



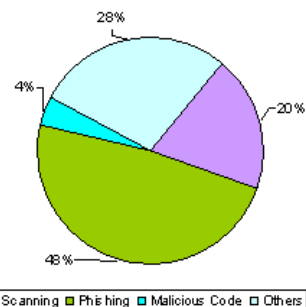
CERT-In Monthly Security Bulletin February 2008

Cyber Intrusion Trends

In this month 85 security incidents were reported to CERT-In from various National/ International agencies. As shown in the figure 48% phishing incidents were reported in this month. 20% unauthorized scanning, 4% incidents related to virus/worm under the Malicious code category and 28% incidents related to technical help under the Others category were reported in this month. As compared to previous month the number of phishing incidents and incidents related to technical help under the Others category have increased while scanning and incidents related to virus/worm under the Malicious code category have decreased.

In this month CERT-In tracked 10 C&C (Command & Control) servers and 1279 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 February 2008



Attack Trends

Propagation of Storm worm variants through Valentines Day greetings: It has been observed that new variants of 'Storm Worm' are circulating via e-mails pretending to be Valentine's Day Greetings. These spam e-mails come with the subject line such as "Valentine's Day", "The Love Train" and other Valentine's Day related phrases. E-mail contains URL in form of IP address, which takes the user to malicious website hosting malware "valentine.exe".

[\[More\]](#)

Fake Microsoft Windows Update Websites:

It has been observed that Malicious files are being propagated through fraudulent websites pretending to be providing updates to Microsoft Windows. Spam emails are being sent to users to trick them to click on link to fraudulent Website. The malicious link directs users to a Webpage asking users to click upon Urgent Install button. As user clicks upon the button an executable file named WindowsUpdateAgent30-x86-x64.exe gets downloaded to the system. This executable file is malware named as Trojan- Dropper:W32/Agent.DYD which then drops another malware, identified as Backdoor:W32/Agent.CVU.

[\[More\]](#)

ActiveX Vulnerabilities in Yahoo! MediaGrid, YMP Datagrid, Facebook and MySpace:

It has been observed in this month that vulnerabilities in several ActiveX controls was used to exploit the vulnerable applications such as Yahoo! MediaGrid ActiveX control, YMP Datagrid ActiveX control and image uploader used by Facebook and MySpace. The vulnerabilities can be used to execute arbitrary code or crash the vulnerable application.

The exploit codes for these vulnerabilities are available on the Internet that could be used by malicious people by creating a specially crafted HTML document and persuading user to open the document (e.g., a web page or an HTML email message or attachment). Successful exploitation allows an attacker to execute arbitrary code with the privileges of the user on a vulnerable system.

[\[More\]](#)

Training

Workshop on "Implementation of Information Security Management in Government & Critical Sector Organisations"

CERT-In conducted a one day Workshop on "Implementation of Information Security Management in Government & Critical Sector Organisations" on 12th February, 2008. The interactive workshop covered the following topics at length:

- ISMS - Overview, Standards and ISO 27001 Requirements, Implementation: STQC Directorate, DIT
- ISMS Implementation Case Study

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

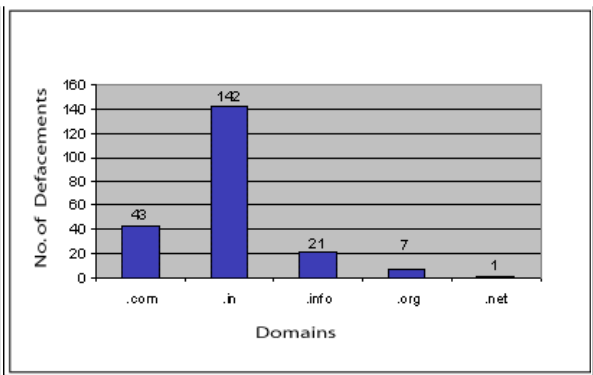
Indian Websites Defacement

In total 214 Indian websites under .in were defaced during February 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. Duplicate Request-Processing and Information Disclosure Vulnerabilities in Apache Tomcat [CIAD-2008-12](#)
2. Microsoft IIS File Change Notification vulnerability [CIVN-2008-12](#)
3. Remote Code Execution Vulnerability in Microsoft Internet Information Services (IIS) [CIVN-2008-13](#)
4. Multiple Vulnerabilities in PHP [CVE-2007-5898](#), [CVE-2007-5899](#), [CVE-2007-5900](#)
5. Denial of service vulnerability in PHP [CVE-2007-6039](#)

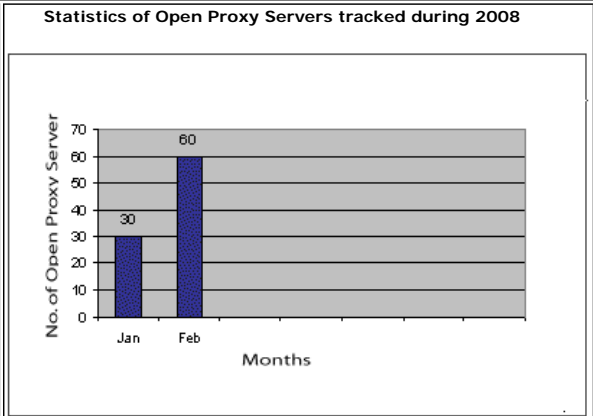
Statistics of Defaced Indian Websites in February 2008



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 67 open proxy servers functioning in India during February 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.



Security Alerts

The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during February 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	Microsoft Windows WebDAV Mini-Redirector Buffer Overflow Vulnerability	February 13, 2008	CIVN-2008-14
Microsoft Windows	Microsoft Object Linking and Embedding (OLE) Automation Heap Based Buffer Overflow Vulnerability	February 13, 2008	CIVN-2008-15
Microsoft Word	Microsoft Word Memory Corruption Vulnerability	February 13, 2008	CIVN-2008-16
Microsoft Internet Explorer	HTML Rendering Memory Corruption, Property Memory Corruption, Argument handling memory corruption and ActiveX object memory corruption vulnerabilities in Microsoft Internet Explorer	February 13, 2008	CIVN-2008-17
Microsoft Office	Microsoft Office Publisher Invalid Memory Reference and Memory Corruption Vulnerabilities	February 13, 2008	CIVN-2008-19
Microsoft Office	Microsoft Office Object Parsing Memory Corruption Vulnerability	February 13, 2008	CIVN-2008-20
Microsoft	Multiple Vulnerabilities in various components of Microsoft Windows, Internet Explorer, IIS Server, Office, Active Directory, Works and Publisher	February 13, 2008	CIAD-2008-10
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Linux Kernel	Linux Kernel "vmsplice" system call, vserver-enabled, fault handler range check Vulnerabilities	February 15, 2008	CIAD-2008-11
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Mozilla Products	Multiple Vulnerabilities in Mozilla Products	February 11, 2008	CIAD-2008-08
Adobe Reader/Acrobat	Multiple vulnerabilities in Adobe Reader/Acrobat	February 11, 2008	CIAD-2008-09
Mozilla Firefox	Multiple Vulnerabilities in Mozilla Firefox	February 11, 2008	CVE-2008-0420 , CVE-2008-0416 , CVE-2008-0593
Medium Vulnerabilities			
Microsoft	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
	Microsoft Active Directory Denial of Service		

Microsoft Windows	Vulnerability	February 13, 2008	CIVN-2008-10		
Windows Vista	Windows Vista DHCP Packet Handling Denial of Service Vulnerability	February 13, 2008	CIVN-2008-11		
Microsoft IIS	Microsoft IIS File Change Notification vulnerability	February 13, 2008	CIVN-2008-12		
Microsoft IIS	Remote Code Execution Vulnerability in Microsoft Internet Information Services (IIS)	February 13, 2008	CIVN-2008-13		
Microsoft Works	Microsoft Works File Converter Vulnerabilities	February 13, 2008	CIVN-2008-18		
Unix	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Apache Tomcat	Duplicate Request-Processing and Information Disclosure Vulnerabilities in Apache Tomcat	February 15, 2008	CIAD-2008-12		
Cisco	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information		
Cisco	SQL injection vulnerability in Cisco Unified communications Manager	February 20, 2008	CIVN-2008-21		
Cisco	Cisco Unified IP Phone Overflow and Denial of Service Vulnerabilities	February 20, 2008	CIVN-2008-22		
Malicious Code Threats					
Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Cutwail Trojan	Trojan	The trojan propagates by attaching a copy of itself to the email messages with message body which lures users into opening up the attachment to get malware installed on their system.	Trojan.Pandex [Symantec], Win32/Cutwail [Microsoft]	February 05, 2008	http://www.cert-in.org.in/virus/Cutwail_Trojan.htm
EXPL_PIDIEF	PDF Exploit	It arrives as an email attachment spammed by another malware or a malicious user. It exploits several vulnerability in versions of Adobe Reader earlier than 8.1.2. Upon successful exploitation the malware gets connected to certain websites to downloads other malwares on the infected system.	Exploit-PDF.b [McAfee], Trojan.Pidief.C [Symantec], HTML/Shellcode.Gen [Avira], Mal/JSShell-B [Sophos], Exploit: Win32/Pdfjsc.A [Microsoft]	February 10, 2008	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=EXPL%5FPIDIEF%2E0&VSec=P
SilentBanker Trojan	Trojan	The trojan can intercept transactions carried out by users and change the user-entered destination bank account details to the attacker's account details without being noticed by the user. It propagates	No Alias	February 11, 2008	http://www.cert-in.org.in/virus/SilentBanker_Trojan.htm

		through web or dropped by some other malware and automatically gets executed on the users system.			
BKDR_AGENT	Backdoor (Trojan)	The backdoor gets dropped into users systems by other malwares or gets installed unknowingly by users while visiting malicious Websites. It creates a backdoor through random ports on the infected system and listen to remote attacker's commands.	Proxy-Agent.af.gen (McAfee), Trojan.Asprox (Symantec), BDS/Backdoor.Gen (Avira), Troj/AgentM-Fam (Sophos), Backdoor:Win32/Agent.ACG (Microsoft)	Feb 21, 2008	http://www.trendmicro.com/vinfo/virusencyclo/default5.asp?VName=BKDR_AGENT.AKJZ

Security News

Malware writers think global, act local

[Source: www.theregister.co.uk]

February 22, 2008

Online miscreants are beefing up their cultural outreach skills.

According to a new report from McAfee, attacks are increasingly being tailored to victims in specific geographical regions. Spam, phishing emails and even malware now address their potential victims in their native tongues, often with flawless grammar. Attackers have also become familiar with local culture, including sports and other pastimes, and often incorporate them into their ploys to further the chances of tricking their Marks. "We really wouldn't have had this conversation two years ago," said Dave Marcus, a security research and communications manager at McAfee. Back then, "the distribution of malware was very English language centric." As a result, spam and malware targeting Germans are likely to target their enthusiasm for the World Cup. Attacks on Japanese, meanwhile, are likely to piggyback on the popularity in that country of Winny, a P2P file sharing program. And Chinese scams will likely involve gold farming, which refers to the harvesting of virtual valuables in games such as World of Warcraft.

[More]

Fraud cases breached £1bn level in 2007

[Source: www.theregister.co.uk]

February 04, 2008

Organised gangs pushed the value of fraud to a 12-year high last year, with the UK government being the largest victim of their criminal activities, according to a new survey. KPMG Forensic, which has been monitoring fraud levels for 20 years, said today that the total value of cases heard by UK courts in 2007 - £1.02bn - was the highest recorded since 1995.

It's a huge leap from the previous year's £221m figure. Despite that, the number of fraud cases was in fact down from 277 in 2006 to 197 for the year. Organised gangs made up close to 90 per cent, or £889m, of all fraud cases brought to crown courts in 2007. The government proved to be the most lucrative target for fraudsters involved in identity theft rings, benefit scams and VAT fraud, with the value of 68 cases totalling an eye-popping £833m. Carousel fraud continued to account for a huge number of losses to Her Majesty's Revenue and Customs (HMRC) last year.

[More]

FTC lists 2007's top consumer frauds

[Source: www.theregister.co.uk]

February 13, 2008

For the seventh year in a row, identity theft is the number one complaint reported to the US Federal Trade Commission. Americans reported 20 per cent more cases of consumer fraud in 2007 over the previous year, with nearly a third of the 813,899 complaints related to stealing personal data. The FTC released its latest damage report in the always-avant-garde annual rag, "Consumer Fraud and Identity Theft Complaint Data. Bathroom reading at its finest, care of the US government. Who were the winners and losers? Well, supposedly everyone on the list came out worse — but let's not look at that glass as half-empty. Chin up! The internet economy is still thriving!

[More]

VMware vuln exposes the perils of virtualization

[Source: www.theregister.co.uk]

February 25, 2008

Security researchers have discovered a bug in VMware desktop virtualization applications that allows attackers to take complete control of the underlying PC, including the execution or modification of files on the host operating system. The vulnerability, which was unearthed by researchers from Core Security Technologies, is particularly important to individuals and companies working in the world of computer security. They frequently turn to VMware Player and Workstation as a means of protecting their machines when analyzing Trojans and other types of malware. In a nutshell, the vulnerability allows attackers to break out of the virtual environment and gain full access to the host computer system.

"This vulnerability provides an important wake-up call to security-concerned IT practitioners," Core researchers wrote. "It signals that virtualization is not immune to security flaws and that 'real' environments aren't safe simply because they sit behind virtual environments." Core has released proof-of-concept code that allows customers to understand exactly how the bug works in real-world settings.

[More]

Europe still top source of spam

[Source: www.news.com]

February 06, 2008

European spam networks have pumped out more unsolicited e-mail than those in the U.S. for the third month in a row, according to security vendor Symantec. Symantec called this a "significant shift" in spam trends as, historically, compromised U.S. computers have been used to send spam, and many spammers have been U.S.-based.

Fredrik Sjostedt, one of Symantec's European product marketing managers, told ZDNet UK on Tuesday that Symantec suspects gangs are taking advantage of the increasing European broadband market. "The penetration of broadband is tremendous in Europe," Sjostedt said. "We've now clearly overtaken the U.S. in sending spam." Symantec also believes many spammers are now based in Europe. "Historically the majority of spammers were U.S.-based, but now we're seeing a lot of Eastern European and Russian spam gangs active. Spammers tend to use closer turf as a jump off point," Sjostedt said.

[More]

DoS attack prevents access to WordPress.com blogs

[Source: www.computerworld.com]

February 19, 2008

The WordPress.com blog-hosting service suffered a denial-of-service (DoS) attack that began Saturday and was still preventing users from logging in or posting to their blogs on Tuesday.

Matt Mullenweg, spokesman for Automattic, confirmed that the service experienced a DoS attack with spikes of up to 6 gigabits of incoming traffic, which was making some blogs inaccessible for about five to 15 minutes on Tuesday. Though service had mostly been restored, Automattic, which maintains WordPress.com, was still working on returning service to normal levels on Tuesday afternoon, he said.

"Obviously that [is not good] and is pretty unusual for our service," he said in an e-mail. "All our people who can are working on the issue." However, an employee at a New York-based company that has blogs hosted by WordPress.com suggested that some users were experiencing outages for longer than 15 minutes. The source, who asked not to be identified, said on Tuesday afternoon that users there were unable to log in to their blogs and post comments for "most of the day." However, the blogs were still able to be viewed publicly. "It's starting to come back to life now, slowly," said the source on Tuesday afternoon. WordPress.com users were notified via e-mail about the DoS attack. In the e-mail, the service provider said that the attack was affecting user log-in and causing some forums to be offline.

[More]

Universities fend off phishing attacks

[Source: www.securityfocus.com]

February 01, 2008

In an ongoing attack, students and faculty at nearly a dozen universities and colleges have been targeted by phishing e-mails since the middle of January. The e-mail messages masquerade as missives from each school's help desk, asking that the student confirm their username and password, as well as requesting more personal information, including date of birth and country of origin. The attacks, which appear to have started as early as January 20 and are ongoing, have targeted a few thousand e-mail addresses at each school, according to reports posted to two security mailing lists used by school information-technology professionals. "The attacks are fairly widespread (with) in U.S. .edu," Douglas Pearson, technical director of the Research and Education Network (REN) Information Sharing and Analysis Center (ISAC), stated in an e-mail interview. "We've seen large, small, public, and private institutions attacked." Schools targeted include Columbia University, Duke University, Princeton University, Purdue University, and the University of Notre Dame. The e-mail accounts of students and faculty that fall prey to the fraud are used, in most cases, to send out further spam as part of a lottery scam, Pearson and IT administrators stated. The attack may have already hit European schools earlier in the month, one university IT administrator stated on a security mailing list. The lottery scam, known also as a Nigerian Advance Fee scam, offers extremely large sums of money to the victim, if the victims first sends a smaller amount to the fraudster. In reality, the group running the scam will continue to ask for money from the victim, delaying the final payoff. The con is also known as a 419 scam, after the Nigerian legal code that it violates.

[More]

E-Mail Carries Love And Viruses For Valentine's Day

[Source: www.informationweek.com]

February 12, 2008

The FBI is warning that an unexpected e-card in your in-box may contain the Storm Worm virus. Just in time for Valentine's Day, Google (NSDO: GOOG) on Tuesday released the results of a survey showing that young people are embracing e-mail to send love letters. Coincidentally, the FBI warned on Tuesday that cybercriminals are embracing e-mail to send fake love letters. "The survey affirmed that e-mail is an increasingly important part of our most intimate and personal interactions, and that younger people are leading the charge: they are more likely to use e-mail for everything from sending love letters to ending relationships," said Google group product marketing manager Jen Grant in a blog post. But the FBI advises caution. "If you unexpectedly receive a Valentine's Day e-card, be careful," the agency said. "It may not be from a secret admirer, but instead might contain the Storm Worm virus."

Security software vendor Trend Micro issued a similar warning on Monday. "As we had already forecast last month, Storm is already sending their Valentine greetings this week," said security researcher David Sancho in a blog post. "The owners of this powerful botnet are doing as much as possible to [sustain the number of compromised machines at their disposal]. This includes spamming people and making them click on malicious links. This time around, the messages are of love."

More and more of this virus-laden e-mail love is coming from Russia. According to Sophos, Russia has overtaken China to become the second largest sender of spam, behind the United States.

[More]

Flaws Found In ActiveX Controls Used By Facebook, MySpace

[Source: www.informationweek.com]

February 05, 2008

US-CERT, part of the Department of Homeland Security, on Monday warned of the existence of an unpatched vulnerability in Aurigma's ImageUploader, image uploading software, which is used by both MySpace and Facebook. "By convincing a user to view a specially crafted HTML document (e.g., a Web page or an HTML e-mail message or attachment), a remote, unauthenticated attacker may be able to execute arbitrary code with the privileges of the user on a vulnerable system," explains US-CERT. The cybersecurity organization on Tuesday issued a similar warning for the Yahoo (NSDQ: YHOO) MediaGrid ActiveX control and the DataGrid ActiveX control. Six distinct buffer overflow vulnerabilities that affect several popular ActiveX controls have been reported in the past week, according to Symantec. The affected software includes Aurigma Imaging Technology ImageUploader4 and ImageUploader5, Yahoo MediaGrid and DataGrid ActiveX controls, and Facebook

Photo Uploader 4 ActiveX Control.

A flaw in MySpace.Uploader.4.1 ActiveX control was reported by Secunia on January 31 and an upgraded version of the software is available. Symantec (NSDO: SYMC) said it was not aware of any public exploitation of these vulnerabilities. Proof of concept exploit code is available, however. US-CERT encourages computer users to disable ActiveX controls to help make Internet browsing more secure.

[\[More\]](#)

Web Browsing, Search, And Online Ads Grow More Risky, Google Says

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

February 12, 2008

Google has found more than 3 million unique URLs on more than 180,000 Web sites that attempt to install malware on visitors' computers. Web browsing and searching are becoming increasingly risky activities, according to a report published by Google on Tuesday. "In the past few months, more than 1% of all search results contained at least one result that we believe to point to malicious content and the trend seems to be increasing," said Niels Provos, a security engineer at Google (NSDO: GOOG), in a blog post. Provos said that in the year and a half since Google began tracking malicious Web pages, the company has found more than 3 million unique URLs on more than 180,000 Web sites that attempt to install malware on visitors' computers. Provos co-authored a technical paper, "All Your IFRAMEs Point To Us," with Panayiotis Mavrommatis, a Google colleague, and two Johns Hopkins University computer scientists, Moheeb Abu Rajab and Fabian Monrose. The paper describes the increasing impact of "drive-by downloads," the exploitation of Web browser vulnerabilities to download and run malware automatically on the computers of Web site visitors. Remarkably, Provos and his co-authors acknowledge that Internet advertising, Google's lifeblood, is contributing to malware distribution. This is an issue that has been raised by security companies recently, but to hear it coming from Google is unusual. In general, industry-backed research tends to confirm business models rather than call them into question. A Google spokesperson didn't immediately reply to a request for comment.

[\[More\]](#)

Orkut worm feeds on scraps

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

February 29, 2008

Malware authors have written a worm for Orkut, Google-owned networking site that's big in Brazil. The Scrapkut worm uses active code injection to spread between victims and their friends on Orkut. The malicious code appears on a victim's scrapbook, containing a link to a supposed YouTube video. People who click on the link are redirected to an external site hosting malware that's disguised as a Flash upgrade. Users duped into installing the software get malicious Javascript code injected into their next active Orkut web session. This malicious scrapbook entry is then sent to all the victims' friends, recommencing the infection cycle. Judging by the counter on a web page associated with the malware (not the most reliable of indicators) about 13,000 users are already infected by the Scrapkut worm, which isn't - for now - doing anything particularly nasty other than spreading. By contrast an earlier worm that spread across the Orkut network last December infected an estimated 655,000 people. Google plugged the cross-site scripting (XSS) error that made the attack possible hours later, thwarting further propagation of that fast-spreading worm.

[\[More\]](#)

Japan brings down Godzilla of spam

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

February 19, 2008

Japanese police have arrested a "prolific spammer" who allegedly bombarded inboxes with hundreds of millions of messages punting internet gambling and dating sites. Investigators reckon Yuki Shiina, 25, sent as many as 2.2 billion spam messages using what appears to be rudimentary spamming techniques. He allegedly purchased a list of 600,000 email addresses for a pricey ¥100,000 (\$927), earning ¥2m (\$18,540) through a subsequent spamming campaign, security vendor Sophos reports. Shiina reportedly faked the message headers of junk mail he sent in a bid to avoid detection, an offence against local anti-spam laws. There's no mention of the use of compromised machines to send spam - standard practice for junk mail scumbags over recent years, and a powerful technique to frustrate both basic spam blocking and investigatory techniques. Complaints from a local ISP over the volume of junk mail it was processing resulted in an investigation that led onto Shiina's arrest by Tokyo's finest.

[\[More\]](#)

MayDay! MayDay! Ruskiies reinvent cyber crime

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

February 13, 2008

Researchers have unearthed two previously undetected botnets that exhibit sophisticated new capabilities that could significantly advance the dark art of cyber crime. One of them, dubbed MayDay by security firm Damballa, uses new ways to send and receive instructions to infected machines. One communication method uses standard HTTP that is sent through an organization's web proxy. That allows the malware to circumvent a common security measure employed by many large companies. Indeed, Tripp Cox, vice president of engineering and operations at Damballa, says he's observed MayDay running inside some of the world's most elite organizations, including Fortune 50 companies, educational institutions and ISPs.

[\[More\]](#)