



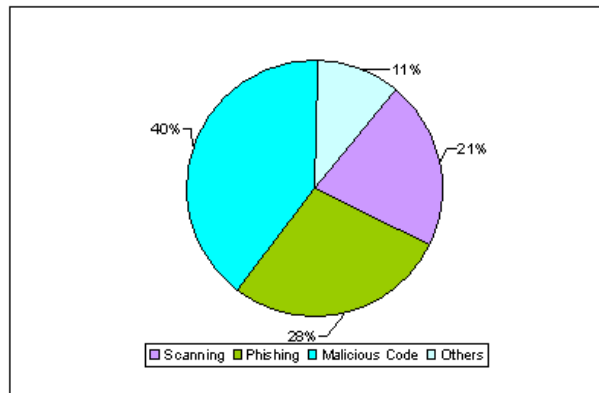
CERT-In Monthly Security Bulletin March 2008

Cyber Intrusion Trends

In this month 57 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 28% phishing incidents were reported in this month. 21% unauthorized scanning, 40% incidents related to virus/worm under the Malicious code category and 11% incidents related to technical help under the Others category were reported in this month. As compared to previous month the number of scanning incidents and incidents related to virus/worm under the Malicious code category have increased while phishing incidents and incidents related to technical help under the Others category have decreased.

In this month CERT-In tracked 19 C&C (Command & Control) servers and 15,160 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 March 2008



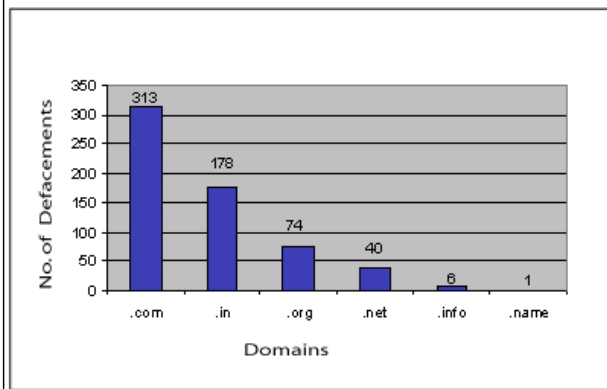
Indian Websites Defacement

In total 612 Indian websites were defaced during March 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. Multiple Vulnerabilities in Apache HTTP Server [CIAD-2008-03](#)
2. Cross Site Scripting Vulnerability in Apache mod_imap Module [CIVN-2007-163](#)
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](#)
8. Apache Tomcat SSL Anonymous Cipher Configuration Information Disclosure [CVE-2007-1858](#)

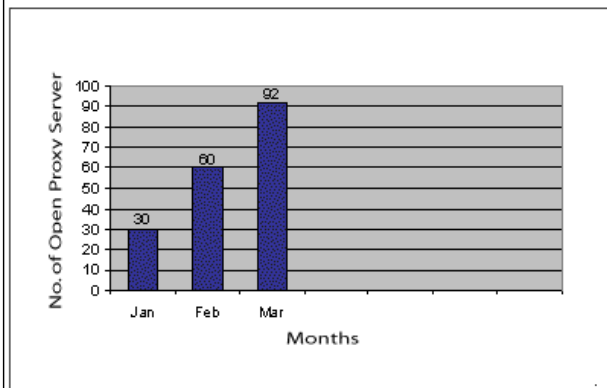
Statistics of Defaced Indian Websites in March 2008



Open proxy servers

CERT-In tracked 89 open proxy servers functioning in India during March 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 - March 2008



Attack Trend

Mass SQL Injection attacks and malicious Java script embedding on websites :

It has been observed in the month of March that various websites have been infected with malicious JavaScript file hosted on domain 211796 DOT net. Remote attackers are launching a SQL injection attacks against web servers running ASP and embedding a link (www DOT 21179 66 DOT net/fuckjp DOT js) to malicious JavaScript file on these websites. When a user visits the infected websites, the code gets executed onto the user's system. Upon execution it tries to exploit several known vulnerabilities on the victim system to download some password stealing malware. The downloaded malware tries to make

outbound connections to IP address 61 DOT 188 DOT 39 DOT 175 on port 2034.
 Vulnerabilities exploited by the JavaScript file are:

- o Microsoft Data Access Components Code Execution Vulnerability (CIVN-2006-31)
- o Microsoft Windows Vector Markup Language Code Execution Vulnerability (CIVN-2007-04)
- o Microsoft Internet Explorer "daxctle.ocx" KeyFrame Memory Vulnerability. (CIVN-2006-91)
- o Microsoft Internet Explorer WebViewFolderIcon Buffer Overflow Vulnerability (CIVN-2006-94)
- o RealPlayer Playlist Buffer overflow Vulnerability (CIVN-2007-138)

It has also been reported that mass attacks were launched against websites running phpBB through IFrame Injection redirecting innocent users to malicious websites.

[\[More\]](#)

Training

Workshop on "Database Security and Auditing" on 28th March, 2008

CERT-In conducted a one day Workshop on "Database Security and Auditing" March 28, 2008. The interactive workshop covered the following topics at length:

- Overview of Database Server Security & Auditing
- Securing and Auditing Oracle Database Server
- Secure configuration of MySQL Database Server
- SQL Server Security and Auditing

The presentation material is available at : [Database Security and Auditing](#)

Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during March 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 Excel | Microsoft Excel Multiple Vulnerabilities | March 12, 2008 | CIVN-2008-25 |
| Microsoft Outlook | Microsoft Outlook "mailto:" URI Handling Vulnerability | March 12, 2008 | CIVN-2008-26 |
| Microsoft Office | Multiple Remote Code Execution Vulnerabilities in Microsoft Office | March 12, 2008 | CIVN-2008-27 |
| Microsoft Office | Multiple Remote Code Execution Vulnerabilities in Microsoft Office Web Components | March 12, 2008 | CIVN-2008-28 |
| Microsoft Office | Multiple Vulnerabilities in Microsoft Office Components | March 12, 2008 | CIAD-2008-15 |
| Unix | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| MIT Kerberos | Multiple Vulnerabilities in MIT Kerberos | March 20, 2008 | CIAD-2008-16 |
| Cisco | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Cisco | Cisco Secure Access Control Server for Windows User-Changeable Password Vulnerabilities | March 20, 2008 | CIVN-2008-31 |
| Cisco | CiscoWorks Internetwork Performance Monitor Remote Command Execution Vulnerability | March 20, 2008 | CIVN-2008-32 |
| Miscellaneous | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| Symantec Products | Symantec Products Symantec Decomposer RAR File Handling Vulnerabilities | March 3, 2008 | CIVN-2008-23 |
| Wireshark | Wireshark (Ethereal) Multiple Protocol Vulnerabilities | March 4, 2008 | CIAD-2008-13 |
| Mozilla Products | MIME External-Body Heap Overflow Vulnerability in Mozilla Products | March 7, 2008 | CIVN-2008-24 |
| Sun Java | Sun Java Multiple Privilege Escalation Vulnerabilities | March 11, 2008 | CIAD-2008-14 |
| RealPlayer | RealPlayer ActiveX controls "Console" property heap memory corruption vulnerability | March 18, 2008 | CIVN-2008-30 |
| Mozilla Products | Multiple Vulnerabilities in Mozilla Products | March 28, 2008 | CIAD-2008-17 |
| Medium Vulnerabilities | | | |
| Unix | Title of Vulnerability | Discovery/Publish Date | CERT-In References & Patch Information |
| GNOME | GNOME Evolution Encrypted Message Format String Vulnerability | March 13, 2008 | CIVN-2008-29 |
| PHP | PHP 5 'php_sprintf_appendstring()' | March 21, 2008 | CVE-2008-1384 |

| | | Remote Integer Overflow Vulnerability | | | |
|-------------------------------|--------|---|--|----------------|---|
| OpenSSH | | OpenSSH Forwarded X Connection Information Disclosure Vulnerability | | March 24, 2008 | CVE-2008-1483 |
| Malicious Code Threats | | | | | |
| Title of Malicious Code | Type | Overview | Aliases | Discovery Date | References |
| InfoJack Trojan | Trojan | It has been observed that a Windows Mobile Pocket PC Trojan named InfoJack is circulating widely. The trojan propagates pretending to be a legitimate application for stock trading and collection of games which when installed by a user will infects their Mobile device. This Trojan also propagates when an infected memory card is inserted into a new mobile device. | WCE/Meiti-A [Sophos], WinCE/Infojack [McAfee], Trojan: WinCE/InfoJack [F-Secure] | March 3, 2008 | http://www.cert-in.org.in/virus/InfoJack_Trojan.htm |
| Scrapkut Orkut Worm | Worm | It has been observed that a worm named Scrapkut targeting Orkut users is spreading widely. Orkut is a social networking site. The worm uses active code injection to propagate itself to Orkut friends of victim user. A malicious scrap message is posted to victim's scrapbook containing a fake link to YouTube video purporting to be from a known member of its friend list. | W32/Scrapkut-A [Sophos], W32.Scrapkut [Symantec] | March 7, 2008 | http://www.cert-in.org.in/virus/ScrapkutOrkut_worm.htm |
| Zonebac Trojan | Trojan | It has been observed that a trojan named Zonebac is circulating widely. It is being propagated via malicious PDF files exploiting recently disclosed vulnerabilities in Adobe Reader/Acrobat described in CIAD-2008-09 [Multiple vulnerabilities in Adobe Reader/Acrobat]. A user could be tricked to open the malicious PDF file 1.pdf via compromised advertisements appearing on legitimate Web sites or | Trojan.Zonebac [Symantec] | March 13, 2008 | http://www.cert-in.org.in/virus/Zonebac_Trojan.htm |

| | | | | | |
|--------------|------|--|----------|----------------|---|
| | | compromised Web pages containing IFRAME or JavaScript which redirects user's browser to the malicious PDF file. | | | |
| Launcer Worm | Worm | It has been observed that a Worm named Launcer is spreading widely. The Worm spreads by copying itself to the removable media. After successful installation it displays fake warnings that the operating system on the compromised computer is pirated. It also closes the opened windows which contains the strings Winamp, Player, jet, CyberLink, VLC and displays a message on window mentioning " You are using a pirated(illegal) version of Microsoft. Some Applications could not be launced" . This window lures users to clicks upon the OK button to get the Internet Explorer executed on their system. | No Alias | March 29, 2008 | http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-032912-0913-99&tabid=1 |

Security News

FTP Hacking on the Rise

[Source: www.darkreading.com]

March 11 , 2008

The File Transfer Protocol (FTP) has attracted renewed interest lately, but not in a good way: The bad guys are now using the '70s disco-era file transfer technology to serve up bot malware, and even as a backdoor into some enterprises that neglect to lock down their FTP servers. Researchers at F-Secure have spotted a new wave of exploits that use FTP -- rather than a malicious URL, or the conspicuous email attachment -- to deliver their malware payloads. "As SMTP and HTTP are much better filtered for malware, FTP might be the best transport protocol for a virus writer," says Mikko Hypponen, chief research officer for F-Secure. "We've just started to observe this phenomenon -- it's not widespread yet, but likely to increase." Last month, researchers at Finjan stumbled onto a cache of stolen FTP server administrative credentials that put nearly 9,000 FTP servers at some major global companies at risk, demonstrating just how widespread the old-school FTP remains at many organizations. Cybercriminals were selling a new crimeware package that would automatically infect those servers, some of which were from the world's top 100 domains. (See [Stolen FTP Credentials Offered for Sale: Major Firms at Risk.](#))

[More]

Mass compromise powers massive drive-by download attack

[Source: www.theregister.co.uk]

March 13, 2008

More than 10,000 web pages have been booby trapped with malware in one of the largest attacks of its kind to date. Compromised web pages include travel sites, government websites, and hobbyist sites that have been modified with JavaScript code that silently redirects visitors to a site in China under the control of hackers. Miscreants likely reprogrammed the web pages after scanning the net for insecure servers. The malware cocktail attempts to exploit vulnerabilities in Windows, RealPlayer, and other applications to break into insecure PCs, according to an analysis by net security firm McAfee. Components of the malware attempt to steal passwords to online games while others leave a back door that allows the installation of additional malicious programs. McAfee Avert Labs first spotted this attack on Wednesday, 12 March. Of the 10,000 pages that were compromised, a number have already been cleaned up. A single organisation or small group is likely behind this attack, as the malicious code on all these pages is served up from the same server in China. Craig Schmugar, threat researcher at McAfee Avert Labs, said the attack illustrated that the conventional wisdom that surfers are safe providing they stick to trusted sites (and away from warez and porn) no longer holds true.

[More]

WhiteHat: 90% of Sites Still Vulnerable

[Source: www.darkreading.com]

March 25, 2008

After years of fighting the hacker wars, today's Websites are still a long way from being secure, according to a new research report. According to a report issued yesterday by WhiteHat Security, nine out of 10 Websites still have at least one vulnerability that attackers could exploit. On average, there are about seven flaws on each site studied.

"While the security posture of some industries is better than others, the difference is largely insignificant when it comes to preventing a Website from becoming compromised -- attackers only need to exploit a single vulnerability," the report says.

Cross-site scripting (XSS) is still the top category of vulnerabilities, appearing in approximately 70 percent of Websites, WhiteHat says. But the researchers are predicting that cross-site request forgery (CSRF) will eventually take the No. 2 spot behind XSS. "Attackers using CSRF can easily force a user's Web browser to send unintended HTTP requests, such as fraudulent wire transfers, changes to passwords and download of illegal content," the report says.

"Effective automated CSRF detection techniques have eluded all technology scanning vendors in the space, making identification a largely manual process." Despite high-profile breaches at chains such as TJX and Hannaford, the retail industry is still performing better than other verticals in terms of protecting Websites from attacks, WhiteHat says. The insurance industry tops the list of the most poorly-protected, with 84 percent of Websites having vulnerabilities that fall into the urgent, critical, or high severity ranking.

[More]

Hackers step up search results attack

[Source: www.vnunet.com]

March 31, 2008

A malware attack targeting search engine results is continuing to haunt several high-profile sites. The attack uses the common cross-site scripting practice of embedding pages with small IFrame tags which redirect the user to a malicious page on a third-party site. Researchers claimed that the latest attack is unique in that it targets search engine results. The hackers have compromised search result pages, using search engine optimisation techniques to hijack search results and send users to sites which host malicious downloads. Among the sites said to be compromised are major news outlets ABC, USAToday and Forbes, and retailers Wal-Mart, Target and Sears. Security researcher Dancho Danchev said in a blog posting that the attacks have been lingering on the web for more than two weeks, despite efforts by Google to delete infected pages from its cache. Danchev estimates that up to one million different search queries will lead users to the infected pages.

[More]

Stolen credit card supermarket exposed

[Source: www.computerworlduk.com]

March 27, 2008

Security firm Finjan has uncovered a website supermarket for stolen card data.

The 'SellCVV2' website was found to be trading the card numbers and other data in a number of sophisticated ways. Criminals visiting the site would be able to earn discounts based on volume bought and choose from a range of tiers, starting at the least valuable Classic Visa or MasterCard - those with the lowest credit limits - through more valuable Gold, Platinum, and Corporate levels. According to Finjan, prices ranged from \$38 (£20) for small volumes of premium card numbers, down to \$10 (£5) for the equivalent low-limit cards in chunks of 100 at a time. Criminals worried about being stung themselves by non-working cards were being offered 'guarantees' as well as trial data sets.

No breakdown was given on where or how the cards might have been stolen, but they are believed to be from around the globe and possibly culled using online Trojan-related techniques. "The site, which appears to use Google's Blogspot service, is typical of a number of portals promoting the exchange of fraudulent card data. But what is apparent from the SellCVV2 site is the level of commercialisation of the traders involved," said Finjan's CTO Yuval Ben-Itzhak.

[More]

Microsoft warns of targeted Word attack

[Source: www.securityfocus.com]

March 24, 2008

Software giant Microsoft warned on Friday that some customers have reported detecting attacks using Microsoft Word and a previously unknown vulnerability in Microsoft's Jet database engine. The attack uses an e-mail message with two attachments -- a Word file and a Microsoft Jet database file -- although Microsoft is investigating whether other programs could also be used, the company said in a security advisory published on Friday. While the software giant has stated that Microsoft database files (.mdb) should be considered unsafe, and do not execute automatically, under the attack conditions described in the latest attacks the database files does execute, security firm McAfee stated in its research blog. "Up until recently attackers typically exploited MS Jet DB vulnerabilities through MDB files, and therefore Microsoft stuck to their 'MDB files are unsafe' story -- well, that's changed," Craig Schmutz, senior antivirus researcher at security firm McAfee, wrote in the post. Flaws in Microsoft's Office productivity applications have become standard weapons for fraudsters conducting targeted attacks aimed at high-level managers and executives. While ten or fewer high-severity flaws were reported in the five major component applications of Microsoft Office each year from 2002 to 2006, at least 26 high-severity flaws were reported in Office applications last year, according to data from the National Vulnerability Database. Earlier this month, Microsoft patched a dozens flaws in Office applications.

[More]

Engineer Gets 24 Year Sentence For Trying To Steal Navy Secrets

[Source: www.informationweek.com]

March 04, 2008

A Chinese-born engineer convicted of conspiring to pass U.S. military secrets to the People's Republic of China was sentenced Monday to 24 years and five months in federal prison. Chi Mak, 65, of Downey, Calif., was formerly employed by defense contractor Power Paragon. He was found guilty last May of trying to obtain U.S. Navy submarine technology and to illegally export that information to China.

"This lengthy prison sentence ensures that Chi Mak will never again steal American military secrets for the benefit of another nation," U.S. Attorney Thomas P. O'Brien said in a statement. "Chi Mak betrayed the United States and endangered our national security, as well as the brave men and women of our armed forces." According to the U.S. Department of Justice, an investigation conducted by the FBI and the Naval Criminal Investigative Service found that co-conspirators from the PRC instructed Mak to obtain specific defense information about current and future naval warship systems. Mak was advised to

attend seminars to collect sensitive, restricted information discussed there and to compile that information on CD-ROM discs. Mak and his wife, Rebecca Laiwah Chiu, assembled the information on discs and gave the discs to Mak's brother, Tai Mak, whose son, Yui "Billy" Mak, helped encrypt the data on the discs. Officials discovered the discs in October 2005 when Tai Mak and his wife, Fuk Heung Li, tried to board a flight for China at Los Angeles International Airport. The co-conspirators in the case all pleaded guilty following Chi Mak's conviction. Tai Mak and Chiu await sentencing in April and May, respectively. Li and Billy Mak were sentenced to time served and now await deportation to China.

[More]

Cyber Attacks Target Pro-Tibet Groups

[Source: www.informationweek.com]

March 21, 2008

A shadow war against organizations supporting Tibetan protesters has erupted in cyberspace, mirroring efforts by Chinese authorities to quell unrest in the Tibet.

"Somebody is trying to use pro-Tibet themed e-mails to infect computers of the members of pro-Tibet groups to spy on their actions," said Mikko H. Hypponen, chief research officer at F-Secure, in a blog post on Friday. "And this is not an isolated incident. Far from it." The cyberattack involves sending e-mail messages to mailing lists, online forums, and people known to be affiliated with pro-Tibet groups. To enhance their legitimacy, the messages contain information related to recent events in Tibet and may appear to come from a trusted person or organization. But the content is simply bait, a social engineering con, to get recipients to open the documents and trigger an exploit. "The exploit silently drops and runs a file called C:\Program Files\Update\winkey.exe," explains Hypponen. "This is a keylogger that collects and sends everything typed on the affected machine to a server running at xsz.8800.org. And 8800.org is a Chinese DNS-bouncer system that, while not rogue by itself, has been used over and over again in various targeted attacks."

Efforts by Chinese authorities to contain protests in Tibet and limit media access to the country have been widely reported. Reporters Without Borders on Thursday said it had identified more than 40 serious violations of the rights of foreign journalists in Tibet and China since March 10. And access to YouTube and mainstream media sites like the BBC, CNN, and Yahoo also has been restricted.

[More]

Trend Micro details its recent failed web attack

[Source: www.informationweek.com]

March 14, 2008

Security software company Trend Micro on Friday confirmed that it had suffered a Web attack early in the week in which hackers embedded malicious code on the security vendor's Web site, but said its investigation showed no one visiting the site was affected.

The code inserted in some Web pages of the site was meant to redirect the visitor to a malicious server that would download malware capable of stealing passwords on an infected computer, Trend Micro spokesman Michael Sweeny said. The attempt, however, failed.

"We now know that the redirect on the site was broken code," Sweeny said. "It didn't work properly and didn't infect anybody." Sweeny declined to provide further details, but said that such attacks in general typically involve the use of ActiveX controls, a Microsoft technology used in building user interfaces; and JavaScript, a popular scripting language supported by most Web browsers. Hackers have exploited such technologies for the last couple of years in trying to embed malicious code in popular Web sites to redirect visitors to malware-carrying servers. Such redirections happen behind the scenes, so the victim doesn't know malware is being downloaded.

Sweeny said the practice is widespread and even security vendors "need to continue to be constantly vigilant, take corrective action, and harden our infrastructure."

[More]

Google report highlights spam as top security issue

[Source: www.informationweek.com]

March 07, 2008

Having recently acquired messaging security company Postini, Google now finds itself in the threat-prediction business. And as is the case with just about every other computer security company, Google has research to show everyone how dangerous the online world has become. Thus we come to the 2008 Annual Google Communications Intelligence Report. Google's security forecast calls for continued spam-blended virus attacks with an increasing focus on identity theft. The attacks will rely on social engineering, the report says, and will rely on messages that reference current events, like the upcoming Olympic Games and natural disasters. "Further, virus attacks will target executives at specific companies whose intellectual property is deemed valuable on the black market by the hackers," the report says. "These attacks will appear to come from legitimate business agencies, such as the Internal Revenue Service, the Better Business Bureau, and the Securities and Exchange Commission." Google said it expects such incidents will prompt organizations to eliminate live links in customer e-mail communications. Google also anticipates an increase in the deployment of outbound message monitoring systems, in the adoption of encryption, and in the use of archiving technology. Identity theft attacks, Google says, will be launched increasingly from sites that let users create and post their own content. And there's this shocker: Google predicts business will be good. "In addition, hosted solutions (SaaS) will play a major role in reducing the cost and complexity of these products," the report says.

Surely, it's a coincidence that Google's Postini sells hosted solutions. Oh, and by the way, hosted messaging costs \$5,000 to \$17,000 annually, compared with \$20,000 to \$69,000 for traditional servers and software, according to Google's calculations. Though Google may be biased about this, it's worth considering whether the company might simultaneously be right.

[More]

Systems disclose sensitive data via SNMP

[Source: www.heise-online.co.uk]

March 04, 2008

A scan of 2.5 million randomly selected IP addresses by Adrian Pastor of GNUCitizen has revealed 5320 systems that can be accessed using SNMP over the internet. Communication via SNMP is usually in plain text, including the exchange of passwords or "community strings". For security reasons, if SNMP is in use, it should be blocked at the network perimeter. However this precaution is often omitted, and the community strings are frequently left by administrators at their well-known default values. According to the report by Pastor, the most frequently detected systems were appliances such as Zyxel Prestige routers, Apple AirPort and base stations, Netopia and Cisco routers and Touchstone VoIP modems from Arris. Windows 2000 servers were also encountered. In his test, Pastor queried only the object ID (OID) 1.3.6.1.2.1.1.1.0, which returns the router model and manufacturer. He did not look for

specific vulnerabilities. Pastor has previously published an analysis which reveals numerous vulnerabilities in popular routers such as the Zyxel Prestige, including SNMP exposures. In principle, SNMP access has been shown to reveal user name lists on Windows 2000 servers, DSL login data on BT Voyager routers, administrator passwords on HP printers and other parameters including login data for dynamic DNS on Zyxel routers.

[\[More\]](#)

ID fraud - the top 25 leaky institutions

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

March 07, 2008

Research by the University of California has identified twenty-five American corporations that top the bill for customer complaints about ID fraud. Data obtained from the Federal Trade Commission under the US Freedom of Information Act reveal just how leaky financial services companies can be. Nevertheless, in terms of raw complaints count, Chris Hoofnagle of the Berkeley Center for Law and Technology found that a small proportion of even this top 25 dominate the field. Bank of America/MBNA came top for raw complaints count, accounting for 7.24 per cent of all complaints in the 2006 sample: almost half as many again as the nearest contender, the AT&T group. Despite some high profile instances of identity fraud in the past, eBay/PayPal came near the bottom of the list at 0.83 per cent of the total complaints. Several ISPs feature in the top 25: notably T-Mobile and Comcast, but banks clearly outperform them in the leakiness stakes, and it seems that in general the larger the bank the more it tends to leak. The one exception to this proved to be HSBC, which had an estimated 20 per cent more incidents per billion dollars deposits than Bank of America/MBNA. However, the relative size of the two banks tends to disguise the real scale of the problem. Whereas HSBC averaged 190 complaints per month, Bank of America/MBNA averaged 1117.

[\[More\]](#)