Indian Computer Emergency Response Team (CERT-In)

Annual Report
(2010)

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

9th March 2011

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.

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

1.1.1 Establishment

CERT-In was operational since January 2004. The constituency of CERT-In is the Indian cyber community. In the Information Technology (Amendment) Act 2008, CERT-In has been designated to serve as the national agency in the area of cyber security.

1.1.2 Constituency

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

- 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
- Promotion best practices and periodic security assessment through Security Assurance Framework

2.1 Incident handling Reports

The summary of activities carried out by CERT-In during the year 2010 is given in the following table:

Activities	Year 2010
Security Incidents handled	**10315**
Security Alerts issued	**43**
Advisories Published	**72**
Vulnerability Notes Published	**274**
Security Guidelines Published	**1**
White papers/Case Studies Published	**1**
Trainings Organized	**26**
Indian Website Defacements tracked	**14348**
Open Proxy Servers tracked	**2492**
Bot Infected Systems tracked	**6893814**

Table 1. CERT-In Activities during year 2010

In the year 2010, CERT-In handled more than 10000 incidents. The types of incidents handled were mostly of Phishing, Malicious Code, Website compromise & propagation of malware and Network Scanning & Probing.

2.1.1 Incident Trends

During the year 2010 CERT-In handled several incidents of intrusions into websites and injecting iFrame and Java script to redirect visitors to malicious websites. By exploiting vulnerabilities in web applications trusted websites are infected with links to malicious websites serving content that contains client side exploits. The return of the attack toolkit Asprox has also been witnessed with a slightly different SQL injection method to penetrate into the web applications.

A rise in the malware infections was observed. Prominent botnet infections were due to Conficker and Mariposa (Rimecud) worms. On the crimeware front, Zeus (the infamous password stealing trojan) was the most effective botnet. Trojan SymbOS/Zitmo - Symbian malware was also propagated by the ZeuS botnet. It is named as **Z**eus **I**n **T**he **MO**bile. The backdoor trojan acts as a spyware and forwards some of the victims SMS messages to another phone number controlled by the malware. Bot families like Pushdo, Taterf, were in the wild. Malware families like Waledac, Mebroot, Rustock were also observed as part of malicious code incidents.

One of the prominent malware with high damage potential is Stuxnet targets industrial control systems (ICS) by modifying the Programmable Logic Controllers (PLC). The threat made use of Windows rootkits , Antivirus evasion techniques, intriguing process injection and hooking, network infection routines, and a command and control interface.

It has been observed that Mariposa Botnet showed large number of infections. This botnet uses blended malwares for fast spread and due to download and execution of arbitrary malicious executables the functionality of botnet is extended effectively.

Rise of WEB 2.0 attacks had been witnessed largely. The social networking sites were used largely to send spam mails (normally a link shortened with *tinyurl* facility) and trick unsuspecting users to fall victim to malware infection. Koobface botnet targeted Facebook users disguising as fake video player/ application.

Fake Antivirus programs posed a rising threat using SEO poisoning techniques to entice users to visit malicious websites and deliver malicious scareware.

Vulnerabilities in Adobe products and Flash player were actively exploited in targeted attacks. Malware targeting mobile platforms also were reported.

2.1.2 Tracking of Indian Website Defacements

CERT-In is tracking the defacements of Indian websites and suggesting suitable measures to harden the web servers to concerned organizations. In all 14348 numbers of defacements were tracked in the year 2010. Most of the defacements were done for the websites under ***.in*** domain. In total 9772 ***.in*** domain websites were defaced.

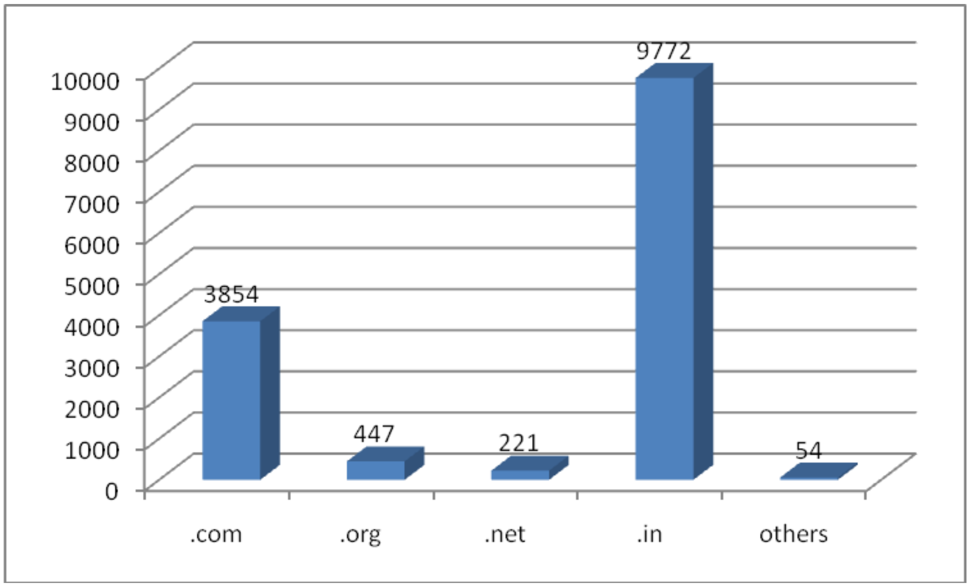

Figure 2. Indian websites defaced during 2010 (Top level domains)

2.1.3 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 2492 open proxy servers were tracked in the year 2010. The month-wise distribution of open proxy servers tracked during this year is shown in the figure 3.

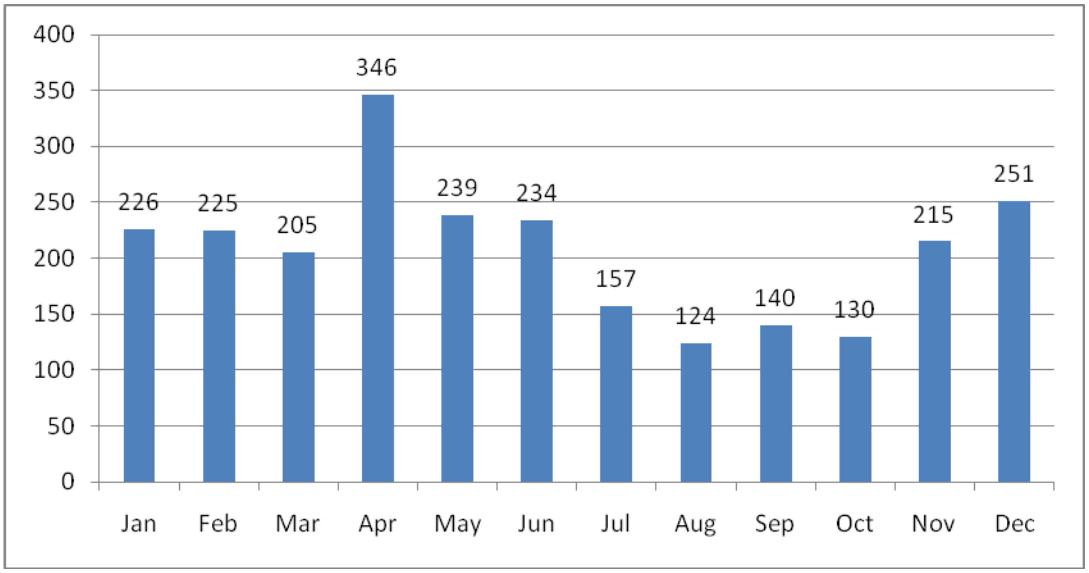

Figure 3. Monthly statistics of Open Proxy Servers in 2010

2.1.4 Botnet Tracking and Mitigation

CERT-In is tracking Bots and Botnets involving Indian systems. Users were advised on suitable measures for dis-infection. Figure 4 shows the number of Bot infected systems and Command & Control servers tracked in 2010.

Month	Number of Bot Infected Systems	C&C Servers
January	35659	19
February	158851	16
March	69183	-
April	1736353	07
May	2116482	-
June	39600	-
July	32242	13
August	263196	9

September	153196	3
October	274224	11
November	617365	13
December	1661156	16

Figure 4. Botnet statistics in 2010

2.2 Abuse statistics

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

Security Incidents	**2004**	**2005**	**2006**	**2007**	**2008**	**2009**	**2010**
Phishing	3	101	339	392	604	374	508
Network Scanning / Probing	11	40	177	223	265	303	477
Virus / Malicious Code	5	95	19	358	408	596	1817
Spam	-	-	-	-	305	285	981
Website Compromise & Malware Propagation	-	-	-	-	835	6548	6344
Others	4	18	17	264	148	160	188
Total	**23**	**254**	**552**	**1237**	**2565**	**8266**	**10315**

Table 2. Year-wise summary of Security Incidents handled

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. The following training programmes were conducted during 2010.

- Workshop on "Stuxnet Malware Threats and Response Measures" on December 15, 2010
- Workshop on "Information Security and Cloud Computing" on December 08, 2010
- Workshop on "Web Server Security" on November 29, 2010
- Workshop on "Intrusion Detection and Mitigation" on November 12, 2010
- Two Workshops on "Secure Coding in C/C++" on October 26-29, 2010 in association with JPCERT/CC
- Workshop on "Windows Security" on October 20, 2010
- Workshop on "Mail Server Security" on October 08, 2010
- Workshop on "Secure coding in .NET" on September 24, 2010
- Workshop on "DDoS Attacks & Mitigation" on September 03, 2010
- Workshop on "Information Security Policy Compliance for CISOs" on September 01, 2010
- Workshop on "DNS Security" on August 20, 2010
- Workshop on "VoIP Security" on August 06, 2010
- Workshop on "Vulnerability Assessment & Penetration Testing" on July 21, 2010
- Workshop on "Crimeware and Financial Frauds" on June 30, 2010
- Workshop on "Secure Code Development in PHP" on June 24, 2010
- Workshop on "Wireless Security" on May 06, 2010
- Workshop on "Virtualization Security and Challenges" on April 23, 2010
- Workshop on "Computer Forensics : Seizing & Imaging of Digital Evidence" on April 07, 2010
- Workshop on "Secure Architecture for System Administrators" on February 26, 2010
- Workshop on "Security Information and Event Management" on February 17, 2010
- Workshop on "Network Security" on January 28, 2010
- Workshop on "Data Centre Security" on January 15, 2010
- Workshop on "Computer Forensics : Seizing and Imaging of Digital Evidence" on January 04, 2010

3.2 Drills

Cyber Security Mock Drills are being conducted to assess preparedness of organizations in critical sectors to withstand cyber attacks. First Cyber security mock drill was conducted in November 2009, the second mock drill was conducted in March 2010 and the third mock drill was conducted on 11th December 2010.

4.0 Achievements

4.1 Presentation

Lectures and presentations have been made by members of CERT-In in various workshops and seminars conducted in the country.

4.2 Publications

The following were published by CERT-In in the year 2010:

1. CERT-In Guide for Securing IIS 7.0 Web Server**:** The purpose of the guideline is to recommend security practices for designing, implementing and operating publicly accessible Microsoft Internet Information Services (IIS) 7.0 Web servers, including related network infrastructure issues
2. Case study on Mariposa Botnet (CICS-2010-01): The case study discusses the propagation and damage capabilities of Mariposa Botnet which is detected as Autorun/Palevo/Rimecud/Pilleuz by different Antivirus systems.
3. 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).

CERT-In has successfully participated in ASEAN CERTs Incident Handling Drill (**ACID 2010**) held in September 2010 and **APCERT Drill 2010** held in January 2010.
Two Training programmes on **"Secure C/C++ Programming"** were conducted in collaboration with **JPCERT/CC** in October 2010.

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:

- Development and implementation of a framework to enable organisations to respond to cyber incidents and assess the preparedness of organisations to withstand cyber attacks. Continuous assessment and improving the security posture of Critical Infrastructure Organisations through regular interaction with CISOs and sectorial CERTs.
- Implementation of projects in the areas of attack detection & prevention

- Promotion of research and development in malware 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