



### CERT-In Monthly Security Bulletin August 2008

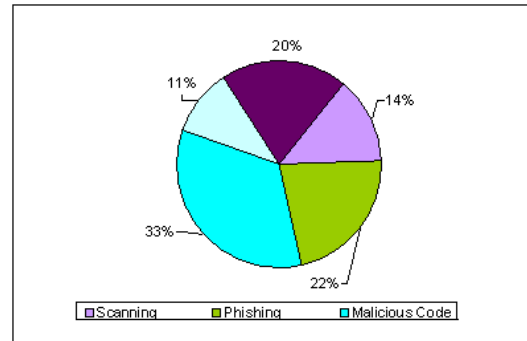
#### Cyber Intrusion Trends

In this month 139 security incidents were reported to CERT-In from various National/International agencies. As shown in the figure, 33%, incidents were related to virus/worm under the Malicious code category, 22% phishing incidents, 20%; incidents related to technical help under the Others category, 14% unauthorized scanning and 11 % spamming incidents were reported in this month. As compared to previous month the number of incidents related to phishing, scanning, virus/worm under the Malicious code category and incidents related to technical help under the Others category have increased.

In this month CERT-In tracked 03 C&C (Command & Control) servers and 7055 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.

Recent detections show that attackers have been compromising Linux-based systems using stolen SSH keys. After gaining access to an affected system, the attacker uses locally exploitable vulnerabilities to gain root privileges, which allow the attacker to install the *phalanx2* rootkit. This rootkit appears to be an updated version of the *Linux.Phalax* Trojan.

Cyber Intrusion during August 2008



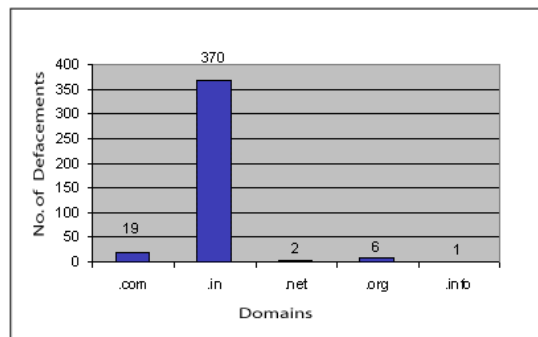
#### Indian Websites Defacement

In total 398 Indian websites were defaced during August 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 mod\_proxy\_ftp module Cross-Site Scripting Vulnerability [CIVN-2008-119](#)
2. Apache Tomcat "UTF-8" Remote Directory Traversal Vulnerability [CIVN-2008-135](#)
3. Apache Tomcat 'RequestDispatcher' Information Disclosure Vulnerability [CIVN-2008-117](#)
4. Apache-SSL Authentication Bypass Vulnerability [CIVN-2008-36](#)
5. phpMyAdmin Shared Host Remote Information Disclosure [CVE-2008-1924](#)
6. PHP 5 'php\_sprintf\_appendstring()' Remote Integer Overflow Vulnerability [CVE-2008-1384](#)
7. Apache Tomcat SingleSignOn Cookie Information Disclosure Weakness [CVE-2008-0128](#)
8. phpMyAdmin Local Information Disclosure [CVE-2008-1567](#)
9. Apache Tomcat AJP Connector Information Disclosure [CVE-2006-7197](#)
10. Apache Tomcat Cross-Site Scripting [CVE-2006-7195](#)

Statistics of Defaced Indian Websites in August 2008

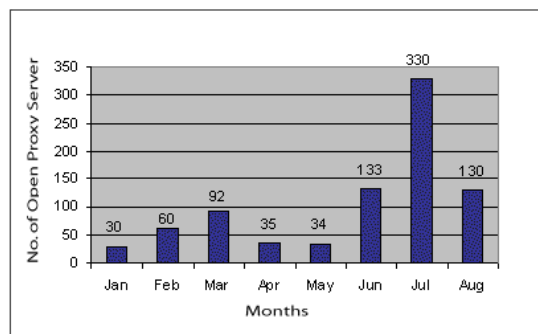


#### Open proxy servers

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 130 open proxy servers functioning in India during August 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 - Aug 2008



#### Attack Trend

##### Propagation of Malware via .doc files

It has been observed that e-mails containing malicious .doc files are circulating widely. These mails arrive as news mostly related to Beijing Olympics 2008 events to trick the users. These trojanised doc files (detected as TROJ\_MDROPPER.ZT) are exploiting the zero day vulnerability (CVE-2008-2244) in

Microsoft word 2000,2002,2003 described in CERT-In vulnerability note [CIVN-2008-104](#) .It can also affect other versions of the popular word-processing applications. Patches for this vulnerability have been released in August 2008.

[\[More\]](#)

#### **Propagation of malware via spam e-mail with the name of MSNBC.com “BREAKING NEWS”**

It has been observed that a new wave of spam e-mails pretending to be from msnbc.com is circulating widely. These spam e-mails comes with the subject line of current affairs and changing with daily current news items, which takes to the user to malicious websites hosting malicious files such as “ adobe\_flash.exe ”. Some of the malicious files are detected as Nuwar Worm.

[\[More\]](#)

#### **Propagation of malware via spam e-mail with the name of “CNN.com Daily Top 10”**

It has been observed that a new wave of spam e-mails pretending to be from CNN.com is circulating widely. These spam e-mails comes with the subject line such as “**CNN.com Daily Top 10 Stories**” and “**CNN.com Daily Top 10 Videos** ” . E-mail contains URLs in the form of current affairs and changing with daily current news items, which takes to the user to malicious websites hosting malicious files such as “ *get\_flash\_update.exe* ”.

[\[More\]](#)

Other important cyber threats observed in this month are...

- A new worm targeting users of MySpace and Facebook online social networks has been discovered. *W32.Koobface.A* , described in IntelliShield Alert 16373, searches the infected system for browser cookies related to the Facebook and MySpace websites.
- Attackers leveraged the insufficient entropy vulnerability in multiple vendors' DNS implementations, to poison the cache of the China Netcom Internet Service Provider (ISP). China Netcom users who mistype a web address may be redirected to a malicious web page that attempts to use a malicious iframe to exploit vulnerabilities in Adobe, Microsoft, and RealNetworks products on the users' systems.

### **Training**

#### **Workshop on "DNSSEC In India " on 18th August, 2008**

A one day Workshop on "DNSSEC in India " was conducted on 18th August, 2008 . The objective of the workshop is to create awareness on DNS Security and to bring together the primary leaders in the internet community in india to move india 's internet operations toward world class security. The workshop covered the following topics at length:

- Need of DNSSEC for Managers and Technologists
- Overview of DNSSEC for Managers and Technologists
- Kaminsky Attack-Demo
- Defining the objectives of DNSSEC in the .IN Domain
- A Role for Everybody-ISPs ,Registrars ,Key Industry Leaders

**Speakers** : Experts from ICANN( USA ),NIXI and CERT-IN

[\[Presentation Material\]](#)

#### **Workshop on "Web Application Security" on 21st August, 2008**

A one day Workshop on "Web Application Security" was conducted on 21st August, 2008 . The objective of the workshop is to create security awareness among the cyber security researchers/professionals from Govt., public and critical sector organizations on current trends on web application security attacks and mitigation techniques. The workshop covered the following topics at length.

- Introduction to Web Application Security
- Top 2 Application Security Attacks.
- Advanced Application Security Attacks.

**Speakers** : Experts from SecurEye.

[\[Presentation Material\]](#)

#### **Workshop on "Cryptographic Primitives" on 29th August, 2008**

A one day Workshop on "Cryptographic Primitives" was conducted on 29th August, 2008 . The objective of the workshop is to train system/network administrators and security professionals how Cryptographical techniques and Digital certificates can be used to improve Enterprise/Organizations network security. The workshop covered the following topics at length:

- Cryptography :Basics
- Applications of Cryptography
- PKI Cryptography
- Digital Signature –Applications and Demo

**Speakers** : Experts from ECIL ,DIT and CCA.

**Security Alerts**

**The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during August 2008 and their countermeasures along with wide-spreading malicious code like virus/ worm/Trojan are given below :**

<b>High Vulnerabilities</b>			
<b>Microsoft</b>	<b>Title of Vulnerability</b>	<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>
Microsoft	Multiple Vulnerabilities in Microsoft Windows Messenger, Windows Mail, Outlook Express, Access, Internet Explorer, Microsoft Office (Word, Excel, Powerpoint ), IPsec Policy Processing and Color Mangement System	August 14, 2008	<a href="#">CIAD-2008-40</a>
Microsoft	Multiple Vulnerabilities in Microsoft Excel	August 14, 2008	<a href="#">CIVN-2008-123</a>
Microsoft	Multiple Vulnerabilities in Microsoft Office Filters	August 14, 2008	<a href="#">CIVN-2008-124</a>
Microsoft	Multiple Remote Code Execution Vulnerabilities in Microsoft Internet Explorer	August 14, 2008	<a href="#">CIVN-2008-125</a>
Microsoft	Microsoft Windows Image Color Management System Remote Code Execution Vulnerability	August 14, 2008	<a href="#">CIVN-2008-126</a>
Microsoft	Multiple Vulnerabilities in Microsoft PowerPoint	August 14, 2008	<a href="#">CIVN-2008-131</a>
Microsoft	Microsoft Visual Studio "Msmask32" ActiveX Code Execution Vulnerability	August 14, 2008	<a href="#">CIVN-2008-137</a>
<b>Unix</b>	<b>Title of Vulnerability</b>	<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>
Linux	Linux kernel uvc_parse_format function buffer overflow vulnerability	August 13, 2008	<a href="#">CIVN-2008-120</a>
Linux	Linux Kernel "dccp_setsockopt_change ()" Integer Overflow Vulnerability	August 20, 2008	<a href="#">CIVN-2008-134</a>
Linux	Linux Kernel "sctp_setsockopt_auth_key ()" Denial of Service Vulnerability	August 29, 2008	<a href="#">CIVN-2008-113</a>
<b>CISCO</b>	<b>Title of Vulnerability</b>	<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>
CISCO Webex	Webex Meeting Manager ActiveX Control Buffer Overflow Vulnerability	August 20, 2008	<a href="#">CIVN-2008-133</a>
<b>Miscellaneous</b>	<b>Title of Vulnerability</b>	<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>
Trend Micro	Trend Micro OfficeScan Web-Deployment ObjRemoveCtrl Class Buffer Overflow Vulnerabilities	August 05, 2008	<a href="#">CIVN-2008-115</a>
Apache Tomcat	Apache Tomcat 'RequestDispatcher ' Information Disclosure Vulnerability	August 06, 2008	<a href="#">CIVN-2008-117</a>
Solaris	Vulnerability in the Solaris snoop utility	August 13, 2008	<a href="#">CIVN-2008-122</a>
Ingres	Multiple vulnerabilities in Ingres Database for Linux	August 13, 2008	<a href="#">CIAD-2008-39</a>
Opera	Multiple vulnerabilities in Opera	August 25, 2008	<a href="#">CIAD-2008-42</a>
Trend Micro	Web Management Authentication Bypass vulnerability in Trend Micro Products	August 29, 2008	<a href="#">CIVN-2008-140</a>
<b>Medium Vulnerabilities</b>			
<b>Microsoft</b>	<b>Title of Vulnerability</b>	<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>
Microsoft	IPsec Policy Processing Information Disclosure Vulnerability	August 14, 2008	<a href="#">CIVN-2008-130</a>
Microsoft	Microsoft Outlook Express and Windows Mail MHTML Handler Cross-Domain Information Disclosure Vulnerability	August 14, 2008	<a href="#">CIVN-2008-129</a>
Microsoft	Microsoft Windows Event System Array Index Verification & 'User	August 14, 2008	<a href="#">CIVN-2008-128</a>

	Subscription Request' Vulnerabilities				
Microsoft	Microsoft Windows Messenger ActiveX Control Information Disclosure Vulnerability		August 14, 2008	<a href="#">CIVN-2008-127</a>	
<b>Unix</b>	<b>Title of Vulnerability</b>		<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>	
Linux	Linux Kernel "snd_seq_oss_synth_make_info()" Information Disclosure Vulnerability		August 13, 2008	<a href="#">CIVN-2008-121</a>	
Linux	Linux Kernel UBIFS Orphan Inode Local Denial of Service Vulnerability		August 19, 2008	<a href="#">CIVN-2008-132</a>	
Linux	Linux Kernel "rt6_fill_node()" Denial of Service Vulnerability		August 25, 2008	<a href="#">CIVN-2008-136</a>	
<b>Miscellaneous</b>	<b>Title of Vulnerability</b>		<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>	
AVG	AVG Anti-Virus UPX Processing Denial of Service Vulnerability		August 05, 2008	<a href="#">CIVN-2008-116</a>	
Apache	Apache mod_proxy_ftp module Cross-Site Scripting Vulnerability		August 07, 2008	<a href="#">CIVN-2008-119</a>	
PHP	Multiple vulnerabilities in PHP		August 20, 2008	<a href="#">CIAD-2008-41</a>	
Apache Tomcat	Apache Tomcat "UTF-8" Remote Directory Traversal Vulnerability		August 25, 2008	<a href="#">CIVN-2008-135</a>	
<b>Low Vulnerabilities</b>					
<b>Solaris</b>	<b>Title of Vulnerability</b>		<b>Discovery/Publish Date</b>	<b>CERT-In References &amp; Patch Information</b>	
Solaris	Vulnerability in Solaris namefs kernel module		August 07, 2008	<a href="#">CIVN-2008-118</a>	
Solaris	Vulnerability in the Solaris NFSv4 Client Kernel Module		August 26, 2008	<a href="#">CIVN-2008-138</a>	
<b>Malicious Code Threats</b>					
<b>Title of Malicious Code</b>	<b>Type</b>	<b>Overview</b>	<b>Aliases</b>	<b>Discovery Date</b>	<b>References</b>
Asprox Botnet	Trojan	It has been observed that a Trojan horse named Asprox is spreading widely.  The Trojan, which was originally used for sending phishing scams, uses fast flux SQL injection Attacks to hack websites and formulates a botnet.	Mal/Badsrc-C (Sophos) Trojan.Asprox.D (BitDefender) Trojan:JS/Aseljo.A (Microsoft)	Original issue date: July 17, 2008 Updated: August 01, 2008	<a href="http://www.cert-in.org.in/virus/Asprox_Botnet.htm">http://www.cert-in.org.in/virus/Asprox_Botnet.htm</a>
Downloader.Swif	Trojan Horse	It has been observed that a Trojan named Swif is spreading in the wild. The Trojan propagates through emails with a link to a malicious .swf file. As novice user clicks upon the link the threat gets	No aliases found	August 29, 2008	<a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-082913-3212-99&amp;tabid=2">http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-082913-3212-99&amp;tabid=2</a>

		installed onto the user's system which further downloads additional malwares onto the infected system.			
Trojan.Bankpatch	Trojan Horse	It has been observed that a Trojan named Bankpatch is spreading in the wild. The Trojan modifies certain DLL files on the infected system and attempts to steal information such as URLs visited from the compromised computer. The Trojan then sends the collected information to a remote server under the control of the attacker.	No aliases found	August 18, 2008	<a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-081817-1808-99&amp;tabid=1">http://www.symantec.com/business/security_response/writeup.jsp?docid=2008-081817-1808-99&amp;tabid=1</a>

#### Security News

##### **CERT: Linux servers under 'Phalanx' attack.**

[Source: <http://www.theregister.co.uk>] – 27 August 2008

Attacks in the wild are under way against Linux systems with compromised SSH keys, the US Computer Emergency Readiness Team is warning.

The attacks appear to use stolen SSH keys to take hold of a targeted machine and then gain root access by exploiting weaknesses in the kernel. The attacks then install a rootkit known as Phalanx2, which scours the newly infected system for additional SSH keys. There's a viral aspect to this attack. As new SSH keys are stolen, new machines are potentially vulnerable to attack.

The CERT advisory makes no mention of the flaw in the Debian random number generator, but that's most likely the starting point for the attack. The flaw caused SSL keys generated for more than a year to be so predictable that they could be guessed in a matter of hours. Debian fixed the flaw in May.

Once a Linux server using a weak key is identified and rooted, it quickly gives up the keys it uses to connect to other servers. Even if these new keys aren't vulnerable to the Debian debacle, attackers can potentially use them to access the servers that use them if both the private and public parts of the key are included. Additionally, attackers can identify other servers that have connected to the infected machine recently, information that may enable additional breaches.

[\[More\]](#)

##### **Malware detected at the International Space Station**

[Source: <http://blogs.zdnet.com>] - 27 August 2008

Malware is reaching new heights, and going into Space through a removable media carrying the W32.Gammima.AG password stealing malware to the International Space Station. According to SpaceRef.com :

“W32.Gammima.AG worm is a level 0 gaming virus intended to gather personal information. Virus was never a threat to any of the computers used for cmd and cntl and no adverse effect on ISS Ops. Theory is virus either in initial software load or possibly transferred from personal compact flash card. Working with Russians (and other partners) regarding ground procedures to protect flown equipment in the future. It was noted that most of the IP laptops and some of the payload laptops do NOT provide virus protection/detection software .”

[\[More\]](#)

##### **Intel ships BIOS fix for Rutkowska's Black Hat flaw**

[Source: <http://blogs.zdnet.com>] - 27 August 2008

Intel has shipped a BIOS update with a fix for a privilege escalation vulnerability that was used by rootkit researcher Joanna Rutkowska to bluepill the Xen hypervisor.

The vulnerability was discussed by Rutkowska at the Black Hat briefings earlier this month but details on the exploit were withheld until Intel could release its patch.

That patch is now available.

[\[More\]](#)

### **Internet traffic begins to bypass the U.S**

[Source: <http://news.cnet.com>] -31 st august 2008

Invented by American computer scientists during the 1970s, the Internet has been embraced around the globe. During the network's first three decades, most Internet traffic flowed through the United States . In many cases, data sent between two locations within a given country also passed through the United States .

Engineers who help run the Internet said that it would have been impossible for the United States to maintain its hegemony over the long run because of the very nature of the Internet; it has no central point of control. And now, the balance of power is shifting. Data is increasingly flowing around the

United States , which may have intelligence--and conceivably military--consequences.

American intelligence officials have warned about this shift. "Because of the nature of global telecommunications, we are playing with a tremendous home-field advantage, and we need to exploit that edge," Michael V. Hayden, the director of the Central Intelligence Agency, testified before the Senate Judiciary Committee in 2006. "We also need to protect that edge, and we need to protect those who provide it to us.

[\[More\]](#)

### **Taiwan busts hacking ring, 50 million personal records compromised**

[Source: <http://blogs.zdnet.com>] - 27 August 2008

Taiwan 's Criminal Investigation Bureau ( CIB ) has successfully tracked down and arrested six people in what the CIB believes to be the biggest personal data breach in Taiwan to date. Apparently, the group also managed to obtain personal data on Taiwan 's current and former presidents :

"The suspects are believed to have stolen more than 50 million records of personal data, including information about President Ma Ying-jeou, his predecessor Chen Shui-bian and police chief Wang Cho-chiun, the official said. They then offered to sell the information for 300 Taiwan dollars (10 US ) per entry, he said. The hackers, based in Taiwan and China , also swindled victims out of millions of Taiwan dollars through their online bank accounts, he said."

When infected machines log onto the social networks the next time their computers automatically send the malicious messages out to new victims grabbed from the friend list, said Ryan Naraine, security evangelist at Kaspersky.

[\[More\]](#)

### **New worm targets Facebook, MySpace**

[Source: <http://news.cnet.com>] - 01 August 2008

A new worm is spreading via Facebook and MySpace, turning victims' computers into zombies on a botnet, Kaspersky Lab said. Basically, infected machines are propagating the worm by sending messages via the social networks to friends in the network.

The messages look like they contain links to video clips. When clicked on they prompt the recipient to download an executable file that purports to be the latest version of Flash Player. Instead, it is the worm itself, infecting yet another victim.

When infected machines log onto the social networks the next time their computers automatically send the malicious messages out to new victims grabbed from the friend list, said Ryan Naraine, security evangelist at Kaspersky.

[\[More\]](#)

### **New Gpcode (encryption) ransomware spreading via botnet**

[ Source: <http://blogs.zdnet.com> ] - 13 August 2008

There are confirmed reports on a new version of the Gpcode ransomware being spread via a botnet.

According to Vitaly Kamluk of Kaspersky Lab the Trojan encrypts files on an infected machine ( AES -256) and leaves a text file named crypted.txt with a ransom note demanding \$10 to decrypt the files. It also changes the desktop wallpaper with a skull/crossbones image that contains a URL, an ICQ number and an e-mail address to contact the author.

[\[More\]](#)

### **Cross-site hacks and the art of self defence**

[Source: <http://www.theregister.co.uk> ] – 29 August 2008

Hackers can force your browser to send requests to any site they want. It's not even hard - all they have to do is get you to view an email or a web page.

Unless the site is specifically protected against this - and almost none are - then attackers can make your browser do anything you can do, and they can use your credentials and your access privileges. They can do things like set preferences, create payees and change passwords .

Generally, browsers stop cross-site communication by following the "same-origin policy". This rule is pretty simple: if your site has a different origin - protocol, domain, and port don't all match - you aren't allowed to access information from or send requests to the other site. Without this simple rule, there would be no security on the internet. Every website could access data from every other one - you'd need a separate web browser for every website.

[\[More\]](#)

#### **Shadow investigation spreads to Big Easy with botnet arrest**

[Source : <http://arstechnica.com/> ] – 24 August 2008

About two weeks ago, the Dutch High Tech Crime Unit released news of its successful botnet sting in late July. Now, we're starting to see American law enforcement file related charges, as investigators crack down on both sides of the Atlantic. The Department of Justice reports that a New Orleans grand jury has formally indicted Brazilian Leni de Abreu Neto on a charge of conspiracy to cause damage to computers worldwide. Counting the two native Dutch brothers, a total of three people have been arrested thus far.

The Dutch man, 19 year-old Nordin Nasiri, has not yet been indicted, but Dutch prosecutors are interviewing him, presumably with the intent to file charges. As for Neto, he was picked up in the Netherlands, and will be transferred to the US pending the results of an extradition hearing.

[\[More\]](#)

#### **Free Spear-Phishing Tool on Tap.**

[Source : <http://www.darkreading.com/> – 19 August 2008

A researcher next month will unleash a new, free open-source tool for conducting targeted phishing attacks in-house.

Targeted phishing attacks, also known as spear-phishing, are increasingly becoming the hacker's method of choice for infecting and/or infiltrating a specific organization. These attacks can be eerily convincing, often using identical message footers and IP addresses as those within an organization, and can easily dupe unsuspecting users into opening them and following their malicious links. Just last week, a spear-phishing attack on New Zealand-based University of Otago resulted in an estimated 1.55 million spams generated from the university's server within 60 hours. (See Spear Phishing Attack Unleashes 1.5M Spam Messages.)

A recent report from iDefense Labs found that over 15,000 corporate victims in the past 15 months have been hit by spear phishing attacks..

[\[More\]](#)

#### **APWG and IEEE partner for Electronic Crime Research Conference**

[Source: <http://www.net-security.org/> ] – 20 August 2008

Anti-Phishing Working Group and IEEE will join forces for the development of the APWG e-Crime Researchers Summit ( [eCRS](#) ), the world's only peer-reviewed technical conference dedicated exclusively to electronic crime research.

This October, at the APWG's conference week in Atlanta, Georgia, the IEEE, via its Standards Association, will join the eCRS as a 'Technical Sponsor' and begin laying the groundwork for the partnership to cultivate the eCRS, as well as the larger discipline of electronic crime studies. The collaboration will leverage the APWG's unique community of electronic crime experts and the IEEE's network of technical experts, as well as its global authority in standards development.

[\[More\]](#)

#### **Google, Microsoft, Yahoo & Others Nearing Completion of Online Human Rights Code**

[Source : <http://www.darkreading.com/> – 20 August 2008

The group of companies that promised to write an online code of human rights for Internet users in 2006 is close to completing the document.

In a letter to two U.S. senators about the human rights code, Yahoo's top legal executive said earlier this month that the group is "working as swiftly as possible" on the code and gave a rough idea on how it will be implemented.

Back in January 2007, Google, Microsoft, and Yahoo led a group of IT companies that promised to "produce a set of principles guiding company behavior when faced with laws, regulations and policies that interfere with the achievement of human rights." The idea was to create a code of conduct that would help companies do the right things in protecting user privacy and provide a method to resist censorship and jailing of bloggers and political dissidents by governments.

If the code is accepted and widely adopted, it could change some enterprises' privacy policies and make it more difficult for corporations or governments to duck through loopholes in rapidly changing and frequently outdated laws, observers say

[\[More\]](#)