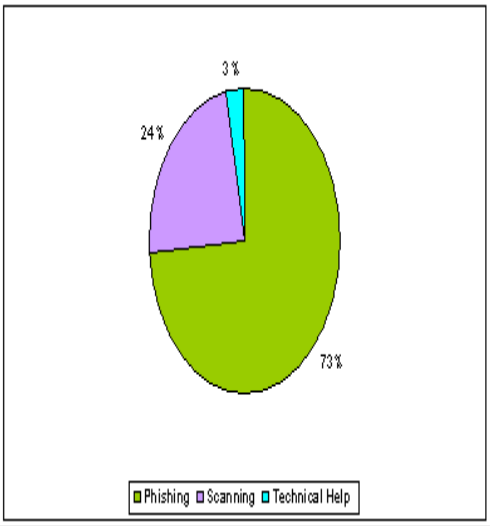
Indian Computer Emergency Response Team
Department of Information Technology
Ministry of Communications & Information Technology
(Government of India)

# CERT-In Monthly Security Bulletin November 2006

## Cyber Intrusion Trends

In this month 34 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. 24% unauthorized scanning incidents and 3% incidents related to virus/worm under the malicious code category were reported. As compared to previous month phishing incidents have increased and scanning incidents have decreased.

**Cyber Intrusion during November 2006**




## Indian Websites Defacement

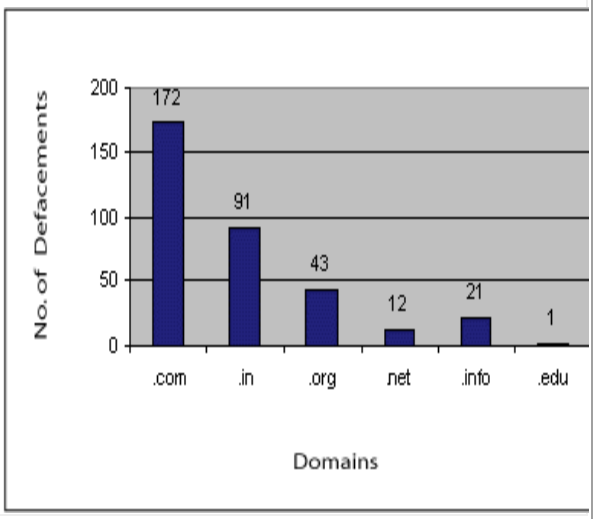
In total 340 Indian websites were defaced during this month. Mostly the websites under .com domain were defaced by the hacker groups. A chart depicting Top Level Domain(TLD) wise defacements is shown in the figure.
The vulnerabilities likely to be in web servers which have exploited for the defacements are:

Apache mod_auth_kerb "der_get_oid()" Off-By-One Vulnerability
November 25, 2006
CIVN-2006-120

PHPMyAdmin Multiple cross-site scripting Vulnerability, NukeAI Module for PHP-Nuke "AIbasedir" Variable Remote File Inclusion Vulnerability
November 27, 2006
CIAD-2006-44

PHP-Nuke "modules/News/index.php" SQL Injection Vulnerabilities
November 29, 2006
CIVN-2006-122

**Statistics of Defaced Indian Websites in November 2006**



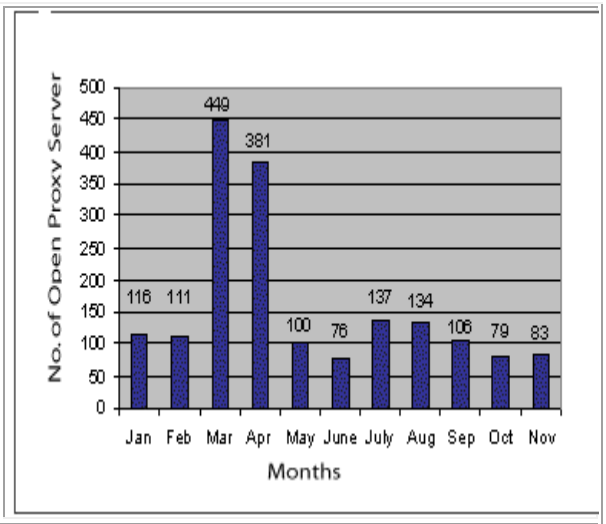

## Open proxy servers

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

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

any IP address and make connections to any Internet resource.

CERT-In tracked 83 open proxy servers functioning in India during November 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 November 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 Visual Studio | Microsoft Visual Studio WMI Object Broker ActiveX Code Execution Vulnerability | November 02, 2006 | CIVN-2006-109 |
| Microsoft Internet Explorer | Microsoft Internet Explorer WScript.Shell Object Arbitrary Code Execution Vulnerability | November 02, 2006 | CIVN-2006-110 |
| Microsoft XML | Microsoft XML Core Services XMLHTTP ActiveX Control Code Execution Vulnerability | November 15, 2006 | CIVN-2006-112 |
| Microsoft Internet Explorer | Microsoft Internet Explorer "daxctle.ocx" KeyFrame and HTML Rendering Memory Corruption Vulnerability | November 15, 2006 | CIVN-2006-115 |
| Microsoft Windows | Microsoft Agent Memory Corruption Vulnerability | November 15, 2006 | CIVN-2006-116 |
| Microsoft Windows | Microsoft Windows workstation Service Memory Corruption Vulnerability | November 15, 2006 | CIVN-2006-117 |
| Microsoft | Multiple Vulnerabilities in Microsoft Windows, Microsoft Internet Explorer and Microsoft XML Core Services | November 15, 2006 | CIAD-2006-43 |
| **Unix** | **Title of Vulnerability** | **Discovery/Publish Date** | **CERT-In References & Patch Information** |
| elinks | elinks SMB protocol handler vulnerability | November 16, 2006 | CIVN-2006-118 |
| LibPNG | LibPNG Graphics Library PNG_SET_SPLT Remote Denial of Service Vulnerability | November 21, 2006 | CIVN-2006-119 |
| Apache mod_auth_kerb | Apache mod_auth_kerb "der_get_oid()" Off-By-One Vulnerability | November 25, 2006 | CIVN-2006-120 |
| Linux | Multiple Vulnerabilities in Linux | November 07, 2006 | CIAD-2006-40 |

| | | | |
|---|---|---|---|
| GNU Radius | GNU Radius "sqllog()" SQL Accounting Module Remote Format String Vulnerability | November 27, 2006 | CVE-2006-4181 |
| **Miscellaneous** | **Title of Vulnerability** | **Discovery / Publish Date** | **CERT-In References & Patch Information** |
| Mozilla | Multiple Vulnerabilities in Mozilla Products | November 13, 2006 | CIAD-2006-41 |
| **Medium Vulnerabilities** | | | |
| **Microsoft** | **Title of Vulnerability** | **Discovery / Publish Date** | **CERT-In References & Patch Information** |
| Microsoft Windows | Microsoft Windows GDI Kernel Structures Handling Vulnerability | November 07, 2006 | CVE-2006-113 |
| Microsoft Windows | Multiple Vulnerabilities in Client Service for NetWare | November 15, 2006 | CVE-2006-114 |
| **Unix** | **Title of Vulnerability** | **Discovery / Publish Date** | **CERT-In References & Patch Information** |
| Linux pam_ldap | pam_ldap "PasswordPolicyResponse" security bypass vulnerability | November 06, 2006 | CIVN-2006-111 |
| PHP-Nuke | PHP-Nuke "modules/News/index.php" SQL Injection Vulnerabilities | November 29, 2006 | CIVN-2006-122 |
| Linux | Multiple Vulnerabilities in Linux | November 27, 2006 | CIAD-2006-44 |
| Linux | libX11 XCOMPOSEFILE File Descriptor Leak Information Disclosure Vulnerability | November 01, 2006 | CVE-2006-5397 |
| Linux Kernel | Linux Kernel ISO9660 Local Denial of Service | November 06, 2006 | CVE-2006-5757 |
| Linux Kernel | Linux Kernel Fragmented IPv6 Packet Filtering Bypass | November 07, 2006 | CVE-2006-4572 |
| openldap | openldap denial of service vulnerability | November 10, 2006 | CVE-2006-5779 |
| Linux | Multiple Vulnerabilities in Linux | November 13, 2006 | CIAD-2006-42 |
| Linux Kernel | Linux Kernel "minix_bmap()" Data Stream Handling Denial of Service Vulnerability | November 20, 2006 | CVE-2006-6058 |
| Dovecot | Dovecot Cache File "file_cache_read()" Function Remote Off-By-One Vulnerability | November 20, 2006 | CVE-2006-5973 |
| OpenSSH | OpenSSH Privilege Separation Monitor Vulnerability | November 15, 2006 | CVE-2006-5794 |
| **Miscellaneous** | **Title of Vulnerability** | **Discovery / Publish Date** | **CERT-In References & Patch Information** |
| Firefox | Firefox Password Manager Information Disclosure Vulnerability | November 27, 2006 | CIVN-2006-121 |
| Wireshark | Multiple vulnerabilities in Wireshark (Ethereal®) | November 06, 2006 | CIAD-2006-39 |

| **Malicious Code Threats** | | | | | |
|---|---|---|---|---|---|
| **Title of Malicious Code** | **Type** | **Overview** | **Aliases** | **Discovery Date** | **References** |
| Spamthru Trojan | Trojan | Trojan has its own spam engine that | No Alias | November 06, 2006 | http://www.cert-in.org.in/virus/spamthru_trojan.htm |

| | | | | | |
|---|---|---|---|---|---|
| | | downloads templates for sending spam messages and using a pirated copy of antivirus engine of Kaspersky Antivirus for WinGate to remove other malware from the infected system. | | | |
| Infostealer.Gampass | Trojan | Trojan horse that steals online game accounts, such as Lineage, Ragnarok online, and Rexue Jianghu. | No Alias | November 12, 2006 | http://www.symantec.com/enterprise/security_response/writeup.jsp?docid=2006-111201-3853-99 |
| Trojan HORST | Trojan | Trojan acts as a proxy server on the affected system and listens to the random TCP port | No Alias | November 20, 2006 | http://www.cert-in.org.in/virus/trojan_horst.htm |
| Spybot | Bot | Bot is exploiting some common buffer overflow vulnerabilities in Microsoft Windows and Symantec Antivirus and opens backdoor on the affected system. | No Alias | November 30, 2006 | http://www.cert-in.org.in/virus/spybot.htm |

**Security News**

**U.S. warns financial firms of al Qaeda threat**
[Source: CNN News]

WASHINGTON (CNN) -- A Department of Homeland Security advisory cautioning that al Qaeda may be planning cyber attacks on banking and financial institution Web sites was issued out of an abundance of caution, although there is no corroboration, a DHS spokesman told CNN Thursday.

The threat apparently was posted on a jihadist Web site, the spokesman said. It was discovered Nov. 27 by DHS and translated. The department decided to send an advisory out to financial institutions out of caution.

[More]

**The Ongoing Evolution of Online Fraud**
[Source: Symantec]

In September, Symantec released the tenth edition of the Internet Security Threat Report. A quick comparison with the first edition of the Report, released in January of 2002, shows just how dramatically the threat landscape has changed.

[More]

**Phishing attacks now using phone calls**
[Source: USA Today]

SAN FRANCISCO — And consumers thought they were safe by not clicking on links in unsolicited e-mails.
Now comes a new batch of phishing scams that rely on an old tool — the phone — to trick people into giving away their personal information.

Vishing — short for voice phishing — is one of the latest iterations of phishing, a long-running e-mail scam that instructs recipients to click a link in the e-mail to confirm data such as their Social Security number and credit card number. But the link is really connected to a bogus

website where the data are stolen.

[More]

**NIST Special Publication 800-100 Information Security Handbook: A Guide for Managers**
[Source: NIST]

NIST is proud to announce the release of Special Publication 800-100, Information Security Handbook: A Guide for Managers . This Information Security Handbook provides a broad overview of information security program elements to assist managers in understanding how to establish and implement an information security program.

[More]

**Bot spreads through anti-virus, Windows flaws**
[Source:The Register]

University security experts warned administrators on Monday that a bot program has started to spread by exploiting five patched Microsoft vulnerabilities and a six-month-old flaw in Symantec's anti-virus software.
The bot program, identified as W32.Spybot.ACYR by Symantec, has compromised a small number of systems at various universities, including about 30 systems at the University of Arkansas and another 150 systems at the University of New South Wales in Australia.

[More]

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

Professionalism of Malware Threats to Watch in 2007 Include Increase in Password-Stealing Web sites, More Spam and Likelihood of Hackers Targeting Video

SANTA CLARA, Calif., November 29, 2006—McAfee, Inc. (NYSE: MFE) today announced its top ten predictions for security threats in 2007 from McAfeeâ Avertâ Labs. According to McAfee Avert Labs data, with more than 217,000 various types of known threats and thousands more not yet identified, it is clear that malware is increasingly being released by professional and organised criminals.

[More]