



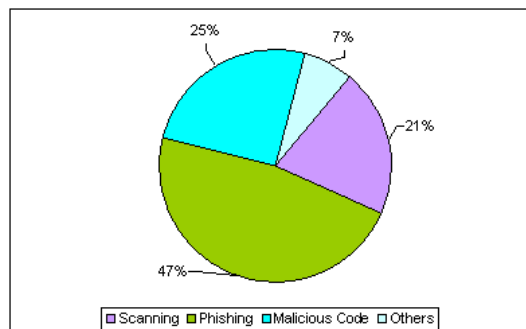
CERT-In Monthly Security Bulletin January 2008

Cyber Intrusion Trends

In this month 87 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 47% phishing incidents were reported in this month. 21% unauthorized scanning, 25% incidents related to virus/worm under the Malicious code category and 7% incidents related to technical help under the Others category were reported in this month. As compared to previous month the number of virus/worm related incidents have increased while scanning incidents have decreased.

In this month CERT-In tracked 2 C&C (Command & Control) servers and 2102 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 January 2008



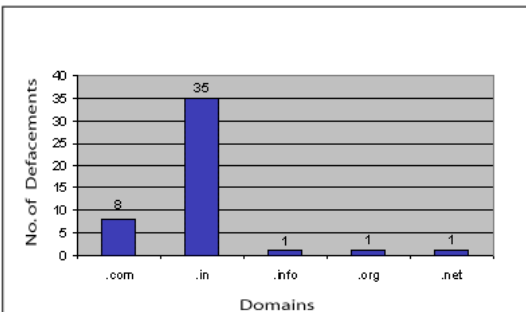
Indian Websites Defacement

In total 46 Indian websites were defaced during January 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. Multiple Vulnerabilities in PHP [CVE-2007-5898](#) , [CVE-2007-5899](#) , [CVE-2007-5900](#)
4. Denial of service vulnerability in PHP [CVE-2007-6039](#)

Statistics of Defaced Indian Websites in January 2008

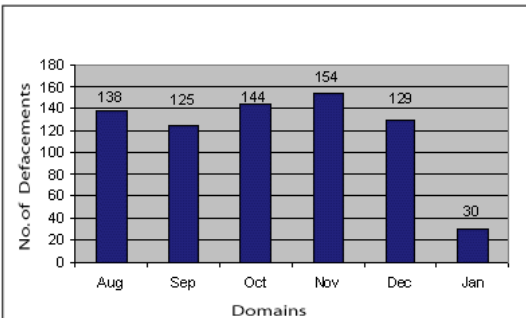


Open proxy servers

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 30 open proxy servers functioning in India during January 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 Aug 2007 - Jan 2008



Attack Trend

Websites compromised with malicious JavaScript injection propagating malware :

In this month various websites/domains are reported to be compromised and serving information stealing malware such as [Trojan Clampi](#) . These websites are injected with malicious JavaScript file known as "Random JS Toolkit" which is in turn infecting visitors of infected websites. Both the malicious binary and the malicious script are hosted on the same domain and visitors unknowingly get infected. The name of the malicious JavaScript file randomly changes because of dynamic embedding of scripts into the webpage. This technique is effectively evading the detection of its hosting on websites. Accordingly a new malicious binary gets dropped onto the user system on every visit.

[\[More\]](#)

Training

Workshop on "Mail Server Security " on 29th January, 2008

CERT-In conducted a one day Workshop on "Mail Server Security" January 29, 2008. The workshop focused on creating awareness among the systems/network administrators and mail server security professionals to secure mail servers in an enterprise/organisation in order to defend against attack. The interactive workshop covered the following topics at length:

- Overview of Mail Server Security
- Securing Sun Messaging Server
- Secure Configuration of Lotus Domain/Notes
- Securing Microsoft Exchange Server

The presentation material is available at : [Mail Server Security](#)

Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during January 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 Windows	Multiple Vulnerabilities in Microsoft Windows components : TCP/IP, LSASS		January 09, 2008	CIAD-2008-02	
Microsoft Windows	Microsoft Windows TCP/IP implementation vulnerabilities		January 09, 2008	CIVN-2008-02	
Microsoft office Excel	Remote Code Execution Vulnerability in Microsoft office Excel		January 19, 2008	CIVN-2008-05	
Unix	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Linux Kernel	Linux Kernel hrtimer_start(), shmem_getpage() and IPv6 Extended header vulnerability		January 02, 2008	CIAD-2008-01	
Linux kernel	"chrp_show_cpuiinfo function (chrp/setup.c) " denial of service in Linux kernel		January 29, 2008	CVE-2007-6694	
Database	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Oracle Database	Multiple Vulnerabilities in various Oracle products		January 24, 2008	CIAD-2008-05	
Cisco	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Cisco	Cisco Unified Communications Manager CTL Provider Heap Overflow		January 28, 2008	CIAD-2008-07	
Solaris	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Solaris	dotoproc() Routine Denial of Service Vulnerability in Solaris		January 24, 2008	CIVN-2008-07	
Solaris	libdevinfo(3LIB) - unauthorized file-access vulnerability in Solaris		January 24, 2008	CIVN-2008-08	
Solaris	libxml2 Denial of Service Vulnerability in Solaris		January 24, 2008	CIVN-2008-09	
Miscellaneous	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Real Player	Real Player Unspecified Buffer Overflow Vulnerability		January 09, 2008	CIVN-2008-01	
Apple QuickTime	Apple QuickTime RTSP buffer overflow Vulnerability		January 14, 2008	CIVN-2008-04	
Mozilla Firefox	Improper handling HTTP Basic Authentication on HTTP servers in Mozilla Firefox		January 18, 2008	CVE-2008-0367	
Winamp	Winamp Ultravox Streaming Metadata Parsing Remote Buffer Overflow Vulnerabilities		January 22, 2008	CIVN-2008-06	
Apple QuickTime	Apple QuickTime Multiple File Processing Code Execution Vulnerabilities		January 24, 2008	CIAD-2008-04	
Medium Vulnerabilities					
Microsoft	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Microsoft Windows	Microsoft Windows LSASS Privilege Escalation Vulnerability		January 09, 2008	CIVN-2008-03	
Unix	Title of Vulnerability		Discovery/Publish Date	CERT-In References & Patch Information	
Apache HTTP Server	Multiple Vulnerabilities in Apache HTTP Server		January 21, 2008	CIAD-2008-03	
Apache Tomcat	"SingleSignOn Valve" unauthorized disclosure of information in Apache Tomcat		January 22, 2008	CVE-2008-0128	
Apache HTTP Server	Cross-site scripting (XSS) vulnerability in the mod_negotiation module in the Apache HTTP Server		January 24, 2008	CVE-2008-0455	
Linux Kernel	Linux Kernel VFS and IPv6 jumbogram packets vulnerabilities		January 28, 2008	CIAD-2008-06	
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Master Boot Record Rootkit	Rootkit	It has been observed that a rootkit named MBR Rootkit is spreading in the wild. The rootkit is hiding itself inside the master boot record of the system. It is exploiting various vulnerabilities to get into unpatched Windows system.	Troj/Mbroot-A [Sophos], StealthMBR [McAfee], TROJ_SINOWAL.AD [Trend]	January 14, 2008	http://www.cert-in.org.in/virus/MBR_Rootkit.htm
		It has been observed that Trojan Clampi is spreading in the wild. This Trojan			

Trojan Clampi	Trojan	gets downloaded on the system while visiting infected website without user's knowledge with random name at location "C:\". The infected websites are victim of the mass attack launched against Linux/Apache server. Downloaded malware can steal credentials such as usernames, passwords, credit card numbers, and online payment accounts from compromised system.	Win32.Trojan-Downloader.Agent.hlp (CAT-QuickHeal), Virus.Win32.Agent.hlp (Kaspersky), Trojan:Win32/Ilobo.gen!A (Microsoft)	January 23, 2008	http://www.cert-in.org.in/virus/Trojan_Clampi.htm
SYMBOS_BESELO Worm	Worm	It has been reported that mobile phone worm SYMBOS_BESELO.A is spreading in the wild. This worm is infecting Symbian S60 enabled devices which include Nokia 6600, 6630, 6680, 7610, N70 and N72 handsets.	No Alias	January 24, 2008	http://www.cert-in.org.in/virus/MMS_Worm.htm
W32.Joydotto	Worm	It has been observed that a Worm named Joydotto is circulating widely. It spreads by copying itself to removable devices. It also downloads malicious files on the compromised computer and collects infected system information such as Computer Name, Current User Name, SKU Number, UUID and sends the collected information to the malicious URLs which are under the control of the attacker.	No Alias	January 29, 2008	http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-012909-5857-99&tabid=1
WORM_AGENT.TBH	Worm	The worm may be downloaded through malicious Web sites or arrive via Advanced Design Systems digital photo frames. It disables Automatic Windows Update. It modifies registry entries to hide files with both System and Read-only attributes. It drops copies of itself in all physical and removable drives.	Packed.Win32.NSAnti.r (Kaspersky), New Malware.aq !! (McAfee), Trojan Horse (Symantec), TR/Crypt.NSPI.Gen (Avira), Mal/Packer (Sophos)	January 29, 2008	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=WORM%5FAGENT%2ETBH&Vsect=P

Security News

New Malware Toolkit Infected More Than 10,000 Web Sites

[Source: www.govtech.com]

January 22, 2008

Finjan's Malicious Code Research Center (MCRC) has identified yet another significant new Web attack -- the latest in a genre of crimeware that threatens to turn highly trusted Web sites into insidious traps for unwary visitors. More than 10,000 Web sites in the U.S. were infected in December by this latest malware. The attack, which has been designated "random js toolkit," is an extremely elusive crimeware Trojan that infects an end user's machine and sends data from the machine via the Internet to the Trojan's "master," a cyber criminal. Data stolen by the Trojan can include documents, passwords, surfing habits, or any other sensitive information of interest to the criminal. The random js toolkit was detected while diagnosing users' Web traffic during December 2007. The random js toolkit is a JavaScript code that is created dynamically and changes every time it is being accessed. As a result, it is almost impossible to be detected by traditional signature-based anti-malware products.

[More]

Mystery web infection grows, but cause remains elusive

[Source: www.channelregister.co.uk]

January 16, 2008

The mystery over a cluster of poisoned websites distributing a toxic malware cocktail may be better understood but it's still not solved. Five days ago, we wrote about the infection of several hundred websites that was unlike anything seasoned researchers had seen before. Mary Landesman, a cyber gumshoe who first brought it to public attention, asked for help from other security pros in figuring out how the unusual new technique worked. And help is what many of her peers have provided. The sites host

malicious javascript that is spontaneously created and randomly named only after a visitor hits the home page. That's unlike any other mass infection most researchers have seen before. Usually, infected sites merely host pointers to attacker-controlled servers, which in turn are used to host malware with static file names.

[More]

Storm's Creators Face a Storm of Their Own

[Source: www.internetnews.com]

January 30, 2008

American and Russian law enforcement agencies have finally identified the criminals behind the Storm worm, one of the nastiest pieces of malware to ever hit the Internet. Now comes the hard part: arresting them. Storm has been one of the toughest worms to eradicate because it was crafted so well. It mutates every 30 minutes, making it impossible for signature-based antivirus products to catch it, and there are no central command and control servers to take out like most other worms. Once a computer is infected, any kind of malicious code can be downloaded, from a spam bot to a key logger. It has been most commonly used to send out spam. Just as the highly infectious code remains elusive to many antivirus applications, the people who created this Storm have managed to stay one step ahead of the law thanks mainly to bureaucratic red tape. The exact number of people involved as well as their identities aren't being released while Russian authorities wind their way through multiple diplomatic, law enforcement and government channels. Things will get even more complicated if U.S. law enforcement agencies demand extradition.

[More]

Hacked embassy websites found pushing malware

[Source: www.theregister.co.uk]

January 23, 2008

One of the most sensitive science and technology labs in the US has been hacked as part of what it called "a sophisticated cyber attack that now appears to be part of a coordinated attempt to gain access to computer networks at numerous laboratories and other institutions across the country." The unknown attackers managed to access a non-classified computer maintained by the Oak Ridge National Laboratory by sending employees hoax emails that contained malicious attachments. That allowed them to access a database containing the personal information of people who visited the lab over a 14-year period starting in 1990. The institution, which has a staff of about 3,800, conducts top-secret research that is used for homeland security and military purposes.

"At this point we have determined that the thieves made approximately 1,100 attempts to steal data with a very sophisticated strategy that involved sending staff a total of seven 'phishing' emails, all of which at first glance appeared legitimate," Thom Mason, the lab's director, wrote in an email sent to employees on Monday. "At present we believe that about 11 staff opened the attachments, which enabled the hackers to infiltrate the system and remove data."

[More]

Gang of hackers hits Texas bank

[Source: www.sacbee.com]

January 25, 2008

Researchers uncovered an attack targeting 'open-recursive' DNS servers that controls where phishing victims go on the Internet. Researchers at Google and the Georgia Institute of Technology are studying a virtually undetectable form of attack that quietly controls where victims go on the Internet. The study, set to be published in February, takes a close look at "open recursive" DNS servers, which are used to tell computers how to find each other on the Internet by translating domain names like google.com into numerical Internet Protocol addresses. Criminals are using these servers in combination with new attack techniques to develop a new generation of phishing attacks. The researchers estimate that there are 17 million open-recursive DNS servers on the Internet, the vast majority of which give accurate information. Unlike other DNS servers, open-recursive systems will answer all DNS lookup requests from any computer on the Internet, a feature that makes them particularly useful for hackers.

[More]

Most malware comes from legit sites, says researcher

[Source: www.computerworld.com]

January 23, 2008

The majority of Web sites serving up attack code are legitimate domains that have been hacked by criminals, a security researcher said in a report released today. It's the first time that legitimate sites outnumber the malicious ones hackers purposefully set up to spread malware. According to data compiled by Websense Inc., 51% of the sites it classified as malicious in the second half of 2007 had been compromised and then seeded with attack code that infected unpatched machines visiting the URLs. The remaining 49% were "intentionally built for malicious intent," the Websense report said. Hacking legitimate sites to make them sling malware gives attackers instant advantages, added Dan Hubbard, Websense's vice president of security research. "It's a great vector because they don't need to drive users to the sites in many cases; they also get free hosting, of course, and [it's] hard to trace ownership," Hubbard said. "Additionally, if someone is allowing access based on reputation, then they may go undetected."

[More]

Massive SQL-based Web attack decoded

[Source: www.news.com]

January 09, 2008

On Wednesday, the SANS Internet Storm Center and others published details about the massive SQL-based Web attack that occurred over the weekend. The attack, says SANS, is similar to a smaller SQL-injection attack seen in November. At least 70,000 sites were compromised in a short period of time, leading some to speculate this was an automated attack. From logs files, the attack code appears to exploit a variety of SQL injection vulnerabilities existing on Web sites using Microsoft SQL or Microsoft IIS. On the vulnerable sites, malicious JavaScript is injected into all variable character fields and text fields in the SQL database such that when visitors hit the site, their browsers, if vulnerable, are then redirected to another domain--in this case, us8010.com.

Roger Thompson, chief research officer at Grisoft, identified one of the exploits served at the malicious server as taking advantage of MS06-014, a Microsoft Data Access Components vulnerability that Microsoft patched in September 2006. He also noted that "this domain uc8010(dot)com was registered just a few days ago (Dec 28), and yet, at one point Google showed script injections pointing to it were showing up on over 70k domains." Yet by January 5, most of these domains had already been cleaned.

[More]

Perl.com sends visitors to porn link farm

[Source: www.theregister.co.uk]

January 19, 2008

Visitors to Perl.com, the O'Reilly Media-owned resource, were redirected yesterday (Thursday) to a link farm pushing porn sites. Geeks who hit the site were sent to grepblogs-dot-net, a site that offers links to live adult webcams, erotic blogs and adult erotic fiction, among other things. Closing the Internet Explorer browser window that contains the site caused another link farm of dubious links to open, from a site called cnomy-dot-com. It carries more porno links and banner ads claiming visitors have won a free iPod. "I was aghast," said Tom Christiansen, author of many of the most popular Perl reference books. "I need to understand the nature of the problem." Christiansen is the owner of Perl.com, but has turned over day-to-day operations of the site to O'Reilly, a publisher of dozens of tech books and websites. The redirection is the result of a change in ownership of the grepblogs-dot-net domain name. Judging from this link, the address was hosted on an open source ad server by the name of phpAdsNet. Effective Thursday, however, the site came under new ownership, according to Whois records.

[\[More\]](#)

Hackers turn Cleveland into malware server

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

January 08, 2008

Tens of thousands of websites belonging to Fortune 500 corporations, state government agencies and schools have been infected with malicious code that attempts to engage in click fraud and steal online game credentials from people who visit the destinations, security researchers say. At time of writing, more than 94,000 URLs had been infected by the fast-moving exploit, which redirects users to the uc8010-dot-com domain, according to this search. Security company Computer Associates was infected at one point, as were sites belonging to the state of Virginia, the city of Cleveland and Boston University. "This is a wide variety of sites that have been impacted," said Mary Landesman, a researcher for ScanSafe, a company that provides real-time information to clients about malicious sites. "It's a real in-your-face example of what we see everyday. It's really time for companies that have a vested interest in a web presence to take a hard look at what their security posture is."

Malicious hackers were able to breach the sites by exploiting un-patched SQL injection vulnerabilities that resided on the servers, according to Johannes Ullrich, CTO for the SANS Internet Storm Center. The injections included javascript that redirected end users to the rogue site, which then attempted to exploit multiple vulnerabilities to install key-logging software that stole passwords for various online games, he and other researchers said.

[\[More\]](#)

Excuse me sir: there's a rootkit in your master boot record

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

January 09, 2008

Security mavens have uncovered a new class of attacks that attach malware to the bowels of a hard drive, making it extremely hard to detect and even harder to remove. The rootkit modifies a PC's master boot record (MBR), which is the first sector of a storage device and is used to help a PC locate an operating system to boot after it is turned on. The result: the rootkit is running even before Windows loads. There have been more than 5,000 infections in less than a month, researchers say. "Master boot record rootkits are able to subvert the Windows kernel before it loads, which gives it a distinct stealth advantage over rootkits that load while Windows is running," said Matthew Richard, director of the rapid response team for iDefense, a security provider owned by VeriSign. "It gives it a great stealth mechanism that allows it to persist even after removal." Such rootkits can even survive reinstallation of the operating system, he said. Because the rootkit lurks deep within the hard drive, well below the operating system, most antivirus programs don't detect the malware. Symantec's antivirus program is an exception, however. It labels the pest Trojan.Mebroot, according to Javier Santoyo, a senior manager for emerging technologies at Symantec. The new rootkit is part of the arms race between security vendors and malware writers, he said. "We're definitely making it harder and harder for the bad guys to do stuff to the operating system," he said. They respond by attacking new parts of a PC.

[\[More\]](#)

Browser vulns and botnets head threat list

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

January 14, 2008

Security experts have looked into the crystal ball to predict the cyber attacks most likely to cause substantial damage this year. The resulting list (below), drawn together by 12 security experts under the auspices of the SANS Institute, is based on an analysis of emerging attack patterns. Two of the resulting predictions - malware on consumer devices and web application security exploits - have already come true in the early days of 2008, evidence that the run down is closer to the mark than other security predictions. As is often the case browser exploit came out as the top threat in the run down but the risk is evolving. Web site attacks have migrated from simple exploits to more sophisticated attacks based on scripts that cycle through multiple exploits to yet more sophisticated attacks featuring packaged modules. One of the latest such modules, mpack, produces a claimed 10-25 per cent success rate in infecting surfers. Attackers are actively placing exploit code on popular, trusted web sites where users have an expectation of security. Placing better attack tools on trusted sites is giving attackers a huge advantage over the unwary public. Meanwhile attackers have broadened the scope of the vulnerabilities they target to encompass components, such as Flash and QuickTime, that are not automatically patched when the browser is patched.

[\[More\]](#)

'Ragtag' Russian army shows the new face of DDoS attacks

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

January 04, 2008

In late April, a Russian-speaking blogger upset with recent events in Estonia posted a series of dispatches calling on like-minded people to attack government servers in that country. "They're really fascists," the user, who went by the name of VolchenoK, wrote of Estonian government officials, according to this translation. "Let us help those who are there and really fought for the memory of our grandfather and grandmother. Yet they are fighting against fascism!"

VolchenoK's dispatch was echoed in posts on other Russian-speaking websites and helped set the groundwork for more than a week of distributed denial of service (DDoS) attacks, which sometimes brought official Estonian websites to their knees.

The assault on the Estonian sites was motivated by the government's removal of a Soviet-era memorial from the center of that country's capital. For decades, the monument stood as a tribute to Soviet soldiers who drove out the Nazis during World War II. Some Russians took the removal as a slap in the face and sought revenge. The attacks should serve as a wake-up call for US government officials about the potency of several new DDoS tools adopted by cyber criminals, says Arbor Networks senior security engineer Jose Nazario. He will speak about about DDoS threats later this month at the US Department of Defense's Cyber Crime Conference.

[\[More\]](#)

Beware of pickpockets and malware-laced banner ads

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

January 04, 2008

If you haven't patched that media player or web browser in a while, now might be a good time. MySpace, Excite and Blink have been caught serving banner ads that attempt to install malware on machines running unpatched software. People who visit MySpace chat forums using out-of-date web browsers and media player plugins such as Macromedia Flash and QuickTime are being treated to drive-by downloads that install a plethora of nastyware on their machines, according to this article on Security Fix. The entries, which include Virtumonde, WinFixer and ClickSpring, come courtesy of banner ads hosted on the social networking site.

Not to be outdone, Excite and German language site Blick.ch are also serving malicious banner ads, according to entries here and here from Sandi Hardmeier, a Microsoft MVP who blogs about security. The incidents are the latest example of the crud that all too often makes its way onto end users machines via the servers owned by ad networks such as DoubleClick and Real Media. Cyber criminals typically create sham companies that pose as legitimate advertisers and then slip malicious code into their banner ads. The networks work hard to snuff out the tainted banners, but sometimes fail.

[\[More\]](#)

Contest seeks the most diminutive XSS worm

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

January 05, 2008

Think you have a gift for writing compact code that replicates using one of the web's most vexing classes of security vulnerabilities? Then Security researcher RSnake (aka Robert Hansen) would like to hear from you. He has set up a contest to see who can write a self-propagating cross-site scripting (XSS) worm using the fewest number of characters.

XSS bugs are the bane of web and application programmers alike because they allow attackers to steal email, bank account credentials and other sensitive information by injecting malicious code into trusted websites. Worse yet, such vulnerabilities can be turned into self-propagating worms that use a victim's browser to multiply the damage.

Over the past few years, some of the biggest web destinations - MySpace, Yahoo and Google's Orkut among them - have been overrun by the pest.RSnake, a researcher who focuses on website security, has seen plenty of XSS worms. But he says he wants to see more still, particularly those that are boiled down to their essence, so that he and other security pros can better defend against them.

[More]

Update: Two-thirds of Oracle DBAs don't apply security patches

[Source: www.computerworld.com]

January 14, 2008

Oracle Corp. issues dozens of security patches every quarter, but that doesn't mean database administrators are necessarily implementing them. In fact, a good two-thirds of all Oracle DBAs appear not to be installing Oracle's security patches at all, no matter how critical the vulnerabilities may be, according to survey results from Sentrigo Inc., a Woburn, Mass.-based vendor of database security products. The results are "surprising, and to be candid, quite frightening," said Mike Rothman, president of consulting firm Security Incite in Atlanta.

Sentrigo polled 305 Oracle database administrators from 14 Oracle user groups between August 2007 and January 2008. The company basically asked the administrators two questions: whether they had installed the latest Oracle patches, and whether they had ever installed any of Oracle's security updates. The results, which come even as Oracle is scheduled to release its next batch of quarterly Critical Patch Updates tomorrow, showed that 206 out of the 305 surveyed said they had never applied any Oracle CPUs. Just 31 said they had installed the most recent security update from the company. In total, only one-third said they had ever installed an Oracle CPU.

[More]

Drive-by pharming attack hits home

[Source: www.news.com]

January 22, 2008

Whenever you type an address into an Internet browser, that address is instantly resolved into the site's numerical Internet address by a DNS server located somewhere in the world. On Tuesday, Symantec announced that online criminals have started to remotely redirect your home network router's DNS server so that whenever you type in a financial institution or other trusted site, your browser will instead be redirected to a bogus or phishing Web site.

The practice, called pharming, usually attacks the DNS servers directly, but this latest attack brings it all home (if you are using broadband connectivity). Fortunately, the routers and institutions affected by this current attack are limited to one country, Mexico, but Symantec warns that word of this real-world attack could bring similar attacks elsewhere. Last year, researchers at Symantec and the University of Indiana reported that remotely changing a home router's DNS server was theoretically possible. The theoretical attack used Javascript on a specially crafted Web page, and affected only wireless routers. The attack in use today uses e-mail, and it can affect non-wireless routers as well.

[More]

Google and eBay thwart phishing redirection ruse

[Source: www.theregister.co.uk]

January 23, 2008

High-profile websites have cleaned up their act after a small team of security researchers documented how they were unwittingly helping phishing fraudsters. Phishing scams often use "open redirector" exploits on major sites to make their attack URL look more legitimate. The trick also makes it more likely that fraudulent emails that form the basis of phishing attacks will slip past spam filters. Typically, security shortcomings on targeted sites allow scammers to furnish links that appear kosher but actually redirect to a fraudulent site. Previous Register stories have covered examples of the ruse practiced on websites including Barclays Bank (story [here](#)), eBay ([here](#)), and others. A campaign by SiteTruth to name and shame high profile firms that fail to block open redirector exploits is beginning to bear fruit. SiteTruth cross-referenced the 10,000 sites listed in PhishTank (a clearing house for reports about phishing sites) with the 1.7 million sites in the Open Directory Project database to discover a list of problem domains. Domains listed typically have a security vulnerability which is being exploited by phishing fraudsters.

[More]

Firefox leaks info that's useful to attackers

[Source: www.computerworld.com]

January 23, 2008

Mozilla's head of security yesterday confirmed a bug in Firefox that could be used by attackers to scout out a system prior to mounting a more thorough assault. The flaw, said Window Snyder, Mozilla Corp.'s chief security officer, is in the browser's chrome protocol, she said in response to reports of the vulnerability and the public posting of a proof-of-concept exploit. "Chrome" is the Firefox term for its user interface.

Access to a user's machine would be through one of many Firefox extensions packaged in a flat file structure, rather than collected into a single Java archive, or .jar file, said Snyder. Several popular add-ons, including Download Statusbar and Greasemonkey, use a flat file structure. "Users are only at risk if they have one of the 'flat' packaged add-ons installed," Snyder said on the Mozilla security blog. By leading users to a tricked-out Web page, criminals could sniff for information that might be useful in more aggressive attacks, Snyder acknowledged. "A visited attacking page is able to load images, scripts or style sheets from known locations on the disk," she said. "Attackers may use this method to detect the presence of files which may give an attacker information about which applications are installed. This information may be used to profile the system for a different kind of attack." Firefox developers are working on a patch, according to a thread on Bugzilla, Mozilla's bug-tracking and management site, but a fix has not yet been coded.

[More]

McAfee spies malware in legit JavaScript apps

[Source: www.channelregister.co.uk]

January 04, 2008

A dodgy anti-virus update from McAfee on Wednesday wrongly identified legitimate JavaScript files as a virus in the second such screw-up by a major security vendor in less than a week. As a result of the snafu McAfee users who applied the update were falsely warned that their systems were infected by the Exploit-BO JavaScript virus after visiting sites including ESPN and Friendster, the SANS Institute's Internet Storm Centre warns.

The dodgy update is DAT 5197 released on January 2. McAfee pulled the update and issued a replacement signature update (DAT 5198) shortly afterwards. Faulty anti-virus signature updates are not uncommon across the industry. Spookily rival vendor CA experienced exactly the same type of problem, again involving legitimate JavaScript files been falsely identified as viruses only on Monday.

[More]

Spam King Ralsky indicted over stock spam scam

[Source: www.channelregister.co.uk]

January 04, 2008

Notorious spammer Alan Ralsky and ten others have been indicted in the US over the alleged use of junk mail to promote stock fraud scams. Ralsky (a long term [fixtore](#) in Spamhaus's list of known spammers) his son-in-law Scott K Bradley and others, including a dual national of Canada and Hong Kong and individuals from Russia, California,

Michigan, and Arizona have been charged over the alleged fraud. The charges stem from a three-year investigation - led by agents from the FBI, with assistance from the US Postal Inspection Service and the Internal Revenue Service - into a "sophisticated and extensive" spamming operation promoting a "pump and dump" scheme. The defendants sent spam touting thinly-traded Chinese penny stocks in a bid to drive up their stock price over the short term and sell at a profit before the inevitable crash and burn. Investigators reckon the defendants earned around \$3m during the summer of 2005 alone as a result of their illegal spamming activities. The types of products and services that the defendants pitched evolved over time, as did the types of illegal spamming techniques they employed.

[\[More\]](#)

Virus writers charged with copyright violation

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

January 24, 2008

Japan has arrested its first suspected virus writers, but in a strange twist the three suspected creators and distributors of a strain of P2P malware have been charged with copyright violation, in an arrest that recalls Al Capone's prosecution for tax evasion.

The trio were cuffed by cops in Kyoto on suspicion of involvement in a plot to infect users of the Winny P2P file-sharing network with a Trojan horse that displayed images of popular anime characters while wiping MP3 and movie files. The malware, called Harada is Japanese reports, is reckoned to be related to the Pirlames Trojan horse intercepting by net security firm Sophos in Japan last year. According to local reports, the three men have confessed to their roles in unleashing the malware. One is said to have created the malware, while the other duo are reckoned to have offered the malware up to prospective marks on Winny. A lack of relevant computer crime law in Japan means that the group have been charged with copyright offences.

"It isn't illegal to write viruses in Japan, so the author of the Trojan horse has been arrested for breaching copyright because he used cartoon graphics without permission in his malware," explained Graham Cluley, senior technology consultant for Sophos. "Because this is the first arrest in Japan of a virus writer, it's likely to generate a lot of attention and there may be calls for cybercrime laws to be made tighter."

[\[More\]](#)