



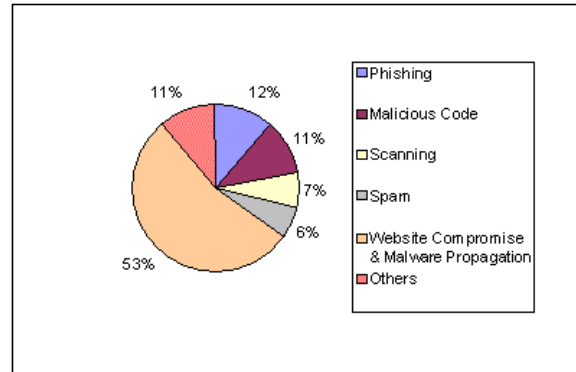
CERT-In Monthly Security Bulletin December 2008

Cyber Intrusion Trends

In this month 255 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure, 53% incidents related to Spreading of malware through website compromise were reported in this month. 11 % incidents related to virus/worm under the Malicious code category , 12 % phishing incidents , 06 % incidents related to spamming ,07 % unauthorized scanning , and 11 % incidents related to technical help under the Others category were also reported in this month.

In this month CERT-In tracked 04 C&C (Command & Control) servers and 8866 bot -infected computers existing in India . The concerned ISPs were intimated to dis-infect the bot infected systems and C&C servers to mitigate botnets .

Cyber Intrusion during December 2008



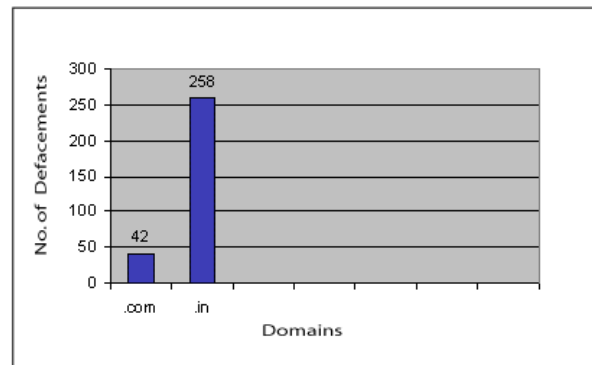
Indian Websites Defacement

In total 300 Indian websites were defaced during December 2008. A chart depicting Top Level Domain (TLD) wise defacements is shown in the figure.

The vulnerabilities which might have been exploited for the defacements are:

1. Microsoft SQL Server Memory Overwrite vulnerability [CIVN-2008-192](#)
2. Microsoft Windows Server Service Vulnerability [CIVN-2008-170](#)
3. Microsoft Windows SMB Credential Reflection Vulnerability [CIVN-2008-177](#)
4. Multiple Vulnerabilities in Microsoft XML Core Services [CIVN-2008-178](#)
5. Apache Tomcat UTF-8 Directory Traversal Vulnerability [CVE-2008-2938](#)
6. Apache Tomcat ' RequestDispatcher ' Information Disclosure Vulnerability [CVE-2008-2370](#)
7. PHP extractTo() '.zip' Files Directory Traversal Vulnerability [CVE-2008-5658](#)
8. PHP Multiple Buffer Overflow Vulnerability [CVE-2008-3658](#)

Statistics of Defaced Indian Websites in December 2008

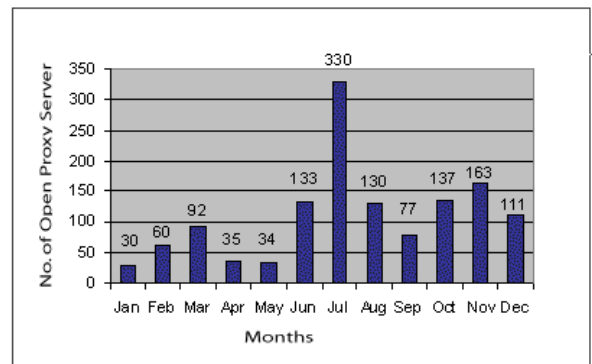


Open proxy servers

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.

CERT-In tracked 111 open proxy servers functioning in India during December 2008. 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.

Statistics of Open Proxy Servers tracked during Jan - Dec 2008



Attack Trend

Malware circulating through Christmas E-card

It has been observed that new malware is circulating via e-mails pretending to be Christmas day and Holiday Greetings. These spam e-mails come with the subject line such as "Merry Xmas!" and "Merry Christmas card for you!" and other Christmas Day related phrases. E-mail contains a URL, which takes the user to malicious website hosting malware "ecard.exe" (dubbed as "[Waledac](#) [Symantec] ").

[\[More\]](#)

Spreading of DNSChanger malware and Rouge DHCP servers

It has been reported that variants of "DNSChanger" malware that use "unauthorized DHCP server" attack to change the DNS configuration of the systems in the same local network, are in the wild. This Trojan may be dropped by other malware or may be downloaded unknowingly by a user when visiting malicious Web sites. It is also reported that some variants are able to change the DNS server settings in ADSL modems/routers/cable modems. The malware is dubbed as Flush.M (Symantec), a variant of "DNS-changing Trojan".

[\[More\]](#)

0-day exploit for Internet Explorer in the wild

It is reported that exploit for the zero -day vulnerability in Internet Explorer described in CERT -In vulnerability note [CIVN 2008-191](#) is circulating in the wild which involves an invalid pointer reference in the data binding function of Internet Explorer when it attempts to parse XML tags. By convincing a user to view a specially crafted XML document (e.g., a web page or email message or attachment), an attacker is able to execute arbitrary code with the privileges of the user.

Several websites are operational hosting obfuscated malicious JavaScript's (detected as [JS_DLOAD.MD](#) ,Trend Micro) that can exploit the said vulnerability through a Heap Spray on SDHTML.

[\[More\]](#)

Training

Workshop on " Managing Organization's Network Security" on 16th December, 2008

A one day Workshop on "Managing Organization's Network Security" was conducted on 16th December, 2008 . The objective of the workshop is to create awareness among Indian IT Infrastructure and IT user organisations on the latest methods of managing organization's Network Security. Delegates were from Corporate and critical sector organizations.

[\[Presentation Material\]](#)

Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during December 2008 and their countermeasures along with 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	Exploitation of critical Microsoft Windows Vulnerabilities	4-Dec-08	CIAD-2008-63
Microsoft	Multiple Vulnerabilities in Microsoft Windows, Internet Explorer, Visual Basic 6.0	11-Dec-08	CIAD-2008-65
Microsoft	Multiple Vulnerabilities Microsoft Visual Basic ActiveX Controls	11-Dec-08	CIVN-2008-183
Microsoft	Multiple Vulnerabilities in Microsoft Windows GDI	11-Dec-08	CIVN-2008-184
Microsoft	Microsoft Office Word Remote Code Execution	11-Dec-08	CIVN-2008-185
Microsoft	Multiple Vulnerabilities in Microsoft Internet Explorer	11-Dec-08	CIVN-2008-186
Microsoft	Microsoft Office Excel Remote Code Execution	11-Dec-08	CIVN-2008-187
Microsoft	Microsoft Windows Explorer Search Handling Vulnerabilities	11-Dec-08	CIVN-2008-188
Microsoft	Microsoft Internet Explorer Data binding Memory Corruption Vulnerability	18-Dec-08	CIVN-2008-191

Microsoft	Microsoft Windows WordPad Text Converter File Handling Memory Corruption Vulnerability	18-Dec-08	CIVN-2008-193		
Microsoft	Microsoft SQL Server sp_replwritetovarbin limited memory overwrite vulnerability	26-Dec-08	CIVN-2008-192		
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Linux	Linux Kernel 'lbs_process_bss()' Remote Denial of Service Vulnerability	1-Dec-08	CIVN-2008-181		
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Mozilla	Multiple Vulnerabilities in Mozilla products	22-Dec-08	CIAD-2008-67		
Adobe	Adobe Flash Player for Linux SWF Processing Vulnerability	11-Dec-08	CIVN-2008-194		
Sun	Multiple vulnerabilities in Sun Java Development Kit and Java Runtime Environment	11-Dec-08	CIAD-2008-64		
Novell	Novell Netware ApacheAdmin Security Bypass Vulnerability	26-Dec-08	CIVN-2008-197		
Trend Micro	Multiple Vulnerabilities in Trend Micro HouseCall ActiveX Control	23-Dec-08	CIVN-2008-196		
Opera	Multiple vulnerabilities in Opera	26-Dec-08	CIAD-2008-68		
Medium Vulnerabilities					
Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Microsoft	Microsoft Windows Media Components Vulnerabilities	11-Dec-08	CIVN-2008-189		
Microsoft	Microsoft Office SharePoint Server Security Bypass Vulnerability	11-Dec-08	CIVN-2008-190		
Linux	sendmsg() and ATM subsystem Denial of Service Vulnerabilities in Linux Kernel	15-Dec-08	CIAD-2008-66		
Linux	Linux Kernel 'parisc_show_stack()' Local Denial of Service Vulnerability	22-Dec-08	CIVN-2008-195		
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Trojan:Win32/Yektel	Trojan	It has been observed that Trojan:Win32/Yektel is circulating widely. It is a rogue security program that display fake warning messages indicating that spyware or malware has been detected on	Win32/Warax.P (CA), Trojan.Win32.FraudPack.gen (Kaspersky), Downloader.MisleadApp (Symantec)	December 22, 2008	http://www.cert-in.org.in/virus/Win32_Yektel.htm

		the machine" in order to convince users to purchase rogue security software.			
Trojan Gimfan	Trojan	It has been observed that a Trojan named Gimfan is spreading in the wild. The Trojan downloads malicious files onto the vulnerable system by exploiting Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (CVE-2008-4250)	No Aliases found	December 22, 2008	http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-122211-3108-99&tabid=1
Trojan Alureon	Trojan	It has been observed that a password stealing family of Trojans named Alureon is spreading in the wild. It spreads through shared and removable drives. These Trojan has the functionality of intercepting network traffic in order to steal user's credentials such as usernames, passwords, and credit cards data. Further the	No Aliases found	December 23, 2008	http://www.microsoft.com/security/portal/Entry.aspx?name=Trojan%3aWin32%2fAlureon!inf

	malware may also change the DNS settings of the infected system to perform the malicious activities.		
--	--	--	--

Security News

Lok Sabha passes IT Act Amendment Bill

[Source: <http://economictimes.indiatimes.com>] 22 December 2008

Publishing and transmitting obscene material in electronic form besides other e-commerce frauds will now be punishable under the amended IT Bill, which was passed by the Lok Sabha.

The Information Technology (Amendment) Bill, 2006, adds provisions to the existing Information Technology Act, 2000, to deal with new forms of cyber crimes like publicising sexually explicit material in electronic form, video voyeurism and breach of confidentiality and leakage of data by intermediary and e-commerce frauds.

The Bill proposes a Cyber Appellate Tribunal and enabling the authentication of electronic records by any electronic signature technique. According to the Bill, the Central government has to decide the number of members of the tribunal later.

[\[More\]](#)

Indian organisations fare better than global organisations in Information System Security according to CERT-IN - FICCI - PWC Survey

[Source: <http://indiaprwire.com>] 18 December 2008

Security in Indian organisations is evolving at a rapid pace. No longer is security merely a line item in the overheads budget of Indian enterprises, nor is it a technical issue easily addressed by an off-the-shelf technology product, according to the Information Systems Security Survey, 2007-08 titled 'From strength to strength', conducted by the Indian Computer Emergency Response Team (CERT-In), Federation of Indian Chambers of Commerce and Industry (FICCI) and PricewaterhouseCoopers (PwC). More than 140 organisations from a broad range of industries took part in the survey.

[\[More\]](#)

About 90 percent of all email is spam: Cisco

[Source: <http://www.crime-research.org>] December 16, 2008

Armies of hijacked computers are flooding the world with spam as hackers devise slicker ways to take over unwitting people's machines, according to a Cisco report.

Virus-infected computers are woven into "botnets" used to attack more machines and to send specious sales pitches to email addresses in low-cost quests to bilk readers out of cash.

"Every year we see threats evolve as criminals discover new ways to exploit people, networks and the Internet," said Cisco chief security researcher Patrick Peterson.

The United States is the biggest source of spam, accounting for 17.2 percent of the messages. Turkey and Russia ranked second and third, accounting for 9.2 percent and 8 percent of spam respectively, according to Cisco.

This year, botnets were used to inject an array of legitimate Websites with an IFrames malicious code that reroutes visitors to websites that download computer viruses into their machines, according to Cisco.

[\[More\]](#)

SSL Security Broken

[Source: <http://news.softpedia.com>] 30 December 2008

A group of researchers from Europe and U.S. have successfully implemented a theoretical attack that subverts the security of the HTTPS protocol. The hackers generated a rogue Certification Authority (CA) certificate that was trusted by all major browsers and could be used to impersonate any secure website.

In a coordinated effort, security researchers from different organizations and institutes have demonstrated that virtually undetectable phishing attacks are possible, because some Certification Authorities still use the vulnerable MD5 hashing function. In fact, the [research](#) conducted by Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger has the specific purpose of convincing Certification Authorities to drop MD5 and move on to more secure algorithms, such as SHA-1, SHA-2, or the upcoming SHA-3.

SSL (Secure Sockets Layer) is a cryptographic protocol aimed at providing network security by preventing data eavesdropping, tampering, or forgery. HTTPS, Hypertext Transfer Protocol Secure, combines the regular HTTP protocol with SSL, or the newer Transport Layer Security

(TLS). “The vulnerability we expose is not in the SSL protocol or the web servers and browsers that implement it, but in the Public Key Infrastructure,” the researchers say.

[\[More\]](#)

Top 9 IT security threats for 2009

[Source: <http://www.net-security.org>] 12 December 2008

2009 will continue the trend of increasing size, scope, and concentration of security attacks on computer networks nationwide. The volume of attacks from international sources will continue to increase, as will the sophistication of application level attacks such as SQL injection, buffer overflow, and cross site scripting (XSS). These will be directed towards high traffic websites (news sites or social networking sites) that when compromised will install malware to a large numbers of users.

[\[More\]](#)

Data center transformation a top priority in 2009 for CIOs

[Source: <http://www.net-security.org>] 19 December 2008

New global research reveals that 84 percent of technology organizations are planning to implement a data center transformation (DCT) project in the next 12 months, primarily to lower costs and reduce business risk.

The HP-commissioned survey further shows that a vast majority of technology decision makers are currently implementing or planning to implement in 2009 consolidation (95 percent), business continuity (93 percent) and virtualization (91 percent) projects.

[\[More\]](#)

Computer scientists find audio CAPTCHAs easy to crack

[Source: <http://arstechnica.com>] December 08, 2008

The Carnegie-Mellon University team behind the reCAPTCHA service is continuing to expand its effort to mix basic security and useful work. CAPTCHAs are the distorted text that helps various online services ensure that the entity opening an account is a human, not a bot bent on using the service to dish out spam. The reCAPTCHA service puts the mental horsepower need to interpret these images to good use, harnessing it to identify text in scanned books where OCR software has failed. Now, the team has turned its attention to the audio CAPTCHAs used by the visually impaired.

[\[More\]](#)

Fighting computer crimes without the threat of a forensic compromise

[Source: <http://www.net-security.org>] 04 December 2008

It seems that no matter what illegal activity is pursued, whether it is pornography, kidnapping, murder, or even terrorism, the so-called criminal masterminds leave a winding but traceable trail of related computer data linking these perpetrators to their crimes. In the current era of escalating crimes involving computer usage, it has become essential that law enforcement has immediate access to potentially critical computer data. Such immediate access not only helps to ensure apprehension and conviction of the perpetrator, but contains within it the promise of the prevention of the unthinkable. While technology currently allows forensically sound and virtually instantaneous access to potentially critical crime-related computer data, this technology is not employed in nearly enough cases.

[\[More\]](#)

The Rise and Rise of Rogue Security Software

[Source: <http://www.net-security.org>] 22 December 2008

Unfortunately for computer users, the number of rogue security and anti-malware software, also commonly referred to as "scareware," found online is rising at ever-increasing rates, blurring the lines between legitimate software and applications that put consumers in harm's way. Industry experts have reported a five-fold year-on-year increase in the number of rogue applications invading the Internet.

"Levels have increased dramatically. Of all the rogue security applications we have in detection, approximately 21 percent of the total in detection have appeared since June 2008. There are clearly vast amounts of money to be made from these rogue programs," says Andrew Browne a malware analyst and Research Team Leader at Lavasoft.

[\[More\]](#)

Phishing Attacks Utilizing Port Numbers

[Source: <https://forums.symantec.com>] 23 December 2008

There are varying types of technologies used by online attackers these days. There are old tricks and of course new ones, but it is the newer ones that make it even more difficult to handle the dilemmas faced in the world of Internet security. One of the trends of attack that was noticed a little while ago was an attack based on a website's "port number."

Statistics were taken for the phishing websites and it was seen that the maximum utilized port number was 82. It also came to light that the maximum amount of fraud against different port numbers came from the United States and Korea .

[\[More\]](#)

DECT wireless eavesdropping made easy

[Source: <http://www.theregister.co.uk>] 31 December 2008

Conversations relayed through cordless household phones might be far easier to snoop upon than previously suspected.

A new attack against phones based on DECT (Digital Enhanced Cordless Telecommunication) technology - demonstrated during the Chaos Communication Congress in Berlin might be carried out cheaply using off-the-shelf kit, together with a little know-how. A modified \$30 VoIP laptop card running on a Linux portable were used to demonstrate the attack, which relies on using specially outfitted equipment to impersonate legitimate wireless base stations.

[\[More\]](#)