



**CERT-In Monthly Security Bulletin May 2008**

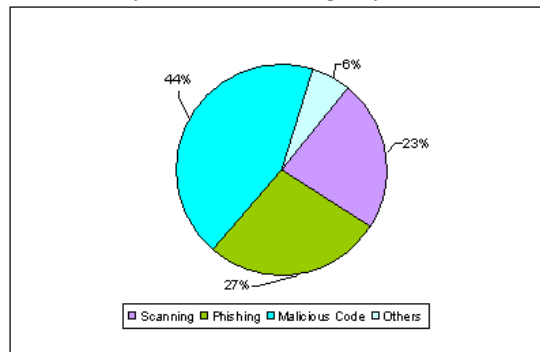
**Cyber Intrusion Trends**

In this month 82 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 27% phishing incidents were reported in this month. 23% unauthorized scanning , 44% incidents related to virus/worm under the Malicious code category and 6% incidents related to technical help under the Others category were reported in this month. As compared to previous month the number of incidents related to virus/worm under the Malicious code category have increased while phishing incidents, scanning incidents and incidents related to technical help under the Others category have decreased.

In this month CERT-In tracked 12 C&C (Command & Control) servers and 6182 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.

During this month SQL injection worm infected a large number of websites which in turn affected the user systems by downloading malicious code from remote servers.

**Cyber Intrusion during May 2008**



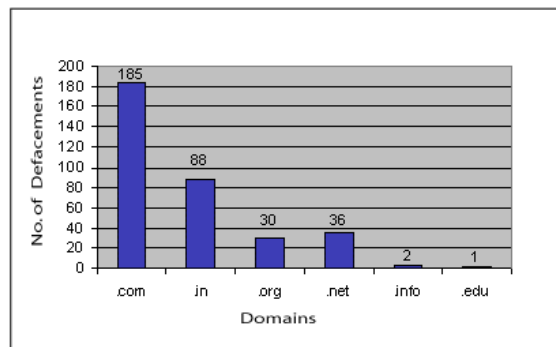
**Indian Websites Defacement**

In total 342 Indian websites were defaced during May 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. Apache-SSL Authentication Bypass Vulnerability [CIVN-2008-36](#)
2. phpMyAdmin Shared Host Remote Information Disclosure [CVE-2008-1924](#)
3. PHP 5 'php\_sprintf\_appendstring()' Remote Integer Overflow Vulnerability [CVE-2008-1384](#)
4. Apache Tomcat SingleSignOn Cookie Information Disclosure Weakness [CVE-2008-0128](#)
5. phpMyAdmin Local Information Disclosure [CVE-2008-1567](#)
6. Apache Tomcat AJP Connector Information Disclosure [CVE-2006-7197](#)
7. Apache Tomcat Cross-Site Scripting [CVE-2006-7195](#)

**Statistics of Defaced Indian Websites in May 2008**

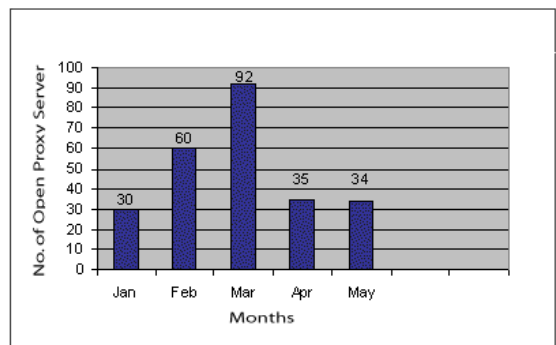


**Open proxy servers**

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 34 open proxy servers functioning in India during May 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 - May 2008**



**Attack Trend**

**SQL Injection Worm**

It has been observed that SQL Injection Worm spreading in the wild by injecting java scripts or iframe into websites. Many websites have been found infected with such scripts. Websites injected with java scripts are redirecting innocent visitors to malicious website "winzicipes DOT cn" which is containing java scripts with numeric names such as 2.js, 4.js.

The java script has been coded to take user to the malicious .asp page which in turn takes user to malicious domain "cnzz DOT com" or "51 DOT la". The SQL injection worm is seems to be infecting machines using vulnerable Real Player versions. Malicious domains involved in attacks with SQL

worm activity are

cnzz DOT com,  
51 DOT la,  
511a DOT ajiang DOT net , and  
http:// bbs DOT jueduizuan DOT com

Malware downloaded from malicious domain makes continuous outbound request to 61 DOT 134 DOT 37 DOT 15 on port 1800.

#### Updated

Since 19 th May some new domains have been observed in SQL injection attack. The attackers are inserting redirection tags in the contents of websites.

[\[More\]](#)

#### Training

##### Workshop on "Computer Forensics for System Administrators "

CERT-In conducted a one day Workshop on "Computer Forensics for System Administrators" on May 07, 2008. The objective of the workshop is to create awareness among system/network administrators to act as a "First Responder", enabling them to handle the cyber-crime related systems & networked infrastructure in a forensically sound manner for collecting electronic evidence and also to apply the best forensic practices. The interactive workshop covered the following topics at length:

- Computer Forensics – Basics, First Responder, Collection of Evidence
- Computer Forensics – Tools, Evidence Analysis, Anti-Forensics
- IT Act on Cyber Crime
- Cyber Crime and Forensics Tools
- Forensics Tools, Demo

The presentation material is available [here](#) .

#### Case Study

##### CICS-2008-01

Website defacement is usually occurs when an intruder maliciously alters a web page by inserting or substituting provocative and frequently offending data .CERT-In tracks defacement of Indian websites on a regular basis. The case study provides analysis of the attack and identified vulnerabilities which were being exploited to compromise the website. It also provides appropriate countermeasures to secure webserver and web applications from such type of attacks.

[\[More\]](#)

#### Security Alerts

**The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during May 2008 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            | Microsoft HeartbeatCtl ActiveX control buffer overflow Vulnerability   | May 06, 2008           | <a href="#">CIVN-2008-52</a>           |
| Microsoft Works      | Microsoft Works WkImgSrv.dll ActiveX Vulnerability   | May 06, 2008           | <a href="#">CIVN-2008-53</a>           |
| Microsoft Windows    | Microsoft Windows I2O Filter Utility Driver (i2omgmt.sys) Local Privilege Escalation Vulnerability                                   | May 13, 2008           | <a href="#">CIVN-2008-56</a>           |
| Microsoft            | Multiple Vulnerabilities in Microsoft Windows, Microsoft word, Microsoft Jet Database Engine and Microsoft Malware Protection Engine | May 14, 2008           | <a href="#">CIAD-2008-25</a>           |
| Microsoft            | Microsoft Word Memory corruption Remote Code Execution Vulnerabilities   | May 14, 2008           | <a href="#">CIVN-2008-57</a>           |
| Microsoft            | Microsoft Publisher Object Handler Validation Vulnerability  | May 14, 2008           | <a href="#">CIVN-2008-58</a>           |
| Microsoft            | Microsoft Malware Protection Engine Input Validation Vulnerability   | May 14, 2008           | <a href="#">CIVN-2008-59</a>           |
| Unix                 | Title of Vulnerability   | Discovery/Publish Date | CERT-In References & Patch Information |
| OpenOffice           | Multiple Remote code Execution Vulnerabilities in OpenOffice.org   | May 01 , 2008          | <a href="#">CIVN-2008-49</a>           |

|                          |   |                               |   |
|--------------------------|---|-------------------------------|---|
| Opera                    | Opera Web Browser Multiple Remote Code Execution Vulnerabilities            | May 01 , 2008                 | <a href="#">CIVN-2008-50</a>                      |
| Red Hat Directory Server | Multiple Vulnerabilities in Red Hat Directory Server                        | May 01 , 2008                 | <a href="#">CIVN-2008-51</a>                      |
| Linux Kernel             | Multiple Vulnerabilities in Linux Kernel                                    | May 06 , 2008                 | <a href="#">CIVN-2008-54</a>                      |
| PHP                      | Multiple Vulnerabilities in PHP   | May 13, 2008                  | <a href="#">CIAD-2008-24</a>                      |
| Linux Kernel             | "ipip6_rcv" Denial of Service Vulnerability in Linux Kernel                 | May 27 , 2008                 | <a href="#">CIVN-2008-64</a>                      |
| <b>Cisco</b>             | <b>Title of Vulnerability</b>   | <b>Discovery/Publish Date</b> | <b>CERT-In References &amp; Patch Information</b> |
| Cisco                    | Cisco Content Switching Module Memory Leak Vulnerability                    | May 23 , 2008                 | <a href="#">CIVN-2008-61</a>                      |
| Cisco                    | Cisco Unified Presence Denial of Service Vulnerabilities                    | May 23 , 2008                 | <a href="#">CIVN-2008-62</a>                      |
| Cisco                    | Cisco Unified Communications Manager Denial of Service Vulnerabilities      | May 23 , 2008                 | <a href="#">CIVN-2008-63</a>                      |
| Cisco                    | Cisco IOS SSH Server Improper Memory Access Denial of Service Vulnerability | May 28 , 2008                 | <a href="#">CIVN-2008-65</a>                      |
| Cisco                    | Cisco Unified Customer Voice Portal Privilege Escalation Vulnerability      | May 28 , 2008                 | <a href="#">CIVN-2008-66</a>                      |
| Cisco                    | Cisco Service Control Engine Denial of Service Vulnerabilities              | May 28 , 2008                 | <a href="#">CIVN-2008-67</a>                      |
| CiscoWorks               | CiscoWorks Common Services Arbitrary Code Execution Vulnerability           | May 30 , 2008                 | <a href="#">CIVN-2008-69</a>                      |
| <b>Miscellaneous</b>     | <b>Title of Vulnerability</b>   | <b>Discovery/Publish Date</b> | <b>CERT-In References &amp; Patch Information</b> |
| Solaris                  | Vulnerabilities in the Tcl/Tk GUI Toolkit Library in Solaris                | May 13 , 2008                 | <a href="#">CIVN-2008-55</a>                      |
| Solaris                  | Print Service Vulnerability in Solaris                                      | May 15 , 2008                 | <a href="#">CIVN-2008-60</a>                      |
| Adobe Flash Player       | Adobe Flash Player Unspecified Remote Code Execution Vulnerability          | May 30 , 2008                 | <a href="#">CIVN-2008-68</a>                      |

**Malicious Code Threats**

| Title of Malicious Code   | Type   | Overview   | Aliases   | Discovery Date | References  |
|---------------------------|--------|--|---|----------------|---|
| Trojan AGENT and variants | Trojan | These Trojans are dropped by other malware or gets downloaded on system while visiting malicious websites. Some of the variants propagate through spam emails containing link to malicious website or as an attachment. The attachments uses MS-WordPad and Adobe PDF file | TROJ_AGENT.ANAF, TROJ_AGENT.XOO, TROJ_AGENT.AMAL<br>(Aliases:<br>Trojan.Dropper (Symantec), Troj/DwnLdr- HCM (Sophos) | May 08, 2008   | <a href="http://www.cert-in.org.in/virus/Trojan_Agent_and_Variants.htm">http://www.cert-in.org.in/virus/Trojan_Agent_and_Variants.htm</a> |

|                 |        |   |                            |               |   |
|-----------------|--------|---|----------------------------|---------------|---|
|                 |        | icons to trick users into thinking that the files are genuine.  |                            |               |   |
| Trojan.Virantix | Trojan | It has been observed that a Trojan named Virantix is spreading widely. After successful installation, the Trojan displays fake security alert message which tricks user to click upon the icon. As user clicks upon the icon, it downloads additional malware onto the infected system. | No Alias                   | May 09, 2008  | <a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-050916-1055-99&amp;tabid=1">http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-050916-1055-99&amp;tabid=1</a> |
| Downloader.Swif | Trojan | It has been observed that a Trojan named Swif is propagating widely. It propagates exploiting Multimedia File Remote Buffer Overflow Vulnerability in Adobe Flash Player. After successful exploitation of the vulnerability, the Trojan downloads additional onto the infected system. | SWF_DLOADER.ZTS<br>[Trend] | May 28 , 2008 | <a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-052714-3021-99&amp;tabid=1">http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-052714-3021-99&amp;tabid=1</a> |

#### Security News

#### **Mass SQL injection hits English language websites**

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

21st May , 2008

Thousands of websites in China have been booby trapped with code written to download Trojan software onto visitors who run vulnerable Windows PCs. Unlike earlier rounds of SQL injection attacks the latest assaults mostly target English language sites (predominantly sites hosted in China but with a .com suffix) and purposefully avoid Chinese government sites, according to net security firm ScanSafe. The latest attacks inject an iFrame onto compromised sites that loads malicious scripts from qiqigm.com, a domain registered on 16 May. These scripts includes the text "silent love china" in an apparently greeting to other Chinese hackers

The malicious code exploit well-known RealPlayer and Internet Explorer vulnerabilities to install a password-stealing Trojan that hides its presence on Windows PCs. More than 7,000 sites have been compromised in this way, reports Mary Landesman, ScanSafe's senior security researcher.

[\[More\]](#)

### **Botnet sics zombie soldiers on gimpy websites**

[Source:www.theregister.co.uk]

14th May 2008

The miscreants who have poisoned more than half a million web pages aren't the only attackers thinking big. People behind a botnet known as Asprox have recently rejiggered their army to infect websites in a similar fashion. Asprox zombies have recently been blessed with a tool that sniffs out potentially vulnerable sites running Microsoft's Active Server Pages and then tries to commandeer them using SQL injections. When infections are successful, the pages then redirect visitors to websites that silently install a malware cocktail that includes the Asprox malware. The vicious cycle gives the scheme worm-like capabilities."Because the tool is distributed by the botnet, it may appear to be worm-like in its operation, which may lead to conflicting reports in the media and blogs about the true nature of the attack," Joe Stewart, the SecureWorks researcher who discovered the attack, wrote in a report. "However, the SQL attack tool does not spread on its own, it relies on the Asprox botnet in order to propagate to new hosts."

[\[More\]](#)

### **Asprox botnet rears its ugly head**

[Source:www.vnunet.com]

21st May, 2008

A new botnet which specialises in sending out phishing spam has prompted security experts to call for enterprises to review their security protection. The Asprox botnet uses a SQL-injection attack tool to hack websites and add yet more hijacked PCs to its army. "Asprox is more than just another piece of botnet malware as it's what we call a 'hybrid,'" said David Hobson, managing director of Global Secure Systems. "It uses an SQL-injection attack tool that attacks legitimate websites to add to the overall botnet swarm." Hobson explained that, while botnets and SQL injection attacks are nothing new, a malware infection that combines the two "darkware" vectors highlights the growing ingenuity of the hacker community. "Most botnets are perpetrated these days by criminal gangs who are after your company's money. And if they can't get your money, they'll use your computers to damage your reputation. It's a simple as that," he said. The rapid evolution of multi-vector malware like Asprox means that companies should now look seriously at multi-vendor and/or multi-layered IT security protection, according to Global Secure Systems.

[\[More\]](#)

### **Drive-by download attack compromises 500K websites**

[Source:www.channelregister.co.uk]

13th May, 2008

More than half a million web pages have been compromised with malware as part of a new attack, Trend Micro warns. Badly configured PHP bulletin board applications are being used to plant malicious JavaScript on web forums. The JavaScript is used to push variants of the Zlob Trojan that come disguised as a video codec installer. The Trojans change DNS and browser settings on infected PCs leaving them open to further attack. Many of the compromised forums were already used to spamvertise knock-down drugs and smut sites. In the UK most of the infected websites belong to small- to medium-size firms whose weak security controls have left the door open to hackers. The malware is served up from systems based in the US and Russia. Trend reckons the latest attack bears the same hallmarks as previous attacks by a Russian and Ukrainian gang punting the Zlob Trojan. Trend has more on the attack in a blog posting here. Cybercrooks are increasingly looking toward planting malicious script onto regular sites rather than attempts to trick users into visiting obviously dodgy sites touting warez and porn. Fake media codecs are becoming a favourite vector for spreading spyware and Trojans.

[\[More\]](#)

### **'State Of The Internet' Shows Attacks, Network Speeds Up**

[Source:www.informationweek.com]

29th May , 2008

Attacks coming from 125 countries targeted 23 unique network ports, with the most malicious traffic coming from the United States and China, Akamai reports. China and the United States accounted for the greatest percentage of Internet attacks in the first quarter of this year, according to a report released this week. Akamai's first "State of the Internet" report covers information about broadband, attacks and other data gathered in Q1 of 2008. The report also offers news and information about Denial of Services attacks, hacking, and network events. It showed attacks coming from 125 countries, targeting 23 unique network ports, but the United States and China accounted for 30% of the attack traffic. Ports with the most attack traffic were targeted by worms, viruses, and bots that spread across the Internet several years ago, Akamai said. It showed attacks coming from 125 countries, targeting 23 unique network ports, but the United States and China accounted for 30% of the attack traffic. Ports with the most attack traffic were targeted by worms, viruses, and bots that spread across the Internet several years ago, Akamai said.

[\[More\]](#)

### **Identity 'at risk' on Facebook**

[Source:www.news.bbc.co.uk]

1st May, 2008

**Personal details of Facebook users could potentially be stolen, the BBC technology programme Click has found.**

The popular social networking site allows users to add a variety of applications to their profile. But a malicious program, masquerading as a harmless application, could potentially harvest personal data. Facebook says users should exercise caution when adding applications. Any programs which violate their terms will be removed, the network said.

### **Stealing details**

Facebook is the darling of the moment, allowing friends to stay in touch, post photos, and share fun little games and quizzes. And it also lets you keep

your details private from the rest of the world. Or at least that is the implication.

We have discovered a way to steal the personal details of you and all your Facebook friends without you knowing. We made up the fictitious profile of Bob Smith. He keeps most of his details on his profile private from non-friends.

While we could not get all details, what we did get, included his name, hometown, school, interests and photograph, would certainly help us to steal someone's identity.

[\[More\]](#)

#### **Hotmail users getting locked out**

[Source: www.news.cnet.com]

30th May , 2008

Imagine getting an e-mail from a friend or family member with the following subject line: "ITS IMPORTANT YOU GET BACK ME TODAY." CNET is aware of a couple of Hotmail users who have recently gotten locked out of their accounts. In one case, someone who had hacked into an account sent a desperate-sounding e-mail asking for money under the account holder's name. Microsoft had no direct comment.

The body of one of the e-mails, sent to a CNET reporter, reads:

"I am in a hurry writing this mail. I had a trip to oxfordshire, United Kingdom for an urgent event . Unfortunately for me all my money got stolen at the hotel where i lodged from the attack of some armed robbers and since then i have been without any money i am even owing the hotel here,So i have only access to emails,my mobile phone can't work here so i did not bring it along. Please can you lend me \$1500 so i can return back and settle the hotel bills i would return it back to you as soon as i get home, I am so confused right now. You can have it sent through western union."The owner of the Hotmail account was confirmed to be at home, safe.

[\[More\]](#)

#### **FBI warns of e-mail scams offering to help Chinese quake victims**

[Source: www.computerworld.com]

21st May , 2008

The FBI is warning Americans looking to send donations in the aftermath of the massive May 12 earthquake in China to beware of a rising number of e-mail scams that tout "relief" efforts. In an announcement yesterday, the FBI said that some of the e-mail scams even offer "free vacation trips to the largest donors" while using fake logos of legitimate online payment services to steal money from unsuspecting donors. Similar fake e-mail campaigns occur after every major disaster, including the Sept. 11, 2001, attacks on the U.S., hurricanes Katrina and Rita, last year's Minneapolis interstate bridge collapse and the recent cyclone in Myanmar, according to the FBI.

"The more awareness there is to these kinds of things, the better off we are so that people don't get lured in," said Paul Bresson, an FBI spokesman.

"Whenever there is some tragic event, these scam artists come out to do their business. It may not be apparent to unwitting victims."

[\[More\]](#)

#### **ID Theft Monitoring Services: What You Need To Know**

[Source:www.theregister.co.uk]

9th May, 2008

What is your identity worth? According to the Global Internet Security Threat Report from Symantec (NSDQ: SYMC), credit card numbers go for as little as 40 cents on the black market. Complete access to a bank account? Just \$10.

Not so long ago, one's identity didn't involve so many dollars and cents. Discussions of privacy seemed better suited to the realm of academic debates or conspiracy theories. Today, unfortunately, the context is too often one of ripped-off consumers, with tales of swiped credit card numbers, false mortgages, and employment fraud leading to many cumulative hours spent, perhaps over years, trying to clean up the mess. Of course when someone comes gunning for granny's life savings, "good Samaritans" won't be far behind.

Take identity theft monitoring service providers. The pitch? Give us your Social Security number and notification of suspicious identity activity is only an e-mail alert or phone call away. These services, which typically cost \$10 to \$20 per month, offer to guard your identity by monitoring the three credit-reporting agencies (Experian, Equifax, and TransUnion), cell phone applications, government databases, and public information. Some also provide insurance (subject to underwriting, and not valid in every state) to help defray costs associated with recovering from identity theft cases.

[\[More\]](#)

#### **Yahoo sues lottery spammers**

[Source:www.computerworld.com]

28th May , 2008

Yahoo Inc. has filed a lawsuit against unidentified spammers for allegedly perpetrating e-mail scams designed to trick unsuspecting users into revealing personal information including credit card and Social Security numbers. The lawsuit against the "Yahoo Lottery Spammers," which includes 25 unidentified companies and 25 unidentified individuals, was filed on May 16 in the U.S. District Court for the Southern District of New York under the Federal Trademark Act, the Federal CAN-SPAM Act and related state laws, according to a company statement released today.

Yahoo is trying to determine the identities of the spammers, some of whom may be located outside of the U.S. The spammers used third-party e-mail providers, such as The Go Daddy Group Inc. and EarthLink Inc., to allegedly send fraudulent e-mails to Internet users, according to court

documents. Yahoo, which is seeking a jury trial, wants the alleged scammers to forfeit their profits and pay damages.

[\[More\]](#)

### **Hackers exploit China earthquake to punt Trojan**

[Source: www.theregister.co.uk]

22nd May, 2008

Unscrupulous virus writers have inevitably latched onto the Chinese earthquake disaster, which killed more than 50,000, to punt malware. The Trojan-laced email attacks follow earlier phishing scams themed around the Sichuan province disaster. Emails with infected Word attachments contaminated by MalDoc-Fam Trojan are being distributed in messages that pose as news about the disaster, net security firm Sophos reports. The malware-tainted emails typically appear with body text suggesting they contain news from China's official press agency, Xinhua. BEIJING, May 20 (Xinhua) -- The death toll from the earthquake in southwest China's Sichuan Province has risen to 34,074 nationwide as of 2 p.m. Saturday, while 198,347 people were injured, according to the Information Office of the State Council. Pay attention to attachment for more. Opening the attached Word document triggers an exploit that downloads malware onto vulnerable Windows PCs. The MalDoc-Fam Trojan is more than a year old, dating from March 2007.

[\[More\]](#)

### **The Storm Worm would love to infect you**

[Source: www.blogs.zdnet.com]

19th May, 2008

The Storm Worm malware is back in the game, with its most recent campaign currently active and trying to entice users into executing iloveyou.exe by spamming them with links to already infected hosts acting as web servers, next to SQL injecting malicious domains into legitimate sites for the campaign to scale faster.

What has changed compared to previous campaigns? Storm Worm is back in the SQL injection attack phrase, with tellicolakerealty .cn/ind.php iframe injected at a small of sites for the time being. Moreover, assessing the storm worm infected hosts can only be done if you spoof your user agent to Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1921), otherwise you will get no indication for any kind of malicious activity going on. Furthermore, despite that there are no exploits used at the infected hosts but, a heavily obfuscated HTML/Rce.Gen was detected in their injected domain which would load automatically upon someone visiting an already injected site.

[\[More\]](#)

### **Educating Managers On Computer Fraud Could Cut Crime**

[Source: www.crime-research.org]

26th May, 2008

Shalini Kesar, a computer scientist at Southern Utah University in Cedar City, has devised an antifraud strategy for business. Writing in the International Journal of Business Information Systems from Inderscience Publishers, he suggests that managers should be made aware of security issues and send out cues to junior staff that they have this knowledge.

Combating digital fraud within any organizations is a growing problem for management. Researchers in this field and security practitioners have recently begun to emphasize the need to take into account the "social" aspects of information security. They also emphasize that a lack of communication at the wider organizational level is often associated with computer fraud.

"Computer fraud can result from incompetence, ignorance, negligence in the use of Information Technology or deliberate misappropriation by individuals," says Kesar. This results in the destruction of not only the main information systems but also backup systems, causing damages up to hundreds and thousands of dollars.

[\[More\]](#)

### **Attack code in the wild targets new (sort of) Adobe Flash vuln**

[Source: www.theregister.co.uk]

27 May, 2008

Updated Security researchers from Symantec have clarified an earlier report of attack code in the wild that targets a previously unknown vulnerability in the latest version of Adobe Flash. They now say current versions of Adobe's stand-alone Flash application are vulnerable, but that updated browser plug-ins are not. At least 20,000 web pages have been found to carry links to a site that hosts malicious Flash applets that exploit the weakness, according to Symantec. While Flash plug-ins for Internet Explorer, Firefox and other browsers are immune to the attack, Adobe's stand-alone application for Flash is vulnerable, said Ben Greenbaum, a senior research manager at Symantec Security Response.

The security bug is a variation of one that Adobe has recently patched, but evidently, the update didn't work as expected. "This was one of the vulnerabilities that was reported as having been fixed," he said. "In the stand-alone versions, it does not happen." The clarification is good news because the number of people using the application is relatively small. The Flash plug-in, by contrast, is installed on just about every computer known to man, thanks to its availability on Windows, Mac and Linux platforms and the huge number of sites that require their visitors to use it. A well-executed attack of a zero-day flaw in the ubiquitous program could prove critical.

[\[More\]](#)

### **Chandigarh gets hi-tech cyber crime cell**

[Source: www.crime-research.org]

15th May, 2008

Chandigarh Police has set up a hi-tech cyber crime investigation cell for checking computer related crimes, such as unauthorised access to a computer, on-line banking fraud, "phishing", sale of illegal articles, on-line gambling, e-mail spoofing and cyber stalking.

The cell that has been set up by the Chandigarh police in association with Nasscom and Punjab Engineering College, Chandigarh was inaugurated by Punjab Governor and Administrator, Union Territory, Chandigarh, Gen. (Retd) S F Rodrigues.

General Rodrigues emphasised the need of strengthening the linkages of this center with a national data base center and Nasscom, through effective coordination with other states, to check computer related crimes.

He said that focus of the whole exercise is synergy and the integration of different services to achieve set goals, as no system can successfully work in isolation.

[\[More\]](#)

### **Spam Turns 30 And Never Looked Healthier**

[Source:www.informationweek.com]

2nd May, 2008

Thirty years ago, on May 3, 1978, Digital Equipment Corp. engineer Carl Gartley sent the first spam e-mail message on behalf of Gary Thuerk, a DEC marketing representative, to promote the new Decsystem-20 line of computers.

Thuerk's message has been preserved and can be seen on the Web site of Brad Templeton, chairman of the board of the Electronic Frontier Foundation, along with details about how the first spam came to be and the reaction it generated. While the message appears to have been composed on May 1, 1978, Templeton's record of the event indicates that the e-mail was sent on May 3. In 2004, Bill Gates predicted the spam problem would be solved in two years. Four years later, there's more spam than ever, though many end users only see a fraction of what's out there because of the diligence of their e-mail service providers. Sophos, an e-mail security company, says that 95% of all e-mail today is spam. Symantec (NSDQ: SYMC) says that figure is more like 80% to 85%. However you count it, there's more spam than most people want.

[\[More\]](#)

### **eBay Seller Faces 20-Year Sentence For Software Piracy**

[Source:www.informationweek.com]

15th May, 2008

An eBay (NSDQ: [EBAY](#)) seller accused of creating more than 40 fake IDs on the auction Web site could spend 20 years in prison after pleading guilty to charges related to the sale of pirated software. The Software & Information Industry Association announced the guilty plea Thursday, while also filing nine new lawsuits against people accused of illegally selling software on [eBay](#). The [SIIA](#) said it has brought 26 cases against people selling counterfeit or pirated software this year. The group also said Jeremiah Mondello, a former student at the University of Oregon, pleaded guilty to copyright infringement, aggravated identity theft, and mail fraud. He faces fines of up to \$500,000 and imprisonment from two to 20 years. He will be sentenced in July.

Last year, the SIIA used a proprietary Auction Enforcement Tool to identify Mondello from an eBay seller ID. The group linked him to several other eBay identities and forwarded its information to the U.S. Department of Justice Computer Crimes and Intellectual Property Section (CCIPS).

[\[More\]](#)