

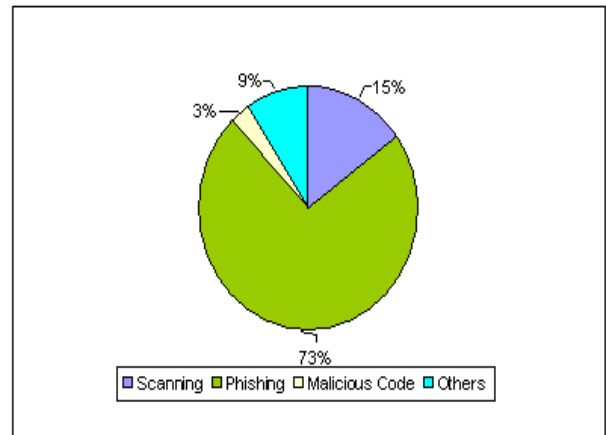
## CERT-In Monthly Security Bulletin September 2007

### Cyber Intrusion Trends

In this month 33 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 73% phishing incidents were reported in the month. 15% unauthorized scanning, 3% incidents related to virus/worm under the malicious code category and 9% incidents from others category were reported in this month. As compared to previous month the number of phishing incidents have increased.

In this month CERT-In tracked 4 C&C (Command & Control) servers and 1976 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 2007



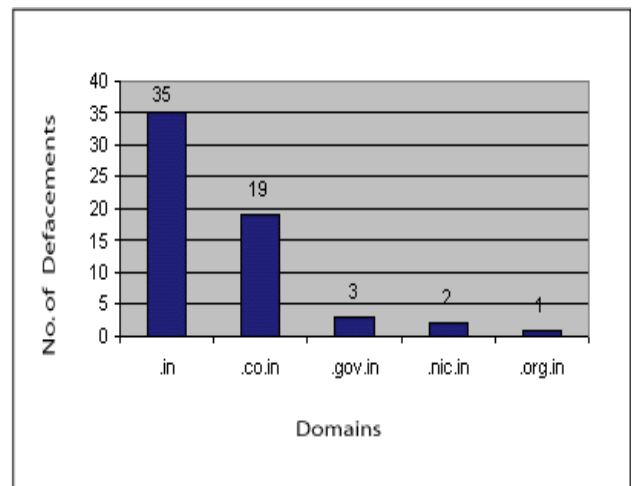
### Indian Websites Defacement

In total 60 Indian websites were defaced during September 2007. 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 Undefined Charset UTF-7 Cross-Site Scripting (XSS) Vulnerability [CIVN-2007-124](#)
2. Multiple Vulnerabilities in PHP [CIAD-2007-48](#)

### Statistics of Defaced Indian Websites in September 2007

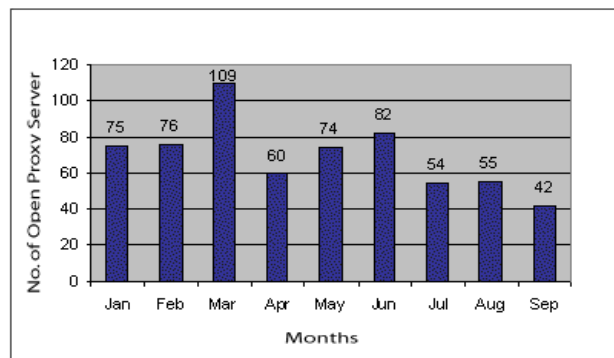


## Open proxy servers

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 42 open proxy servers functioning in India during September 2007. 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 – Sept. 2007**



## Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during September 2007 and their countermeasures alongwith 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 Agent ActiveX	Remote Code Execution Vulnerability in Microsoft Agent ActiveX (agentdpv.dll) control	September 12,2007	CIVN-2007-117
Microsoft	Multiple Vulnerabilities in various components of Microsoft Windows, Visual Studio , Windows Services for UNIX, Subsystem for UNIX-based Applications , MSN Messenger, Windows Live Messenger	September 12,2007	CIAD-2007-49
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
MIT Kerberos	MIT Kerberos Multiple Vulnerabilities	September 06,2007	CIAD-2007-47
PHP	Multiple Vulnerabilities in PHP	September 11,2007	CIAD-2007-48
OpenOffice	OpenOffice TIFF file Buffer Overflow Vulnerability	September 19,2007	CIVN-2007-122
Linux Kernel	Information disclosure vulnerability in Linux Kernel	September 27,2007	CIVN-2007-127
Cisco	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Cisco	XSS and SQL Injection in Cisco CallManager/Unified Communications Manager Logon Page	September 07 , 2007	CIVN-2007-114
Cisco	Denial of Service Vulnerabilities in Content Switching Module	September 07 , 2007	CIVN-2007-115
Cisco	Cisco Video Surveillance IP Gateway and Services Platform Authentication Vulnerabilities	September 07 , 2007	CIVN-2007-116
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
MSN Messenger and Windows Live Messenger	Remote Code Execution Vulnerability in MSN Messenger and Windows Live Messenger	September 12,2007	CIVN-2007-120

OpenSSH	OpenSSH Trusted X11 Forwarding Vulnerability	September 12,2007	CIVN-2007-121
Mozilla Firefox	Mozilla Firefox 2.0.0.6 Unspecified Protocol Handling Command Injection Vulnerability	September 12,2007	CVE-2007-4841
Mozilla	disclosure of information vulnerability in Mozilla	September 13,2007	CVE-2007-4879
Apple QuickTime	Apple QuickTime Remote Code Execution Vulnerability	September 22,2007	CIVN-2007-125
google	Cross-Site Scripting (XSS) Vulnerabilities in google	September 27,2007	CIAD-2007-50

#### Medium Vulnerabilities

Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Microsoft Visual Studio	Remote Code Execution Vulnerability in Crystal Reports for Microsoft Visual Studio	September 12,2007	CIVN-2007-118
Microsoft Windows	Microsoft Windows Services for UNIX Privilege Escalation Vulnerability	September 12,2007	CIVN-2007-119
Microsoft Windows	Microsoft Windows CFileFind Class "FindFile()" Buffer Overflow vulnerability	September 19,2007	CIVN-2007-123
Microsoft ISA Server	Information Disclosure Vulnerability in Microsoft ISA Server SOCKS4 Proxy Connection	September 26,2007	CIVN-2007-126
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
PHP	Multiple Iconv functions denial of service vulnerability in PHP	September 12,2007	CVE-2007-4840
Apache	Apache Undefined Charset UTF-7 Cross-Site Scripting (XSS) Vulnerability	September 20,2007	CIVN-2007-124

#### Malicious Code Threats

Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Pykse Worm Variant	Worm	This worm is spreading via Skype Instant Messenger or removable drives.It collects e-mail addresses from the compromised computer and send messages to download a copy of itself by using various social engineering techniques.	WORM_SKIPI.A [Trend], W32/Pykse.worm.b [McAfee], WORM_SKIPI.B [Trend], W32.Pykspa.D [Symantec]	September 14,2007	<a href="http://www.cert-in.org.in/virus/Pykse_Worm.htm">http://www.cert-in.org.in/virus/Pykse_Worm.htm</a>
Virut	Virus	It is a polymorphic file infector virus which infects the file with .exe and .scr extensions. This virus creates an IRC backdoor on the infected system to connect itself to the IRC server and listen commands from the remote attacker.	Virus.Win32.Virut.n [Kaspersky], W32/Virut.gen [McAfee], W32.Virut.U [Symantec], W32/Virut.U [Avira]	September 14,2007	<a href="http://www.cert-in.org.in/virus/Virut_Virus.htm">http://www.cert-in.org.in/virus/Virut_Virus.htm</a>
W32.Yalove	Worm	This worm spreads through Yahoo! Instant Messenger and by copying itself to all drives.It redirects the Internet browser to the malicious Urls which hosts copy of the worm.	No Alias	September 20,2007	<a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-092102-4040-99&amp;tabid=1">http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-092102-4040-99&amp;tabid=1</a>

W32.Imaut.BA	Worm	This worm spreads itself by sending a malicious link embedded in different messengers like Yahoo! Instant Messenger, AOL.	No Alias	September 20,2007	<a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-092105-2813-99&amp;tabid=1">http://www.symantec.com/business/security_response/writeup.jsp?docid=2007-092105-2813-99&amp;tabid=1</a>
Googbot	Worm	The worm exploits Trend Micro ServerProtect multiple stack-based buffer overflow vulnerability and Windows LSA (Local Security Authority) Service Stack-Based Buffer Overflow vulnerability.	WORM_AGEN T.AAWD [Trend], W32 Duce.a@mm [McAfee], Backdoor.W3 2.GoogBot.A [Kaspersky]	September 24,2007	<a href="http://www.cert-in.org.in/virus/Googbot.htm">http://www.cert-in.org.in/virus/Googbot.htm</a>

## Security News

### Botnet Steals eBay Accounts

[Source: [www.pcworld.com](http://www.pcworld.com)]

September 04, 2007

Online auction site eBay has been targeted by identity thieves, who are wielding a botnet that uses brute force to uncover valid account log-in information, a Tel Aviv-based security company said. The attacks against eBay Inc. may have started as long ago as early August, said Ofer Elzam. He said that he and other researchers at Aladdin Knowledge Systems Ltd. have not been successful in notifying eBay of their weekend findings. According to Elzam, the product manager of Aladdin's eSafe threat-protection line, the brute-force attacks are launched by a large botnet that the identity thieves have built using a sophisticated, multistage campaign that begins with compromised legitimate Web sites. "My best estimate is that there are at least 300 compromised sites," said Elzam, who noted that they are spread worldwide and in several languages. Two sites are based in Israel, he said, including a price-comparison Web site and another operated by one of the country's largest unions. Other sites identified in a search run with information provided by Elzam included scores of real estate Web sites in Florida and Massachusetts, and a Microsoft security message forum in Italian.

[More]

### Skype Warns Users of P-to-P Worm

[Source: [www.pcworld.com](http://www.pcworld.com)]

September 10, 2007

Skype users are under attack from a new worm that spreads through the peer-to-peer Internet phone application's chat feature. The attack begins when a user receives an instant message containing a link from someone in their contact list or an unknown Skype user, said Villu Arak, a Skype spokesman based in Tallinn, Estonia. There are several versions of the chat messages, which are "cleverly written" to fool users, Arak wrote on the Skype heartbeat blog. The link appears to contain a JPEG photo file, but if clicked causes the Windows run/save dialog box to appear, which asks whether the user wants to save or run a ".scr" file. The file is malicious software that can then access a user's PC via Skype's API (application programming interface). The malicious file has been named W32/Ramex.A. "Users whose computers are infected with this virus will send a chat message to other Skype users asking them to click on a web link that can infect" their computers, Arak wrote.

[More]

### Microsoft downplays stealth update concerns

[Source: [www.computerworld.com](http://www.computerworld.com)]

September 13, 2007

today essentially called the concerns over undercover updates to Windows XP and Windows Vista a tempest in a teapot, saying that silent modifications to the Windows Update (WU) software have been a longtime practice and are needed to keep users patched. "Windows Update is a service that primarily delivers updates to Windows," said Nate Clinton, program manager in the WU group on the team's blog today. "To ensure ongoing service reliability and operation, we must also update and enhance the Windows Update service itself, including its client-side software." Microsoft was moved to respond after the popular "Windows Secrets" newsletter looked into complaints that WU had modified numerous files in both XP and Vista, even though users had set the operating system to not install updates without their permission. In many cases,

users who dug into Windows' event logs found that the updates had been done in the middle of the night.

[More]

### **New cracks in Google mail**

[Source: [www.theregister.com](http://www.theregister.com)]

September 28, 2007

*This story was updated on 28th September to report that the vulnerability has been patched.*

Yesterday, we reported on an unholy trinity of Google vulnerabilities that put emails, private photos and website security at risk. Today came word of a new weakness that makes it easy for bad guys to silently put a backdoor in Gmail accounts. The technique comes courtesy of Petko D. Petkov, a researcher at GNU Citizen, who writes in a blog post that the backdoor is installed simply by luring a victim to a specially crafted website while logged in to Gmail. The naughty site uses a sleight of hand known as a multipart/form-data POST, which writes a filter to Gmail that causes all email with attachments to be forwarded to collect@evil.com.

Petkov didn't provide a proof of concept or detailed documentation, but Ryan Naraine of the Zero Day blog writes here that the exploit was demonstrated for him. The bug "is particularly nasty because of the way the exploit works without any user action and the fact that it's difficult for the average Gmail user to know that emails are being stolen," he writes.

[More]

### **Unholy trinity of flaws put Google users at risk**

[Source: [www.theregister.com](http://www.theregister.com)]

September 24, 2007

If you use Google to send email, organize photos or help administer your website, doomwatchers have cataloged three new ways to steal your data and compromise the security of your users. All three of the techniques rely on cross site scripting, or XSS, in which hackers inject unauthorized code by making it appear as if it's hosted by a trusted website. The most serious vulnerability resided in the so-called polls application, a part of Google Groups . It made it possible to steal contacts and messages from Gmail accounts. A Google spokesman on Monday afternoon said the flaw had been fixed. Multiple pieces of proof-of-concept code posted online graphically demonstrated the potential for attacks that target the weakness. One stole all contacts listed in a Gmail account, while a second sent all incoming Gmail messages to an email account of the researcher's choosing. "If you're good at JavaScript, writing a good exploit for those vulns is [a] trivial matter" Giorgio Maone, a researcher told *El Reg* . He added that the weaknesses could be exploited "serially," meaning that a single piece of attack code will compromise virtually any Gmail account.

[More]

### **China leads Asia in malicious online activity**

[Source: [www.news.com](http://www.news.com)]

September 20, 2007

China leads Asia in malicious online activity, racking up 42 percent of the action in the first half of 2007, up from 39 percent last year.

According to Symantec's biannual Internet security threat report released on Wednesday, China topped the Asia-Pacific region, including Japan, in malicious activity, producing the most malicious code, spam zombies, bots and attacks between January 1 and June 30. China's bot-infected computers made up 78 percent of those in the region. Taiwan had the next highest number of bots, but only at 7 percent. China's high level of malicious activity can be attributed to its high rate of counterfeit software. Noting that the majority of China's Windows users use counterfeit versions, Ooi Szu Khiam, a senior security consultant at Symantec Singapore, said during a press briefing: "If you don't have a genuine version, you can't register for patches, and those who don't patch their systems are open to a growing number of exploits."

[More]

### **Hacked GOP site infects visitors with notorious bot-making malware**

[Source: [www.computerworld.com](http://www.computerworld.com)]

September 14, 2007

A Republican Party Web site has been hacked, and for some time it has been spreading a variation of the long-running Storm Trojan horse to vulnerable visitors, a security researcher said today. This is the first time that Storm has taken to the Web for its victims, said Dan Hubbard, head of research at San Diego-based Websense Inc. "The big news is that Storm has added infecting sites to its arsenal," said Hubbard. Storm debuted in January but only cracked the top malware lists early this summer, and has become infamous for its ability to adapt its infection strategies. "They have a knack for latching onto the latest newsworthy events and capitalizing on the public interest in them," Symantec Corp. researcher Hon Lau said last month. "And if no newsworthy events are happening at the time, then they will just make them up."

[More]

### **New twist on Nigerian email scam**

[Source: [www.abclocal.go.com](http://www.abclocal.go.com)]

August 22, 2007

By now you know to take a very skeptical view of emails from people you don't know that are asking for money. But what if the email came from a friend? A Harris County man's email nightmare started last week when his computer was hacked. Now everyone in his address book is getting an email asking for money. Kamel Fotouh wants everyone to know he is not stuck in Nigeria. "I have not traveled for the past year," he said. "I have never been in Nigeria and I am safe."

The reason Fotouh wants to share this obvious fact can be traced back to his computer. Last week someone gained control of Fotouh's home computer, changed the password then started sending e-mails to everyone Fotouh knows with an urgent plea for money. "The guy is speaking on my behalf, from my email address, to make people believe I am the one who originated the message," Fotouh said.

[More]

### **Trojan planted on US Consulate website**

[Source: [www.theregister.co.uk](http://www.theregister.co.uk)]

September 20, 2007

Webpages of the US Consulate General in St. Petersburg, Russia, were infected by malware earlier this week. The US consulate site was caught up in a much larger hack attack and is not thought to have been targeted as such. The infected pages have since been cleaned up, reports net security firm Sophos which monitored results of the assault. The attack on the US consulate was part of a larger campaign by cybercriminals targeting vulnerable web servers. The majority of the 400 compromised web pages hit by the attack were hosted in Russia. Hackers planted malicious scripts on compromised hosts.

[More]

### **Viruses: One in 28 e-mails**

[Source: [www.crime-research.org](http://www.crime-research.org)]

September 12, 2007

With the Internet becoming the order of life for more and more Indians, who depend on e-mails to stay in touch, their computers are facing an increasing virus threat with one in every 28 e-mails being infected, says a recent study. A study by the messaging security and management services provider, MessageLabs, reveals that malicious websites are on the rise. A new virus, StormWorm, which uses virtual postcards and YouTube video for its attack, is affecting computers. According to the study, 1.8 million computers have been affected by StormWorm worldwide.

[More]

### **Canadian police detain Nigerian in alleged 419 scam**

[Source: [www.theregister.co.uk](http://www.theregister.co.uk)]

September 13, 2007

A Nigerian national who had been living in Canada was taken into custody by Winnipeg police in connection with a West African email scam alleged to have bilked an 84-year old man of \$30,000. Toluwalade Alonge Owolabi, 36, of Toronto, was charged with fraud in excess of \$5,000, fraud of less than \$5,000 and five other offenses, according to an article in the *Edmonton Sun*. The suspect was nabbed at the victim's Winnipeg home, after traveling there to pick up another payment, police said. By then, the victim had grown wise to the scam and alerted the cops. The con began when the victim replied to an email that promised a share of a \$1.5m inheritance that - surprise, surprise - turned out not to exist. He was instructed to wire an upfront fee of \$37,500, but sent only \$30,000 to a bank account in Ghana. The victim was then pressured to send more.

[More]

### **Symantec: Bank account details fetch \$400 online**

[Source:www.computerworld.com]

September 17, 2007

Stolen bank account numbers are commanding the highest price in an underground trade of personal details stolen by hackers, according to a survey released Monday by security vendor Symantec Corp. Bank account details command prices of up to \$400, while credit card details sell for between 50 cents and \$5, e-mail passwords from \$1 to \$350 each, and e-mail addresses from \$2 to \$4 per megabyte, according to Symantec's "Internet Security Threat Report," which covers the first half of the year.

The online trade in stolen data highlights the commercialization of Internet crime, with gangs researching, developing and marketing nefarious software for other criminals, said William Beer, director of Symantec's security practice for Europe.

[More]

### **AIM vulnerable to worm attack, researchers warn**

[Source:www.computerworld.com]

September 26, 2007

A critical flaw in the way that the AOL LLC 's instant messaging client displays Web-based graphics could be exploited by criminals to create a self-copying worm attack, security researchers are warning. The flaw was **discovered** by researchers at Core Security Technologies Inc., which has been working with AOL over the past few weeks to patch the problem. AOL's servers are now filtering instant messaging traffic to intercept any attacks, but the company has yet to patch the underlying problem in its client software, security researchers said Tuesday. The flaw has to do with the way the AOL Instant Messaging (AIM) software uses Internet Explorer 's software to render HTML (Hypertext Markup Language) messages. By sending a maliciously encoded HTML message to an AIM user, an attacker could run unauthorized software on a victim's computer or force the IE browser to visit a maliciously encoded Web page, said Core Chief Technology Officer Ivàn Arce.

[More]

### **Infrastructure threats: Botnets show DoS who's boss**

[Source:www.infoworld.com]

September 18, 2007

Malware-infected botnet PCs have overtaken DoS attacks as the top security issue facing Internet service providers and other Web infrastructure hosting players, according to a new survey of the organizations. Arbor Networks published the results of its third-annual Infrastructure Security Report on Monday -- a survey of 75 large ISPs, hosting companies, and other providers -- which found for the first time that botnets currently outrank DoS threats as the most serious concern for the firms. Tens of millions of PCs are likely infected with botnet programs worldwide, according to survey results, and Arbor researchers said the ISPs they questioned admitted to spending more time and resources battling botnets than ever before.

Infrastructure providers are finding botnets hard to pin down, as the people responsible for controlling the zombie machines are increasingly employing more advanced detection evasion techniques, said Craig Labovitz, chief scientist at

Arbor. As they can't accurately gauge the size of the problem, he said, infrastructure providers are afraid they're only scraping the tip of the iceberg in taking on the botnet phenomenon.

[\[More\]](#)

### **Cybercrime is a US\$105 billion business now**

[Source:[www.crime-research.org](http://www.crime-research.org)]

September 26, 2007

"Citing recent highly publicized corporate data breaches that have beset major companies like Ameritrade, Citigroup, and Bank of America, McAfee CEO David DeWalt, said that cyber-crime has become a US\$105 billion business that now surpasses the value of the illegal drug trade worldwide.

Despite the increase in government compliance requirements and the proliferation of security tools, companies continue to underestimate the threat from phishing, data loss, and other cyber vulnerabilities, DeWalt said. 'Worldwide data losses now represent US\$40 billion in losses to affected companies and individuals each year, DeWalt says.

But law enforcement's ability to find, prosecute, and punish criminals in cyberspace has not kept up: "If you rob a 7-11 you'll get a much harsher punishment than if you stole millions online," DeWal remarked. "The cross-border sophistication in tracking and arresting cyber-criminals is just not there."

[\[More\]](#)

### **Investigators: Homeland Security Computers Hacked**

[Source:[www.edition.cnn.com](http://www.edition.cnn.com)]

September 26, 2007

Hackers compromised dozens of Department of Homeland Security computers, moving sensitive information to Chinese-language Web sites, congressional investigators said Monday. Investigators pointed a finger at a government contractor, saying the firm hired to protect DHS computers tried to hide the incidents from the department. The FBI is investigating the incidents, a congressional staffer said, and two members of Congress have asked the department's inspector general to also launch an investigation."The results of our [committee] investigation suggest that the department is the victim not only of cyber attacks initiated by foreign entities, but of incompetent and possibly illegal activity by the contractor charged with maintaining security on its networks," Democratic Reps. Bennie Thompson of Mississippi and James Langevin of Rhode Island said in a written statement.