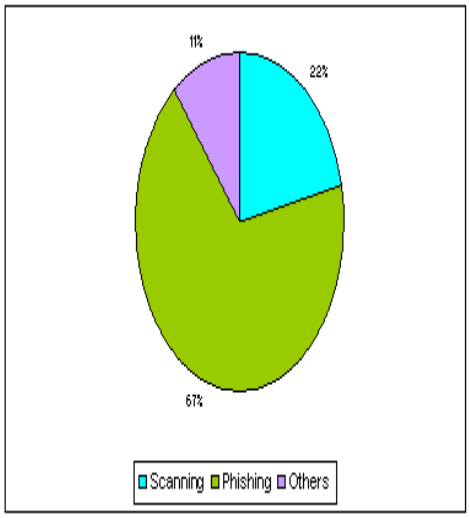
Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)

CERT-In Monthly Security Bulletin December 2006

Cyber Intrusion Trends

37 security incidents were reported to CERT-In from various national/ International agencies in December 06.As shown in the figure 67% phishing incidents were reported in this month.22% unauthorized scanning incidents and 11% incidents related to virus/worm under the malicious code category were reported. As compared to previous month the number of phishing incidents have decreased while virus/worm incidents have increased.

Cyber Intrusion during December 2006



Indian Websites Defacement

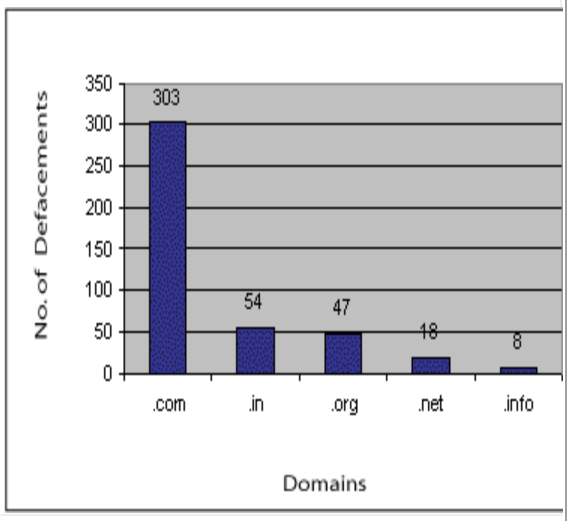
In total 430 Indian websites were defaced during December 06. Mostly the websites under .com domain were defaced by the hacker groups. A chart depicting Top Level Domain(TLD) wise defacements is shown in the figure.

The vulnerabilities which might have exploited for the defacements are:

PHPNews "link_temp.php" Cross-Site Scripting Vulnerabilities
December 04 , 2006
CVE-2006-6356
CVE-2006-6357

PHP "sscanf()" Format Specifier Handling Security Bypass and Code Execution Vulnerability
September 26, 2006
CIAD-2006-35

Statistics of Defaced Indian Websites in December 2006



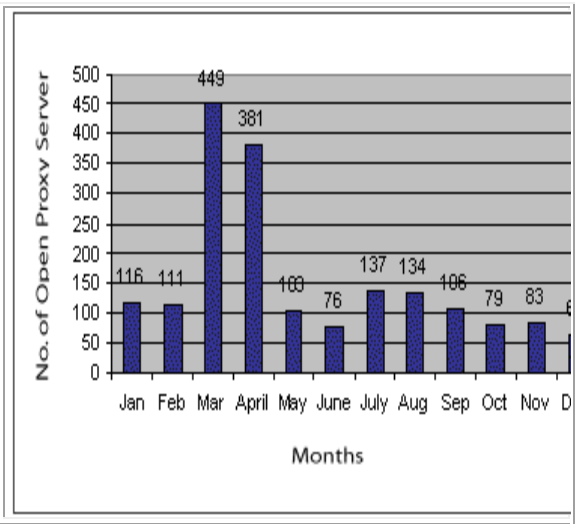
Open proxy servers

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

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

address and make connections to any Internet resource.

CERT-In tracked 62 open proxy servers functioning in India during December 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.



CERT-In Participated in APCERT International Incident Handling Drill 2006

On 19 th December, 2006 Asia Pacific Computer Emergency Response Team (APCERT) conducted APCERT International Incident Handling Drill, 2006. This annual drill was aimed to test the timeliness and response capability of leading Computer Incident Response Teams (CSIRTs) from Asia Pacific region. This year, 15 security Teams from 13 economies (Australia, Brunei, China, Hong Kong, India, Japan, Korea, New Zealand, Malaysia, Singapore, Thailand, Chinese Taipei and Vietnam) participated in the APCERT Drill 2006. CERT-In actively participated in the APCERT Drill, 2006.

[More]

Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during December 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 Word Document	Microsoft Word Document Handling Memory Corruption and Code Execution Vulnerability	December 06, 2006	CIVN-2006-125
Microsoft Windows	Microsoft Windows Media Player ASX Playlist Heap Overflow Vulnerability	December 13, 2006	CIVN-2006-126
Microsoft Internet Explorer	Microsoft Internet Explorer Memory Corruption and TIF Folder Information Disclosure Vulnerabilites	December 13, 2006	CIVN-2006-127
Microsoft Windows	Microsoft Windows Media Format Remote Code execution Vulnerability	December 13, 2006	CIVN-2006-132
Microsoft Word	Microsoft Word Remote Code Execution Vulnerability	December 28, 2006	CIVN-2006-135
Microsoft Word	Microsoft Word malformed data structure vulnerability	December 28, 2006	CIVN-2006-136
Microsoft Windows	Multiple Vulnerabilities in Microsoft Windows, Internet Explorer, Outlook Express, Visual Studio and Windows Media Player	December 13, 2006	CIAD-2006-46
Microsoft Internet Explorer	Microsoft Internet Explorer ADODB.Connection code execution vulnerability	December 28, 2006	CIVN-2006-138
Unix	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
KOffice	KOffice readBigBlockDepot () PPT file handling integer overflow vulnerability	December 13, 2006	CIVN-2006-133

Sun Java JRE	Vulnerabilities in Sun Java JRE	December 21, 2006	CIAD-2006-49
Sun Java	Sun Java Runtime Environment Multiple Remote Integer and Buffer Overflow Vulnerabilities	December 20, 2006	CVE-2006-6731
GnuPG and Linux Kernel	Multiple Vulnerabilities in GnuPG and Linux Kernel	December 19, 2006	CIAD-2006-47
Linux Kernel	Linux Kernel Unspecified "init_timer()" Security Issue	December 29, 2006	CVE-2006-5749
Xine-lib Real Media, GnuPG and libgsf	Buffer Overflow vulnerabilities in Xine-lib Real Media, GnuPG and libgsf	December 06, 2006	CIAD-2006-45
Database	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
Oracle	Oracle Portal Vulnerabilities	December 27, 2006	CIAD-2006-50
Medium Vulnerabilities			
Microsoft	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
Microsoft Windows	Microsoft Windows Print Spooler Denial of Service Vulnerability	December 05, 2006	CIVN-2006-124
Microsoft Windows	Remote Code Execution Vulnerability in SNMP	December 13, 2006	CIVN-2006-128
Microsoft Windows	Microsoft Windows File Manifest Corruption Vulnerability	December 13, 2006	CIVN-2006-129
Microsoft Windows	Windows Address Book Contact Record Vulnerability	December 13, 2006	CIVN-2006-130
Microsoft Windows	Remote Code Execution Vulnerability in Microsoft Windows RIS	December 13, 2006	CIVN-2006-131
Microsoft Windows	Microsoft Windows Workstation Service Denial of Service Vulnerability	December 28, 2006	CIVN-2006-134
Microsoft Windows	Windows CSRSS HardError Message Box Vulnerability	December 28, 2006	CIVN-2006-137
Unix	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
PHPNews	PHPNews "link_temp.php" Cross-Site Scripting Vulnerabilities	December 02, 2006	CVE-2006-6356 CVE-2006-6357
KDE JPEG	KDE JPEG kfile-info EXIF Denial of Service Weakness	December 04, 2006	CVE-2006-6297
Linux Kernel	Linux Kernel "ip_summed" Memory Corruption Vulnerability	December 08, 2006	CVE-2006-6333
Linux Kernel	Linux Kernel "do_coredump" Function Security Bypass and File Manipulation Vulnerability	December 15, 2006	CVE-2006-6304
Linux Kernel	Linux Kernel "mincore()" Deadlock Denial of Service	December 20, 2006	CVE-2006-4814
OpenOffice.org	OpenOffice.org Word Document Handling Client-Side Denial of Service Vulnerability	December 18, 2006	CVE-2006-6628
GNOME	GNOME Display Manager "gdmchooser" Host Name Handling Format String Vulnerability	December 15, 2006	CVE-2006-6105
Miscellaneous	**Title of Vulnerability**	**Discovery/Publish Date**	**CERT-In References & Patch Information**
Adobe	Adobe Reader / Acrobat AcroPDF ActiveX Control Vulnerability	December 01, 2006	CIVN-2006-123
Mozilla	Multiple Vulnerabilities in Mozilla Products	December 21, 2006	CIAD-2006-48
Malicious Code Threats			
Title of	**Type** **Overview** **Aliases**	**Discovery Date**	**References**

Malicious Code					
JS_QSPACE.A	worm	It is a JavaScript based worm that exploits an XSS vulnerability in the MySpace Web service. It also attempts to steal MySpace user credentials and modifies MySpace users profile in order to spread	JS_QSPACE.A [Trend Micro], JS/QSpace [McAfee]	December 3, 2006	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=JS%5FQSPACE%2EA
Allaple Worm	worm	It is a polymorphic network worm cause DoS (Denial of Service) attack on a few websites.	No Alias	December 8, 2006	http://www.cert-in.org.in/virus/allaple_worm.htm
Virus PE_Sality/Beagle	worm	It is a polymorphic virus which infects win32 PE executable files and uses an infected copy of a Beagle variant to make its propagation.	Win32.Sality.A [Computer Associates], Virus.Win32.Sality.{a-j} [Kaspesky Lab], W32.Sality.{a, b, d-l} [McAfee]	December 14, 2006	http://www.cert-in.org.in/virus/PE_Sality.htm
Trojan.Booha	Trojan	It is a Trojan horse program that downloads additional malware. It uses rootkit technology to hide its presence and gathers confidential information.	No Alias	December 8, 2006	http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-120812-1846-99&tabid=1
Trojan.Daum	Trojan	It is a Trojan horse that redirects Internet keyword searches through a	No Alias	December 13, 2006	http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-121314-2529-99&tabid=1

		remote server when visiting certain Web sites			
Happy New Year Worm	worm	It is a mass mailing worm which uses its own SMTP engine. It contains the string "HAPPY NEW YEAR" in the subject line of the mails.	Luder.A (Fsecure), W32/Dref-U (Sophos)	December 30, 2006	http://www.cert-in.org.in/virus/Happy_N_Year.htm

Security News

Cyber Crime Hits the Big Time in 2006
[Source: washingtonpost.com]

Call it the "year of computing dangerously."

Computer security experts say 2006 saw an unprecedented spike in junk e-mail and sophisticated online attacks from increasingly organized cyber crooks. These attacks were made possible, in part, by a huge increase in the number of security holes identified in widely used software products.

[More]

Phishing 2006: The Year in Review
[Source: Symantec]

Now that we're near the end of the year, I thought I'd spend some time looking back at the phishing threat and reviewing some of the noteworthy trends. There are three high-level aspects that I'd like to touch upon:
1) The overall increase in phishing activity
2) New phishing attack vectors
3) New antiphishing techniques

[More]

MCAfee Avert Labs Unveils Predictions For Top Ten Security Threats In 2007 As Hacking Comes Of Age
[Source: MCAfee]

SANTA CLARA, Calif., November 29, 2006-McAfee, Inc. (NYSE: MFE) today announced its top ten predictions for security threats in 2007 from McAfee Avert Labs. According to McAfee Avert Labs data, with more than 217,000 various types of known threats and thousands more as yet unidentified, it is clear that malware is increasingly being released by professional and organized criminals.
In no particular order, McAfee Avert Labs' top 10 security threats for 2007 are:

1. The number of password-stealing Web sites will increase using fake sign-in pages for popular online services such as eBay
2. The volume of spam, particularly bandwidth-eating image spam, will continue to increase
3. The popularity of video sharing on the Web makes it inevitable that hackers will target MPEG files as a means to distribute malicious code

[More]

Hackers target 4,000 Indian websites
[Source: First.org]

Even amid growing concern over cyber security, hacker groups defaced at least 340 Indian websites during November 2006, up from 244 sites targeted during last month. This takes the total number of Indian sites (government and non-government), that came under attack by hackers in the first nine months of the year, to over 4,000.

[More]

'Merry Christmas to our heroes' e-mail installs malicious code
[Source:Computerworld]

A popular Christmas PowerPoint file has been modified to incorporate malicious code that gives an attacker unauthorized access to infected systems, iDefense warned today.

In an e-mail warning, iDefense said that the e-mail with the subject "Merry Christmas to our hero sons and daughters!" and the attachment Christmas+Blessing-4.ppt "silently installs a backdoor Trojan horse on vulnerable computers." This version of the Hupigon (sometimes also called Hupigeon) Trojan installs two files on a compromised system, according to Ken Dunham, director of iDefense's Rapid Respones Team: msupdate.dll (18,507 bytes) and sdfsc.dll (3 bytes).

[More]

Ball drops on 'Happy New Year!' worm
[Source: Computerworld]

VeriSign Inc. is warning of a new e-mail worm arriving in in-boxes with the subject "Happy New Year!"

The message, currently being spread from 160 e-mail domains, requires users to click on the attached "postcard.exe" file in order to cause damage. The file will install several different malicious code variants, including Tibs, Nwar, Banwarum and Glowa, on the computer. It then executes mass mailings from the infected computer.

[More]

First MMS exploit for phones has been released
[Source:First.org]

On late Friday the 29th of December, Collin Mulliner published proof-of-concept exploits of MMS vulnerabilities that he discovered six months ago. When Collin first discovered the vulnerabilities he informed the software vendors, but as he has not received a report within half-a-year, he decided to now publish the exploit at the 23rd Chaos Communication Congress in Berlin.

[More]

Phishers' Latest Platforms: VoIP, SMS
[Source:informationWeek]

Phishers have branched out beyond e-mail, a security researcher said, and are now exploring both VoIP and text messaging as attack avenues.

Voice over IP is attractive to identity fraudsters, said Zulfikar Ramzan of Symantec's Advanced Threat Research group, in a company blog entry Tuesday, because it's an affordable way to dial large numbers of phone numbers. Dubbed "vishing" for voice phishing, "such attacks can be conducted cheaply enough that phishers might see a sufficient return on their investment," Ramzan said. Phishers substitute phone numbers for URLs in traditional e-mailed come-ons or dial consumers directly, circumventing e-mail entirely.

[More]

Researchers developing tool to combat Internet auction fraud
[Source:smh.com.au]

Carnegie Mellon University researchers are relying on an old adage to develop anti-fraud software for Internet auction sites: It is not what you know, it is who you know.
At sites like eBay, users warn each other if they have a bad experience with a seller by rating their transactions. But the CMU

[More]

Financial services firms share security tactics
[Source:ComputerWorld]

Some of the top players in the financial services arena -- such as Visa U.S.A Inc., JPMorgan Chase & Co. and Experian International Ltd. -- are expanding their tactics for preventing customer data loss.

IT security managers convening at two interrelated conferences in New York this week said their firms are adopting both new network

defenses and organizational structures to lower risk of a data breach.

[More]