



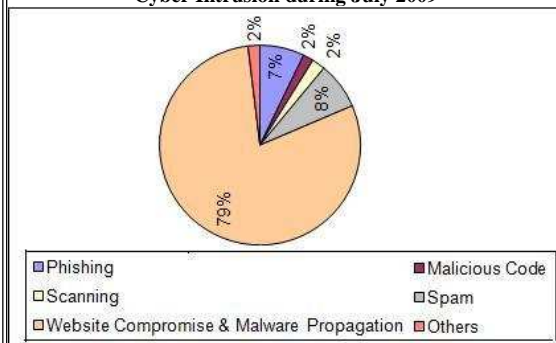
CERT-In Monthly Security Bulletin July 2009

Cyber Intrusion Trends

In this month 834 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure, 79 % incidents related to Spreading of malware through website compromise were reported in this month. 08 % incidents related to spamming, 07 % phishing incidents , 02 % incidents related to virus/worm under the Malicious code category, 02 % unauthorized scanning, 02 % incidents related to technical help under the Others category were also reported in this month.

In this month CERT -In tracked 28854 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 July 2009



Indian Websites Defacement

549 Indian websites were defaced during July 2009. The vulnerabilities which might have been exploited for the defacements are :

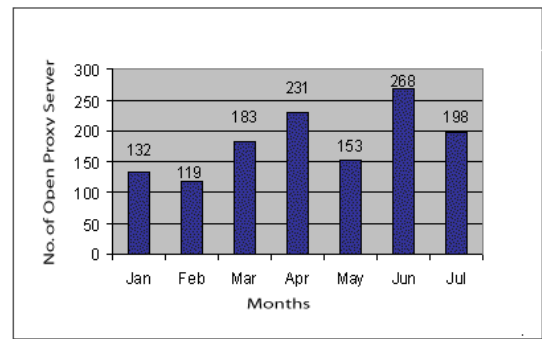
Vendor/Product	Title of Vulnerability	References & Patch Information
Microsoft -IIS	Remote Authentication Bypass Vulnerability in Microsoft IIS 6.0 WebDAV	CIVN-2009-63
WordPress	SQL injection vulnerability in BTE_RW_webajax.php in the Related Sites plugin 2.1 for WordPress allows remote attackers to execute arbitrary SQL commands via the guid parameter	CVE-2009-2383
dm_album	PHP remote file inclusion vulnerability in template/album.php in DM Albums 1.9.2, as used standalone or as a WordPress plugin, allows remote attackers to execute arbitrary PHP code via a URL in the SECURITY_FILE parameter.	CVE-2009-2396
PHP	CRLF injection vulnerability in bs_disp_as_mime_type.php in the BLOB streaming feature in phpMyAdmin	CVE-2009-1149
PHP	Static code injection vulnerability in setup.php in phpMyAdmin 2.11.x before 2.11.9.5 and 3.x before 3.1.3.1	CVE-2009-1151
Joomla!	SQL injection vulnerability in the PHP (com_php) component for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameter to index.php.	CVE-2008-2400
Joomla!	SQL injection vulnerability in the Ice Gallery (com_ice) component 0.5 beta 2 for Joomla! allows remote attackers to execute arbitrary SQL commands via the catid parameter to index.php.	CVE-2008-6852
Joomla!	com_php for Joomla "id" Parameter Remote SQL Injection Vulnerability	CVE-2009-2400
Simple Machines Forum	SQL injection vulnerability in the awardsMembers function in Sources/Profile.php in the Member Awards component 1.0.2 for Simple Machines Forum (SMF) allows remote attackers to execute arbitrary SQL commands via the id parameter in a profile action to index.php.	CVE-2009-2385
phpMyBlockchecker	admin.php in phpMyBlockchecker 1.0.0055 allows remote attackers to bypass authentication and gain administrative access by setting the PHPMYBCAdmin cookie to LOGGEDIN.	CVE-2009-2382
AIST NetCat	SQL injection vulnerability in modules/poll/index.php in AIST NetCat 3.0 and 3.12 allows remote attackers to execute arbitrary SQL commands via the PollID parameter.	CVE-2008-6853

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.

Statistics of Open Proxy Servers tracked during July 2009

CERT -In tracked 198 open proxy servers functioning in India during July 2009. 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.



Attack Trend

Microsoft Office web components ActiveX exploit

It is reported that an exploit for the zero -day vulnerability in Microsoft Office web components described in CERT -In vulnerability note CIVN 2009 -83 is being reported.This vulnerability is due to a memory corruption error in the Office Web Components ActiveX Controls (OWC10.dll and OWC11.dll).

Microsoft Office Web Components are a collection of Component Object Model (COM) controls for publishing spreadsheets, charts, and databases to the Web, and for viewing the published components on the Web.

[\[More\]](#)

Trojan:Win32/InternetAntivirus

It has been observed that Trojan:Win32/InternetAntivirus is circulating widely. It is a rogue security program that displays fake warning messages indicating that “ spyware or malware has been detected on the machine” in order to convince users to purchase rogue security software. It also impersonates “ Windows Security Center.

[\[More\]](#)

Training

Workshop on "Defending Phishing Attacks" on July 30, 2009

A one day workshop on “Defending Phishing Attacks” was conducted on 30th July 2009. The objective of the workshop is to create security awareness within the Government, Financial /Public/ Private sector organisations and ISPs on Phishing scams & attacks, and how to tackle the Phishing threats to keep alert to avoid becoming victim of Phishing attack in order to minimize the financial frauds and information leakage. Delegates were from Government, Corporate and critical sector organizations.

[\[Presentation Material\]](#)

Workshop on " Identity and Access Management " on July 24, 2009

A one day workshop on “Identity and Access Management ” was conducted on 24th July 2009. The objective is to create awareness within the Government, public and critical sector organisations on maintaining and managing the identity of users and the access to the services & Information Infrastructure of an organization in order to minimize the information leakage & security risk. Delegates were from Government, Corporate and critical sector organizations.

Workshop on "Web Application Security – Current Trends" on July 3, 2009

A one day workshop on “Web Application Security – Current Trends” was conducted on 3rd July 2009. The objective is to create awareness within the Government, public and critical sector organisations on latest security attacks and defense techniques to secure the web applications. Delegates were from Government, 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 July 2009 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 Internet Explorer Memory Corruption vulnerabilities	29-Jul-09	CIVN-2009-93
Microsoft	Multiple Vulnerabilities in Microsoft Products	16-Jul-09	CIAD-2009-33
Microsoft	Microsoft Video Streaming ActiveX control stack buffer overflow vulnerability	16-Jul-09	CIVN-2009-89
Microsoft	Microsoft Office Publisher 2007 Pointer	16-Jul-09	CIVN-2009-87

	Dereference Vulnerability				
Microsoft	Multiple Vulnerabilities in Embedded OpenType Font Engine		16-Jul-09	CIVN-2009-86	
Microsoft	Multiple Remote Code Execution Vulnerabilities in Microsoft DirectShow		16-Jul-09	CIVN-2009-85	
Microsoft	Microsoft Office Web Components Spreadsheet ActiveX Control HTML Code Execution Vulnerability		14-Jul-09	CIVN-2009-83	
Microsoft	Microsoft Video Streaming ActiveX control stack buffer overflow vulnerability		7-Jul-09	CIVN-2009-79	
Oracle	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Oracle	Multiple Vulnerabilities in various Oracle Products		16-Jul-09	CIAD-2009-32	
Solaris	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Solaris	Solaris Ultra-SPARC T2 Crypto Provider Device Driver Vulnerability		9-Jul-09	CIVN-2009-81	
Miscellaneous	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Adobe	Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability		27-Jul-09	CIVN-2009-91	
Mozilla	Mozilla Firefox HTML Element Processing Arbitrary Code Execution Vulnerability		20-Jul-09	CIVN-2009-84	
	Vulnerability in BIND (9) causes denial of service via dynamic update request		29-Jul-09	CIAD-2009-34	
	DDoS attacks against US and South Korean sites		10-Jul-09	CIAD-2009-31	
Medium Vulnerabilities					
Microsoft	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Microsoft	Microsoft Visual Studio Active Template Library (ATL) Multiple Vulnerabilities		29-Jul-09	CIVN-2009-92	
Microsoft	Elevation of Privileges Vulnerability in Microsoft Virtual PC and Virtual Server		16-Jul-09	CIVN-2009-90	
Microsoft	Vulnerability in Microsoft ISA Server 2006 Radius OTP Bypass Vulnerability		16-Jul-09	CIVN-2009-88	
Miscellaneous	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
IBM	IBM Tivoli Identity Manager Cross-Site Scripting Vulnerabilities		13-Jul-09	CIVN-2009-82	
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Daprosy	Worm	It has been observed that a Worm named Daprosy is spreading in the wild. It spreads through mapped, fixed, and removable drives. It also spreads through email by sending a copy of itself as an attachment. After successful execution the Worm hides file extensions and folders and copies itself as the folder name using the Windows folder icon. If the icon is clicked, it executes the worm. The worm also launches the genuine folder in a separate Window to infect files in it.	No aliases found	July 16, 2009	http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-071521-4358-99&tabid=1
Hacktool.	Trojan	It has been observed that a Trojan named Hacktool.Stonedbootkit is spreading in the wild. It replaces the Master Boot Record with its own MBR that will gain control of the	No aliases	July 28, 2009	http://www.symantec.com/business/security_response/writeup.jsp?

Stonedbootkit		compromised computer when it restarts. The new MBR then hooks certain Windows system files, which allow all users to run code with elevated privileges.	found		docid=2009-072815-0454-99&tabid=2
Trojan:Win32/InternetAntivirus	Trojan	It has been observed that Trojan:Win32/InternetAntivirus is circulating widely. It is a rogue security program that displays fake warning messages indicating that" spyware or malware has been detected on the machine" in order to convince users to purchase rogue security software.	Personal Antivirus, General Antivirus	July 2, 2009	http://www.cert-in.org.in/virus/Internet_Antivirus.htm

Security News

US websites buckle under sustained DDoS attacks

[Source: www.theregister.co.uk] July 8, 2009

Websites belonging to the federal government, regulatory agencies and private companies have been struggling against sustained online attacks that began on the Independence Day holiday, according to multiple published reports.

Most of the targets appeared to be afloat. Nonetheless, several targets have buckled under the DDoS, or distributed denial of service, attacks, which try to bring down a website by bombarding it with more traffic than it can handle. FTC.gov was experiencing "technical issues" on Monday and Tuesday that prevented many people from reaching the site.

Other sites, including FAA.gov, Treas.gov and DOT.gov also experienced outages, a person said familiar with the attacks.

[\[More\]](#)

BIND crash bug prompts urgent update call

[Source: theregister.co.uk] July 29, 2009

A vulnerability in BIND creates a means for miscreants to crash vulnerable Domain Name System servers, posing a threat to overall internet stability as a result.

Exploits targeted at BIND (Berkeley Internet Name Domain Server) version 9 are already in circulation, warns the Internet Software Consortium, the group which develops the software. ISC urges sys admins to upgrade immediately, to defend against the "high risk" bug.

Sys admins are urged to upgrade BIND servers to versions 9.4.3-P3, 9.5.1-P3 or 9.6.1-P1 of the software, which defend against the flaw.

The vulnerability involves BIND servers that act as a master (slave systems are unaffected) and involves problems in dealing with malformed update messages, which can be used to cause a server to crash.

[\[More\]](#)

Researchers find insecure BIOS 'rootkit' pre-loaded in laptops

[Source: [http://http://blogs.zdnet.com](http://blogs.zdnet.com)] July 30, 2009

A popular laptop theft-recovery service that ships on notebooks made by HP, Dell, Lenovo, Toshiba, Gateway, Asus and Panasonic is actually a dangerous BIOS rootkit that can be hijacked and controlled by malicious hackers.

The service — called Computrace LoJack for Laptops — contains design vulnerabilities and a lack of strong authentication that can lead to "a complete and persistent compromise of an affected system," according to Black Hat conference presentation by researchers Alfredo Ortega and Anibal Sacco from Core Security Technologies.

Computrace LoJack for Laptops, which is pre-installed on about 60 percent of all new laptops, is a software agent that lives in the BIOS and periodically calls home to a central authority for instructions in case a laptop is stolen. The call-home mechanism allows the central authority to instruct the BIOS agent to wipe all information as a security measure, or to track the whereabouts of the system.

[\[More\]](#)

One extra ampersand in code leads to IE exploit

[Source: arstechnica.com] July 29, 2009

Microsoft has admitted that one of the out-of-band security updates it released was actually caused by a single typo in the code. The security flaw in Internet Explorer was caused by an unnecessary ampersand character, according to The Security Development Lifecycle blog: "The extra '&' character in the vulnerable code causes the code to write potentially untrusted data, of size cbSize, to the address of the pointer to the array, pbArray, rather than write the data into the array, and the pointer is on the stack. This is a stack-based buffer overrun vulnerability." The typo corrupted the code of the MSVIDCUI ActiveX control used by Internet Explorer.

Microsoft says it will update its tools to help find COM stream-related issues quickly and will tell teams they must use new ATL libraries (Microsoft previously did not tell its programmers what to use). In this specific case, an older library with flaws was used.

[\[More\]](#)

Report: Spam and malware at all-time highs

[Source: <http://news.cnet.com>] July 29, 2009

Spam and botnets have hit their highest levels ever, according to McAfee's second-quarter **Threats Report**, released Wednesday. McAfee's Avert Labs says spam recorded in the second quarter shot up 80 percent compared with the first quarter of the year.

This follows a brief reprieve from spam following last year's shutdown of the **McColo ISP**. June alone saw the largest amount of spam recorded by McAfee, surpassing the previous monthly high in October by more than 20 percent. McAfee now estimates that spam accounts for 92 percent of all e-mail.

[\[More\]](#)

Wildcard certificate spoofs web authentication

[Source: <http://www.theregister.co.uk>] July 30, 2009

Black Hat In a blow to one of the net's most widely used authentication technologies, a researcher has devised a simple way to spoof SSL certificates used to secure websites, virtual private networks, and email servers.

The attack, unveiled at the Black Hat security conference in Las Vegas, exploits a weakness in the process for generating secure sockets layer certificates. It works by adding a null string character to several certificate fields, a technique that tricks browsers and other SSL-enabled programs into misinterpreting the domain name that is being authenticated.

Security researcher Moxie Marlinspike created what he called a universal wildcard certificate that in many ways resembles certificate authority certificates that VeriSign and other companies use to generate SSL certificates. He did it by applying for a normal certificate for his website thoughtcrime.org. In the commonName field he listed the site as *(0.thoughtcrime.org, giving him a certificate that tricks many programs into authenticating virtually every address on the internet.

[\[More\]](#)

Rogue Antivirus Terminates EXE Files

[Source: <http://blog.trendmicro.com/>] July 26, 2009

TrendLabs came across a FAKEAV variant similar to the one peddled in the solar eclipse 2009 in America attack in this recent blog post. This one, however, introduces another new scare tactic (so far the latest new ploy we've seen is the ransomware/FAKEAV that encrypts files in the infected computer and offers a bogus fixtool for a price).

This FAKEAV variant terminates any executed file with an .EXE file extension and displays a pop-up message saying that the .EXE file is infected and cannot execute.

[\[More\]](#)

Clampi Trojan stealing online bank data from consumers and businesses

[Source: news.cnet.com] 20 July 2009

LAS VEGAS--Hundreds of thousands of Windows computers are believed to be infected with a Trojan called "Clampi" that has been stealing banking and other log-in credentials from compromised PCs since 2007, a security researcher said on the eve of the Black Hat security conference.

Clampi, also known as Ligats, Ilomo, or Rscan, infects computers in drive-by downloads when people visit Web sites hosting malicious code that exploits vulnerabilities in browser plug-ins Flash and ActiveX, said Joe Stewart, director of malware research for the Counter Threat Unit of SecureWorks.

When the infected computer is used to access a targeted banking or other site, the log-in and other information is stolen.

Clampi has spread quickly through Microsoft-based networks in a worm-like fashion in recent months, Stewart said. It uses domain administrator credentials that were either stolen by the Trojan or based on an administrator logging into an infected system. It then uses a Windows executable SysInternals tool, "psexec," to copy itself to all the computers on the domain, he said.

[\[More\]](#)

419 scammers using Dilbert.com

[Source: <http://blogs.zdnet.com>] July 28,2009

On their way to search for clean IPs through which to send out yet another scam email, 419 con-artists (Mrs Sharon Goetz Massey) have recently started using Dilbert.com's recommendation feature in an attempt to bypass anti-spam filters — and it works. The use of Dilbert.com's clean IP reputation comes a month after 419 scammers used the same tactic on NYTimes.com 'email this' feature.

Isolated incidents or an indication of a trend? 419 scammers are like spammers circa 1997, technically unsophisticated but fully capable of maintaining a fraudulent infrastructure by using legitimate services only.

Case in point - automatically registered email accounts next to compromised ones already represent the source of a close to 20% of the overall spam volume.

and these levels remain steady. A logical question arises, why hasn't 419 advance-fee fraud reached the efficiency levels of phishing or spam in general, taking into consideration the fact that spam is already outsourced as a process? It's because South Africa-based scammers lack the networking skills necessary to approach international cybercrime groups which would not only manage the entire scamming process for them, but would help them improve the quality of the campaigns.

[\[More\]](#)

Open-source firmware vuln exposes wireless routers

[Source: <http://www.theregister.co.uk>] July 21, 2009

A hacker has discovered a critical vulnerability in open-source firmware available for wireless routers made by Linksys and other manufacturers that allows attackers to remotely penetrate the device and take full control of it.

The remote root vulnerability affects the most recent version of DD-WRT, a piece of firmware many router users install to give their device capabilities not available by default. The bug allows unauthenticated users to remotely gain root access simply by luring someone on the local network to a malicious website.

"This means someone can even post some crafted [img] link on a forum and a dd-wrt router owner visiting the forum will get owned," a user named Leka Vecher "gat3way" wrote in this posting to Milw0rm. "A weird vulnerability you're unlikely to see in 2009 :) Quite embarrassing I would say."

[\[More\]](#)

MS adds sandboxing to Office 2010

[Source: <http://www.theregister.co.uk>] July 24, 2009

Microsoft has announced plans to introduce sandboxing technology with the next version of its Office suite.

Office 2010 will incorporate sandboxing technology so that when users want to simply read Office documents, these files will have no access to other files or information. "Even if the file is malicious, it can't get out of the sandbox and do harm to your computer or data," explains Brad Albrecht, a Microsoft security specialist on the Office 2010 blog.

The sandboxing approach is a well-known mechanism for safely running untrusted programs that has been applied to Java Applets and (more recently) to Google's Chrome browser software. The technology will be used in conjunction with enhanced file (format inspection) blocker features and validity checks to provide a layered defence for Office 2010.

The file blocker, introduced in Office 2007, automatically prevents access to some document types. Improvements introduced with 2010 give users more granular control in managing how Word, Excel, and PowerPoint open their file types.

As Microsoft acknowledges, Office files have become a common payload in targeted hacking attacks over recent months.

[\[More\]](#)

Sober worm returns and uses social engineering techniques

[Source: net-security.org] July 09, 2009

PandaLabs has recorded the appearance of a new variant of the Sober worm, Sober.Y, which spreads using social engineering techniques in emails sent in English or German.

The worm uses two types of mail to propagate: Firstly, an email in English with the subject "Your new password," which tries to make users think it is notification of a change of password, asking them to check the data in an attached file, pword_change.zip.

Secondly, an email written in German claiming to contain a photograph of old school friends in the file KlassenFoto.zip. Both compressed files contain the executable PW_Klass.Pic.packed-bitmap.exe, which is a copy of the worm itself.

[\[More\]](#)

Clever attack exploits fully-patched Linux kernel

[Source: www.theregister.co.uk] July 17, 2009

A recently published attack exploiting newer versions of the Linux kernel is getting plenty of notice because it works even when security enhancements are running and the bug is virtually impossible to detect in source code reviews.

The exploit code was released Friday by Brad Spengler of grsecurity, a developer of applications that enhance the security of the open-source OS. While it targets Linux versions that have yet to be adopted by most vendors, the bug has captured the attention of security researchers, who say it exposes overlooked weaknesses.

Linux developers "tried to protect against it and what this exploit shows is that even with all the protections turned to super max, it's still possible for an attacker to figure out ways around this system," said Bas Alberts, senior security researcher at Immunity. "The interesting angle here is the actual thing that made it exploitable, the whole class of vulnerabilities, which is a very serious thing."

The vulnerability is located in several parts of Linux, including one that implements functions known as net/tun. Although the code correctly checks to make

sure the tun variable doesn't point to NULL, the compiler removes the lines responsible for that inspection during optimization routines. The result: When the variable points to zero, the kernel tries to access forbidden pieces of memory, leading to a compromise of the box running the OS.

[\[More\]](#)

PCI Group Spells Out Guidelines For Deploying PCI-Compliant WiFi

[Source: darkreading.com] July 17, 2009

A working group of the PCI Security Standards Council has created a set of recommendations for wireless deployment that pick up where the PCI Data Security Standard (DSS) specifications leave off: the PCI DSS Wireless Guideline (PDF) provides specific suggestions for secure installation and procedures to ensure the WLAN meets PCI requirements.

Major data breaches that began with a WiFi hack like TJX today haunt retailers as cautionary tales of the dangers of a porous WLAN configuration. The PCI Wireless Special Interest Group -- made up of POS and security vendors, banks, and merchants including Capita, McDonald's, and Motorola -- was formed to provide merchants with steps for locking down their 802.11 WLANS in accordance with PCI DSS v1.2.

The document includes a step-by-step process for complying with PCI's wireless requirements.

"The guidelines are not a pass/fail grading system they are an operator's guide for merchants," says Doug Manchester, chair of the Wireless SIG and director of product security for VeriFone. "The guidelines are not adding any new control objectives nor any subordinate control objects" beyond the PCI specifications, he says.

[\[More\]](#)