Indian Computer Emergency Response Team (CERT-In)

Annual Report (2008)

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

15th May 2009

Indian Computer Emergency Response Team (CERT-In)

1.0 About CERT-In:

1.1 Establishment and Constituency

CERT-In was operational since January 2004. The constituency of CERT-In is the Indian cyber community.

CERT-In is the national nodal agency for responding to computer security incidents as and when they occur. CERT-In creates awareness on security issues through dissemination of information on its website (http://www.cert-in.org.in) and operates 24X7 Incident Response Help Desk. It provides Incident Prevention and Response services as well as Security Quality Management Services.

In the recent Information Technology (Amendment) Act 2008, CERT-In has been designated 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

2.0 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 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 2008 is given in the following table:

Activities	Year 2008
Security Incidents handled	**2565**
Security Alerts issued	**49**
Advisories Published	**76**
Vulnerability Notes Published	**197**
Security Guidelines Published	**1**
White papers Published	**1**
Trainings Organized	**18**
Indian Website Defacements tracked	**5475**
Open Proxy Servers tracked	**2332**
Bot Infected Systems tracked	**146891**

Table 1. CERT-In Activities during year 2008

2.2 Cyber Security Assurance Framework

CERT-In has taken steps to implement National Information Security Assurance Programme (NISAP) to create awareness in government and critical sector organisations and to develop and implement information security policy and information security best practices based on ISO/IEC 27001 for protection of their infrastructure. For communicating with these organisations, CERT-In maintains a comprehensive database of more than 800 Point-of Contacts (PoC) and Chief Information Security Officers (CISO). As a proactive measure, CERT-In has also empanelled 76 information security auditing organisations to carry out information security audit, including the vulnerability assessment and penetration test of the networked infrastructure of government and critical sector organisations. The technical competency of the empanelled orgnanisations is regularly reviewed by CERT-In with the help of a test network.

CERT-In plays the role of mother CERT and is regularly interacting with the cyber security officers of sectorial CERTs in Defense, Finance and other sectors to advise them in the matters related to cyber security.

To facilitate its tasks, CERT-In has collaboration arrangements with IT product vendors, security vendors and Industry in the country and abroad. Security Cooperation agreements and MoUs have been signed with Microsoft, RedHat, Cisco, EMC^2, eBay, Trend Micro, Symantec, Quickheal, Radware, McAfee and Afilias. This collaboration facilitates exchange of information on vulnerabilities in relevant products, developing suitable countermeasures to protect these systems and providing training on latest products and technologies.

2.3 Incident Handling Reports

2.3.1 Summary of Computer Security Incidents handled by CERT-In during 2008

In the year 2008, more than 2500 incidents were reported and handled by CERT-In. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing.

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

Security Incidents	2004	2005	2006	2007	2008
Phishing	3	101	339	392	604
Network Scanning / Probing	11	40	177	223	265
Virus / Malicious Code	5	95	19	358	408
Spam	-	-	-	-	305
Website Compromise & Malware Propagation	-	-	-	-	835
Denial of Service	-	-	-	-	54
Others	4	18	17	264	94
Total	**23**	**254**	**552**	**1237**	**2565**

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.

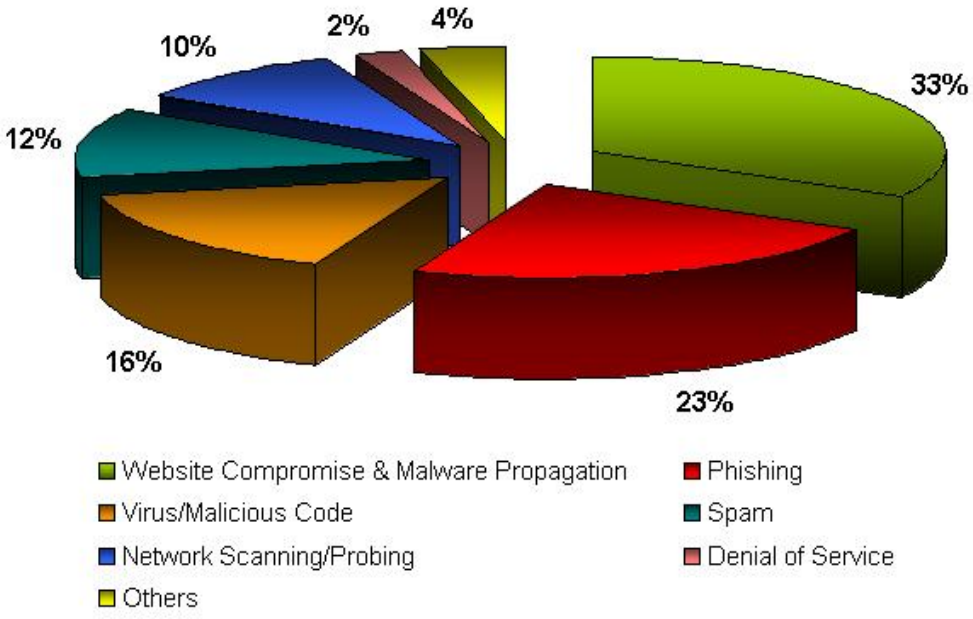

Figure 1. Summary of incidents handled by CERT-In during 2008

2.3.3 Incident Trends

CERT-In has observed many new innovative attack trends during 2008. The prominent types of attacks were malware propagation through compromised websites. Attackers exploited Web application vulnerabilities, especially SQL injection, to compromise websites and inject iFrame and Javascript links to malicious websites to propagate malware through drive by downloads. Toolkits such as mPack, Neosploit, Random JS CuteQQ, AdM, FirePack, were actively used in these attacks.

Many incidents of mass scale SQL injection on websites running ASP were reported since March 2008. Subsequently the ASPROX botnet actively compromised many websites through SQL injection and redirected users of these websites to malicious domains hosted on Fastflux DNS. Similarly rise in exploitation of Cross site scripting and Remote File Inclusion (RFI) attacks to exploit vulnerabilities in PHP were also observed.

There has been a massive increase in the number of Trojans such as 'Trojan.FakeAV.Winfixer' pretending to be Antivirus products known as "scareware".

Malware was also propagated using various social engineering techniques through malicious .doc, pdf , codec files , autorun methods, and spamming of popular news items.

CERT-In handled various cases of information theft through Trojans such as WOW, Hupigun, Nethell, Zbot, affecting users of online transactions.

Many incidents of propagation of Conficker worm exploiting Microsoft Windows Server Service vulnerability (MS08-067) were reported.

CERT-In has observed different types of spam such as Image-based, Animated GIF, PDF spam, Spam messages containing complicated HTML frameworks that intersperse random characters between the actual spam text.

The phishing attacks reported in 2008 were primarily carried out against Financial services and e-commerce sector. While phishing attacks on Financial services sector accounted for 59% of the total phishing attacks, the second most targeted sector is E-Commerce sector which accounts for 37% of the total number. The phishing incidents affecting Indian Financial Institutions were around 36% of total phishing incidents reported, while remaining incidents were affecting brands of other countries. Further, domain phishing incidents through Registrar impersonation were also reported.

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 organizations. In all 5475 numbers of defacements have been tracked. Most of the defacements were done for the websites under .in domain. In total 3042 .in domain websites were defaced.

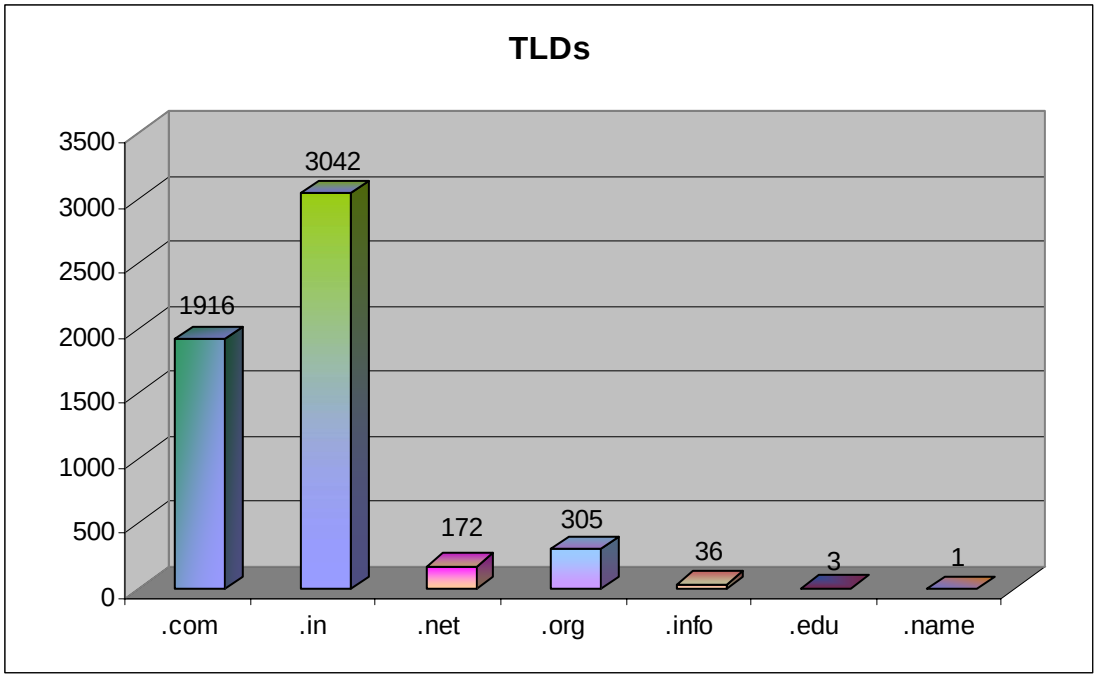

Figure 2. Indian websites defaced during 2008 (Top level domains)

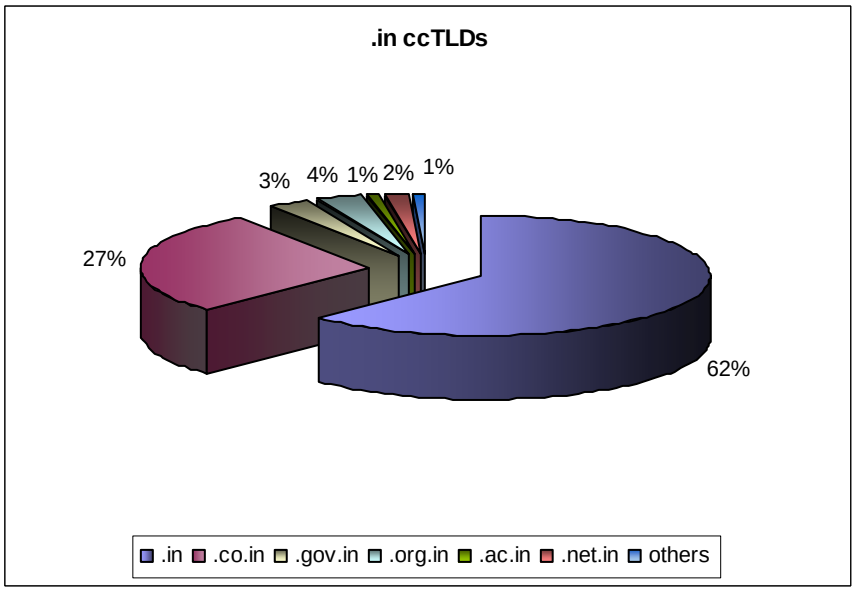

Figure 2.1 .in ccTLD defacements during 2008

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 2332 open proxy servers were tracked in the year 2008. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

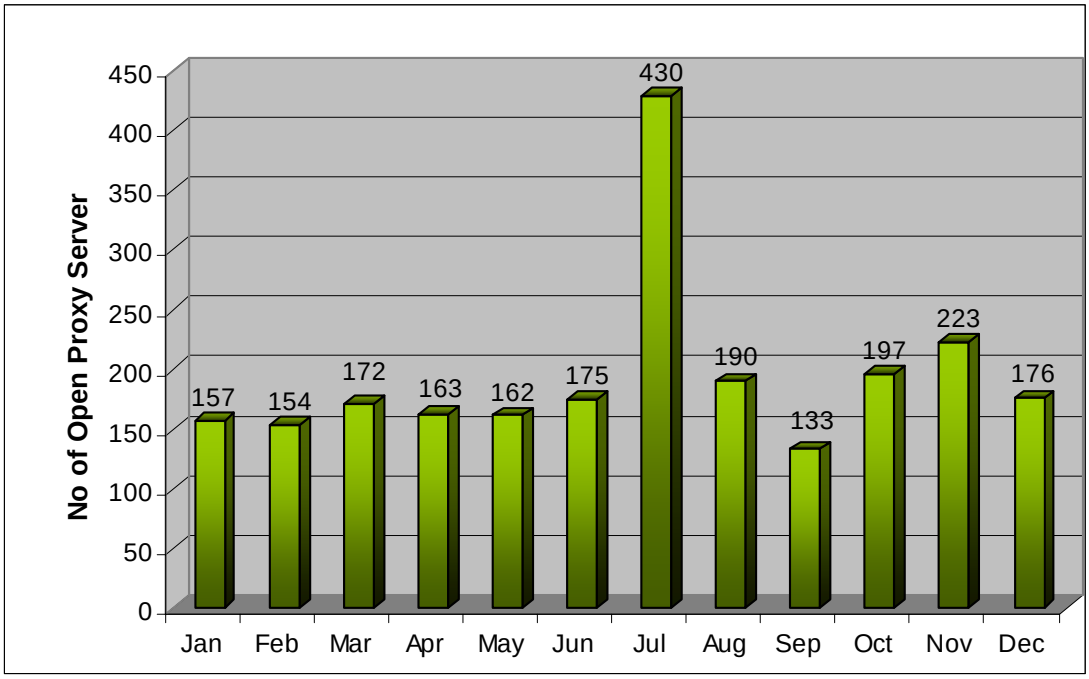

Figure 3. Monthly statistics of Open Proxy Servers in 2008

2.4.3 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. After tracking the IP addresses of Command and Control servers and Bots operating within India, actions are being taken to clean the respective systems and prevent malicious activities. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2008.

Month	Number of Bot Infected Systems	C&C Servers
January	2102	2
February	1279	10
March	15160	19
April	8514	14
May	6182	12
June	5537	13
July	74753	2
August	7055	3
September	5903	4
October	5219	3
November	6435	2
December	8866	4

Figure 4. Botnet statistics in 2008

2.5 Computer Forensics

CERT-in has established the facility for Computer Forensics for investigation of cyber crimes and to provide hands on training to the law enforcement agencies and judiciary. This infrastructure is being augmented to include network forensics and mobile forensics investigation facility. CERT-In is cooperating with defence, banks, judiciary and law enforcement agencies in training their officials as well as extending the support in investigation of cyber crimes.

3.0 Events organized/ co-organized

3.1 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 2008.

- Workshop on "Mail Server Security" on 29th January, 2008
- Workshop on "Implementation of Information Security Management in Government & Critical Sector Organizations" on 12th February, 2008
- Workshop on "Database Security and Auditing" on 28th March, 2008
- "Consumer Information Security Awareness Week" during 1-7 May 2008 jointly organised with Confederation of Indian Industry
- Workshop on "Computer Forensics for System Administrators" on May 07, 2008
- Workshop on "Network Security" on 25th June, 2008
- Workshop on "Windows Web Server Security" on 26th June, 2008
- Workshop on "Linux Security" on 31st July, 2008
- Workshop on "DNSSEC in India" on 18th August, 2008
- Workshop on "Web Application Security" on 21st August, 2008
- Workshop on "Cryptographic Primitives" on 29th August, 2008
- Workshop on "Cyber Security: Latest Attack Methods" on 04th September, 2008
- Workshop on "Intrusion Prevention System Technology" on 05th September, 2008
- Workshop on "Wireless Security" on 29th September, 2008
- Workshop on "Information Security Best Practices and Compliance" on 30th September, 2008
- Workshop on "Information Security-Risk Management and Business Continuity Management" on 27th November, 2008
- Workshop on "Identity Theft and Access Management" on 14th November, 2008
- Workshop on "Crimeware and Financial Frauds" on 5th November, 2008
- "Cyber Security Awareness Program" jointly organised with Data Security Council of India during 10-12 November 2008
- Workshop on "Managing Organization's Network Security" on 16th December, 2008

3.2 Forums

CERT-In, Department of Information Technology and Confederation of Indian Industry (CII) have established the Information Security Advisory Forum to foster cooperation between government, industry, consumer and law enforcement agencies on information security issues. As part of its many activities the Forum organizes Conferences, Training and Awareness Programs for the internet consumers (that include children, parents and teachers) who are often susceptible to cyber attacks, and aims to provide tools and resources to counter such threats.

CERT-In is collaborating with National Association of Software & Service Companies (NASSCOM) and Data Security Council of India to spread the cyber security awareness and facilitate interaction with various user groups.

4.0 Achievements

4.1 Presentations

Various lectures were delivered by the staff of CERT-In in the national and international workshops/conferences/seminars.

CERT-In participated in the following international seminars/conferences:

- Botnet Task Force Conference held in Lyon, France in February 2008
- Digital Phishnet Conference held in San Diego, USA in September 2008
- Internet Governance Forum meeting held in Hyderabad, India in December 2008
- Association of Antivirus Asia Researchers (AVAR) Conference held in New Delhi, India in December 2008

4.2 Publications

The following papers were published by CERT-In in the year 2008:

1. Whitepaper "Analysis of Phishing Incidents year-2007" CIWP-2008-01

   This document provides analysis of phishing incidents reported to CERT-In during the year 2007. The phishing incidents described in the document includes the cases in which either the phishing websites are hosted in India or domain registrant belongs to India. The document provides details on the incidents analyzed, targeted sectors, brands hijacked etc.

2. Guidelines for Auditing and Logging (CISG-2008-01)

   This guideline attempts to provide some insights into the issues related to Auditing and Log Management and suggest best practices for enabling and maintaining Auditing and logging on Windows hosts, Linux hosts, Microsoft IIS Web server, Apache Web server, Oracle 10g Database Server and Microsoft SQL Server 2005. Implementation of these best practices will enable administrators to acquire vital information to identify and respond to the computer security incidents.

3. Case study "Website compromise and launch of further attacks by exploiting PHP Remote File Inclusion vulnerability" (CICS-2008-01)

   The case study provides analysis of the attack and identified vulnerabilities which were exploited to compromise the website. It also provides appropriate countermeasures to secure webserver and web applications from such type of attacks.

4. Case study "Website compromise and launch of further attacks by exploiting SQL injection vulnerability" (CICS-2008-02)

   This case study provides analysis of mass scale SQL Injection attacks used to compromise websites and inject Javascript links to malicious websites.

5. Paper titled "Propagation of malware through compromised websites: Attack trends and countermeasures" (11^{th} International AVAR Conference, New Delhi, India)

   This paper attempts to examine the current trends in malware propagation and functionalities of large scale botnets such as operating Fast Flux DNS, hosting of malicious websites and injecting malicous links on legitimate websites. Various types of attacks on Indian websites, observed by CERT-In are examined. Typical attack scenarios are discussed in detail. The mitigation of these threats demands greater cooperation among various agencies such as

CERTs, Security vendors, ISPs, Domain Registrars. Ways and means of such cooperation are explored.

4.3 Awards

A staff member of CERT-In Mr. Madhur Verma was awarded as "Most Valuable Professional" in the area of Consumer Security by Microsoft in December 2008.

5.0 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 member of FIRST since December 2006. CERT-In has become full member of Asia Pacific CERT (APCERT) since August, 2008. CERT-In has become Research Partner of Anti-Phishing Working Group (APWG) in May 2008.

5.1 MoUs:

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. Members of CERT-In visited Mauritius for setting up of CERT-MU in Mauritius and provided training on CERT operations to technical staff of CERT-Mauritius. CERT-MU has been operationalised and launched in May 2008.

5.2 Drills

- CERT-In participated in the ASEAN CERTs Incident Handling Drill (ACID 2008) held on 30th July 2008.
- CERT-In participated in the APCERT International Incident Handling Drill 2008 held on 4th December, 2008.

6.0 Future Plans/Projects

CERT-In has been evolved as the most trusted referral agency in the area of information security in the country. CERT-In is regularly interacting with CISOs of Critical Infrastructure Organisations and sectorial CERTs to ensure security of the critical systems, collaboration with IT product and security vendors to mitigate the vulnerabilities in various systems, 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 implementing a project for Attack Detection and Threat Assessment at ISP and organisation level. This project will enable detection of cyber threats and attacks and issuance of early warning to take appropriate countermeasures to mitigate the attacks and contain the damage.

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