



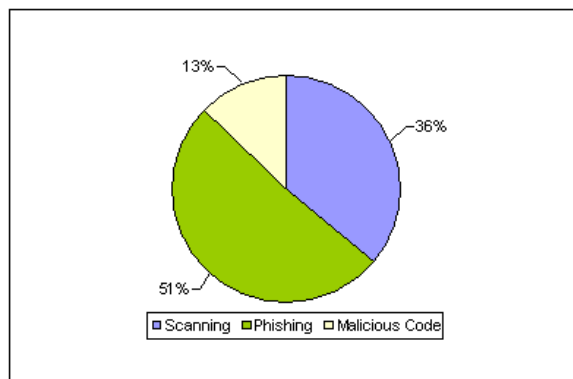
CERT-In Monthly Security Bulletin November 2007

Cyber Intrusion Trends

In this month 47 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 51% phishing incidents were reported in this month. 36% unauthorized scanning and 13% incidents related to virus/worm under the malicious code category were reported in this month. As compared to previous month the number of phishing incidents have decreased while scanning and malicious code incidents have increased.

In this month CERT-In tracked 2 C&C (Command & Control) servers and 1020 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. It has been observed that information stealing trojans such as **Nethell** are spreading widely which are capturing login credentials of online users through keyloggers.

Cyber Intrusion during November 2007



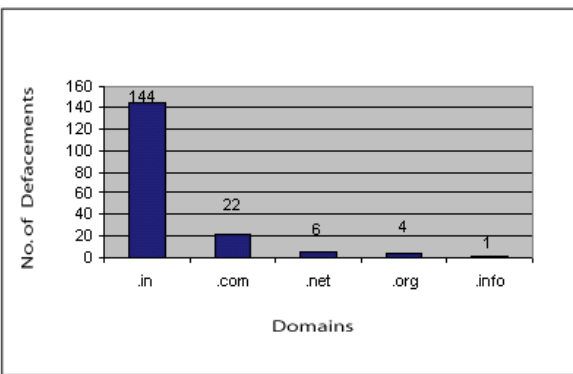
Indian Websites Defacement

In total 177 Indian websites were defaced during November 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. Multiple Vulnerabilities in PHP [CVE-2007-5898](#), [CVE-2007-5899](#), [CVE-2007-5900](#)
2. Denial of service vulnerability in PHP [CVE-2007-6039](#)

Statistics of Defaced Indian Websites in November 2007

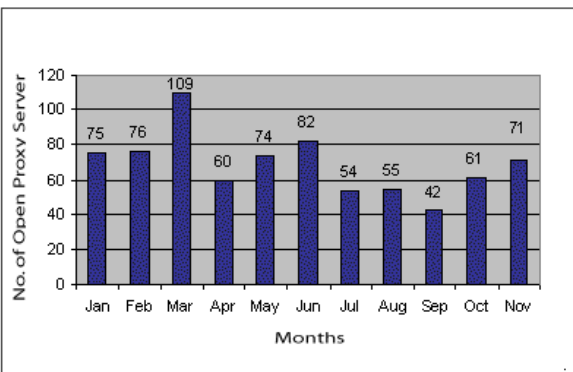


Open proxy servers

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 71 open proxy servers functioning in India during November 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 - Nov 2007



Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during November 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	Multiple Vulnerabilities in various components of Microsoft Windows: Microsoft DNS Server, Microsoft Windows URI	November 14, 2007	CIAD-2007-59

Unix	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
PHP	Multiple Vulnerabilities in PHP		November 12, 2007	CVE-2007-5898 , CVE-2007-5899 , CVE-2007-5900	
Linux Kernel	Linux Kernel CIFS VFS Buffer Overflow Vulnerability		November 16, 2007	CIVN-2007-144	
Cisco	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Cisco	Cisco Unified MeetingPlace XSS Vulnerability		November 15, 2007	CIVN-2007-143	
Cisco	Cisco VPN Client for Windows Multiple Local Privilege Escalation Vulnerabilities		November 21, 2007	CIAD-2007-61	
Cisco	Cisco Unified IP Phone Remote Eavesdropping		November 30, 2007	CIAD-2007-64	
Miscellaneous	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Apple QuickTime	Multiple File Processing Code Execution Vulnerabilities in Apple QuickTime		November 07, 2007	CIVN-2007-140	
Mozilla Firefox	jar: Protocol URI Handling Vulnerability in Mozilla Firefox		November 13, 2007	CIVN-2007-141	
IBM AIX	Multiple Vulnerabilities in IBM AIX		November 19, 2007	CIAD-2007-60	
Apple QuickTime	Apple QuickTime RTSP "Content-Type" Header Buffer Overflow Vulnerability		November 28, 2007	CIVN-2007-146	
Medium Vulnerabilities					
Microsoft	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Microsoft DNS Server	Remote Code Execution Vulnerability in Microsoft DNS Server		November 14, 2007	CIVN-2007-142	
Unix	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
PHP	Denial of service vulnerability in PHP		November 20, 2007	CVE-2007-6039	
Samba	Multiple Vulnerabilities in Samba		November 29, 2007	CIAD-2007-63	
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
RJump Worm	Worm	The worm propagates by dropping its copy into removable drives and network drives with random names. It establishes a SOCKS Proxy on infected system for facilitating malicious activities such as Spam.	Worm:Win32/RJump [Microsoft], Worm.Win32.RJump [Kaspersky], W32.Rajump [Symantec]	November 01, 2007	http://www.cert-in.org.in/virus/RJump.htm
Mac OS Trojan OSX/RSPUG	Trojan	It has been observed that a trojan named OSX/Plug affecting Mac OS is circulating in the wild. It arrives on the victim users system by exploiting browser vulnerabilities or by any other social engineering technique.	OSX/RSPUG-A [Sophos], OSX/Puper [McAfee], OSX.RSPUG.A [Symantec]	November 05, 2007	http://www.cert-in.org.in/virus/Mac_OS_Trojan.htm
		ZLOB Trojans first appeared in late 2005. Initial variants use to download malware and update copies of malware, ensured running of the other variants			

ZLOB Trojan		of the malware by re-executing their process. In the year 2006 ZLOB variants started spreading through email spam containing links to the video file. Some ZLOB variants also get dropped by other malware.		November 06, 2007	http://www.cert-in.org.in/virus/ZLOB_Trojan.htm
Jeefo Virus	Virus	It has been observed that a parasitic file infector virus named Jeefo is circulating in the wild. It infects Portable Executable files with size equal to or greater than 102,400 Bytes using the technique of first encrypting its target host file and then appending the encrypted host code to its viral code. After successful infection the size of the infected file gets increased by 36,352 bytes.	Virus.Win32.Hidrag.a [Kaspersky]	November 20, 2007	http://www.cert-in.org.in/virus/Jeefo_Virus.htm
Rontokbro Worm	Worm	The trojan propagates by attaching a copy of itself to the email messages with the subject line and message body which lures users into opening up the attachment to get malware installed on their system. It also spread by copying itself to network shares .	W32.Rontokbro@mm [Symantec], W32/Brontok-N [Sophos], Win32.Brntok.a [Kaspersky]	November 20, 2007	http://www.cert-in.org.in/virus/Rontokbro_Worm.htm
Conhook Trojan	Trojan	The Trojan propagates by being dropped by other malware or by pretending to be harmless file which gets downloaded by innocent users while navigating some malicious websites.	Trojan-Downloader.Win32.ConHook.b [Kaspersky Lab], Downloader-ZM [McAfee], Trojan Horse [Symantec]	November 30, 2007	http://www.cert-in.org.in/virus/Conhook-Trojan.htm

Security News

FBI crackdown on botnets gets results, but damage continues
 [Source:www.theregister.co.uk]

November 29, 2007

FBI agents engaged in a crackdown on botnet crime issued a progress report of the ongoing initiative, reporting more than \$20m in losses to consumers, businesses and other organizations and the identification of one million infected machines in the past five months. In addition, eight individuals have been indicted, have pleaded guilty or been sentenced for crimes related to botnets since "Operation Bot Roast," as the ongoing investigation is known, was announced in June. Thirteen search warrants connected to the operation have been served in the US and overseas, and at least seven FBI field offices have participated. Combined with the FBI's previous tally, federal investigators have now identified more than two million zombie computers, so called because they mindlessly follow the orders of their devious masters.

[\[More\]](#)

Targeted e-mail attacks spoof DOJ, business group

[\[Source: www.news.com\]](#)

November 20, 2007

Security experts warned this week of two separate e-mail attacks launched Monday that take aim at specific individuals within corporations. The first attack, detected by MessageLabs at 4:55 p.m. GMT Monday, was sent to more than 400 individuals at financial institutions, with the e-mail addressed specifically to that individual and purporting to be a complaint from the U.S. Department of Justice. A second attack, spotted three and a half hours later, was similar, but claimed to be from the Better Business Bureau. In both cases, the e-mails contained malicious attachments that could lead to the recipient's system being taken over. The Trojan horse that gets installed on a computer allows an attacker to have remote access to the machine, but MessageLabs security analyst Paul Wood said the attacker's exact purpose was not clear. "Once they get access to the machine remotely, they can use that machine for anything," Wood said.

[\[More\]](#)

Feds Put More Botmasters, Phishers Behind Bars

[\[Source: www.blog.washingtonpost.com\]](#)

November 29, 2007

The FBI today released details of several cybercrime cases against individuals accused of defrauding banks, companies and consumers of more than \$20 million with the help of "botnets," large groupings of hijacked personal computers. The computer crime crackdown is Part Two of "Operation Bot Roast," a series of investigations the FBI first detailed this summer. To date, the operation has identified more than two million individual PCs compromised by at least 10 individuals who have since pleaded guilty, been indicted or sentenced for various bot-related computer crimes.

[\[More\]](#)

Government-sponsored cyberattacks on the rise, McAfee says

[\[Source: www.computerworld.com\]](#)

November 30, 2007

Governments and allied groups worldwide are using the Internet to spy and launch cyberattacks on their enemies, targeting critical systems including electricity, air traffic control, financial markets and government computer networks, according to McAfee's annual report examining global cybersecurity.

This year, China has been accused of launching attacks against the United States, India, Germany and Australia, but the Chinese are not alone: 120 countries including the United States are said to be launching Web espionage operations, according to McAfee's Virtual Criminology Report (PDF format), issued today and developed with input from NATO, the FBI, the United Kingdom's Serious Organized Crime Agency, and various groups and universities.

"Cyber assaults have become more sophisticated in their nature, designed to specifically slip under the radar of government cyber defenses," McAfee states.

"Attacks have progressed from initial curiosity probes to well-funded and well-organized operations for political, military, economic and technical espionage."

[\[More\]](#)

Trojan spreads using PI wiretapping scare

[\[Source: www.theregister.co.uk\]](#)

November 20, 2007

Miscreants are trying to convince email users that their telephone conversations are being recorded in a ruse designed to scare prospective marks into buying bogus security software. Emails promoting the campaign are laced with a new Trojan horse malware. The Dorf-AH Trojan horse appears as an attachment in emails claiming that the sender is a private detective listening into a recipient's phone calls. This "detective" claims he's prepared to switch sides and reveal who has paid for the surveillance at a later date.

In the meantime, prospective marks are asked to listen to the supposed recording of one of their recent phone calls that comes attached to the email in the form of a password-protected RAR-archived MP3 file. In reality, however, the MP3 file is not an audio file of a telephone conversation or anything else but a malicious executable program that installs malware onto victim's computer.

[\[More\]](#)

Botmaster owns up to 250,000 zombie PCs

[\[Source: www.theregister.com\]](#)

November 09, 2007

An American computer security consultant on Friday admitted using massive botnets to illegally install software on at least 250,000 machines and steal online banking identities of Windows users by eavesdropping on them while they made financial transactions. John Kenneth Schiefer, 26, of Los Angeles, pleaded guilty to four felonies, including accessing protected computers to conduct fraud, disclosing illegally intercepted electronic communications, wire fraud and bank fraud. He faces a maximum sentence of 60 years in federal prison and a fine of \$1.75m, according to documents filed Friday in federal court.

Schiefer, who went by names such as "Acid" and "Acidstorm," has long been a fixture in underground hacking circles. He sometimes adorned his instant message handles with phrases such as "remember the name or feel the pain" and "crime pays, and it also has an excellent benefits package." He was employed at a Los Angeles-based security firm known as 3G Communications, where he sometimes carried out his crimes, according to court documents.

[\[More\]](#)

Website for computer security experts hacked

[\[Source: www.theregister.co.uk\]](#)

November 08, 2007

First Forensic Forum - a UK based association of computer security professionals - has been hacked. F3.org's website was defaced (screen shot here) with a message poking fun at the association of computer forensic experts. The timing of the defacement on Thursday was fortuitous (or well planned) since the organisation is coming to the end of a two day conference. The perpetrator of the attack posted a message taunting the organisation. "The F3 For Security Hacked."

What's Happened In The world. They Are No Security Or What," S4udi-S3curity-T3rror writes. Ouch. Well at least First Forensic Forum has no shortage of experts in recovering from security attacks to call on for help. Curiously other pages (example) behind the front page defacement are operating normally. Defacements are the high-tech equivalent of digital graffiti. Normally they arise from misconfiguration of web server software or vulnerabilities left open by third party hosting firms or webmasters. Such attacks are generally trivial even though, when inflicted on security related organisations, no less embarrassing for all that.

[More]

Deconstructing the Fake FTC E-mail Virus Attack

[Source: www.blog.washingtonpost.com]

November 05, 2007

A targeted e-mail virus disguised as an identity theft inquiry from the Federal Trade Commission appears to have successfully compromised more than 500 PCs, including victims at banks, real estate brokerages, law firms and marketing companies.

Each of the victims received the invitation to open the virus-infected attachment via an e-mail that addressed the recipient by name, and in some cases included the name of the recipient's employer. Security Fix was able to gain access to one of several Internet addresses where data stolen from victims' PCs was uploaded by the virus. The link did not require a user name or password. There are several security outfits working to get the site taken down, but the longer it stays live there is the potential that the sensitive information could be obtained by more criminals.

[More]

Storm Worm Victims Get Stock Spam Pop-Up

[Source: www.blog.washingtonpost.com]

November 13, 2007

If you're a Windows users and today received a surprise pop-up advertisement urging you to invest in an obscure penny stock, it is highly likely that your computer is infected with the virulent Storm worm, a nasty intruder that currently resides on an estimated 200,000 PCs worldwide.

Criminal groups that control the pool of Storm-infected computers have traditionally used those systems to pump out junk e-mail ads touting thinly traded penny stocks as part of an elaborate and ongoing series of "pump-and-dump" schemes. But today, according to security researchers, the Storm worm authors went a step further by causing a pop-up ad for a particular penny stock to be shown on all infected machines.

[More]

Storm Brews Over Geocities

[Source: www.blog.trendmicro.com]

November 15, 2007

Storm is back, and according to TrendLabs researchers, the infamous malware family has added yet another twist to its tactics.

"(It) looks like Yahoo! will have its hands full in the next couple of days," Senior Threat Researcher Ivan Macalintal says. "There are limited reports that the Storm worm may be spamming emails with links to a Geocities site. This was seen in the monitoring of the spam templates being sent via Storm communications to its botnets."

An example of a Geocities URL found in the spam templates is: <http://geocities.com/{BLOCKED}Ramirez26>.

The links contained within the said messages point to various accounts created under the popular Yahoo!-managed Geocities site. However, what appears to be links to personal Web sites hosted on Geocities are actually URLs that redirect to <http://{BLOCKED}.geocities.com/{BLOCKED}.238.36/aes/>, where a user is coaxed into downloading an "iPix plug-in" (from <http://{BLOCKED}.geocities.com/{BLOCKED}.238.36/iPIX-install.exe>

[More]

U.K. government's lost data 'worth billions to criminals'

[Source: www.news.com]

November 29, 2007

Two lost HM Revenue & Customs CDs containing the personal and financial details of 25 million people could be worth \$3.12 billion to criminals, says a member of Britain's Parliament. Liberal Democrat acting leader Vince Cable, speaking in the House of Commons, said a single stolen identity is worth 60 pounds on the black market.

"We are therefore considering a stock of criminal value of around 1.5 billion pounds (\$3.12 billion), which makes the Brinks Mat robbery the equivalent of stealing the church collection. An enormous amount remains at stake," he said, referring to the 1983 robbery of the Brinks Mat warehouse at England's Heathrow Airport. But the chancellor of the exchequer, Alistair Darling, said: "The police inform me that they still have no evidence or intelligence that this data has fallen into the wrong hands and no evidence of fraud or criminal activity."

[More]

Google asks for help finding malicious Web sites

[Source: www.computerworld.com]

November 30, 2007

The company has created an online form designed to make it easy for people to report sites they suspect of hosting malicious code. It's the latest step by Google to expand its database of the bad Web sites it knows about, as those sites continue to proliferate.

"Currently, we know of hundreds of thousands of Web sites that attempt to infect people's computers with malware. Unfortunately, we also know that there are more malware sites out there," Google's Ian Fette wrote in the company's security blog.

The simple form has an entry box for the Web site's URL and a space to provide additional information. Users also fill out a "captcha" to prevent software robots from reporting sites automatically.

Google displays a warning in its search results if it believes a Web site is malicious. But earlier this week researchers noted that some Google searches for relatively mundane topics were producing results loaded with malicious sites, apparently the result of a campaign by hackers.

[More]

Hackers re-poison Google search results

[Source:www.theregister.co.uk]

November 30, 2007

Hackers have responded to a purge of malicious links within search results by Google with a fresh effort to subvert the search giant's page rank system. As previously reported, miscreants recently set out to poison search results with links to malware infested sites. The tactic involved gaming search engines' ranking systems by automatically posting links to malign sites in blog and forum posts. Hackers automated this link spamming process using networks of compromised zombie PCs.

Google cleaned up its search index earlier this week, but the original hackers (along with a new group) have responded with a fresh assault, reports anti-spyware firm Sunbelt Software.

Once again, plugging innocuous terms into Google, such as "funny drunk quote", can lead to search results where at least some point to malware. The tactic goes hand in hand with establishing thousands of pages on compromised servers that mention targeted terms to obtain a relatively high search engine ranking score.

[\[More\]](#)