



**CERT-In Monthly Security Bulletin June 2008**

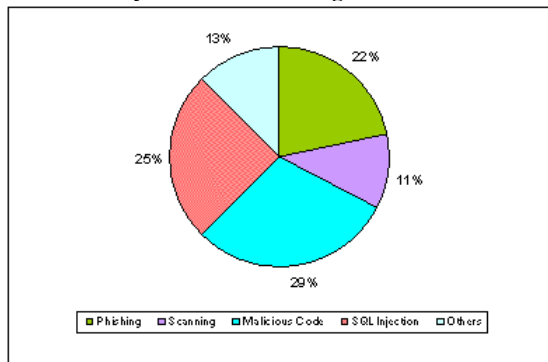
**Cyber Intrusion Trends**

In this month 119 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 22% phishing incidents were reported in this month. 11% unauthorized scanning , 29% incidents related to virus/worm under the Malicious code category, 25% incidents were of SQL injection attacks and 13% incidents related to technical help under the Others category were reported in this month. As compared to previous month the number of incidents related to phishing and incidents related to technical help under the Others category have increased while incidents related to virus/worm under the Malicious code category and scanning incidents have decreased.

In this month CERT-In tracked 13 C&C (Command & Control) servers and 5537 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.

During this month SQL injection worm infected a large number of websites which in turn affected the user systems by downloading malicious code from remote servers.

**Cyber Intrusion during June 2008**



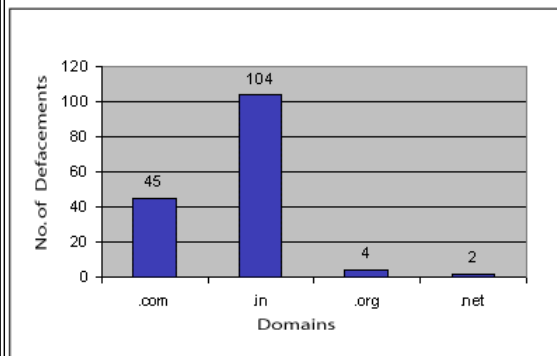
**Indian Websites Defacement**

In total 155 Indian websites were defaced during June 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. Apache-SSL Authentication Bypass Vulnerability [CIVN-2008-36](#)
2. phpMyAdmin Shared Host Remote Information Disclosure [CVE-2008-1924](#)
3. PHP 5 'php\_sprintf\_appendstring()' Remote Integer Overflow Vulnerability [CVE-2008-1384](#)
4. Apache Tomcat SingleSignOn Cookie Information Disclosure Weakness [CVE-2008-0128](#)
5. phpMyAdmin Local Information Disclosure [CVE-2008-1567](#)
6. Apache Tomcat AJP Connector Information Disclosure [CVE-2006-7197](#)
7. Apache Tomcat Cross-Site Scripting [CVE-2006-7195](#)

**Statistics of Defaced Indian Websites in June 2008**

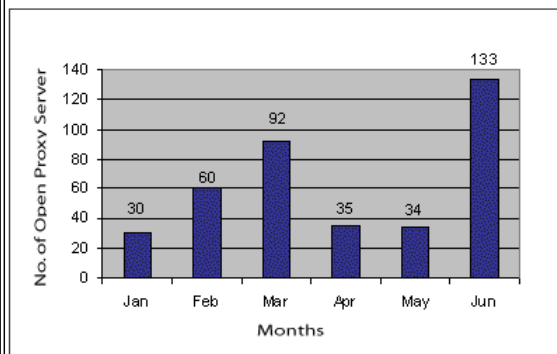


**Open proxy servers**

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 133 open proxy servers functioning in India during June 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 - June 2008**



**Attack Trend**

## SQL Injection Worm

The spreading of SQL injection worm by injecting java scripts or iframe into websites, which is happening from the month of March, continued in June also.

[\[More\]](#)

## Mass SQL Injection attacks and malicious Java script embedding on websites

In the new wave of attacks using SQL injection attack, websites have been compromised and injected with malicious scripts. These script redirects user to malicious URL containing ShockWave (SWF) files that are exploiting Adobe Flash Player Vulnerabilities. Successful exploitation downloads Trojans on the vulnerable system.

[\[More\]](#)

## Global Microsoft SQL server version Buffer Overflow Attempt

It has been observed that the scanning or probing attempts on UDP port 1434 have increased.

These attempts are for exploiting the buffer overflow vulnerability in "Server Resolution" service for Microsoft SQL Server ( [CVE-2002-0649](#) , [MS02-39](#) ) to gain control over the server.

## Ransomware GPcode

Virus named *Ransomware GPcode* was circulating in the wild in the month of June.

The virus creates an encrypted copy of each original file that it finds suitable for infection. These encrypted copies have the original file name, with \_CRYPT being added to the end of the encrypted file name. It then deletes the original file from the infected system.

[\[More\]](#)

## Trojan 2.0 Crimeware Threats exploiting Web 2.0 Technologies

It has been observed that new breed of Trojans called Trojan 2.0 are propagating using Web 2.0 Technologies. These Trojans are using Social Engineering and tricking users of Social Networking sites to open malicious messages and download malware to user's systems.

[\[More\]](#)

## Training

### Workshop on "Network Security" on 25th June, 2008

A one day Workshop on "Network Security" was conducted on June 25, 2008 . The objective of the workshop is to create security awareness among system/network administrators on how to secure network in an enterprise/organizations to defend against the attacks. Delegates were from Government, public sector, financial institutions and critical infrastructure organizations. The workshop covered the following topics at length:

- Overview of Network Security
- Network Perimeter Security & VPN and Wireless LAN Security
- Network Penetration Testing

The presentation material is available [here](#) .

### Workshop on "Windows Web Server Security" on 26th June, 2008

A one day Workshop on "Windows Web Server Security" was conducted on June 26, 2008 . The objective of the workshop is to create security awareness among system/network administrators on how to secure Windows Web Server and underlying windows operating system in an enterprise/organization to defend against the attacks. Delegates were from Government, public sector, financial institutions and critical infrastructure organizations. The workshop covered the following topics at length:

- Web Server Security an Overview
- Windows 2003 & 2008 Servers Secured Environment
- IIS Security and Management

The presentation material is available [here](#) .

## Security Alerts

**The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during June 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	CERT-In References & Patch Information
-----------	------------------------	-------------------	--

		Date	
Microsoft Windows	Apple Safari Client-side Code Execution Vulnerability on Microsoft Windows Systems	June 04, 2008	<a href="#">CIVN-2008-70</a>
Microsoft Windows	Microsoft Windows Bluetooth Stack Allows Remote Code Execution Vulnerability	June 04, 2008	<a href="#">CIVN-2008-77</a>
Microsoft	Microsoft Internet Explorer Memory corruption and Information Disclosure Vulnerabilities	June 04, 2008	<a href="#">CIVN-2008-78</a>
Microsoft	Microsoft DirectX MJPEG Decoder and SAMI Format parsing vulnerabilities	June 04, 2008	<a href="#">CIVN-2008-80</a>
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
OpenOffice	Integer overflow Vulnerability in OpenOffice.org	June 13, 2008	<a href="#">CIVN-2008-85</a>
Linux	Linux Kernel "pppol2tp_recvmsg()" Denial of Service Vulnerability	June 24, 2008	<a href="#">CIVN-2008-92</a>
Cisco	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Cisco	Multiple Vulnerabilities of Security bypass and DoS in Cisco PIX and Cisco ASA	June 09, 2008	<a href="#">CIAD-2008-27</a>
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Sun Java System	Multiple Vulnerabilities in Sun Java System Active Server Pages	June 05, 2008	<a href="#">CIAD-2008-26</a>
Solaris	Vulnerability in Solaris Samba Domain logons	June 06, 2008	<a href="#">CIVN-2008-74</a>
Adobe Acrobat Reader	Adobe Acrobat Reader Arbitrary Code Execution and Unspecified Remote Denial-of-Service Vulnerability	June 10, 2008	<a href="#">CIVN-2008-76</a>
Apple QuickTime	Multiple vulnerabilities in Apple QuickTime 7.x	June 13, 2008	<a href="#">CIAD-2008-32</a>
Adobe Reader	Adobe Reader and Adobe Acrobat JavaScript method handling remote code execution Vulnerability	June 25, 2008	<a href="#">CIVN-2008-93</a>
Mozilla Firefox	Mozilla Firefox Remote Code Execution Vulnerability	June 27, 2008	<a href="#">CIVN-2008-94</a>
Medium Vulnerabilities			
Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Microsoft	Microsoft WINS Elevation of Privilege Vulnerability	June 12, 2008	<a href="#">CIVN-2008-81</a>
Microsoft	Microsoft Active Directory Remote Denial of Service	June 12, 2008	<a href="#">CIVN-2008-82</a>
Microsoft	Microsoft Pragmatic General Multicast Denial of Service Vulnerabilities	June 12, 2008	<a href="#">CIVN-2008-83</a>
Microsoft	Microsoft Internet Explorer 6 Cross-Domain Vulnerability	June 27, 2008	<a href="#">CIVN-2008-95</a>
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Apache	Apache Tomcat Host Manager "name" Cross-Site Scripting Vulnerability	June 05, 2008	<a href="#">CIVN-2008-71</a>
Sun Java System	Sun Java System Web Server Advanced Search Mechanism Cross Site Scripting Vulnerability	June 05, 2008	<a href="#">CIVN-2008-72</a>
OpenSSL	OpenSSL Multiple Denial of Service Vulnerabilities	June 05, 2008	<a href="#">CIVN-2008-73</a>
Linux	Linux Kernel ASN.1 BER Decoding Vulnerability	June 13, 2008	<a href="#">CIVN-2008-84</a>

Apache	Multiple vulnerabilities in Apache HTTP Server 2.2.x		June 18, 2008	<a href="#">CIVN-2008-86</a>	
<b>Cisco</b>	<b>Title of Vulnerability</b>		<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>	
Cisco	Cisco Intrusion Prevention System Jumbo Frame Denial of Service Vulnerability		June 20, 2008	<a href="#">CIVN-2008-90</a>	
<b>Miscellaneous</b>	<b>Title of Vulnerability</b>		<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>	
Solaris	SNMPv3 improper HMAC validation vulnerability		June 12, 2008	<a href="#">CIAD-2008-30</a>	
Solaris	Multiple vulnerabilities in the Solaris X Server		June 20, 2008	<a href="#">CIVN-2008-91</a>	
<b>Low Vulnerabilities</b>					
<b>Microsoft</b>	<b>Title of Vulnerability</b>		<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>	
Solaris	Vulnerability in Solaris Corntab		June 06, 2008	<a href="#">CIVN-2008-75</a>	
Microsoft	Microsoft Windows Speech API Remote Code Execution		June 12, 2008	<a href="#">CIVN-2008-79</a>	
Solaris	Denial of Service (DoS) Vulnerability in the Solaris e1000g(7D) Gigabit Ethernet Driver		June 19, 2008	<a href="#">CIVN-2008-87</a>	
Solaris	Vulnerability of Local Denial of Service Sun Solaris UltraSPARC Kernel Module		June 19, 2008	<a href="#">CIVN-2008-88</a>	
Solaris	Vulnerability in the Solaris 10 Event Port Implementation		June 19, 2008	<a href="#">CIVN-2008-89</a>	
<b>Malicious Code Threats</b>					
<b>Title of Malicious Code</b>	<b>Type</b>	<b>Overview</b>	<b>Aliases</b>	<b>Discovery Date</b>	<b>References</b>
Trojan Mespam	Trojan	It has been observed that a Trojan named Mespam is circulating widely. It gets dropped by <a href="#">Storm Worm</a> /Trojan Peacomm Variants or propagates through malicious links which are embedded within Internet Messenger, e-mails, forum posts. The Trojan communicates via HTTP to certain remote websites to download the message body. This message body appears to be legitimate which tricks users to click upon the link provided within the	Troj/SpamToo-U [Sophos], Spam-Mespam [McAfee], WORM_ZHELATIN.CH [Trend], Troj/SpamToo-X [Sophos]	June 05, 2008	<a href="http://www.cert-in.org.in/virus/Trojan_Mespam.htm">http://www.cert-in.org.in/virus/Trojan_Mespam.htm</a>

		abovesaid mediums to download malware onto the system.			
Taterf Worm	Worm	<p>It has been observed that a Worm named <b>Taterf</b> is propagating widely. It may appear as a packed executable and propagates via mapped drives. The Worm copies itself to the root of the drive using different names which consists of random letters and numbers with extensions such as '.com', 'cmd' or an '.exe'. It creates an 'autorun.inf' file which is used to execute the worm whenever the drive is viewed with Windows Explorer.</p>	<p>Packed.Win32.NSAnti.r [Kaspersky], W32/NSAnti.gen3 [Norman ], Mal/Behav-204 [Sophos], Win32/Pacex.Gen [ESET], WORM_NSMP.TASH [Trend Micro]</p>	June 23, 2008	<a href="http://www.cert-in.org.in/virus/Taterf_Worm.htm">http://www.cert-in.org.in/virus/Taterf_Worm.htm</a>
Worm Tixcet.A	Worm	<p>It has been observed that a Worm named Tixcet.A is circulating widely. The worm reaches the computer in a file that has the icon of a Word document, to trick users into thinking that the files are genuine.</p>	W32/Tixcet.A.worm	June 24, 2008	<a href="http://www.cert-in.org.in/virus/Worm_Tixcet.A.htm">http://www.cert-in.org.in/virus/Worm_Tixcet.A.htm</a>
		<p>It has been observed that a virus named <b>Ransomware GPcode</b> is circulating in the wild. It scans the infected system for files of</p>			

Ransomware GPcode	Virus	different extensions and encrypts those files which have size between 10 bytes to 734003200 bytes using RC4 algorithm. The virus encrypts data using RSA public key which is 1024 bits in length and is present within the body of the virus. Subsequently a message demanding money for buying decryptor is displayed.	Virus.Win32.Gpcode.ak [Kaspersky],Virus.Win32.Gpcode.ac, Virus.Win32.Gpcode.ad,	June 25, 2008	<a href="http://www.cert-in.org.in/virus/Ransomware_GPcode.htm">http://www.cert-in.org.in/virus/Ransomware_GPcode.htm</a>
----------------------	-------	---	---	---------------	---

#### Security News

##### **Chinese crackers blamed for US power blackouts**

[ Source:www.theregister.co.uk ]

June 02, 2008

Thousands of websites in China have been booby trapped with code written to download Trojan software onto visitors who run vulnerable Windows PCs.Unlike earlier rounds of SQL injection attacks the latest assaults mostly target English language sites (predominantly sites hosted in China but with a .com suffix) and purposefully avoid Chinese government sites, according to net security firm ScanSafe. The latest attacks inject an iFrame onto compromised sites that loads malicious scripts from qiqigm.com, a domain registered on 16 May. These scripts includes the text "silent love china" in an apparently greeting to other Chinese hackers

The malicious code exploit well-known RealPlayer and Internet Explorer vulnerabilities to install a password-stealing Trojan that hides its presence on Windows PCs. More than 7,000 sites have been compromised in this way, reports Mary Landesman, ScanSafe's senior security researcher.

[\[More\]](#)

##### **About 50% of malicious sites bound to 10 networks (6 in China)**

[ Source:www.theregister.co.uk ]

June 24, 2008

Almost half the websites pushing malware are hosted by just 10 networks, according to a new report that adds new support to the growing argument that a relatively few number of actors are responsible for most of the net-based threats. The report from StopBadware.org also showed a dramatic rise in China 's role in the malware epidemic. Six of the 10 networks were internet service providers or backbone providers based in China and hosted more than 41 percent of the malicious websites. Not that US companies weren't also contributing to the problem. Three American companies also made the list, including Google, whose blogs hosted 4,261 sites, or about 2 percent of the booby-trapped destinations.

The findings come a few weeks after anti-spam outfit Knujon released a separate report that found that almost 75 percent of spam sites were signed up by just 10 registrars. Once again, the three biggest offenders were located in China and included Xinnet Bei Gong Da Software, BEIJINGNN and Todaynic. In many cases, owners of sites found pushing counterfeit watches, Viagra and other merchandise touted in spam failed to include correct contact information when registering the sites, as required. In an attempt to crack down on abusers, Knujon has begun reporting offenders to ICANN, which requires all website owners to be listed in a whois director. The sheer volume of the complaints has in some cases put a strain on ICANN's servers.

[\[More\]](#)

##### **ICANN and IANA's domains hijacked by Turkish hacking group**

[Source: <http://blogs.zdnet.com>]

June 26, 2008

What happens when the official domain names of the organizations that issue the domain names in general, and provide all the practical guidance

on how the prevent DNS hijacking, end up having their own domain names hijacked? A wake up call for the Internet community.

The official domains of [ICANN](#) , the Internet Corporation for Assigned Names and Numbers, and [IANA](#) , the Internet Assigned Numbers Authority were hijacked earlier today, by the NetDevilz Turkish hacking group which also [hijacked Photobucket's domain](#) on the 18th of June. [Zone-H mirrored the defacements](#) , some of which still remain active for the time being :

The ICANN and IANA websites were defaced earlier today by a Turkish group called "NetDevilz". ICANN is responsible for the global coordination of the Internet's system of unique identifiers. These include domain names, as well as the addresses used in a variety of Internet protocols. The Internet Assigned Numbers Authority (IANA) is responsible for the global coordination of the DNS Root, IP addressing, and other Internet protocol resources.

[\[More\]](#)

#### **Australia tops cyber crime list**

[Source:<http://www.crime-research.org>]

June 20, 2008

Australia has the highest incidence of cyber crime in the world, according to a global survey of nine countries by software security vendor, AVG. The study, which canvassed 1000 users each in Australia, the US, France, Germany, Italy, Spain, Sweden, Brazil, and the Czech Republic, found that more than 39 per cent of Australians had been the victim of cyber crime, compared to 32 per cent in Italy, 28 per cent of Americans, and just 14 per cent in Sweden and Spain.

The most common forms of cyber theft experienced by Australians were:

- Not receiving goods paid for at an online auction (16 per cent);
- Fraudulent e-mails that resulted in financial damage (14 per cent);
- Phishing (10 per cent);
- Not receiving goods ordered online (eight per cent);
- Credit card fraud (five per cent); and
- Unauthorised bank transfers (three per cent).

Lloyd Borrett, marketing manager of AVG (AU/NZ), said t[he fact that Australia experienced more cyber crime was a little surprising, although it might have been impacted by the fact that Australians are more active online users than most other nations.

[\[More\]](#)

#### **Phishers eye India brands**

[Source: <http://howrah.org> ]

June 29, 2008

Indian brands have emerged as the favourite target of phishers after the US , according to Indian Computer Emergency Response Team (CERT-IN), which handles computer securities incidents in the country. Phishing is a fraudulent activity to acquire personal information of a user like bank account number, user name, password, credit card details by using social engineering techniques. Phishing uses e-mail messages that purport to come from legitimate businesses that one might have dealings with like banks, Internet service providers and insurance agencies. Typically, they ask for verification of certain information, such as account numbers and passwords, allegedly for auditing purposes. When the users enter the information, data is immediately sent to the phisher who thereby uses this information to transfer money from user's account.

[\[More\]](#)

#### **Hacker Launches Botnet Attack via P2P Software**

[Source:<http://blog.wired.com>]

June 27, 2008

A 19-year-old hacker is agreeing to plead guilty to masterminding a botnet to obtain thousands of victims' personal data in an anonymous scheme a federal cybercrime official described Friday as the nation's first such attack in which peer-to-peer software was the "infection point". The defendant, Jason Michael Milmont, launched the assault last year from his Cheyenne , Wyoming residence, and anonymously controlled as many as 15,000 computers at a time, said Wesley L. Hsu, chief of the Cyber and Intellectual Property Crimes Section for federal prosecutors in Los Angeles . As part of the deal, in which a judge could hand him up to five years imprisonment, Milmont has agreed to pay \$73,000 in restitution, the government said, "It's the first time that we know of that peer-to-peer software was used as the infection point," Hsu said in an interview with Threat Level.

The malware infection became commonly known as the [Nugache Worm](#) , which embedded itself in the Windows OS.

[\[More\]](#)

#### **Google Calendar now the target of phishers**

[Source:<http://news.cnet.com>]

June 30, 2008

A few months ago, spam came to Google Calendar. Now, phishing has arrived. Intrepid Google watcher Philipp Lenssen wrote late last week about

being the target of a phishing attempt via Google Calendar. He received an e-mail to his Gmail account with a reference to a legitimate event from his calendar. The sender was listed as "customer care" and it asked him to verify his account by supplying his user name and password. "We are having congestions (sic) due to the anonymous registration of Gmail accounts so we are shutting down some Gmail accounts and your account was among those to be deleted. We are sending you this email to so that you can verify and let us know if you still want to use this account," the e-mail said, complete with grammatical and spelling mistakes that can tip people off to phishing attempts.

[\[More\]](#)

#### **Internet Explorer 'feature' causing drive-by malware attacks**

[Source:[http:// www.blogs.zdnet.com](http://www.blogs.zdnet.com)]

June 27th, 2008

It has been discovered that a drive-by malware download taking advantage of what Microsoft describes as an Internet Explorer "feature" to launch cross-site scripting attacks. The attack, discovered at a compromised legitimate site, is using a modified GIF file to exploit the cross-site scripting feature/vulnerability.

It is reported the vulnerability to Microsoft a long time ago, warning the company that JavaScript embedded into GIF files can be executed under certain circumstances. Microsoft disagreed and the issue was never patched. Fast forward to the latest site compromise — on a high traffic Web site — where a GIF file containing an embedded [iFrame](#) is pointing IE users to a known malicious site. (The malicious site is currently offline but there's evidence that it's tied to ID-theft attacks).

[\[More\]](#)

#### **HSBC sites vulnerable to XSS flaws, could aid phishing attacks**

[ Source:[http:// www.blogs.zdnet.com](http://www.blogs.zdnet.com)]

June 29th, 2008

What would the perfect phishing attack from a social engineering perspective? The one that compared to using typosquatted domains impersonating the bank's web application directory structure is in fact using the bank's legitimate domain names as redirectors due to XSS flaws within. It's even more interesting to measure the average time it takes for a bank to fix the XSS flaws within its sites upon getting notified of them, which in some cases is longer than the average time it takes to shut down a phishing site.

[\[More\]](#)