



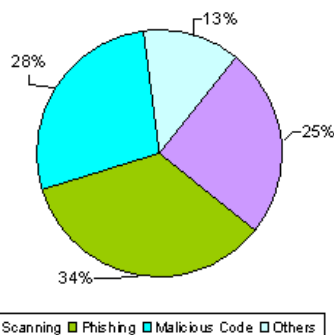
CERT-In Monthly Security Bulletin April 2008

Cyber Intrusion Trends

In this month 61 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 34% phishing incidents were reported in this month. 25% unauthorized scanning, 28% incidents related to virus/worm under the Malicious code category and 13% incidents related to technical help under the Others category were reported in this month. As compared to previous month the number of phishing incidents, scanning incidents and incidents related to virus/worm under the Malicious code category have increased while incidents related to technical help under the Others category have decreased.

In this month CERT-In tracked 14 C&C (Command & Control) servers and 8,580 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 April 2008



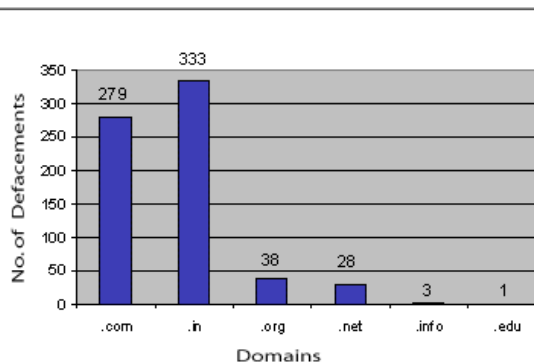
Indian Websites Defacement

In total 682 Indian websites were defaced during April 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 April 2008

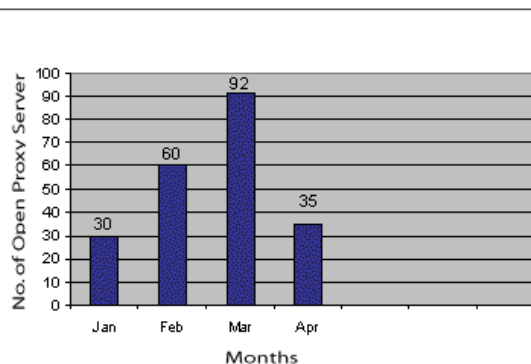


Open proxy servers

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 35 open proxy servers functioning in India during April 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 - April 2008



Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during April 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	Multiple Vulnerabilities in Microsoft Windows and Office Components: Microsoft Project, Microsoft Visio, Internet Explorer, Windows DNS Client, Windows Kernel, VBScript and JScript	April 10, 2008	CIAD-2008-20		
Microsoft	Microsoft Project Memory Validation Vulnerability	April 10, 2008	CIVN-2008-37		
Microsoft	Microsoft windows GDI Files Remote Code Execution Vulnerability	April 10, 2008	CIVN-2008-40		
Microsoft	Microsoft Windows VBScript and JScript Remote Code Execution Vulnerability	April 10, 2008	CIVN-2008-41		
Microsoft Internet Explorer	Microsoft Internet Explorer 'hvxz.dll' ActiveX Control Memory Corruption Vulnerability	April 10, 2008	CIVN-2008-42		
Microsoft	Microsoft Data Stream Handling Memory Corruption Vulnerability	April 10, 2008	CIVN-2008-43		
Microsoft Internet Explorer	Microsoft Internet Explorer Popup Window Address Bar URI spoofing vulnerability	April 11, 2008	CIVN-2008-45		
Database	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Oracle	Multiple Vulnerabilities in various Oracle products	April 23, 2008	CIAD-2008-22		
Cisco	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Cisco	Cisco Unified Communications Disaster Recovery Framework Command Execution Vulnerability	April 04, 2008	CIVN-2008-33		
Cisco	Multiple vulnerabilities in Cisco IOS	April 04, 2008	CIAD-2008-18		
Cisco	Cisco Network Admission Control Shared Secret Disclosure Vulnerability	April 29, 2008	CIVN-2008-48		
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Wireshark	Multiple Vulnerabilities in Wireshark	April 04, 2008	CIAD-2008-19		
Apple QuickTime	Multiple vulnerabilities in Apple QuickTime	April 11, 2008	CIAD-2008-21		
Mozilla Products	JavaScript Garbage Collector Vulnerability in Mozilla Products	April 23, 2008	CIVN-2008-47		
Adobe Flash player	Multiple Remote code Execution Vulnerabilities in Adobe Flash player	April 25, 2008	CIAD-2008-23		
Medium Vulnerabilities					
Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Microsoft	Microsoft Crypto API X.509 Certificate Validation Remote Information Disclosure Vulnerability	April 04, 2008	CIVN-2008-34		
Microsoft	Microsoft Visio Object Header and Memory Validation Vulnerabilities	April 10, 2008	CIVN-2008-38		
Microsoft	Microsoft DNS stub resolver Spoofing Vulnerability	April 10, 2008	CIVN-2008-39		
Windows Kernel	Windows Kernel Elevation of Privilege Vulnerability	April 10, 2008	CIVN-2008-44		
Microsoft Windows	Microsoft Windows SeImpersonatePrivilege Local Privilege Escalation Vulnerability	April 19, 2008	CIVN-2008-46		
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
OpenSSH	OpenSSH Forwarded X11 Connection Information Disclosure Vulnerability	April 07, 2008	CIVN-2008-35		
Apache	Apache-SSL Authentication Bypass Vulnerability	April 09, 2008	CIVN-2008-36		
phpMyAdmin	phpMyAdmin HTTP POST Request File Disclosure Vulnerability	April 23, 2008	CVE-2008-1924		
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
		It has been observed that a			

Bancorkut Worm	Worm	<p>mass mailing worm named Bancorkut is spreading widely. It spreads when a user clicks upon the malicious link embedded within the email message body. The worm collects the confidential information such as username and passwords from the infected system and some websites to send the collected information to a remote server under attacker's control. These credentials are further used for performing illegal banking activities.</p>	No Alias	April 08, 2008	http://www.cert-in.org.in/virus/Bancorkut_Worm.htm
Goldun Trojan	Trojan	<p>It has been observed that an information stealing Trojan called Goldun is spreading via email. It comes as an email attachment or as a malicious link inside the email body which pretends to appear from E-Gold online bank or from Yahoo Shopping. The "subject line" of the email entices users to open the attachment or visit the malicious link and install the trojan on their system. Upon successful installation the Trojan opens a backdoor and steals confidential information such as usernames and passwords for financial accounts from the infected system and sends this information to the remote server which is under the control of the attacker.</p>	Trojan.Goldun.G [Symantec]	April 15, 2008	http://www.cert-in.org.in/virus/Goldun_Trojan.htm
		<p>It has been observed that a trojan named Vundo is circulating widely. It is</p>			

Trojan Vundo	Trojan	dropped by some dropper as a DLL component on user's system. It installs itself as browser helper object (BHO) and gets injected into Explorer DOT exe . After successful installation it generates popup ads for rogue antispayware installation on the infected system which may appear as visible or hidden window.	Win32/Vundo! generic [CA], W32/Virtumonde.TY [Norman], Adware.VirtuMonde [Symantec]	April 25, 2008	http://www.cert-in.org.in/virus/Trojan_Vundo.htm
W32.Zatyudi.A	Worm	It has been observed that a Worm named Zatyudi is spreading widely. It spreads by copying itself to network shares and removable drives with the file name SETUP.exe which is kept in an achieve with .zip extension..After successful infection the worm collects email addresses from the compromised computer and attempts to connect to certain websites to send a notification of the infection. It also attempts to terminate certain processes and services whose name or description contains the strings such as: SysMech, PDFIND, avtask, mav, process.	No Alias	April 30 , 2008	http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-043015-2430-99&tabid=1

Security News

India assists Mauritius to fight cyber crime

[Source: www.crime-research.org]

28th April , 2008

A team of Indian experts in computer technology is expected in Mauritius Monday to assist that African country in the setting up a "National Computer Emergency Response Team" (CERT-MU) which will help to secure computer data, an official source said on Friday. The official said that CERT-MU had become a priority project on information and communication technologies (TIC) which is aimed at reducing the vulnerability of countries facing cybercrime threats, broadcasting and disseminating alert programmes in the face of such threats, and co-ordinating actions to be undertaken in response to offences committed through the Internet. "CERT-MU will also ensure co-operation between state services, the private sector and the public in such cases," he said. According to the official, the project will help to create direct jobs in the short term for university graduates in computer technologies, and in the long term a more considerable number of jobs will be created in order to increase the resilience of countries in case of cybercrime threats.

[More]

Department of Homeland Security website hacked!

[Source: www.theregister.co.uk]

25th April 2008

The sophisticated mass infection that's injecting attack code into hundreds of thousands of reputable web pages is growing and even infiltrated the website of the Department of Homeland Security. While so-called SQL injections are nothing new, this latest attack, which we reported earlier, is notable for its ability to infect huge numbers of pages using only a single string of text. At time of writing, Google searches here, here and here showed almost 520,000 pages containing the infection string, though the exact number changes almost constantly. As the screenshot below shows, even the DHS, which is responsible for protecting US infrastructure against cyber attacks, wasn't immune. Other hacked sites include those belonging to the United Nations and the UK Civil Service.

[\[More\]](#)

U.S. reveals plans to hit back at cyberthreats

[\[Source: www.news.com\]](http://www.news.com)

04 April , 2008

The U.S. Air Force Cyber Command is developing capabilities to inflict denial of service, confidential data loss, data manipulation, and system integrity loss on its adversaries, and to combine these with physical attacks, according to a senior U.S. general. Air Force Cyber Command (AFCYBER), a U.S. military unit set up in September 2007 to fight in cyberspace, is due to become fully operational in the autumn under the aegis of the U.S. Eighth Air Force. Lieutenant general Robert J. Elder Jr., who commands the Eighth Air Force's Barksdale base, told ZDNet.co.uk at the Cyber Warfare Conference 2008 that Air Force is interested in developing its capabilities to attack enemy forces as well as defend critical national infrastructure. "Offensive cyberattacks in network warfare make kinetic attacks more effective, (for example) if we take out an adversary's integrated defense systems or weapons systems," Elder said. "This is exploiting cyber to achieve our objectives." However, this is a double-edged sword, as adversaries will also attempt to develop similar capabilities, especially considering the U.S. military's heavy use of technology, said Elder.

"Terrorists and criminals are doing the same thing. We depend so heavily as a military on the use of cyber, we have to be cautious about it," Elder said. "Cyber gives us a huge advantage, but adversaries look at our capabilities and see areas they can undermine. We need to protect our asymmetric advantage--on the one hand by having people further exploit cyber, and on the other by having mission assurance."

[\[More\]](#)

New attack technique threatens databases

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

28th April 2008

Database security expert David Litchfield has published details of a new type of database attack technique. Lateral SQL injection creates a means for hackers to access database data or inject hostile code onto vulnerable systems. Exploitation is difficult and only possible in limited circumstances, Litchfield notes. Nonetheless, the discovery of the approach - a variant on earlier attack methods - means that database admins can no longer consider DATE or NUMBER data types safe from attack. Lateral SQL injection is a variant of SQL injection attacks, one of the most common methods for attacking database systems. Litchfield first outlined the new approach during a presentation at the Black Hat security conference in Washington in late February. He published details of the approach in a paper (pdf) last week. SQL injection attacks involve attempts by hackers to trick database servers into running SQL commands, typically after crackers use vulnerabilities to inject character strings onto databases. Lateral SQL injections are a variant of the theme that use other forms of data - DATE and NUMBER data types - to much the same effect. The new attack relates to the Procedural Language/SQL programming language used by Oracle developers, and involves the possible development of exploits that involve hostile DATE or even NUMBER data types instead of user input, the fodder for conventional SQL injection attacks.

[\[More\]](#)

Huge Web hack attack infects 500,000 pages

[\[Source: www.computerworld.com\]](http://www.computerworld.com)

25th April , 2008

Attacks on legitimate Web domains, including some belonging to the United Nations, have expanded dramatically this week, security researchers said today. Hundreds of thousands of pages have been hacked already. One antivirus vendor said the sites might have been compromised through a "security issue" in Microsoft Web server software that has been reported to Microsoft Corp. engineers. On Wednesday, several security companies, including San Diego-based Websense Inc., said large numbers of legitimate sites, including ones with URLs belong to the U.N., had been hacked and were serving up malware. Those latest compromises were only the most recent SQL injection attacks, however. Similar attacks have been launched since the first of the year and were last detected in large numbers in March. Earlier in the week, Dan Hubbard, Websense's vice president of security research, estimated the number of hacked sites to be in the low six figures. By today, that number had soared as firms such as Panda Security pegged the number at 282,000, and F-Secure said its infected-page count was above a half-million.

[\[More\]](#)

Web infection attacks more than 100,000 pages

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

24th April, 2008

Hackers have injected malicious code into hundreds of thousands of reputable web pages, turning them into launchpads for attacks that silently install malware on the machines of those who visit them. The UK 's Civil Service and the United Nations were among those who had been hacked. This Yahoo search returned 173,000 results for the term "nihaorr1," which is part of the address that uses a malicious javascript to attack end users. The rogue URL horns its way onto web pages through a SQL injection vulnerability in IIS and possibly other web servers, according to IT-related web forums. Websense, which wrote about the mass infection Tuesday, said the attackers perpetrated a similar assault a few weeks ago on news and travel sites. Little is known about the group responsible, except that they're using the nihaorr1.com domain name, which appears on the surface to be registered to someone in Shanghai. Users visiting an infected site will be redirected to a series of sites that eventually tries to exploit eight different vulnerabilities, all of which have been patched.

[\[More\]](#)

Microsoft Botnet-hunting Tool Helps Bust Hackers

[Source: www.pcworld.com]

29th April , 2008

Botnet fighters have another tool in their arsenal, thanks to Microsoft.

The software vendor is giving law enforcers access to a special tool that keeps tabs on botnets, using data compiled from the 450 million computer users who have installed the Malicious Software Removal tool that ships with Windows. Although Microsoft is reluctant to give out details on its botnet buster -- the company said that even revealing its name could give cyber criminals a clue on how to thwart it -- company executives discussed it at a closed door conference held for law enforcement professionals Monday. The tool includes data and software that helps law enforcers get a better picture of the data being provided by Microsoft's users, said Tim Cranton, associate general counsel with Microsoft's World Wide Internet Safety Programs. "I think of it ... as botnet intelligence," he said. Microsoft security experts analyze samples of malicious code to capture a snapshot of what is happening on the botnet network, which can then be used by law enforcers, Cranton said. "They can actually get into the software code and say, 'Here's information on how it's being controlled.'" Botnets are networks of hacked computers that can be used, almost like a supercomputer, to send spam or attack servers on the Internet. They have been on Microsoft's radar for about four years, ever since the company identified them as a significant emerging threat. In fact, the software vendor has held seven closed-door botnet conferences for law enforcement officials over the years, including an inaugural event in Lyon, France, hosted by Interpol, Cranton said. Microsoft had not previously talked about its botnet tool, but it turns out that it was used by police in Canada to make a high-profile bust earlier this year. In February, the Sûreté du Québec used Microsoft's botnet-buster to break up a network that had infected nearly 500,000 computers in 110 countries, according to Captain Frederick Gaudreau, who heads up the provincial police force's cybercrime unit. The case illustrates how useful Microsoft's software and data can be.

[More]

Cyber criminals to target mobiles

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

29th April , 2008

Mobile networks and handsets are becoming more of a target for criminals with a technical bent, security experts are warning. "There's a real transition from online in to the mobile space," said Simeon Coney, head of business development at Adaptive Mobile, which helps operators keep an eye on the malicious traffic flowing across their networks. In the PC world malicious programs started with viruses designed to be a nuisance but now they have evolved into software designed solely to help their creators make money. There is no doubt that hi-tech criminals have cottoned on to the fact that making malicious programs, be they trojans or viruses, can be a very profitable business. That evolutionary process took, said Mr Coney, about 15 years.

[More]

Phishers offer credit card discounts to prospective marks

[Source: www.theregister.co.uk]

10th April 2008

Phishing fraudsters are using promises of financial discounts to trick unwary users into handing over their credit card details. Scam emails that form the basis of the fraud claim to be part of MasterCard's SecureCode scheme. Con men are attempting to exploit a lack of familiarity with the recently introduced programme, which ironically promises to offer greater security to credit card transactions. Phishing emails attempt to lure prospective marks into "signing up" to SecureCode, by offering a 16 per cent discount on future purchases made with the card. More typically, phishing campaigns ask users to confirm details for maintenance purposes or due to database corruption. In reality, users that click on the link contained within the email are redirected to a phishing site, set up to look almost identical to the genuine MasterCard website. Visitors are then asked to supply confidential information including credit card expiration date, date of birth, and the three digit security code located on the back of the card - enough information for the cybercriminals to abuse the compromised account themselves and sell on the details through the underground black market. The scam emails were intercepted by net security firm Sophos. "MasterCard has been very successful in positioning SecureCode as the answer to online fraud, and with so many computer users growing increasingly worried about the risks of shopping online, the prospect of greater security and money off can be too much to resist," said Carole Theriault, senior security consultant at Sophos.

[More]

'Long-Term' Phishing Attack Underway

[Source: www.darkreading.com]

28th April , 2008

The notorious Rock Phish gang has added a new twist to its phishing exploits that doesn't require its victim to visit a malicious Website -- instead, it just loads a malicious keylogging Trojan onto the victim's machine that steals information or credentials. Both Trend Micro and F-Secure over the past few days spotted new iterations of the attack, which was first reported by RSA last week. The latest tack is phishing emails posing as Comerica Bank and Colonial Bank that ask banking customers to renew their digital certificates. When they click on the link for more information on the phony renewal process, it downloads the nasty Trojan onto their desktops. "In a way, it's so blatant that it reminds me of the worms of '04 and '05... such as Bagel. They would come via email, and you'd receive an executable file" in them, says Jamz Yaneza, threat research project manager for Trend Micro.

The danger of the so-called Zeus Trojan is that it can execute what Yaneza calls a "long-term" phishing attack on the victim. "It can stay there and log credentials, personal information, and steal personal information. Basically anything you type," he says. The version Trend has been studying has the ability to receive downloaded updates to itself, he says.

[More]

Move over Storm - there's a bigger, stealthier botnet in town

[Source: www.theregister.co.uk]

7th April , 2008

This story was updated to correct information about detection of Kraken. 20 percent of PCs using anti-virus products detect the malware, not 20 percent of

anti-virus products, as erroneously reported earlier. Researchers have unearthed what they say is the biggest botnet ever. It comprises over 400,000 infected machines, more than twice the size of Storm, which was previously believed to be the largest zombie network. Machines from at least 50 Fortune 500 companies have been observed to be running the malicious software that's at the heart of "Kraken," the botnet that security firm Damballa has been tracking for the last few weeks. So far, only about 20 percent of PCs running anti-virus products are detecting the malware. Just as a con artist might throw off detectives by changing his hair color or other physical characteristics, Kraken's ability to morph its code base has allowed it to evade the majority of malware detectors. "Kraken, despite being on all these people's computers, has such low anti-virus coverage," said Paul Royal, principal researcher at Atlanta-based Damballa. "Anti-virus companies can't keep up with the arms race because of the number of variants and the frequency of the updates." In addition, the code inside the executable file that infects a PC has been arranged in a way that makes it hard for malware analysis tools to accurately disassemble the malicious program. "It raises the question of whether this basically has been authored specifically with anti-virus evasion in mind," Royal added. Kraken most likely spreads by tricking end users into clicking on a malicious file that's disguised as an image. When it's executed, the program automatically copies itself to the hard drive in a slightly altered format. In the event AV programs are eventually able to recognize the original file, Kraken can use the altered file to reinfect the machine. Moreover, zombie machines regularly update themselves as an additional measure to prevent detection.

[\[More\]](#)

Kraken stripped of World's Largest Botnet crown (maybe)

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

9th April 2008

If you're looking for a good reason why security professionals might want to pool their research about botnets and other cyber threats, look no further than findings released earlier this week about a botnet dubbed Kraken. Zombie hunters at Damballa said they were tracking a new bot army that claimed more than 400,000 infected machines and had managed to infiltrate at least 50 networks belonging to Fortune 500 companies. The malware at the heart of Kraken, as they dubbed the botnet, was undetected on 80 percent of computers running anti-virus protection. The thing is, other researchers say Kraken isn't new at all. According to Joe Stewart, a cyber gumshoe at SecureWorks, the reported bot army is actually one that goes by the name Bobax and is one of the oldest known botnets used for spamming. Damballa researchers respectfully reject this contention, saying Kraken bots use fundamentally different means to connect to command and control channels, where they receive their spamming instructions. The mix-up is understandable, given the way malware is spread. Distributors frequently infect a PC with multiple bots at the same time, and often use vastly different variants, all making identification difficult. Complicating matters, competing botnet operators frequently appropriate snippets of code belonging to their competitors.

[\[More\]](#)

Spam filtering services throttle Gmail to fight spammers

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

10th April 2008

The growing abuse of webmail services to send spam has led anti-spam services to throttle messages from Gmail and Yahoo! Over recent months security firms have reported that the Windows Live CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) used by Hotmail, and the equivalent system at Gmail, have been broken by automated attacks. CAPTCHAs typically help ensure that online accounts can't be created until a user correctly identifies letters depicted in an image. The tactic is designed to frustrate the use of automated sign-up tools by spammers and other miscreants. Obtaining a working Gmail account has a number of advantages for spammers. As well as gaining access to Google's services in general, spammers receive an address whose domain is highly unlikely to be blacklisted, helping them defeat one aspect of anti-spam defences. Gmail also has the benefit of being free to use. Anti-spam filtering services such as MessageLabs have responded by throttling or slowing down the connection. "We're seeing more spam coming from Gmail and Yahoo!. Where a service is widely abused its reputation goes down and it's held back in the queue. This happens automatically," explained MessageLabs security analyst Paul Wood. The approach, one stage in a multi-stage scanning and filtering process, is designed to make life difficult for spammers using botnets to send spam through compromised webmail accounts. "These traffic management controls are not designed to block messages, they are intended only to slow down their transit. For messages that are subsequently blocked there should be a reason given in the non-delivery report," Wood told EI Reg.

[\[More\]](#)

Google to open suspect Orkut albums to Brazil police

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

12th April 2008

Google is to give Brazilian police access to 3,261 private photo albums on social networking website Orkut, which may contain child pornography. The move is part of a strategy announced by the head of the company in Brazil, Alexandre Hohagen, to a Senate Committee set up to investigate cases of paedophilia in the country. During a hearing this week, Alexandre Hohagen and Felix Ximenes, director of communication for Google Brazil, claimed they are currently implementing more effective image filters that will detect and prevent the uploading of child pornography. Ximenes told The Register the new filter is 60 per cent more efficient than the current technology. "But I can't tell how you it works, or we would just be telling how to fool it and throwing away months of development." Orkut has more than 60 million users, most of them in Brazil. According to Sergio Suizama, the federal prosecutor for Sao Paulo, in the last two years nearly 90 per cent of the 56,000 complaints in Brazil about net-based paedophilia were linked to the website. Ximenes said that until September 2007, all requests for information about users suspected of crimes such as racism or paedophilia were sent to Google US to be examined. "But since then we have been dealing directly with that, providing the police with user IPs and navigation logs whenever it is requested. It's happened in more than 1,000 cases so far." He said giving investigators personal information about suspects and access to their private albums "is not an issue", but conceded that Google has not yet received any official communication, so he can't say when this information is to be handed out. Ximenes and Hohagen told the Senate panel that Orkut will keep users' navigation logs for six months, instead of the current 30 days. However, he explained there was a legislative grey zone regarding child pornography in Brazil.

[\[More\]](#)

Chinese spammers target 1,200 US, UK firms

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

11th April 2008

The Royal Institute of British Architects' (RIBA) members database was hacked at the weekend, causing the institute to close access to the members' area, which remains shut. RIBA reports that 1,200 other organisations in the US and UK have also been attacked in a similar way, but "neither the RIBA nor other organisations contacted have yet found any evidence of fraudulent activity or attempts to extract information from the databases". According to a RIBA spokeswoman, the attacker "planted a web address on the databases. The source has been traced to an organisation in China known for its large scale spamming. We cannot be certain of the purpose but it is likely to be the capture of email addresses." Technical staff at the institute spotted the problem and closed access to the database as a precaution. RIBA sent an email on Thursday warning its 40,000 members to keep an eye on bank accounts and credit card statements that may have been used for payments to RIBA. However, it assured them there is no evidence that any information was stolen. It has also reported the incident to the Metropolitan Police. The institute refused to comment on whether the database was encrypted or password protected.

[\[More\]](#)

Symantec internet security threat report thirteenth version released

[\[Source: www.symantec.com\]](http://www.symantec.com)

08 April 2008

The Symantec Internet Security Threat Report offers analysis and discussion of threat activity over a six-month period. It covers Internet attacks, vulnerabilities, malicious code, phishing, spam and security risks as well as future trends. The thirteenth version of the report, released April 8, 2008, is now available..

[\[More\]](#)

Yahoo! pimping malware from banner ads

[\[Source: www.symantec.com\]](http://www.symantec.com)

28th April 2008

Over the past three days, Yahoo has been exposing visitors to banner ads that try to trick them into installing malware, and there's no indication anyone at the company is even aware of the problem. According to Microsoft MVP Sandi Hardmeier's "Spyware Sucks" blog, the ads are displayed across a wide swath of the web portal's sprawling empire, including Yahoo Mail, Yahoo Groups and Yahoo Astrology. Hardmeier first sounded the alarm on Saturday, and yet on Monday, Yahoo continued to run the rogue ads, she reported. El Reg emailed three different Yahoo PR reps but never did get a response. "I wonder how many hits Yahoo gets per day, and how many people are being exposed to fraudware, while these advertisements are allowed to remain online," Hardmeier wrote.

The ads pitch women's deodorant, but behind the scenes, they contact servers that have been used by previous rogue ads targeting high-traffic websites. Typically, the ads produce a pop up that looks strikingly similar to official Windows dialog pop-ups that urge the end user to download software to fix problems. Expedia, Rhapsody, MySpace, Excite, Blick, and CNN.com have all served up similar malicious ads in the past.

[\[More\]](#)