



CERT-In Monthly Security Bulletin October 2008

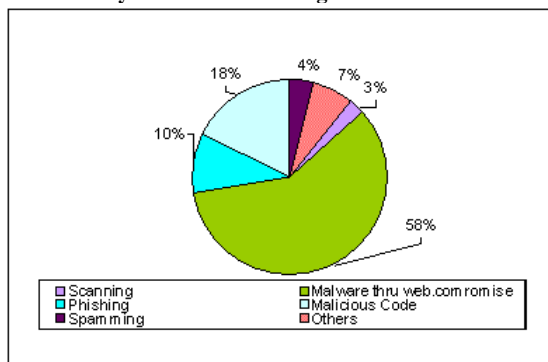
Cyber Intrusion Trends

In this month 229 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure, 58% incidents related to Spreading of malware through website compromise were reported in this month. 18% incidents related to virus/worm under the Malicious code category , 10 % phishing incidents , 04 % incidents related to spamming ,03 % unauthorized scanning , and 07% incidents related to technical help under the Others category were also reported in this month.

In this month CERT-In tracked 03 C&C (Command & Control) servers and 5219 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 .

In this month , several criminal gangs have acquired administrative log-in credentials for more than 200 Indian Web sites and have used the compromised domains to attack unsuspecting users' PCs with a notorious hacker exploit kit. CERT-In has informed the concerned authorities of compromised Indian domains and suggested the countermeasures.

Cyber Intrusion during October 2008



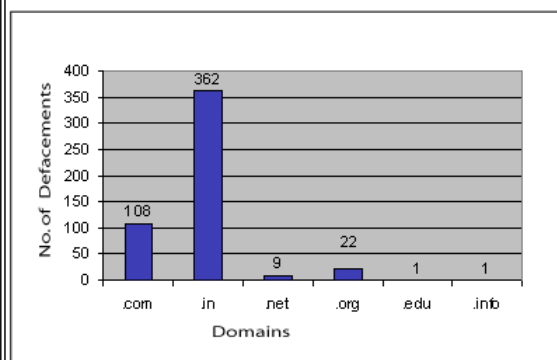
Indian Websites Defacement

In total 503 Indian websites were defaced during October 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. PHP Multiple Buffer Overflow Vulnerability [CVE-2008-3658](#)
2. Apache Tomcat ' RemoteFilterValve ' Security Bypass Vulnerability [CVE-2008-3271](#)
3. Apache Tomcat UTF-8 Directory Traversal Vulnerability [CVE-2008-2938](#)
4. Apache Tomcat ' RequestDispatcher ' Information Disclosure Vulnerability [CVE-2008-2370](#)
5. phpMyAdmin Shared Host Remote Information Disclosure [CVE-2008-1924](#)
6. PHP 5 ' php_sprintf_appendstring ()' Remote Integer Overflow Vulnerability [CVE-2008-1384](#)

Statistics of Defaced Indian Websites in October 2008

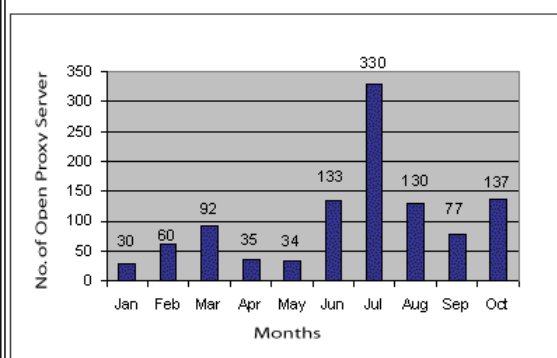


Open proxy servers

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 137 open proxy servers functioning in India during September 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 - Oct 2008



Attack Trend

Trojan Gimmiv.A exploits Microsoft Windows Server Service Vulnerability

It is reported that **Trojan Gimmiv.A** is exploiting Microsoft Windows Server service vulnerability([MS08-067](#)), which involves improper handling

of specially crafted remote procedure call (RPC) requests. Further details of the vulnerability are available in CERT -In vulnerability note [CIVN 2008-170](#) dated 24 th October 2008.

[\[More\]](#)

New Phishing Hits Domain Owners Accounts At eNom , NetworkSolutions

Sophos have reported a new kind of phishing campaign. Instead of the regular bank phish , or the more recent university/ webmail email account phish , this new campaign targets domain registrar accounts. The email fakes the From address (purports to come from tech@enom.com) and ask the user to update their account due to some maintenance, in a manner similar to bank phishes . The following two subject lines were seen in the phish emails, some with additional words such as “attention”, “warning”, or “ IncidentID : #####”. Clicking on the link will take the user to a link in the url format of www.enom.com.someotherdomain .

[\[More\]](#)

Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during August 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	Microsoft Windows WRITE_ANDX SMB packet Denial of service Vulnerability	24-Oct-08	CIVN-2008-171
Microsoft	Microsoft Windows Server Service Vulnerability	24-Oct-08	CIVN-2008-170
Microsoft	Microsoft Windows Active Directory Buffer Overflow Vulnerability	16-Oct-08	CIVN-2008-161
Microsoft	Microsoft Host Integration Server Remote Command Execution Vulnerability	16-Oct-08	CIVN-2008-160
Microsoft	Microsoft Internet Explorer Multiple Cross-Domain Vulnerabilities	16-Oct-08	CIVN-2008-159
Microsoft	Multiple Vulnerabilities in Microsoft Excel	16-Oct-08	CIVN-2008-158
Microsoft	Multiple Vulnerabilities in Microsoft Windows, Microsoft Internet Explorer, Microsoft Host Intergation Server, Microsoft Office Share Point Server and Microsoft Office	16-Oct-08	CIAD-2008-51
Oracle	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Oracle	Vulnerability in Oracle WebLogic plug-in for Apache causes Denial of Service	15-Oct-08	CIVN-2008-156
Oracle	Multiple Vulnerabilities in various Oracle products	15-Oct-08	CIAD-2008-50
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Linux	Linux Kernel 'truncate()' Local Privilege Escalation Vulnerability	31-Oct-08	CIVN-2008-172
Linux	Multiple Vulnerabilities in Linux Kernel	03-Oct-08	CIAD-2008-47
CISCO	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
CISCO Webex	Multiple Multicast Vulnerabilities in Cisco IOS Software	10-Oct-08	CIAD-2008-49
CISCO Webex	Cisco IOS IPS Feature SERVICE.DNS Signature Engine Network Traffic Handling Denial of Service Vulnerability	10-Oct-08	CIVN-2008-155
CISCO Webex	Cisco IOS Multiprotocol Label Switching Virtual Private Network Information Disclosure Issue	10-Oct-08	CIVN-2008-154

CISCO Webex	Cisco IOS Software Session Initiation Protocol (SIP) Message Memory Leak Denial of Service Vulnerability	08-Oct-08	CIVN-2008-153		
CISCO Webex	Cisco Security Advisory: Vulnerability in Cisco IOS While Processing SSL Packet	08-Oct-08	CIVN-2008-152		
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Adobe	Adobe Flash Player Clipboard Security Vulnerability	17-Oct-08	CIVN-2008-149		
Apache Tomcat	Buffer-Overflow Vulnerability in HTTP Unescaping Functions in Red Hat Fedora Directory Server	06-Oct-08	CIVN-2008-151		
Sun	Sun Java System Web Proxy Server FTP Subsystem Heap Based Buffer Overflow Vulnerability	20-Oct-08	CIVN-2008-168		
Mozilla	Multiple Vulnerabilities in Mozilla Products	06-Oct-08	CIAD-2008-48		
Opera	Opera Web Browser Multiple Vulnerabilities	24-Oct-08	CIAD-2008-54		
Ingres	Multiple vulnerabilities in Opera	20-Oct-08	CIAD-2008-52		
Ingres	Opera Web Browser Unicode Whitespace Cross-Site Scripting Vulnerability	06-Oct-08	CIVN-2008-150		
Medium Vulnerabilities					
Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Microsoft	Microsoft Ancillary Function Driver (AFD) Kernel Overwrite Vulnerability	16-Oct-08	CIVN-2008-167		
Microsoft	Microsoft Message Queuing Service Remote Code Execution Vulnerability	16-Oct-08	CIVN-2008-166		
Microsoft	Microsoft Windows Virtual Address Descriptor Privilege Escalation Vulnerability	16-Oct-08	CIVN-2008-165		
Microsoft	Microsoft Windows SMB Buffer Underflow Vulnerability	16-Oct-08	CIVN-2008-164		
Microsoft	Microsoft Windows IPP Service Integer Overflow Vulnerability	16-Oct-08	CIVN-2008-163		
Microsoft	Multiple Vulnerabilities in Windows Kernel	16-Oct-08	CIVN-2008-162		
Oracle	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Oracle	Multiple Vulnerabilities in Oracle WebLogic Products	27-Oct-08	CIAD-2008-55		
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Linux	Linux Kernel "snd_seq_oss_synth_make_info ()" Information Disclosure Vulnerability	03-Oct-08	CIVN-2008-121		
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Trend Micro	Trend Micro OfficeScan CGI Parsing Buffer Overflow Vulnerability	24-Oct-08	CIVN-2008-169		
Low Vulnerabilities					
Solaris	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Solaris	Microsoft Office CDO URI Handling Cross-Site Scripting Vulnerability	16-Oct-08	CIVN-2008-157		
Wireshark	Multiple Denial of Service Vulnerabilities in Wireshark	24-Oct-08	CIAD-2008-53		
Malicious Code Threats					
Title of Malicious	Type	Overview	Aliases	Discovery Date	References

Code					
Win32/Sinowal	Worm	<p>It has been observed that Worm: WIN 32/Sinowal is spreading widely. Win32/Sinowal is a family of password-stealing and backdoor Trojans. This Trojan is downloaded unknowingly by a user when visiting a malicious Web site. It can also be dropped by other malware. Win32/Sinowal may also steal user names and passwords for e-mail accounts. It may steal FTP and HTTP client account credentials in particular for online banking Web sites.</p>	<p>Mebroot (other) Trojan.Mebroot (Symantec) TRJ_SINOWAL.AD (Trend micro)</p>	October 17, 2008	<p>http://www.cert-in.org.in/virus/win32_sinowal.htm</p>
Trojan Nilage	Trojan	<p>It has been observed that a Trojan named Nilage is spreading in the wild. It arrives as a PE EXE file which is 52 925 bytes in size and is packed using FSG. After successful infection, the Trojan sends the notification of infection to the attacker through email.</p>	<p>Trojan-PSW.Win32.Lineage.a (Kaspersky Lab), Trojan Horse (Symantec), Trojan.PWS.Lineage (Doctor Web)</p>	October 17, 2008	<p>http://www.cert-in.org.in/virus/Nilage_Trojan.htm</p>
Slenfbot Worm	Worm	<p>Worm:Win32/Slenfbot is a family of worms that propagate or spread via instant messenger and available mounted drives. This Worm attempts to propagate</p>	<p>W32/Slenfbot. C.worm(Panda), Backdoor. Win32.IRCBot.blf (Kaspersky), Generic.dx (McAfee)</p>	October 21, 2008	<p>http://www.cert-in.org.in/virus/slenfbot_worm.htm</p>

		via the instant messaging client, MSN Messenger.			
Worm Hamweq	Worm	Worm:Win32/Hamweq is a worm that spreads via removable drives, such as USB memory sticks. This Bot contains an IRC-based backdoor, which may be used by a remote attacker to order the affected machine to participate in Distributed Denial of Service attacks, or to download and execute arbitrary files.	Win32:Trojan-gen (Avast) , Klon.W (AVG (GriSoft)), TR/Crypt.XPACK. Gen(Avira)	October 21, 2008	http://www.cert-in.org.in/virus/worm_hamweq.htm
Mabezat Worm	Worm	Virus:Win32/Mabezat is a polymorphic virus that infects PE files. This file infector may be dropped by other malware or may be downloaded unknowingly by a user when visiting malicious Web sites.	Win32/Mabezat.worm.32768 (AhnLab) W32/AutoRun.APZ (Norman) W32/Mabezat-B (Sophos) W32.Mabezat-3 (Clam AV)	October 24, 2008	http://www.cert-in.org.in/virus/mabezat_worm.htm

Security News

Hackers penetrate South Korean missile manufacturer

[Source: <http://www.theregister.co.uk>] - 01 October 2008

Black hat hackers were able to steal information from a South Korean missile manufacturer after planting malicious code on the company's computer system, according to news reports.

According to the country's National Security Research Institute, the code was installed on the computer network of LIGNex1 Hyundai Heavy Industries, a manufacturer of guided missiles, ground-to-air weapons, war ships, and submarines.

"The research institute suspects the culprits are Chinese or North Korean hackers but doesn't know specifically what information they stole," an official said. "In the worst case, the blueprints of missiles and Aegis ship could have been stolen."

[\[More\]](#)

TCP flaws allow deadly DoS attacks, finders say

[Source: <http://www.securityfocus.com>] 02 October 2008

Two security researchers claimed that flaws in the network stacks used by most operating systems could allow attackers to send a low-bandwidth denial-of-service attack that could leave victims' systems unresponsive.

The researchers -- Jack Louis and Robert E. Lee, both of vulnerability assessment firm Outpost24 -- discovered the flaws while creating a scalable network scanner to test large numbers of Internet addresses. Some of the servers scanned by the tool became non-responsive, and after further investigation, the duo discovered a class of issues in the network stacks used by most operating systems. In the more "interesting" cases, the target machines fail to recover after the attack ceases, Lee, the chief security officer for Swedish company, told *SecurityFocus* .

[\[More\]](#)

Trojan attacks Microsoft's emergency patch vuln

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

A day after Microsoft released an emergency patch for a critical flaw that could allow self-replicating attacks, researchers have identified a nasty trojan that attempts to exploit the vulnerability.

Variants of the data-stealing trojan known by names including Gimmiv.A and Spy-Agent.da have morphed over the past few weeks to exploit a major weakness in virtually all versions of the Windows operating system. If successful, the exploit could transform the malware into a virulent worm that allows a single infected machine to contaminate any other vulnerable machine over a local network without requiring any interaction on the part of the end users.

[\[More\]](#)

Phishing e-mail says it's from FBI

[Source: <http://www.virusbuster.hu>] 24 October 2008

Do not open unsolicited e-mails!

A spam e-mail claiming to be from FBI Deputy Director John S. Pistole is currently being circulated. This attempt to defraud is the typical e-mail scam using the name and reputation of an FBI official to create an air of authenticity.

As with many scams, the e-mail advises the recipient that they are the beneficiary of a large sum of money which they will be permitted to access once fees are paid and personal banking information is provided. The appearance of the e-mail leads the reader to believe that it is from FBI Deputy Director John S. Pistole. The scam e-mails give the appearance of legitimacy through the use of pictures of FBI officials, seal, letter head, and/or banners.

[\[More\]](#)

Survey: 88% of Mumbai's wireless networks easy to compromise

[Source: <http://blogs.zdnet.com>] 16 October 2008

Deloitte's recently released Wireless Security Survey assessing Mumbai's — India's financial capital — state of security awareness in respect to wireless security, shows an ugly picture of insecure wireless networks in both, business, and residential districts. With Mumbai being the home of India's most important financial institutions, next to the majority of multinational corporations, it may also turn into the playground for the next high profile data breach.

The key findings of the survey are:

- Of the 6729 wireless networks seen, 36% appeared to be unprotected i.e. without any encryption
- 52% were using low level of protection i.e. Wired Equivalent Privacy (WEP) encryption
- Over 95% of the networks broadcast their SSID, with 25% of these using their router's default SSID
- Balance 12% were using the more secure Wi-Fi Protected Access (WPA)

[\[More\]](#)

Researchers find keyboards to be tattletales

[Source: <http://www.securityfocus.com>] - 20 October 2008

Two researchers at the Swiss Federal Institute of Technology (EPFL) in Lausanne, Switzerland have surveyed 11 different wired computer keyboards and found that all leaked keystroke information.

The researchers, Martin Vuagnoux and Sylvain Pasini, used four different attacks to gather information at a distance of up to 20 meters via the electrical signals emitted from the they keyboards. The antenna used by the researchers could read the data even through walls, Vuagnoux said.

"We conclude that wired computer keyboards sold in the stores generate compromising emanations -- mainly because of the cost pressures in the design," Vuagnoux wrote on a Web page describing the attacks. "Hence they are not safe to transmit sensitive information. No doubt that our attacks can be significantly improved, since we used relatively unexpensive equipments (sic)."

[\[More\]](#)

Anonymous domain registration nixed amid fraud complaints

[Source: <http://www.theregister.co.uk>] – 2- October 2008-11-12

A company that provides a controversial service to domain name registrars says it is severing ties with Estdomains amid complaints that the Eastern European company makes it too easy to register sites that are used by spammers and scammers.

Directi, through a subsidiary called LogicBoxes, had been providing an array of products and services to Estdomains, including one known as PrivacyProtect, which shields the identity of domain-name owners. Critics have long claimed it is used by operators of sites that engage in spam, malware and other illegal acts.

About a month ago, Directi amended its relationship with Estdomains and stopped providing the Estonian registrar with the PrivacyProtect service, company officials said. While PrivacyProtect is used by many registrars, they say most of the abuse came from customers registering sites through Estdomains. That, in turn, prompted Directi to terminate its agreement in hopes that anti-fraud proponents would stop targeting the service.

[\[More\]](#)

ICANN cast as online scam enabler

[Source: <http://www.theregister.co.uk>] – 3 October 2008

Two recently issued reports portray the Internet Corporation for Assigned Names and Numbers (ICANN) as a bureaucracy that enables cyber criminals.

In [one report \(PDF\)](#), researchers Jart Armin, James McQuaid and Matt Jonkman detail how one of ICANN's prized sponsors has ties to one of the net's more prolific sources of malware and illegal online pharmacies. It's called LogicBoxes, and over the past two years, ICANN has listed it as a sponsor for meetings that took place in Los Angeles and Delhi, India.

It turns out that LogicBoxes has an association with Atrivo, a network provider that also goes by the name of Intercage. According to the study, a random sampling of 2,600 addresses hosted by Atrivo revealed 7,340 malicious web links, 910 infected websites, 310 malicious binaries, and 113 botnet command and control servers. As an autonomous systems (AS) provider, the Concord, California-based company controls a large number of IP addresses.

[\[More\]](#)

Secure Coding

Easily avoided software defects are a primary cause of commonly exploited software vulnerabilities. The CERT /CC has observed, through an analysis of thousands of vulnerability reports, that most vulnerabilities stem from a relatively small number of common programming errors. By identifying insecure coding practices and developing secure alternatives, software developers can take practical steps to reduce or eliminate vulnerabilities before deployment.

The CERT Secure Coding Initiative works with software developers and software development organizations to reduce vulnerabilities resulting from coding errors before they are deployed. We work to identify common programming errors that lead to software vulnerabilities, establish standard secure coding standards, educate software developers, and to advance the state of the practice in secure coding.

[\[More\]](#)