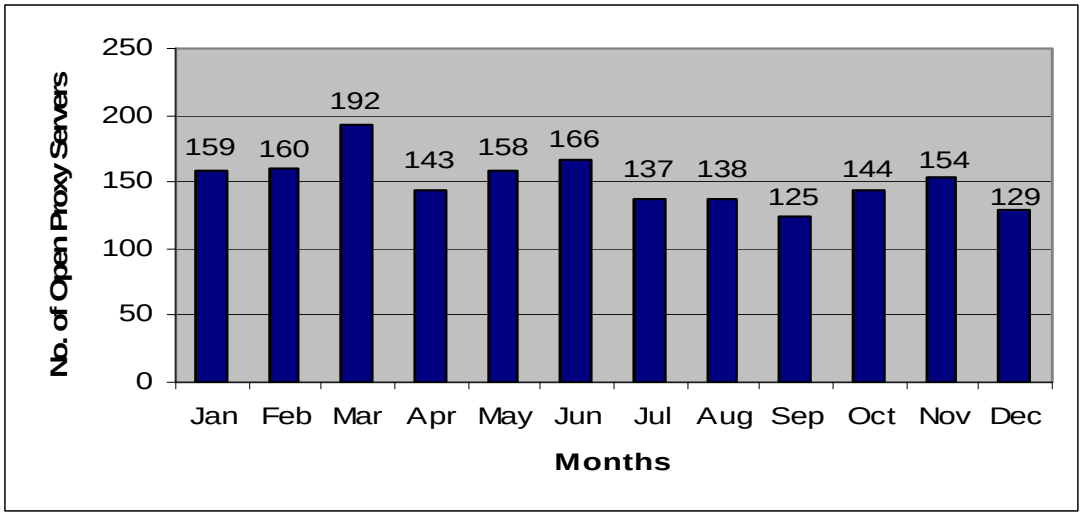

Figure 4. Monthly statistics of Open Proxy Servers in 2007

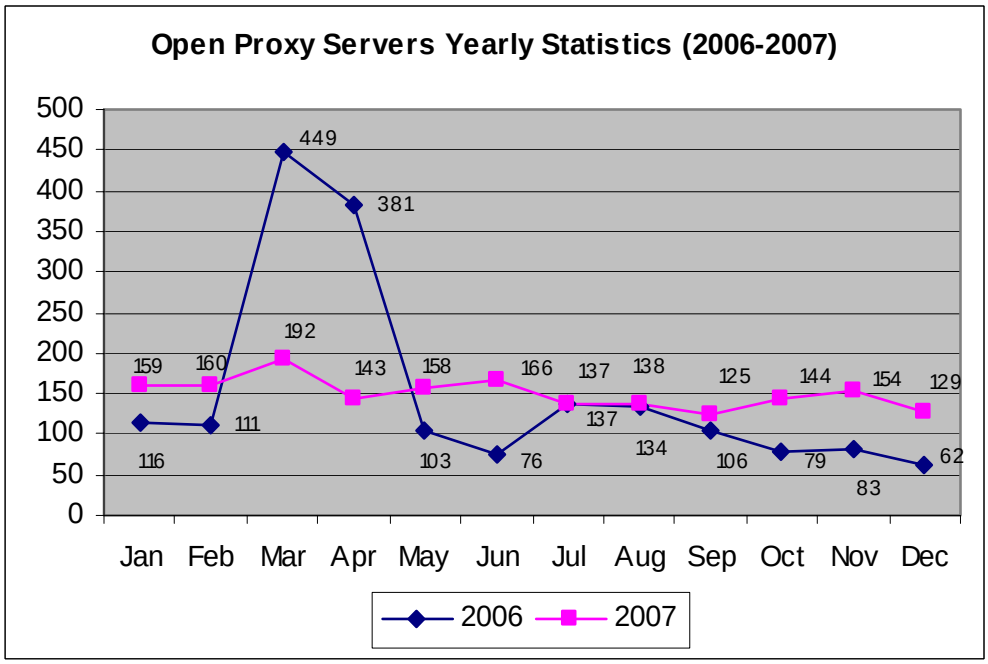

Figure 4.1 Comparison of Open Proxy Servers month-wise (2006 -2007)

2.4.3 Botnet Tracking and Mitigation

CERT-In started the activity of tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of C&C servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 5 shows the number of Bot infected systems and Command & Control servers tracked from June 2007.

Month	Number Of Bot Infected Systems	C&C Servers	
		C&C Servers- Outside India	C&C Servers in India
June	760	93	4
July	14835	138	4
August	4934	55	4
September	1976	57	4
October	1370	56	4
November	1020	48	2
December	1020	46	2
Top Ports used for the Botnet communication 6667, 1231, 4001, 5005, 65500, 3159, 9997, 7777, 13830, 34567			

Figure 5. Botnet statistics from June to December 2007

3.0 Events organised/ co-organised

3.1 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 staff. CERT-In has conducted the following training programmes for CIOs and System Administrators during 2007.

1. Workshop on "Implementing Secure Coding Practices" on 16th January, 2007
2. “Information Security Executives Readiness Training Programme for CISOs" on 12-14 February, 2007
3. Workshop on "Security aspects related to setting up SWAN" on 30 April 2007
4. Workshop on "Vulnerability Assessment Methodologies" on 16 October, 2007
5. Workshop on "Botnet Attacks and Defenses" on 26th October, 2007
6. “Brainstorming session on tackling the Phishing menace” on 2nd November 2007

3.2 Seminars/ Forums

CERT-In has formed forums in coordination with Confederation of Indian Industry (CII) for facilitating information exchange and joint programmes to combat Phishing attacks and Spam.

4.0 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 is general member of APCERT and member of FIRST.

4.1 Memorandum of Understanding (MoU):

CERT-In has signed MoUs with National Cyber Security Centre, Republic of Korea, JPCERT/CC and National Computer Board, Mauritius for mutual cooperation in the area of cyber security.

4.2 Incident Handling Drills

- CERT-In participated in the ASEAN CERTs Incident Handling Drill (ACID 2007) held on 16th July 2007.
- CERT-In participated in the APCERT International Incident Handling Drill 2007 held on 22nd November, 2007.

5.0 Future Plans/Projects

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 following activities:

- Building a network of CISOs 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 Research and Development activities in the areas of Artifact analysis, 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 patterns

Contact Information

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

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: 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
