



Indian Computer Emergency Response Team (CERT-In)

Annual Report (2009)

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

Indian Computer Emergency Response Team (CERT-In)

1.0 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.

In the 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 2009 is given in the following table:

Activities	Year 2009
Security Incidents handled	8266
Security Alerts issued	29
Advisories Published	61
Vulnerability Notes Published	157
Case Studies Published	1
Trainings Organized	19
Indian Website Defacements tracked	6023
Open Proxy Servers tracked	2583
Bot Infected Systems tracked	3509166

Table 1. CERT-In Activities during year 2009

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 1000 Point-of Contacts (PoC) and Chief Information Security Officers (CISO). As a proactive measure, CERT-In has also empanelled 40 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 organisations is regularly reviewed by CERT-In with the help of a test network.

CERT-In also conducted a cyber security mock drill to assess the preparedness of organizations in the critical sector to withstand cyber attacks.

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. 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. CERT-In in collaboration with CII, NASSCOM and Microsoft have created a portal “secureyourpc.in” to educate consumers on cyber security issues.

2.3 Incident Handling Reports

2.3.1 Summary of Computer Security Incidents handled by CERT-In during 2009

In the year 2009, CERT-In handled more than 8000 incidents. 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 handled is given below:

Security Incidents	2004	2005	2006	2007	2008	2009
Phishing	3	101	339	392	604	374
Network Scanning / Probing	11	40	177	223	265	303
Virus / Malicious Code	5	95	19	358	408	596
Spam	-	-	-	-	305	285
Website Compromise & Malware Propagation	-	-	-	-	835	6548
Denial of Service	-	-	-	-	54	15
Others	4	18	17	264	94	145
Total	23	254	552	1237	2565	8266

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.

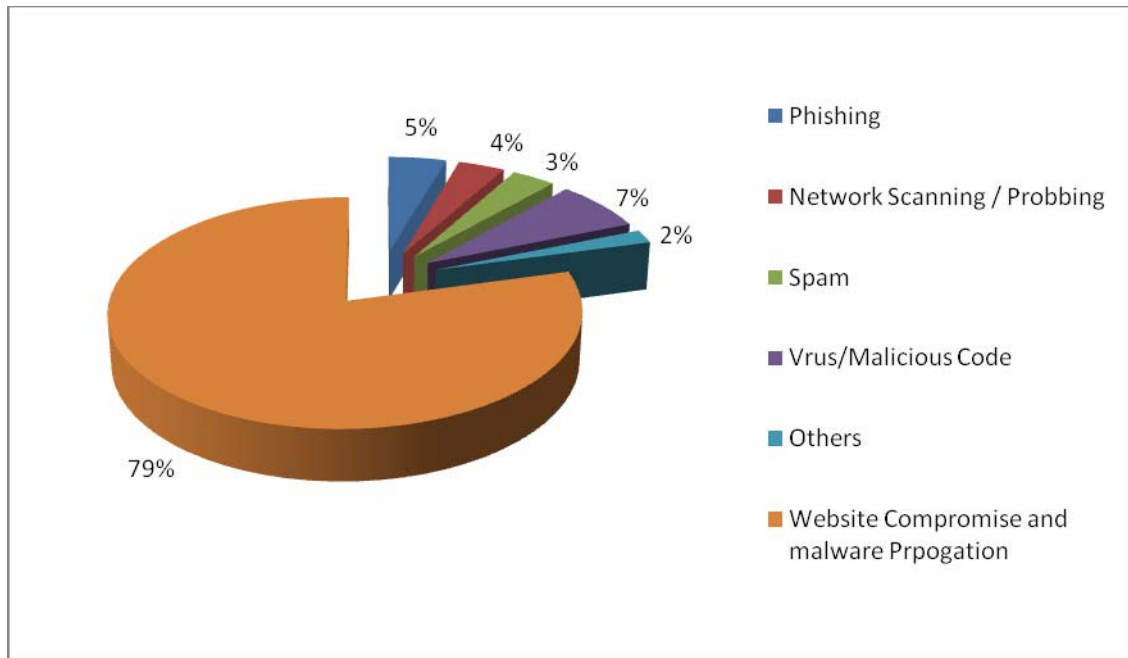


Figure 1. Summary of incidents handled by CERT-In during 2009

2.3.3 Incident Trends

During the year 2009 CERT-In handled several incidents of intrusions into websites and injecting iFrame and Java script to redirect visitors to malicious websites. By exploiting vulnerabilities such as SQL injection and XSS flaws, trusted websites are converted to malicious websites serving content that contains client side exploits

CERT-In has observed that commonly used programs such as Adobe PDF Reader ,Adobe Flash and Microsoft office are exploited widely to steal data from the target computers and also to install back doors through which the attackers can gain control for further exploitations.. Also there has been an increase in the number of Zero Day Vulnerabilities.

It has been observed that the Koobface worm propagating through social networking sites such as Facebook, MySpace, hi5, Bebo, Friendster and Twitter etc.

It is reported that a stealth worm “Psybot” targeting home routers and DSL modems are in the wild. The worm infects any of a family of Linux Mipsel devices that contain one of several administration interfaces.

It has been reported that Worm:iPhoneOS/Ikee and variants - the first worm to target the Apple iPhone- are in the wild spreading using the default root password in SSH among jail-broken iPhones.

Incidents of stealing of user credentials due to infection of client systems by Zeus and Clampi botnets were on the rise. Various variants of Win32/Zbot , part of Zeus botnet , observed.

Incidents of malicious domains such as Gumblar that was hosting the malware exploit , has been actively used for compromising thousands websites. It is a drive by download with multiple stages. The first stage of exploit is to attempt to inject malicious code onto the vulnerable website primarily through stolen FTP credentials, poor configuration settings, vulnerable web application etc.

Propagation of malware through new and innovative techniques such as impersonation of "mail administrator" etc were noticed.

The Conficker worm which transpired in November 2008 was propagating widely till May 2009 infecting large number of systems in India.

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 6023 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.

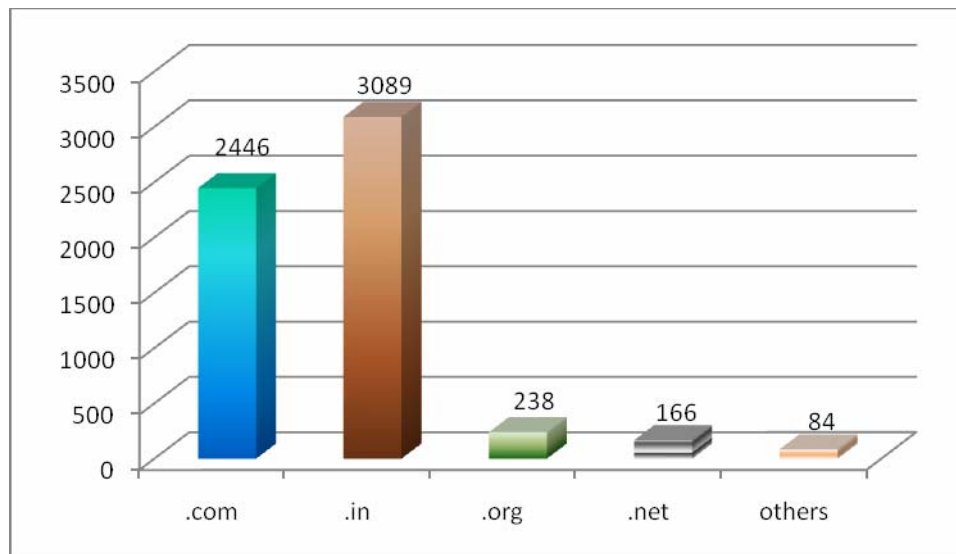


Figure 2. Indian websites defaced during 2009 (Top level domains)

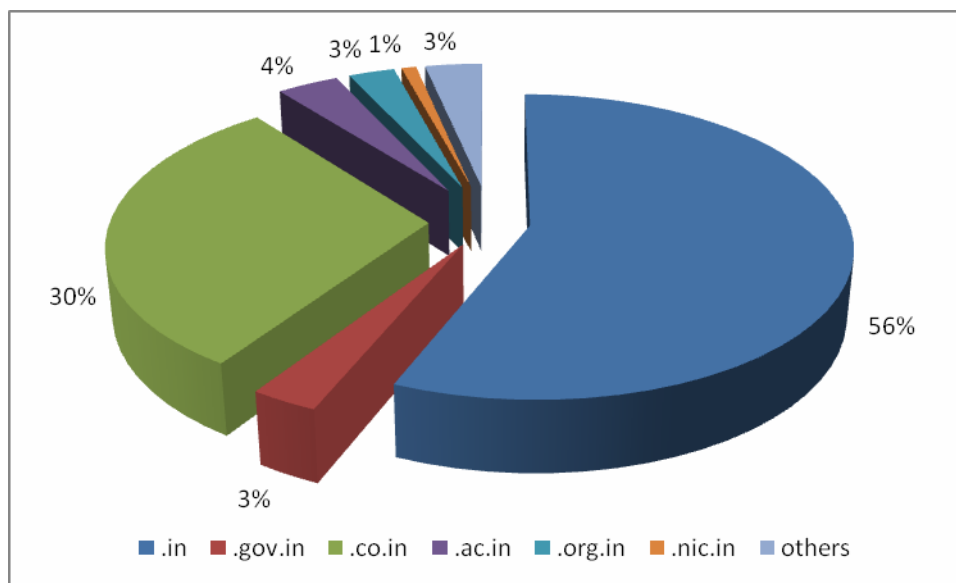


Figure 2.1 .in ccTLD defacements during 2009

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 2583 open proxy servers were tracked in the year 2009. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

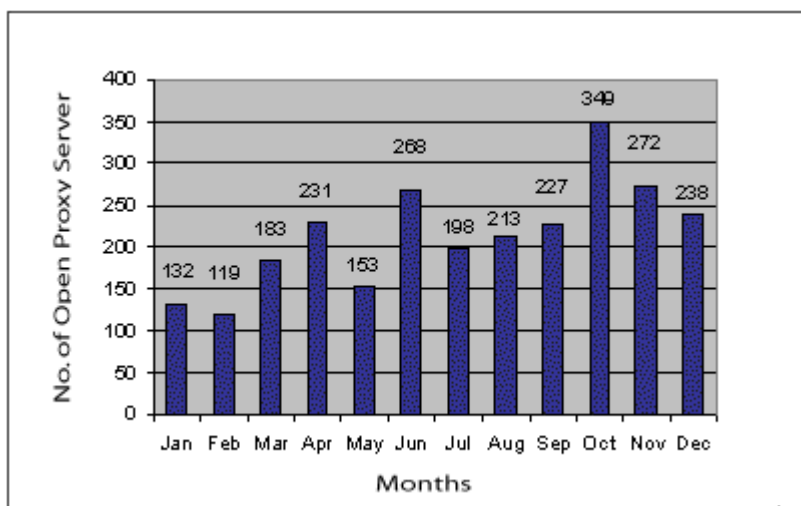


Figure 3. Monthly statistics of Open Proxy Servers in 2009

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 2009.

Month	Number of Bot Infected Systems	C&C Servers
January	277697	5
February	590362	07
March	30025	02
April	1495485	07
May	453076	07
June	68824	10
July	28854	-

August	188295	-
September	202478	-
October	96114	-
November	49759	18
December	28197	-

Figure 4. Botnet statistics in 2009

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 2009.

- Workshop on " Linux Security" on December 17-18, 2009
- Workshop on " Secure Code Review for PHP Applications" on December 08, 2009
- Workshop on " Secure Coding in PHP: Developing Defensive Applications " on December 07, 2009
- Workshop on "Secure Code Review for JAVA Applications" on November 20, 2009
- Workshop on "Developing Secure Code in JAVA" on November 06, 2009
- Workshop on " Database Server Security" on October 14, 2009
- Workshop on " Advanced Web Application Security" on September 23, 2009
- Workshop on " Computer Forensics " on August 27-28, 2009
- Workshop on " Threat Infiltration and Mitigation " on August 3, 2009
- Workshop on "Defending Phishing Attacks" on July 30, 2009
- Workshop on " Identity and Access Management " on July 24, 2009
- Workshop on "Web Application Security – Current Trends" on July 3, 2009
- Workshop on "Windows Security" on June 26, 2009
- Workshop on "Wireless Security" on May 28-29, 2009
- Workshop on "Critical Information Infrastructure Resiliency" on May 19-21, 2009
- Workshop on "Application Code Security Review" on March 25, 2009
- Workshop on "Development of Secure Code guidelines for .NET" on March 18, 2009
- Workshop on " Web Application Security : Advanced Topics" February 09, 2009
- Workshop on "Application Security : Latest Trends" , January 30, 2009

3.2 Forums

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

4.0 Publications

The following were published by CERT-In in the year 2009:

1. Paper titled “cyber terrorism: current threats and challenges” (52nd Annual Technical Convention on Technology and Terror role of ICT in war against terror September 26-27,2009 conducted by IETE) . This paper examines the current threats of cyber terrorism and methods of cyber criminals. The challenges in combating the cyber threats and possible solutions are highlighted from the technical and social perspective.
2. Series of Mass iframe Injection on Websites-Serving Blended Malware (CICS-2009-01). It has been observed that thousands of websites have been compromised and infected with iframe script tags linking users to malicious JavaScript file hosted on domain " a0v [d0t] org ". It has been found that most of the websites running in support of ASP engine are infected. Details of multiple redirections and infection is illustrated in CERT-In Case Study CICS-2009-01.
3. Survey "State of Data Security and Privacy in the Indian Industry" conducted in association with Data Security council of India (DSCI). This is an attempt to assess the preparedness of Indian organizations in IT and IT enabled services facing the challenge of securing their IT infra structure. The results of the survey showed that information security is getting its due priority among majority of enterprises in the country.
4. Monthly security bulletins: Monthly security bulletin comprises of Statistics of incidents handled by CERT-In, information on vulnerabilities in various operating systems and applications tracked, Cyber intrusion trends and other relevant IT security issues.

5.0 International collaboration

CERT-In has established collaborations with international security organisations and CERTs to facilitate exchange of information related to latest cyber security threats and international best practices. CERT-In is a member of Forum of Incident Response and Security Teams (FIRST), APCERT and Anti-Phishing Working Group (APWG).

5.1 Drills

- CERT-In has successfully participated in ASEAN CERTs Incident Handling Drill (ACID 2009) held in July 2009 involving CERTs from Asia Pacific region and Europe.

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. Following are the future plans:

- Regular interaction with CISOs of Critical Infrastructure Organisations and sectorial CERTs to ensure security of the critical systems.
- Development and implementation of a framework to enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks
- Collaboration with IT product and security vendors to mitigate the vulnerabilities in various systems and cooperation with international CERTs and security organizations on information sharing and incident response
- Promotion of R&D activities in the areas of attack detection & prevention and Cyber Forensics

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
