



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

**Cyber Intrusion Trends**

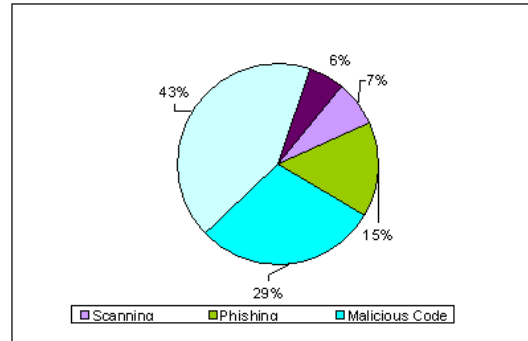
In this month 155 security incidents were reported to CERT-In from various National/International agencies. As shown in the figure, 43% incidents were of SQL injection attacks ,29% incidents related to virus/worm under the Malicious code category 15% phishing incidents 7% unauthorized scanning , and 06% incidents related to technical help under the Others category were reported in this month. As compared to previous month the numbers of incidents related to SQL Injection Attacks have increased while phishing incidents, scanning incidents, and incidents related to technical help under the Others category have decreased. The incidents related to virus/worm under the Malicious code category maintain the same momentum.

In this month CERT-In tracked 02 C&C (Command & Control) servers and 74753 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 also a sweep of attacks began exploiting the SQL injection vulnerabilities. The user systems are affected by downloading malicious code from remote servers.

In this month, a pervasive flaw within the Domain Name System (DNS) has been reported which allows the insertion of malicious DNS records into the cache of the target name server. CERT-In has issued advisory suggesting countermeasures to be taken by the ISPs and organizations running DNS Services.

**Cyber Intrusion during July 2008**



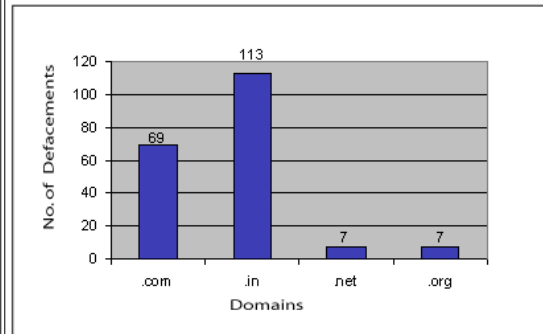
**Indian Websites Defacement**

In total 196 Indian websites were defaced during July 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 July 2008**

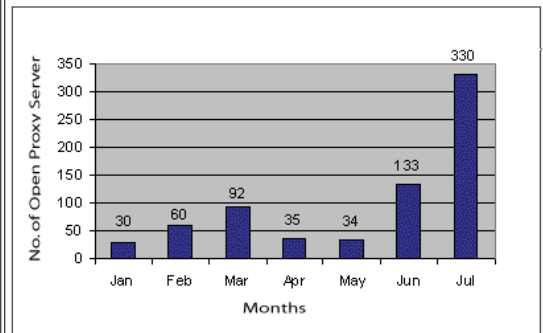


**Open proxy servers**

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 330 open proxy servers functioning in India during July 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 - July 2008**



**Attack Trend**

[Malware stealing online game credentials spreading](#)

It has been observed that different variants of malware which steals online game credentials are spreading widely. Some of the variants spread as packed executables. These variants steal confidential information such as username and passwords related to the online games and send this information to a remote website by HTTP POST.

[\[More\]](#)

It has been observed that SQL Injection Worm spreading in the wild by injecting java scripts or iframe into websites. The [Asprox](#) botnet is also launching the SQL Injection attacks. Many websites have been found infected with such scripts.

[\[More\]](#)

DNS cache poisoning is injecting false information into the caches of the DNS system so that future requests are diverted to rogue site. Successful exploitation of cache poisoning attack can cause a DNS server's clients to contact the rogue and possibly malicious hosts. The [CERT advisory](#) highlights three problems in the existing DNS infrastructure:

- Lack of sufficient randomness in the selection of source ports for DNS queries
- DNS transaction ID values that also exhibit insufficient randomness
- Multiple outstanding requests for the same resource record

[\[More\]](#)

Significant spam, scams and malware campaigns surrounding the highly anticipated July 11th release of Apple's new iPhone. Scams will be especially prevalent if supply is unable to meet demand.

The Srizbi botnet to gain momentum and to account for approximately 50 percent of all spam volume circulating on the Internet.

A Storm Worm's Independence Day( July 4 th Storm Worm) campaign is circulating online using email as propagation vector, attempting to trick users into visiting a Storm Worm infected host, where a multitude of what looks like over five different exploits attempt to automatically infect the visitors next to the malware binary fireworks.exe .

### Training

Workshop on "Linux Security" on 31 st July, 2008

A one day Workshop on "Linux Security" was conducted on July 31, 2008 . The objective of the workshop is to train system/network administrators how to secure Linux systems and Servers in an enterprise/organization. Delegates from Government, public sector and private sector organizations participated in the workshop. The workshop covered the following topics at length:

Linux Security an Overview :

- [Redhat Enterprise Linux Security & Linux Server Security](#)
- [Linux System Security](#)

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

### Case Study

#### CICS-2008-02

In the month of May it has been observed that SQL Injection Worm spreading in the wild by injecting java scripts or iframe into vulnerable websites.. Database Security and vulnerability Analysis Team of CERT-In thoroughly analyzed the attack and identified the vulnerabilities which were being exploited to compromise the website. After compromising the website, the attacker injected Javascript that redirects visitors to malicious websites and malware hosted on these websites gets automatically downloaded onto user's computer system. The download malware may include key loggers, backdoor Trojans and bots etc.

CERT-In devised appropriate countermeasures to secure web server and web applications from such type of attacks and communicated to the affected Organizations and user community.

[\[More\]](#)

### Security Alerts

**The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during July 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	Microsoft Word Memory Corruption Vulnerability	July 10, 2008	<a href="#">CIVN-2008-104</a>
Microsoft	Microsoft Access Snapshot Viewer ActiveX control remote code execution vulnerability	July 14, 2008	<a href="#">CIVN-2008-106</a>
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Linux	Linux Kernel LDT Denial of Service Vulnerability	July 29, 2008	<a href="#">CIVN-2008-113</a>

ORACLE	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Oracle	Multiple Vulnerabilities in various Oracle products		July 16, 2008	<a href="#">CIAD-2008-37</a>	
Oracle	Oracle Weblogic Apache Connector Buffer Overflow Vulnerability		July 31, 2008	<a href="#">CIVN-2008-114</a>	
Miscellaneous	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Opera	Multiple vulnerabilities in Opera Software		July 04, 2008	<a href="#">CIVN-2008-97</a>	
Mozilla	Multiple Vulnerabilities in Mozilla Products		July 08, 2008	<a href="#">CIAD-2008-33</a>	
Sun JDK and JRE	Multiple critical vulnerabilities in Sun Java Development Kit and Java Runtime Environment		July 16, 2008	<a href="#">CIAD-2008-36</a>	
RealPlayer	Multiple Security Vulnerabilities RealNetworks RealPlayer		July 31, 2008	<a href="#">CIAD-2008-38</a>	
Medium Vulnerabilities					
Microsoft	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Microsoft	Microsoft Windows DNS Spoofing Vulnerabilities		July 10, 2008	<a href="#">CIVN-2008-100</a>	
Microsoft	Microsoft Windows Saved Search Vulnerability		July 10, 2008	<a href="#">CIVN-2008-101</a>	
Microsoft	Microsoft Outlook Web Access for Exchange Server XSS Vulnerabilities		July 10, 2008	<a href="#">CIVN-2008-102</a>	
Microsoft	Microsoft SQL server Elevation of Privilege Vulnerabilities		July 10, 2008	<a href="#">CIVN-2008-103</a>	
Unix	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Linux	Multiple Vulnerabilities in Linux Kernel		July 14, 2008	<a href="#">CIVN-2008-108</a>	
ORACLE	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Oracle	Oracle Database Local Untrusted Library Path Vulnerability		July 29, 2008	<a href="#">CIVN-2008-110</a>	
Oracle	Oracle Internet Directory Pre-Authentication LDAP Denial of Service Vulnerability		July 29, 2008	<a href="#">CIVN-2008-111</a>	
Oracle	Oracle Database DBMS_AQELM Package Buffer Overflow Vulnerability		July 29, 2008	<a href="#">CIVN-2008-112</a>	
CISCO	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
CISCO	Multiple Vulnerabilities in Cisco Unified Communications Manager		July 01, 2008	<a href="#">CIVN-2008-96</a>	
CISCO	Cisco Wide Area Application Services (WAAS) Common UNIX Printing System (CUPS) Vulnerability		July 09, 2008	<a href="#">CIVN-2008-99</a>	
Miscellaneous	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Wireshark	Multiple Vulnerabilities in Wireshark 0.9.5 to 1.0.0		July 04, 2008	<a href="#">CIVN-2008-98</a>	
Solaris	Vulnerability in Solaris snmpXdmid		July 11, 2008	<a href="#">CIVN-2008-105</a>	
DNS	Cache poisoning vulnerability in multiple DNS implementations		July 11, 2008	<a href="#">CIAD-2008-35</a>	
Wireshark	Wireshark Packet reassembly Denial of Service Vulnerability		July 14, 2008	<a href="#">CIVN-2008-107</a>	
Mozilla	Mozilla Firefox URI Splitting Security Bypass Vulnerability		July 23, 2008	<a href="#">CIVN-2008-109</a>	
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
		It has been observed that various variants of Win32/Frethog family of Trojans			

Win32/Frethog	Trojan	are spreading widely. Win32/Frethog is a large family of password-stealing Trojans that target confidential data from Massive Multiplayer Online Role Playing Games (MMORPGs).	PWS-Mmorpg.gen, PWS-WOW.gen.e (McAfee), Trojan-PSW.Win32.OnLineGames.ajsz (Kaspersky,F-Secure) PWS-LegMir, Infostealer.Gampass.	July 11, 2008	<a href="http://www.cert-in.org.in/virus/Win32_Frethog.htm">http://www.cert-in.org.in/virus/Win32_Frethog.htm</a>
Asprox Botnet	Trojan	It has been observed that a Trojan horse named Asprox is spreading widely. The Trojan, which was originally used for sending phishing scams, uses fast flux SQL injection Attacks to hack websites and formulates a botnet.	Mal/Badsrc-C (Sophos), Trojan.Asprox.D (BitDefender), Trojan:JS/Aseljo.A (Microsoft)	July 17, 2008	<a href="http://www.cert-in.org.in/virus/Asprox_Botnet.htm">http://www.cert-in.org.in/virus/Asprox_Botnet.htm</a>
Malware stealing online game credentials spreading	Malware	It has been observed that different variants of malware which steals online game credentials are spreading widely. Some of the variants spread as packed executables. These variants steal confidential information such as username and passwords related to the online games and send this information to a remote website	PSW.OnlineGames.APEY (AVG), Win32/PSW.OnLineGames.NOA (ESET), Infostealer.Gampass (Symantec)	July 11, 2008	<a href="http://www.cert-in.org.in/currentacts/currentact07.htm#MSOG">http://www.cert-in.org.in/currentacts/currentact07.htm#MSOG</a>
Infostealer Ldpinch	Trojan	It has been observed that an Information stealing Trojan named Infostealer Ldpinch is spreading widely. The Trojan overwrites certain files with a copy of itself inorder to execute	No Aliases found	July 28, 2008	<a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-072811-4729-99&amp;tabid=2">http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-072811-4729-99&amp;tabid=2</a>

itself on every  
system start  
up.

## Security News

### **Lithuania Attacked by Russian Hacktivists, 300 Sites Defaced**

Source: <http://securityratty.com>] - 07 July 2008

Last week's mass defacement of over 300 Lithuanian sites hosted on the same ISP, an upcoming attack that was largely anticipated due to the on purposely escalated online tensions out of Lithuan's accepted legislation banning communist symbols across the country, once again demonstrates information warfare building capabilities in action.

[\[More\]](#)

### **US is the most prolific source of spam and viruses**

Source: <http://www.net-security.org>] - 31 July 2008

The US has continued its rule as the most prevalent source of spam and viruses, according to threat statistics analyzed by managed security company, Network Box. The country has held this unwanted title throughout 2008 and, based on July's figures, this trend looks set to continue.

This month, the US was responsible for one in four viruses (25.2 per cent), outstripping its nearest rival, Australia , by more than four to one (5.8 per cent). More than one-in-ten (11.6 per cent) spam emails emanated from the US , with Turkey trailing behind in second place (8.4 per cent).

[\[More\]](#)

### **Gmail, PayPal and Ebay embrace DomainKeys to fight phishing emails**

[Source: <http://blogs.zdnet.com>] - 09 July 2008

Brad Taylor, Google's Gmail Spam Czar, has just posted details on the ongoing cooperation with PayPal and Ebay, two of the most targeted brands in phishing emails, the effect of which is rejecting compared to flagging as spam each and every email pretending to be coming from paypal.com and ebay.com as well as from their international domain extensions. It's a win-win-win move for users, and the companies themselves which are now digitally signing all of their emails, making phishing emails spoofing their origin easier to detect.

[\[More\]](#)

### **PhishLock pro-active anti-phishing solution**

[Source: <http://www.net-security.org>] - 30 July 2008

PhishLock offers protection in real-time and can operate in the cloud, putting a stop to online identify theft, lowering fraud costs and preventing disruption to web services, while protecting brands and corporate reputations. The software operates on the end user client, or in the cloud.

Unlike traditional anti-virus, anti-spyware and anti-phishing solutions which rely on identifying malware or black lists which become out-of-date almost instantly, SentryBay's solutions detect virtually 100% of spyware and phishing attacks from the second they are launched, protecting against 'zero-day' attacks.

[\[More\]](#)

### **Developer fixes 33-year-old Unix bug**

[Source: <http://www.computerworld.com>] - 10 July 2008

An OpenBSD developer has discovered and fixed a bug in the software that has been traced back to an AT&T version of Unix from 1975.

OpenBSD is a variant of the Berkeley Software Distribution (BSD), a widely used, open-source, Unix-like operating system. BSD's variants include OpenBSD, FreeBSD and NetBSD, and it forms the basis of Apple's Mac OS X operating system.

The latest bug, which affected the YACC parser generator, followed the May discovery of a BSD flaw that was 25 years old.

[\[More\]](#)

### **Multiple Facebook vulnerabilities reported on Full-Disclosure**

[Source: <http://blogs.zdnet.com>] - 02 July 2008

Facebook and other social networks that are heavily populated are increasingly drawing the eye of security researchers and hackers alike, as due to the heavy amount of traffic they receive, they provide an excellent attack deployment point. In fact, there will be a wonderful talk this year at Black Hat Las Vegas 2008 on attacking Social Networks, called "Satan is on My Friends List: Attacking Social Networks", by Shawn Moyer and Nathan Hamiel.

[\[More\]](#)

### **Cybercriminals reinventing attack method**

[Source: <http://www.ciol.com>] - 08 July 2008

Trend Micro Inc. reported that cybercriminals are not only leveraging new technologies to propagate cybercrime, but are also reinventing forms of social engineering to cleverly ensnare both consumers and businesses, according to the "Trend Micro Threat Roundup and Forecast 1H 2008" report. As a result, the last six months saw an upswing in Web threats, but steady decreases in adware and spyware that are generated by outdated technical methods and can no

longer compete with high-level security solutions.

[\[More\]](#)

#### **Cyber-crooks celebrate independence**

[Source:www.vnunet.com] - 04 July 2008

Malware writers are looking to cash in the upcoming 4th of July weekend, say security experts.

With the US gearing up to celebrate its Independence Day on the 4th and the release of the iPhone scheduled for the 11th, the first two weeks of July could be a busy time for malware, according to security firm MX Logic.

MX Logic noted that the 4th of July was used by Storm last year to spread itself to new users. The malware writers behind the Storm botnet often make use of current events and holidays when crafting their social engineering attacks, and the company said that it doesn't expect this year to be any different.

[\[More\]](#)

#### **Malware authors declare start of World War III (again)**

[Source: http://www.theregister.co.uk] - 12 July 2008

It beggars belief that anyone would think that they'd first hear of World War III through a spam email. But hackers are relying on such credulous fools in an attempt to spread a new Trojan.

Widely spammed emails with subject lines including "Third World War has begun", "20000 US Soldiers in Iran", and "US Army crossed Iran's borders" link to a website displaying what poses as a video player displaying the mushroom cloud of a nuclear bomb and text on a supposed US invasion of Iran.

The tactic is far from the first time hackers used rising tensions between Iran and the West as the theme for malware-based attacks. Iran 's controversial decision to continue building a nuclear plant was used to bait attacks designed to spread a series of Trojans back in 2005, Sophos reports.

[\[More\]](#)

#### **Trojan Attacks Multimedia Files Stored on Hard Drives**

[Source:http://www.darkreading.com] - 10 July 2008

A particularly aggressive Trojan is on the loose that infects multimedia files stored on a user's hard drive.

"We've not seen such a sophisticated Trojan infecting multimedia files before," says Christoph Alme, lead for the anti-malware team at Secure Computing, which has been studying the Trojan. "We've been seeing infected multimedia files for about a month now and [had been] wondering where they came from."

Like many malware infections, it starts with a visit to a sketchy site -- in this case, a Warez site, where the user downloads what he thinks is a serial key for a copy-protected software package, for example, but instead gets the Trojan that automatically infests all of his multimedia files. When he shares one of those music or video files with another user via a peer-to-peer network, the recipient in turn gets infected by a fake codec: no Warez visit required.

[\[More\]](#)

#### **IE 8 to have antimalware protection**

[Source:http://news.cnet.com] - 02 July 2008

22nd May , 2008

Microsoft announced new security features within the upcoming release of Internet Explorer 8 Beta 2. The features are designed to combat the rising tide of drive-by downloads and malicious scripts contained within carefully crafted links embedded in e-mail and Web pages. Most of the new features require systems to be running Windows Vista SP1 or Windows XP SP3.

Perhaps the most anticipated addition is Internet Explorer's new antimalware protection. Opera 9.5 and Firefox 3 both recently added antimalware protection. Safari has so far not announced plans for similar protection. Using mostly its own antimalware technology, Microsoft will block emerging threats by masking the entire IE 8 browser screen with a warning to users. The addition of malware protection to the existing antiphishing protection will be re-branded as the Microsoft SmartScreen filter.

[\[More\]](#)