



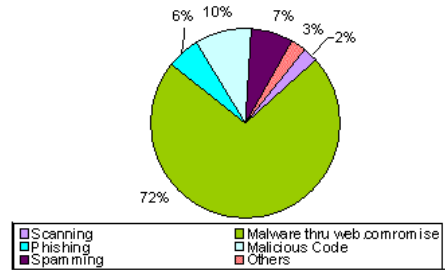
CERT-In Monthly Security Bulletin November 2008

Cyber Intrusion Trends

In this month 401 security incidents were reported to CERT -In from various National/ International agencies. As shown in the figure, 72% incidents related to Spreading of malware through website compromise were reported in this month. 10 % incidents related to virus/worm under the Malicious code category , 06 % phishing incidents , 07 % incidents related to spamming ,02 % unauthorized scanning , and 03 % incidents related to technical help under the Others category were also reported in this month.

In this month CERT -In tracked 02 C&C (Command & Control) servers and 6435 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 November 2008



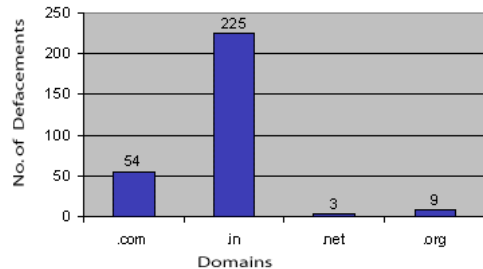
Indian Websites Defacement

In total 291 Indian websites were defaced during November 2008. A chart depicting Top Level Domain (TLD) wise defacements is shown in the figure.

The vulnerabilities which might have been exploited for the defacements are:

1. Microsoft Windows Server Service Vulnerability [CIVN-2008-170](#)
2. Microsoft Windows SMB Credential Reflection Vulnerability [CIVN-2008-177](#)
3. Multiple Vulnerabilities in Microsoft XML Core Services [CIVN-2008-178](#)
4. PHP Multiple Buffer Overflow Vulnerability [CVE-2008-3658](#)
5. Apache Tomcat ' RemoteFilterValve ' Security Bypass Vulnerability [CVE-2008-3271](#)
6. Apache Tomcat UTF-8 Directory Traversal Vulnerability [CVE-2008-2938](#)
7. Apache Tomcat ' RequestDispatcher ' Information Disclosure Vulnerability [CVE-2008-2370](#)
8. phpMyAdmin Shared Host Remote Information Disclosure [CVE-2008-1924](#)
9. PHP 5 ' php_sprintf_appendstring () ' Remote Integer Overflow Vulnerability [CVE-2008-1384](#)

Statistics of Defaced Indian Websites in November 2008

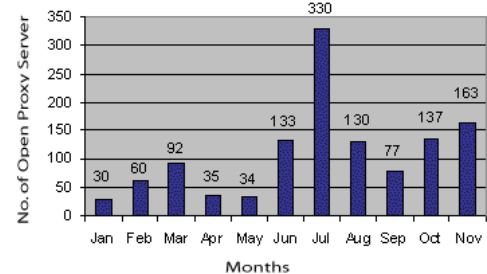


Open proxy servers

Any proxy server that doesn't restrict its client base to its own set of clients and allows any other client to connect to it is known as an open proxy server. An open proxy server will accept client connections from any IP address and make connections to any Internet resource.

CERT -In tracked 163 open proxy servers functioning in India during November 2008. All the concerned ISPs were alerted immediately to shut down the open proxy servers. A bar chart of open proxy servers tracked during this year is shown in the figure.

Statistics of Open Proxy Servers tracked during Jan - Nov 2008



Attack Trend

Domain Name Phishing Attacks

Domain Name Phishing, Domain Phishing or Registrar Impersonation is a form of Phishing attack targeting the domain name registrants. Similar to a typical phishing, it also involves impersonated fraudulent e-mails and fake web pages. The attacker uses an impersonated identity of a domain name registrar and sends a spoofed correspondence to the registrar's customer (a registrant) regarding a domain name related matter. The majority of Domain name registrars use electronic mail for many types of domain name registration related communication. The attackers exploit this fact in conducting the

socially engineered and fraudulent correspondence with the registrants.

[\[More\]](#)

- Win32/Conficker is a worm that spreads by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability ([CVE-2008-4250](#) / [CIVN-2008-170](#)). If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled.
- W32.Wecorl and W32.Kernelbot.A are actively exploiting a RPC request handling vulnerability in the Microsoft Windows Serve to propagate to other systems that reside on the same local subnet. Additionally, a variant of the Pidief family of trojans is actively exploiting a buffer overflow vulnerability in the util.printf() function of Adobe Acrobat products to download and execute additional malicious files onto infected systems.
- A variant of the *Mytob* family of worms threatened the computer systems of three London hospitals, causing shutdowns and initiating emergency response policies. *Mytob*, is a mass-mailing worm that allows attackers to gain unauthorized remote access to the compromised system via IRC channels. The worm is likely to cause network congestion and flood e-mail servers. The worm makes numerous modifications to an impacted system and continues to be a serious threat, even though first discovered in 2005.

Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during November 2008 and their countermeasures along with wide-spreading malicious code like virus/ worm/Trojan are given below:

| High Vulnerabilities | | | |
|------------------------|---|------------------------|--|
| Microsoft | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Microsoft | Multiple Vulnerabilities in Microsoft Windows and Microsoft XML Core Services | 12-Nov-08 | CIAD-2008-59 |
| Microsoft | Multiple Vulnerabilities in Microsoft XML Core Services | 12-Nov-08 | CIVN-2008-178 |
| Unix | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Linux | Linux Kernel 'hfs_cat_find_brec' Local Denial of Service Vulnerability | 21-Nov-08 | CIVN-2008-180 |
| Solaris | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Solaris | Vulnerability in the Solaris IP Filter Network Address Translation | 19-Nov-08 | CIVN-2008-179 |
| CISCO | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| CISCO Webex | Vulnerability in Wi-Fi Protected Access WPA Protocol | 25-Nov-08 | CIAD-2008-62 |
| CISCO Webex | Cisco VLAN Trunking Protocol Vulnerability | 10-Nov-08 | CIVN-2008-176 |
| CISCO Webex | Multiple Vulnerabilities in Cisco ASA and PIX IPv6 | 03-Nov-08 | CIAD-2008-56 |
| Miscellaneous | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Mozilla | Multiple Vulnerabilities in Mozilla products | 18-Nov-08 | CIAD-2008-60 |
| Adobe | Multiple Vulnerabilities in Adobe Flash player | 18-Nov-08 | CIAD-2008-61 |
| Adobe | Multiple Vulnerabilities in Adobe Acrobat and Reader | 10-Nov-08 | CIAD-2008-57 |
| IBM | IBM DB2 Denial of Service and Information Disclosure Vulnerabilities | 04-Nov-08 | CIVN-2008-175 |
| Opera | Opera Web Browser History Search & Links Panel XSS Vulnerability | 03-Nov-08 | CIVN-2008-173 |
| Medium Vulnerabilities | | | |
| Microsoft | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Microsoft | Microsoft Windows SMB Credential Reflection Vulnerability | 12-Nov-08 | CIVN-2008-177 |
| Low Vulnerabilities | | | |
| Sun | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Sun | Vulnerability in the Search Feature of the Sun Java System LDAP JDK | 03-Nov-08 | CIVN-2008-174 |

Malicious Code Threats

| Title of Malicious Code | Type | Overview | Aliases | Discovery Date | References |
|-------------------------|--------|---|--|-------------------|---|
| PWS:Win32/Lolyda | Trojan | Win32/Lolyda is a family of trojans that steal details relating to various MMORPGs (Massively Multiplayer Online Role -Playing Game) such as Fantasy Westward Journey, The Warlords and Zero Online. It has been distributed as a 16,697 -byte, UPACK- packed Win32 executable | Infostealer.Lineage (Symantec), Cryp_Mangled (Trend) Trojan-GameThief.Win32.OnLineGames (Kaspersky) | November 10, 2008 | http://www.cert-in.org.in/virus/win32_lolyda.htm |
| Worm:Win32/Conficker | Worm | Win32/Conficker is a worm that spreads by exploiting the Microsoft Windows Server Service RPC Handling Remote Code Execution Vulnerability (CVE-2008-4250 / CIVN-2008-170). If the vulnerability is successfully exploited, it could allow remote code execution when file sharing is enabled | W32.Downadup (Symantec) W32/Downadup.A [F-Secure], Conficker.A [Panda Software] | November 28, 2008 | http://www.cert-in.org.in/virus/win32_conficker.htm |
| Rustock | Trojan | It has been observed that a Rootkit enabled Trojan named Rustock is spreading in the wild. The Trojan has the functionality to send large volume of spam email messages from the infected computer. | Trojan.Rootkit. Rustock.E (BitDefender) Win32/Rustock.BH (CA) Win32/Rustock.NFW (ESET) Trojan.Win32.Multis.cp (Kaspersky) W32/Nuwar.sys (McAfee) | November 20, 2008 | http://www.microsoft.com/security/portal/Entry.aspx?name=Backdoor%3aWinNT%2fRustock.E |

MS08-067 worms squirming in the wild

[Source: <http://blogs.zdnet.com>] - 04 November 2008

First came Microsoft's emergency patch. Then the public release of reliable exploit code. Now, virus hunters are reporting two new in-the-wild worms exploiting the critical MS08-067 vulnerability.

The worms, intercepted on Chinese-language versions of Windows, are being used to install a Trojan downloader, a denial-of-service bot and a rootkit to maintain stealthy presence on infected machines.

The in-the-wild attacks are using portions of the proof-of-concept code that's publicly available, according to a source tracking this new threat.

One of the two worms spotted is capable of conducting DDoS (distributed denial-of-service) attacks against several Chinese sites, including the two big search engines Google and Baidu. It also downloads the eMule peer-to-peer program and drops an erotic movie on the hijacked system.

[\[More\]](#)

Microsoft: Malware for Windows on the rise

[Source: <http://www.theregister.co.uk>] 03 November 2008

Malware and unwanted software made strides in the first half of 2008, according to the latest security intelligence report from Microsoft, which tallied a 43 percent increase in the number of programs exorcised by the the company's malicious software removal tool.

In the first six months of this year, there were some 62 million disinfections on 23.8 million machines, according to the report which was published Monday. In the second half of last year, 42 million programs were removed on 15 million computers. Because it runs on hundreds of millions of machines worldwide, Microsoft's MSRT, or malicious software removal tool, functions as something of a bellwether for the state of successful attacks affecting Windows computers.

The increase was driven in part by the addition of new strains of malware that the MSRT checks for, said Jeff Williams, principal architect for the Microsoft Malware Protection Center. Win32/Taterf, a family of worms that steals login credentials for a host of online games, was one such addition and was removed 2.7 million times.

[\[More\]](#)

Virus hits nearly 75% of systems on Afghanistan military base

[Source: <http://blogs.zdnet.com>] 29 November 2008

A virus outbreak affected 75% of all systems at the largest U.S. military base in Afghanistan .

Details are still sparse, but both the LA Times and the U.S. News and World Report are reporting that the intrusion was severe enough to raise the INFOCON status, the information security equivalent of the DEFCON alert, and also necessitate the briefing of the president. The source of the attack is not known, but signs point to state rather than non-state actors, with the most popular contenders being either Russia or China.

[\[More\]](#)

Domain hijack fears over Gmail exploit

[Source: <http://www.theregister.co.uk>] 24 November 2008

A Gmail exploit which might be abused to allow domain hijacking has reared its ugly head once more.

The reported vulnerability revolves around the potential ability for hackers to create a malicious filter without needing to obtain the login credentials for a Gmail account. A flaw of this type hit web designer David Airey back in December 2007. Security watchers thought that Google had a handle on the problem, but now it seems that this confidence might have been misplaced.

The exploit kicks off by tricking surfers into visiting a maliciously constructed website. This site uses cross-site request forgery trickery to set up a filter on a targeted Gmail account which forwards email to a hacker's account while deleting it from a victim's inbox. The exploit involves stealing a cookie and creating a fake iFrame with a URL containing the variables that instruct Gmail to create a filter.

[\[More\]](#)

Malware found in Lenovo software package

[Source: <http://blogs.zdnet.com>] 19 November 2008

Computer maker Lenovo is shipping a malware-infected software package to Windows XP users, according to warning from anti-virus researchers at Microsoft.

The malicious file was identified by Microsoft as Win32/Meredrop, a Trojan dropper that is used to install and execute multiple malicious executables on an infected computer. Other anti-virus vendors are detecting the threat as a 'hooligan' virus or a porn dialer. It was found the Lenovo Trust Key software for Windows XP, a digitally signed driver package available to Windows XP SP2 users.

[\[More\]](#)

Security breach gives PayPal phish the personal touch

[Source: <http://www.theregister.co.uk>] - 24 November 2008

Skype users who use a piece of software dubbed Pamela to manage their online phone accounts should be on the lookout for customized phishing attacks following revelations that one or more user databases containing names and email addresses have been breached.

The attack, which took place on second week of November, has already led to one phishing campaign that calls recipients by their real names and then tries to trick them into turning over personal information. That added personal touch could throw some users off guard because most phishing emails address their marks by generic terms such as "Dear PayPal User."

[\[More\]](#)

Free tool for testing VoIP networks for targeted eavesdropping vulnerability

[Source: <http://www.net-security.org/>] 26- November 2008

Sipera Systems VIPER Lab released UCSniff, a free application that enables enterprises to determine if their VoIP networks are vulnerable to targeted eavesdropping. Jason Ostrom, Director of VIPER Lab, first publicly demonstrated UCSniff in September at the ToorCon X Conference, reviewing how administrators can validate this vulnerability, imitate an enterprise IP phone, download a corporate directory, then automatically monitor and record confidential conversations by targeting key employees and departments.

[\[More\]](#)

Microsoft ranks 5th on inglorious spam-friendly ISP list

[Source: <http://www.theregister.co.uk>] 26 November 2008

Microsoft is the world's fifth worst spam service ISP, according to a new list compiled by Spamhaus.org.

The software giant's high ranking in the unsolicited email game might, it would be fair to surmise, cause a few blushes among Redmond wonks.

Not so, according to Spamhaus chief information officer Richard Cox, who claims to have repeatedly notified MS about its rise up the inglorious list, to no avail.

He told the *Washington Post* that the company's live.com and livefilestore.com web properties are being abused by swindlers and scammers who are increasingly redirecting visitors to sites that sell porn, dodgy medicine and peddle Nigeria 419 scams.

[\[More\]](#)

Anti-malware testing group release standards

[Source: <http://www.securityfocus.com>] 11 November 2008

The recently-formed group, known as the Anti-Malware Testing Standard Organization (AMTSO), published *The Fundamental Principles of Testing and Best Practices for Dynamic Testing* on its Web site. Among the principles espoused by the organizations are open and transparent testing, the validation of test sample to classify their malicious nature, and verifying the statistic validity of the tests. The testing guidelines stress that any battery of tests must deliver reproducible results, recommends against the use of virtual machines and to define different levels of success.

[\[More\]](#)

AVG-incorrectly-flags-user32-dll-in-Windows-XP-SP2/SP3

[Source: <http://arstechnica.com/>] 11 November 2008

After a virus definition update, AVG's antivirus software began to mistakenly warn users that their system had a virus entitled PSW. banker4.APSA and suggested it had to be removed. The file that was being flagged was actually "user32.dll," a key Windows file. Many users chose to delete the file, which resulted in their Windows systems going into an endless reboot cycle, or stopped them from booting at all. Only users of Windows XP Service Pack 2 and Service Pack 3 seem to have been affected (users who have moved to Vista can apparently breathe a sigh of relief). Both AVG 7.5 or 8.0 was affected by the flawed definition file.

Complaints started to flood the AVG forums and the security company instructed affected users to boot their computers from the original Windows XP installation CD and run the repair option. Eventually AVG also posted a FAQ entry which outlined how to download and use a tool that could fix the problem for those without the original operating system install disc.

[\[More\]](#)

Spam rates massively down on shutdown of rogue ISP

[Source: <http://blogs.zdnet.com>] 12 November 2008

Computer maker Lenovo is shipping a malware-infected software package to Windows XP users, according to warning from anti-virus researchers at Microsoft.

The malicious file was identified by Microsoft as Win32/Meredrop, a Trojan dropper that is used to install and execute multiple malicious executables on an infected computer. Other anti-virus vendors are detecting the threat as a 'hooligan' virus or a porn dialer. It was found the Lenovo Trust Key software for Windows XP, a digitally signed driver package available to Windows XP SP2 users.

[\[More\]](#)

Mobility with centralized monitoring and auditing in StoneGate SSL VPN 1.2

[Source: <http://www.net-security.org/>] 13 November 2008

Stonesoft introduced the StoneGate SSL VPN 1.2 . With the new version, SSL VPN monitoring status and log details are integrated with the StoneGate Management Center , providing a centralized view of all remote connections. The StoneGate SSL VPN 1.2 enables organizations to offer their employees and partners controlled and secure, yet flexible, access to important data from anywhere, at any time and with any device. Administrators can now easily access log data and monitor the status of SSL VPN appliances, as well as all other StoneGate network security appliances in one centralized view via the StoneGate Management Center .

[\[More\]](#)

SSH sniffer attack poses minor risk

[Source: <http://www.theregister.co.uk>] 18 November 2008

UK security researchers have discovered hard-to-exploit cryptographic weaknesses in the Secure Shell (SSH) remote administration protocol.

The shortcoming creates a potential means to recover the plain text of encrypted sessions, depending on remote access configurations. Potential attacks - which would take ninja-like hacking skills to pull off - would involve inducing and observing error conditions. It's much more likely that a potential attack would crash a conversation than yield useful results.

[\[More\]](#)