



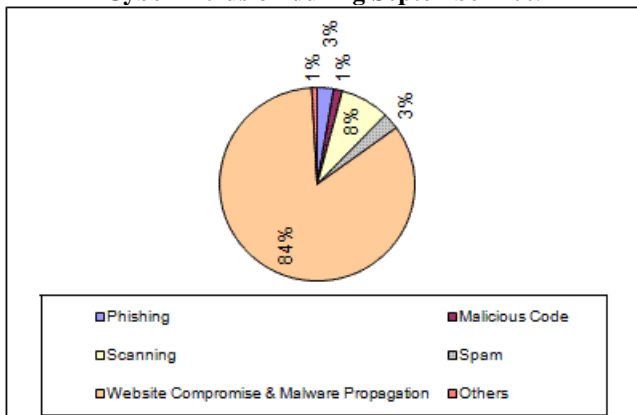
CERT-In Monthly Security Bulletin September 2009

Cyber Intrusion Trends

In this month 550 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure, 84 % incidents related to Spreading of malware through website compromise were reported in this month. 08 % unauthorized scanning, 03 % incidents related to spamming, 03 % phishing incidents , 01 % incidents related to virus/worm under the Malicious code category, and 01 % incidents related to technical help under the Others category were also reported in this month.

In this month CERT -In tracked 202478 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 September 2009



Indian Websites Defacement

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

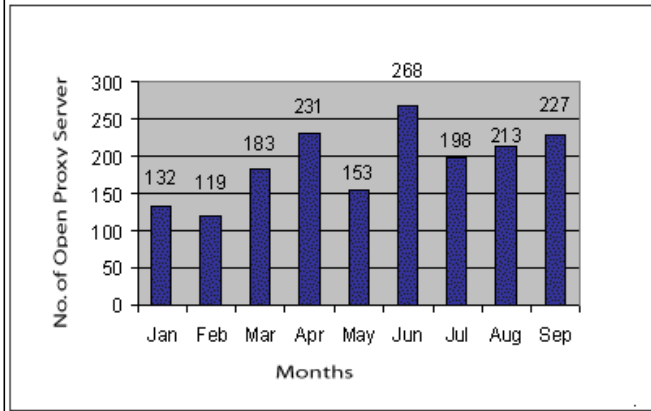
Vendor/Product	Title of Vulnerability	References & Patch Information
Microsoft -IIS	Multiple Vulnerabilities in Microsoft IIS FTP Service	CIVN-2009-107
PHP	Multiple Vulnerabilities in PHP	CIAD-2009-44
Microsoft -IIS	Remote Authentication Bypass Vulnerability in Microsoft IIS 6.0 WebDAV	CIVN-2009-63
Apache	Apache "Options" and "AllowOverride" Security Bypass Vulnerability	CIVN-2009-66
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
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

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
September 2009**

CERT -In tracked 227 open proxy servers functioning in India during September 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

Social Engineering Watch: Another IRS Scam

There is a spam campaign that targets US taxpayers with Foreign Bank and Financial accounts. The said spam rides on the September 23 extended deadline set by the Internal Revenue Service (IRS) for filing 'FBAR' or the Report of Foreign Bank and Financial Accounts.

The spammed message bears the subject "Notice of Underreported Income" and lures users to click the link that supposedly contains the tax statement. Users who click the URL are led to a site where they get infected by various ZBOT variants. ZBOT variants are notorious for their information theft routines. Trend Micro detected these ZBOT variants as TSPY_ZBOT.BZI, TSPY_ZBOT.BZT, TSPY_ZBOT.BZS, and TSPY_ZBOT.COB.

[\[More\]](#)

Malvertisements in NYTimes.com Lead to FAKEAV

People who get their regular dose of news from the New York Times website were recently told to be careful when browsing through the said site as malicious advertisements —also known as "malvertisements" —are found on its pages and are displaying pop-up windows that falsely report malware infections on their systems.

[\[More\]](#)

Bogus Sponsored Link Leads to FAKEAV

Apart from SEO poisoning, cybercriminals have found another avenue to proliferate FAKEAV malware—bogus sponsored links (sitio patrocinados in Spanish). Just recently, Trend Micro researchers were alerted to malicious search engine ads that appeared in Microsoft's Bing and AltaVista, among others, when a user searches the string "malwarebytes." (Malwarebytes is a free antivirus product, but of course, not a FakeAV.) Clicking the malicious URL points the user to an executable file named MalwareRemovalBot.exe-1

[\[More\]](#)

Training

Workshop on " Advanced Web Application Security" on September 23, 2009

A Workshop on "Advanced Web Application Security" was conducted on September 23 2009. The objective of the workshop is to create awareness within the Government, public and critical sector organisations on latest and advanced attacks on the Web and Applications therein and to apply defense mechanisms and countermeasures against these attacks. Delegates were from Government Departments/Ministries, PSUs, Banking/Financial and Critical sector organisation.

[\[Presentation Material\]](#)

Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during September 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	Multiple Vulnerabilities in Microsoft IIS FTP Service	1-Sep-09	CIAD-2009-107
Microsoft	Multiple Vulnerabilities in Microsoft JScript Scripting Engine,DHTML Editing Component ActiveX Control,Windows Media Format, Windows TCP/IP Implementation, Windows Wireless LAN AutoConfig Service	10-Sep-09	CIAD-2009-41
Microsoft	Microsoft Windows SMB 2.0 "srv2.sys" remote code execution vulnerability	10-Sep-09	CIVN-2009-114
Microsoft	Microsoft Windows Wireless LAN AutoConfig Service Buffer Overflow Vulnerability	10-Sep-09	CIVN-2009-113
Microsoft	Multiple Vulnerabilities in Microsoft Windows TCP/IP Implementation	10-Sep-09	CIVN-2009-112
Microsoft	Multiple Remote Code Execution vulnerabilities in Windows Media Format	10-Sep-09	CIVN-2009-111
Microsoft	Microsoft DHTML Editing Component ActiveX Control Remote Code Execution Vulnerability	10-Sep-09	CIVN-2009-110
Microsoft	Microsoft JScript Scripting Engine Memory Corruption Vulnerability	10-Sep-09	CIVN-2009-109
CISCO	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Cisco	Cisco Nexus 5000 Series Switches Remote TCP Denial of Service Vulnerability	15-Sep-09	CIVN-2009-115
Linux	Linux Kernel sock_sendpage() Local Privilege Escalation Vulnerability	15-Sep-09	CIVN-2009-108
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information

PHP	Adobe Acrobat, Reader, and Flash Player Remote Code Execution Vulnerability	25-Sep-09	CIAD-2009-44		
Mozilla	Multiple Vulnerabilities in Mozilla Firefox	14-Sep-09	CIAD-2009-43		
Apple	Mozilla Firefox HTML Element Processing Arbitrary Code Execution Vulnerability	14-Sep-09	CIAD-2009-42		
Medium Vulnerabilities					
Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Linux	Multiple Vulnerabilities in Linux Kernel	30-Sep-09	CIAD-2009-45		
Opera	Multiple Vulnerabilities in Opera	07-Sep-09	CIAD-2009-40		
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Perz	Worm	It has been observed that a Worm named <i>Perz</i> is spreading in the wild. It spreads through file sharing networks. The Worm opens a backdoor on the infected system and download additional malware onto the infected system. Further it also injects malicious Javascripts into the vulnerable webpages to redirects users to malicious websites.	No aliases found	September 15, 2009	http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-091516-2255-99&tabid=2
		It has been observed that a Virus named <i>Lafee</i> is spreading in the wild. It infects files having extensions .exe and .scr by appending malicious code at the end of	No	September 23,	http://www.symantec.com/business/security_response/

Lafee	Virus	each file. Further the virus connects itself to remote malicious websites using HTTP to send the sensitive information that stored on the infected system.	aliases found	2009	writeup.jsp?docid=2009-092316-0020-99&tabid=2
Opachki	Trojan	It has been observed that a Trojan Horse named Opachki is spreading in the wild. It injects itself into every process running on the compromised computer. It injects Web pages with HTML which directs users to the malicious website when the injected pages are viewed in web browser.	No aliases found	September 22, 2009	http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-092213-3317-99&tabid=2

Security News

Cybercriminals use Trojans and Money Mules to Loot Online Bank Accounts

[Source: finjan.com] 30 September 2009

The cybercriminals used compromised legitimate websites as well as fake websites, utilizing the crimeware toolkit LuckySploit to infect visitors. After infection a bank Trojan was installed on the victims' machines and started communication with its Command & Control (C&C) server for instructions. These instructions included the amount to be stolen from specific bank accounts and to which money mule accounts the stolen money should be transferred. Furthermore, the Trojan forged onscreen bank statements concealing the true transaction amount to dupe the account holders and their banks.

[\[More\]](#)

Tropical Storm Leads to FAKEAV

[Source: blog.trendmicro.com] 29 September 2009

Cybercriminals leveraged on the tropical storm, *Ondoy* (International name: Ketsana) that hit the Philippines and killed around 140 people. Senior Threat Analyst Joseph Pacamarra found several malicious sites that appeared each time the users search the strings, "manila flood," "Ondoy Typhoon," and "Philippines Flood," among others. The said sites emerged as one of the top search results.

Once the user clicks the URL, they will be redirected to several landing pages where they are asked to download an EXE file, *soft_207.exe*. Trend Micro detects it as TROJ_FAKEAV.BND. This attack does GeoIP checks, which mean it only targets specific regions or location (one of the landing sites is `hxxp://{BLOCKED}uterbestscan11.com/scan1/geoip.php`).

[\[More\]](#)

Firms most often infected by smaller botnets

[Source: . securityfocus.com] 30 September 2009

While big botnets get the lion's share of attention in the media, smaller botnets of less than 100 machines are the rule among most compromise corporate networks, according to a research released last week by security firm Damballa.

The company analyzed 600 botnets that it encountered in enterprise networks in a three-month period, and found that the majority -- 57 percent -- were smaller than 100 nodes. Most of the smaller networks consisted of customized code created using one of the do-it-yourself malware kits available online.

"It looks to me as though these small botnets are highly-targeted at particular enterprises -- or enterprise vertical sector(s) -- typically requiring a sizable degree of familiarity with the breached enterprise itself," Gunter Ollmann, vice president of research for Damballa, wrote in a blog post.

[\[More\]](#)

Several Compromised Thai Sites Serve Malware

[Source: blog.trendmicro.com] 28 September 2009

Trend Micro researchers discovered another wave of mass compromised websites involving several Thai government agencies' sites. One of the compromised sites, the Thai Police site, was injected with malicious codes to redirect users to several malicious sites. One of the landing pages, [http://{BLOCKED}t.ru/ip/bchqu1.exe](http://t.ru/ip/bchqu1.exe) served a downloader detected by Trend Micro as TROJ_DLOADER.DNG. This Trojan downloader is responsible for downloading several malware (detected as TROJ_FAKEREAN.BW, TROJ_CUTWAIL.GQ, and TSPY_ZBOT.ACH).

According to Senior Threat Analyst Joseph Pacamara who found out about the mass compromise, cybercriminals are now entertaining the idea of employing compromised legitimate sites as an avenue to proliferate FAKEAVs.

[\[More\]](#)

Defence hauled in over PM website attack

[Source: .blogs.zdnet.com] 10 September 2009

The Attorney General's Department (AGD) has called in the Defence Signals Directorate's Cyber Security Operations Centre and has provided IT security advisors to each of the targeted agencies in yesterday's attack, according to an AGD spokesperson.

The only website that appears to have been affected by yesterday's distributed denial-of-service (DDOS) attack on government web servers was the site belonging to the Prime Minister & Cabinet. But it was not hacked, according to the spokesperson.

"I can confirm that the Prime Minister's website was unavailable for a short time shortly after 7pm on 9 September 2009. Visitors to the site received an error message stating that the service was unavailable," said the spokesperson. "There was no unauthorised access to the website's infrastructure."

[\[More\]](#)

Fake Windows Live Malware Spreads via Email

[Source: blog.trendmicro.com] 28 September 2009

Trend Micro threat analysts recently snagged an email pushing a bogus Windows Live Messenger residing in http://{BLOCKED}s-live-msn.serveftp.com/Windows_Live_9.0_beta.exe (detected as [WORM_VB.PAB](#)). The .EXE file is, of course, not the "real" Windows Live Messenger but a bot that reports to an IRC-based C&C with the following details about the infected system:

The said bot's primary function seems to be MSN spamming. As of this writing, the C&C channel is currently idle, as it has not yet issued commands. Apart from MSN spamming, the said bot was also designed to spread via USB autorun and P2P networks like Kazaa and Limewire.

[\[More\]](#)

From Gimmiv to Conficker: The lucrative MS08-067 flaw

[Source: .blogs.zdnet.com] 23 September 2009

The critical MS08-067 vulnerability used by the Conficker worm to build a powerful botnet continues to be a lucrative security hole for cyber criminals.

During a presentation at the Virus Bulletin 2009 conference here, a trio of Microsoft researchers dissected the malware attacks linked to MS08-067 and found that criminal gangs are still exploiting the flaw to plant data-theft Trojans on vulnerable Windows machines.

Even before the appearance of Conficker in November 2008, the Microsoft research team said three different malware families — Arpoc, Gimmiv and Clort — were already using the code execution hole to “test the effectiveness” of exploit code.

The researchers — Elda Dimakiling, Francis Allan Tan Seng and Scott Wu — said the three malware families used different techniques and tricks to launch exploits copied from public Web sites like Milw0rm.com but it wasn't until the appearance of Conficker that the attacks took on a professional — and sinister — turn.

[\[More\]](#)

A simple way to protect removable drives from malware

[Source: net-security.org] 22 September 2009

You don't need a lot of time or knowledge to execute the few changes that Trend Micro suggests protecting your drive against the Autorun feature.

To be able to do this, you must first format the drive using NTFS (if you haven't already), because only this type of formatting allows you to execute the wanted procedure.

Create inside the root directory of the drive a file or folder named Autorun.inf. As worms are known to bypass this simple solution by replacing the legitimate file with the malicious one, use file permissions and restrict possible changes.

Additionally, create (also in the root directory) 4 more file or folders and name them "recycle", "recycler", "recycled" and "setup". Why? Because these are the names malware uses more often.

[\[More\]](#)

Brute-force attacks target two-year hole in Yahoo! Mail

[Source:.theregister.co.uk] 18 September 2009

Scammers are exploiting a two-year-old security hole in Yahoo's network that gives them unlimited opportunities to guess login credentials for Yahoo Mail accounts, a researcher said.

The vulnerability resides in a web application that automates the process of logging in to the widely used webmail service. Because it fails to carry out a variety of security checks followed by the login page Yahoo! Mail users typically use, it's providing criminals with a backdoor through which user accounts can be breached, said Ryan Barnett, director of application security research at Breach Security.

"If the front gate of your castle is your login page to Yahoo Mail, they've done a good job of securing it," he told The Register. The web application amounts to "some sort of water tunnel that the bad guys are walking right through."

Over the past seven weeks, a sensor deployed by WASC, or the Web Application Security Consortium, has detected "a few thousand" or more attempts to use the unprotected web application to carry out brute-force attacks on user passwords, Barnett said. Because the sensor is installed on just one of a massive number of open proxies, the honeypot is likely detecting only a small fraction of the overall activity, he added.

[\[More\]](#)

Remote exploit released for Windows Vista SMB2 worm hole

[Source: blogs.zdnet.com] 17 September 2009

Security researchers at penetration testing firm Immunity have created a reliable remote exploit capable of spawning a worm through an unpatched security hole in Microsoft's dominant Windows operating system.

A team of exploit writers led by Kostya Kortchinsky attacked the known SMB v2 vulnerability and created a remote exploit that's been fitted into Immunity's Canvas pen-testing platform. The exploit hits all versions of Windows Vista and Windows

Server 2008 SP2, according to Immunity's Dave Aitel.

Immunity's Canvas is used by IDS (intrusion detection companies) and larger penetrating testing firms as a risk management tool.

Exploit writers at the freely available Metasploit Project are also close to finishing a reliable exploit for the vulnerability, according to Metasploit's HD Moore.

[\[More\]](#)

SANS outlines the top cyber security risks

[Source: net-security.org] 15 September 2009

SANS released the "Top Cyber Security Risks" report which covers covers March-August 2009 that features attack data from TippingPoint intrusion prevention systems protecting 6,000 organizations, vulnerability data from 9,000,000 systems compiled by Qualys, and additional analysis and tutorial by the Internet Storm Center and key SANS faculty members.

The report's target audience is major organizations that want to ensure their defenses are up-to-date and are tuned to respond to today's newest attacks and to the most pressing vulnerabilities.

The report uses current data from appliances and software in thousands of targeted organizations to provide a reliable portrait of the attacks being launched and the vulnerabilities they exploit.

[\[More\]](#)

New York Times pwned to serve scareware pop-ups

[Source: <http://www.theregister.co.uk>] 14 September 2009

The New York Times was co-opted into pushing fake anti-virus malvertisements after hackers broke into its banner ad feed over the weekend.

Surfers visiting the site were confronted by malicious pop-up window that falsely warned that their systems were infected. The ruse was designed to scare people into buying a clean-up utility of little or no value.

The NYT issued a warning (extract below) on the front page of the website and via its Twitter feed on Sunday. The paper explained that the pop-ups were the result of an "unauthorised advertisement".

[\[More\]](#)

Linux webserver botnet pushes malware

[Source: www.theregister.co.uk] 12 September 2009

A security researcher has discovered a cluster of infected Linux servers that have been corralled into a special ops botnet of sorts and used to distribute malware to unwitting people browsing the web.

Each of the infected machines examined so far is a dedicated or virtual dedicated server running a legitimate website, Denis Sinegubko, an independent researcher based in Magnitogorsk, Russia, told The Register. But in addition to running an Apache webserver to dish up benign content, they've also been hacked to run a second webserver known as nginx, which serves malware.

[\[More\]](#)

Cutwail botnet spamming 'IRS unreported income' themed malware

[Source: blogs.zdnet.com] 10 September 2009

Researchers from MX Logic — now part of McAfee — have intercepted a new malware campaign spammed by the Pushdo/Cutwail botnet, that's using an 'IRS unreported income' notices in an attempt to trick the recipients into downloading a tax-statement.exe executable.

The Pushdo/Cutwail botnet remains among the most aggressively spamming cybercrime platforms, with the latest campaign traffic averaging about 90,000 emails per hour according to the company.

The latest campaign is dynamically including the recipient's email within the page, as well as the user name within the executable link in an attempt to establish authenticity, using the following URL structure - `irs.gov.hyu11hep.eu/fraud_application/directory/statement.php`. Upon execution, the executable (Trojan-Spy.Win32.Zbot.gen) downloads more malicious content from known crimeware command and control servers.

[\[More\]](#)

Serious security bug found in Windows Vista

[Source: securityfocus.com] 09 September 2009

An independent security consultant publicized this week the details to a critical flaw in the server message block version 2 (SMB2) component of Microsoft's Windows Vista, Windows Server 2008, and the release candidate for Windows 7.

The researcher, Laurent Gaffié, claimed in his advisory that the vulnerability causes a Blue Screen of Death, a pernicious crash on Windows system, but other researchers have subsequently concluded that the flaw is actually remotely exploitable, a more serious issue.

Microsoft acknowledged the flaw on Tuesday in an advisory. The flaw does not affect the latest version of Windows 7, Windows Server 2008 R2, nor Windows XP, the company stated. Microsoft took the researcher to task for disclosing the information before it fixed the security issue.

Yet, Gaffié argued that the disclosure was fair. The software company should have done more software quality assurance (SQA) on the networking components, he said in an e-mail interview with SecurityFocus. If they did, they would have easily found the issue -- it took his fuzzer only 15 packets to crash the component, he said.

[\[More\]](#)

New scam adds live chat to phishing attack

[Source: news.cnet.com] 16 September 2009

Online scammers have created a phishing site masquerading as a U.S.-based bank that launches a live chat window where victims are tricked into revealing more information, researchers at the RSA FraudAction Research Team said .

After a user accesses the phishing site, the chat window messages come through the browser and not via a typical instant messenger application, RSA said in a [blog post](#).

The chat window is displayed if the log-in credentials are typed in or if any other link on the page is clicked, said Sean Brady, an online fraud expert at RSA.

The scammer claims to be from the bank's fraud department and says that the bank is requiring members to validate their accounts, asking for additional information such as name, phone number, and e-mail address, according to screenshots. That information could be used to get access to accounts and money online or over the phone.

The scammers are using the open-source Jabber IM protocol to manage the one-on-one chat, RSA said, declining to identify the bank involved in the scam.

[\[More\]](#)

Web 2.0 security risks scrutinized

[Source : news.cnet.com] 16 September 2009

Web 2.0 sites that enable people to create content are increasingly used to carry out a wide range of attacks, according to a new security study.

Websense's "State of Internet Security" document notes that attackers are focusing their attention on interactive Web 2.0 elements. Some 95 percent of user-generated comments on blogs, message boards, and chat rooms are either spam or contain malicious links, the security vendor warned.

"The very aspects of Web 2.0 sites that have made them so revolutionary--the dynamic nature of content on the sites, the ability for anyone to easily create and post content, and the trust that users have for others in their online networks--are the same characteristics that radically raise the potential for abuse," Websense said in its report.

Web 2.0 sites, the company added, comprise "many" of the most visited sites on the Internet. The top 100 most visited Web properties, tended to be classified as social-networking or search sites. Nearly half, or over 47 percent, of the top 100 Web sites support user-generated content.

[\[More\]](#)