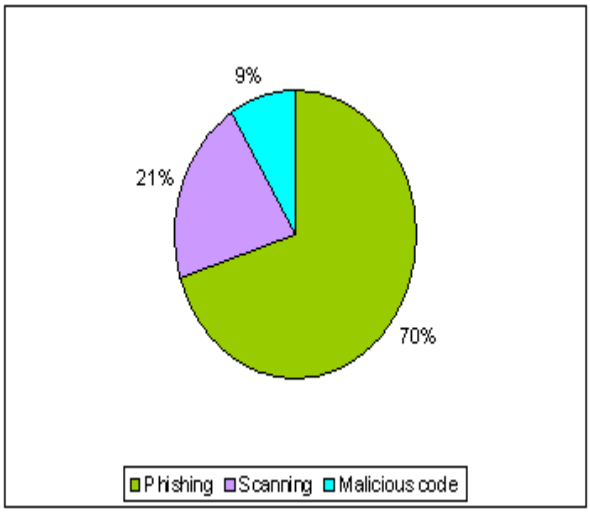
Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)

CERT-In Monthly Security Bulletin October 2006

Cyber Intrusion Trends

In this month 43 security incidents were reported to CERT-In from various national/ International agencies. A large number of phishing incidents were reported in this month as shown in the chart below. 9% incidents related to virus/worm under the malicious code category and 21% unauthorized scanning incidents were reported. As compared to previous month phishing incidents have increased and scanning incidents have decreased.

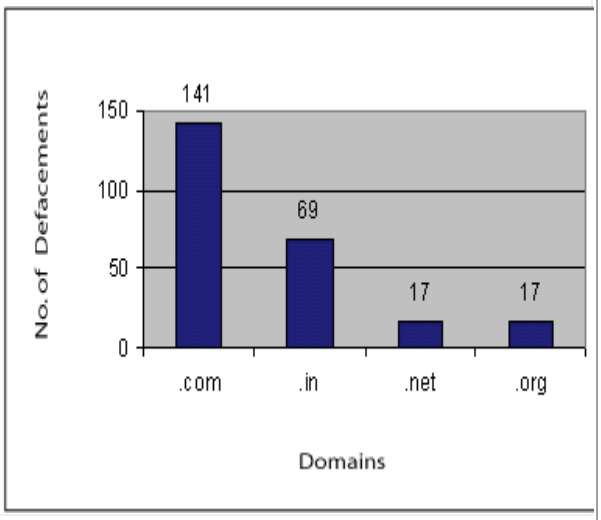
Cyber Intrusion during October 2006



Indian Websites Defacement

In total 244 Indian websites were defaced during this month. Mostly the websites under .com domain were defaced by the hacker groups. A chart depicting Top Level Domain(TLD) wise defacements is shown in the figure.

Statistics of Defaced Indian Websites in October 2006

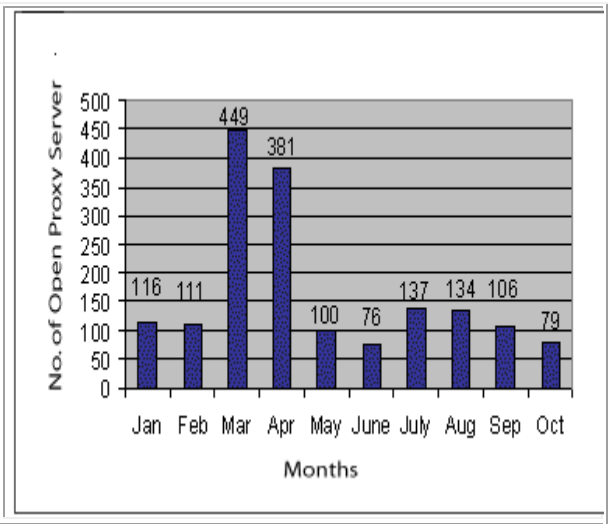


Open proxy servers

Any proxy server that doesn't restrict its client base to its own set of clients and allows any other client to connect to it, is known as an open proxy server. An open proxy server will accept client connections from any IP address and make connections to any Internet resource.

Statistics of Open Proxy Server tracked during 2006 (up to October)

CERT-In tracked 79 open proxy servers functioning in India during October 2006. All the concerned ISPs were alerted immediately to shut down the open proxy servers. A bar chart of open proxy servers tracked during this year is shown in the figure.



Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during October 2006 and their countermeasures alongwith wide-spreading malicious code like virus/ worm/Trojan are given below:

High Vulnerabilities

Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Microsoft PowerPoint	Microsoft PowerPoint Remote Code Execution Vulnerability	October 11, 2006	CIVN-2006-96
Microsoft Excel	Microsoft Excel Malformed DATETIME Record, STYLE Record, Lotus file, COLINFO Record Vulnerabilities	October 11, 2006	CIVN-2006-97
Microsoft Word	Multiple Remote Code Execution Vulnerabilities in Microsoft Word	October 11, 2006	CIVN-2006-98
Microsoft XML	Microsoft XML Core Services vulnerabilities	October 11, 2006	CIVN-2006-99
Microsoft Office	Microsoft Office Multiple Vulnerabilities	October 11, 2006	CIVN-2006-100
Microsoft	Multiple Vulnerabilities in Microsoft Windows, Microsoft Office and Microsoft XML Core Services	October 11, 2006	CIAD-2006-37
Database	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
Oracle	Multiple Remote SQL Injection and Security Bypass Vulnerabilities in Oracle Products	October 18, 2006	CIAD-2006-38
Unix	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
PHP	PHP unserialize() Array Creation Integer Overflow vulnerability	October 12, 2006	CIVN-2006-104
Apache	Apache Mod_TCL Remote Format String Vulnerability	October 17, 2006	CIVN-2006-106
Opera	Opera Software Opera Web Browser URL Parsing Heap Overflow Vulnerability	October 17, 2006	CVE-2006-4819
Mambo	Mambo MambWeather Module "mosConfig_absolute_path" File Inclusion	October 23, 2006	CVE-2006-5519
OpenSSH	Multiple vulnerabilities in OpenSSH	October 29, 2006	CVE-2006-5051 CVE-2006-5052

Medium Vulnerabilities			
Microsoft	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
Microsoft Windows	Microsoft .NET Framework 2.0(ASP.NET 2.0) Cross-Site Scripting Vulnerability	October 11, 2006	CIVN-2006-95
Microsoft Internet Explorer	Denial of Service in Server Service Vulnerability	October 11, 2006	CIVN-2006-101
Microsoft Windows	Multiple Denial of Service Vulnerabilities in Microsoft Windows TCP/IP IPv6	October 11, 2006	CIVN-2006-102
Microsoft Windows	Microsoft Windows Object Packager Dialogue Spoofing Vulnerability	October 11, 2006	CIVN-2006-103
Microsoft Windows	Microsoft Windows NAT Helper Components DNS Denial of Service Vulnerability	October 31, 2006	CIVN-2006-108
Microsoft Internet Explorer	Microsoft Internet Explorer 7 Popup Address Bar Spoofing Vulnerability	October 28, 2006	CIVN-2006-107
Unix	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
Linux Kernel	Linux Kernel "clip_mkip()" Denial of Service Vulnerability	October 13, 2006	CIVN-2006-105
PHP	PHP "ini_restore()" Security Bypass Vulnerability	October 10, 2006	CVE-2006-4625
Python	Python "repr()" Function Unicode String Handling Buffer Overflow Vulnerability	October23, 2006	CVE-2006-4980
Linux	kdelibs integer overflow vulnerability	October23, 2006	CVE-2006-4811
PHP-Nuke	PHP-Nuke "eid" SQL Injection Vulnerability	October23, 2006	CVE-2006-5525

Malicious Code Threats					
Title of Malicious Code	**Type**	**Overview**	**Aliases**	**Discovery Date**	**References**
Instant Messaging Worm_Sohanad	Worm	It is propagating in the wild via instant messaging applications like Yahoo instant messenger. It sends messages with malicious links to all the addresses contain in the contact list of Yahoo messenger user	No Alias W32.Imaut.A [Symantec], WORM_SOHANAD.A [Trend Micro]	October 3, 2006	http://www.cert-in.org.in/virus/worm_sohanad.htm
W32.Wikedir@mm	worm	It is a worm that spreads through email and file sharing networks. The worm installs a copy of	No Alias	October 17, 2006	http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-101715-1841-99&tabid=1

		backdoor on to the compromised computer.			

Security Guidelines

In this month CERT-In published a security guideline on **Securing IIS 6.0 Web Server.** A secure web server provides a foundation for the organization's hosting environment, where its configuration plays a critical role in the overall security of the Web applications and services . This guideline provides a step-by-step approach to secure the IIS 6.0 Web Server hosted on Windows 2003 platform. The guideline is available at

http://www.cert-in.org.in/knowledgebase/guidelines/cisg-2006-01.htm

Security Workshop

Workshop for Points-of-Contact from critical sectors on Cyber Security (31st October, 2006)

CERT-In organised the Workshop for the points of contact from critical sectors. The workshop was attended by chief information officers from the critical sectors. The workshop covered topics on Cyber Security and critical information infrastructure protection and case studies. The presentation material of the workshop is available at

http://www.cert-in.org.in/training/31oct06.htm

Security News

Cabinet approves changes in IT Act
[16 Oct, 2006 1731hrs IST INDIATIMES NEWS NETWORK]

DELHI : The Union Cabinet on Monday gave its approval to the amendment proposed in the Information Technology Act, 2000. The Information Technology Act was originally enacted in the year 2000, which primarily aimed to boost e-commerce in the country and also to create an enabling environment for e-Governance in the country. It provides a legal framework for transactions carried out using computers and the Internet technologies.

The Act was enacted keeping in view the technology directions and scenario existing at that time. As the technology is an ever-evolving process for providing efficient and cost effective options, it was felt that a fresh look into the technology driven law needs to be given.