



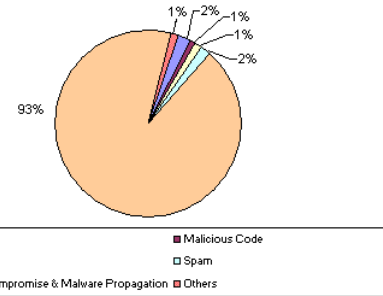
## CERT-In Monthly Security Bulletin May 2009

### Cyber Intrusion Trends

In this month 1222 security incidents were reported to CERT -In from various National/ International agencies. As shown in the figure, 93 % incidents related to Spreading of malware through website compromise were reported in this month. 01 % incidents related to virus/worm under the Malicious code category, 02 % phishing incidents , 01 % unauthorized scanning ,02 % incidents related to spamming , 01 % incidents related to technical help under the Others category were also reported in this month..

In this month CERT -In tracked 07 C&C (Command & Control) servers and 4, 53,076 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 May 2009



### Indian Websites Defacement

364 Indian websites were defaced during May 2009. The vulnerabilities which might have been exploited for the defacements are :

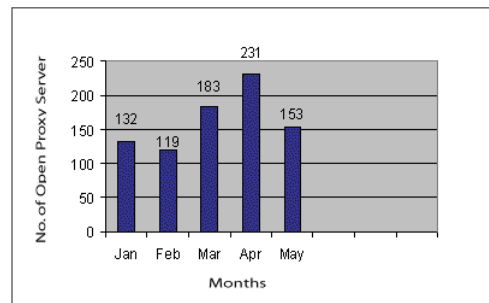
Vendor/Product	Title of Vulnerability	References & Patch Information
Microsoft -IIS	Remote Authentication Bypass Vulnerability in Microsoft IIS 6.0 WebDAV	<a href="#">CIVN-2009-63</a>
Apache	Apache "Options" and "AllowOverride" Security Bypass Vulnerability	<a href="#">CIVN-2009-66</a>
PHP	PHP remote file inclusion vulnerability in linkadmin.php in Beerwin PHPLinkAdmin 1.0	<a href="#">CVE-2009-1025</a>
PHP / Joomla!	Multiple PHP remote file inclusion vulnerabilities in the InterJoomla ArtForms (com_artforms) component 2.1b7 for Joomla	<a href="#">CVE-2009-1822</a>
PHP	CRLF injection vulnerability in bs_disp_as_mime_type.php in the BLOB streaming feature in phpMyAdmin	<a href="#">CVE-2009-1149</a>
PHP	Static code injection vulnerability in setup.php in phpMyAdmin	<a href="#">CVE-2009-1151</a>
Joomla!	SQL injection vulnerability in the com_musica module in Joomla!	<a href="#">CVE-2008-6234</a>
Joomla!	SQL injection vulnerability in the Versioning component (com_versioning) 1.0.2 in Joomla! and Mambo	<a href="#">CVE-2008-6184</a>

### 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 153 open proxy servers functioning in India during May 2009. 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 May 2009



### Attack Trend

#### Email scams circulating related to the Swine Flu

It has been reported that malicious users are taking advantage of the recent Swine Flu outbreak by distributing unsolicited emails with swine-flu-themed subjects. The attacks arrive through an unsolicited email message typically containing a subject line related to the Swine Flu. These email messages may contain a link or an attachment. If users click on this link or open the attachment, they may be directed to a phishing website or infected with malicious code.

[\[More\]](#)

#### Worm Conficker/Downadup/Kido widely propagating

It has been observed that worm Win32/Conficker/Downadup/kido is spreading widely by exploiting a previously reported Server Service vulnerability described in CERT - In vulnerability note [CIVN-2008-170](#) and Microsoft Security Bulletin [MS08-067](#).

Apart from exploiting the said vulnerability, the attack vectors include network shares (ADMINIS shares with a long list of hard-coded passwords), removable drives (drops a hidden autorun.inf file), scareware (fake security alerts to frighten consumers into purchasing bogus computer security software) and most recently Metasploit payload (the exploitation method derived from the metasploit ms08\_067\_netapi module to spread itself).

It is reported that this worm is actively infecting Windows systems with specific language operating systems such as English, Chinese, Arabic, Portugese.

[\[More\]](#)

**Training**

**Workshop on "Critical Information Infrastructure Resiliency" on 19 - 21 May 2009**

A 3 day workshop "Critical Information Infrastructure Resiliency" was conducted on 19 - 21 May 2009. The objective of this workshop is to create awareness among Government/ Govt. organisations and critical information infrastructure providers to advance critical information infrastructure security and resiliency. Delegates were from Government, Corporate and critical sector organizations.

**Workshop on "Wireless Security" on 28 - 29 May 2009**

A 2 day workshop on "Wireless Security" was conducted on 28 - 29 May 2009. Wi-Fi security incidents and malicious use are on rise in India . Unsecured Wi-Fi can provide easy access to attackers to cause severe damage while remain invisible and undetected. The objective of this workshop is to create awareness within the Government, critical sector and Communications & Information Infrastructure organizations on wireless(Wi-Fi) security, wireless network vulnerabilities & wireless attacks. Delegates were from Government, Corporate and critical sector organizations.

**Security Alerts**

**The critical and medium vulnerabilities in various Operating Systems, Application software and Network devices discovered during March 2009 and their countermeasures along with 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 Office PowerPoint	May 13, 2009	<a href="#">CIAD-2009-24</a>
Microsoft	Remote Code Execution Vulnerability in Microsoft DirectShow	May 31, 2009	<a href="#">CIVN-2009-65</a>
Microsoft	Remote Authentication Bypass Vulnerability in Microsoft IIS 6.0 WebDAV	May 19, 2009	<a href="#">CIVN-2009-63</a>
IBM	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
IBM	IBM Tivoli Storage Manager Remote Agent Service Buffer Overflow Vulnerabilities	May 11, 2009	<a href="#">CIVN-2009-62</a>
Linux	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Linux	Multiple Vulnerabilities in Linux Kernel	May 15, 2009	<a href="#">CIAD-2009-25</a>
Miscellaneous	Title of Vulnerability	Discovery/Publish Date	CERT-In References & Patch Information
Adobe	Adobe Flash Media Server RPC Call Privilege Escalation Vulnerability	May 05, 2009	<a href="#">CIVN-2009-61</a>
Wireshark	Wireshark Denial of Service Vulnerability	May 28, 2009	<a href="#">CIVN-2009-64</a>

**Malicious Code Threats**

Title of Malicious Code	Type	Overview	Aliases	Discovery Date	References
Mibling Worm	Worm	It has been observed that a worm named Mibling is spreading in the wild. It spreads through instant messaging clients and opens a backdoor on the infected system to connect itself to the IRC channel to listen to remote attacker commands.	No aliases found	May 24, 2009	<a href="http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-060421-2348-99&amp;tabid=1&amp;docid=2009-060421-2348-99&amp;tabid=1">http://www.symantec.com/business/security_response/writeup.jsp?docid=2009-060421-2348-99&amp;tabid=1&amp;docid=2009-060421-2348-99&amp;tabid=1</a>
Backdoor QAKBOT	Backdoor	It has been observed that a Backdoor named QAKBOT is spreading in the wild. It gets downloaded into the user's system when user visits malicious websites. It opens a hidden window and connects to remote websites to downloads possible commands issued by the attacker.	No aliases found	May 12, 2009	<a href="http://threatinfo.trendmicro.com/vinfo/apac/virusencyclo/default5.asp?VName=BKDR%5FQAKBOT%2EAF&amp;VSet=T">http://threatinfo.trendmicro.com/vinfo/apac/virusencyclo/default5.asp?VName=BKDR%5FQAKBOT%2EAF&amp;VSet=T</a>
Worm NEERIS	Worm	It has been observed that a Worm named Neeris is spreading in the wild. It spreads through infected removable drives and may be downloaded when user visits malicious websites.	No aliases found	May 26, 2009	<a href="http://threatinfo.trendmicro.com/vinfo/apac/virusencyclo/default5.asp?VName=WORM%5FNEERIS%2EL&amp;VSet=PVName=WORM%5FNEERIS%2EL&amp;VSet=P">http://threatinfo.trendmicro.com/vinfo/apac/virusencyclo/default5.asp?VName=WORM%5FNEERIS%2EL&amp;VSet=PVName=WORM%5FNEERIS%2EL&amp;VSet=P</a>

**Security News**

**Experts: Gumblar attack is alive, worse than Conficker**

[Source: <http://news.cnet.com>] 28 May 2009

Gumblar, a new attack that compromises Web sites, has added new domain names that are downloading malware onto unsuspecting computers, stealing FTP credentials to compromise more sites, and tampering with Web traffic, a security firm said on Thursday.

The Gumblar attack started in March with Web sites being compromised and attack code hidden on them. The malware downloaded onto those sites came from the gumblar.cn domain, a Chinese domain associated with Russian and Latvian IP addresses that were delivering code from servers in the U.K. , ScanSafe said last week.

As Web site operators cleaned up their sites, the attackers replaced the original malicious code with dynamically generated and obfuscated JavaScript, making it difficult for security tools to identify. Attackers also changed the domain to martuz.cn, but now both domains have been shut down, according to ScanSafe.

Because the attackers made changes to the configurations of servers hosting compromised Web sites, they are able to continue controlling them and adding new domains for downloading exploit code onto computers of visitors to the sites, Mary Landesman, a senior security researcher at ScanSafe said on Friday. "At some point these attacks (on Web sites) will start again," she said.

[\[More\]](#)

#### **Pirated Windows 7 RC builds botnet**

[Source: <http://news.cnet.com>] 14 May 2009

A pirated version of [Windows 7](#) Release Candidate infected with a Trojan horse has created a botnet with tens of thousands of bots under its control, according to researchers at security firm Damballa.

The software, which first appeared on April 24, spread as quickly as several hundred new bots per hour, and controlled roughly 27,000 bots by the time Damballa took over the network's command and control server on May 10, the firm said Tuesday.

The pirated software was spread via popular piracy sites and online forums, Damballa said.

The software is primarily designed to download and install other malicious packages under a "pay-per-install" scheme, under which the botmasters are paid based on the number of other pieces of malware they cause to be installed, Damballa said.

Infected installations are continuing to appear at a rapid rate, according to the company.

"We continue to see new installs happening at a rate of about 1,600 per day with broad geographic distribution," Tripp Cox, Damballa's vice president of engineering, said in a statement. "Since our takedown (of the command and control server), any new installs of this pirated distribution of Windows 7 RC are inaccessible by the botmaster."

However, the botmaster still controls the existing installations, Damballa said. The infected systems are mainly concentrated in the U.S. , with 10 percent, and the Netherlands and Italy , with 7 percent each.

[\[More\]](#)

#### **Microsoft IIS vuln played no role in server breach, uni says**

[Source: <http://www.theregister.co.uk>] 21 May 2009

Network administrators at Ball State University have retracted their claims that a campus website was brought down by a zero-day vulnerability in Microsoft's Internet Information Services webserver.

"Microsoft and Ball State now have identified the cause of the breach [as] a Ball State iWeb user [who] either misused or allowed the misuse of their account, and that was determined just this afternoon," Ball State University spokesman Tony Proudfoot said on Thursday.

The account corrects an advisory campus officials issued that claimed the breach was the result of someone targeting a vulnerability in versions 5 and 6 of IIS that allows attackers to list, access, and in some cases upload files in a password-protected folders of vulnerable machines. The vulnerability exists when IIS uses the WebDAV protocol. The advisory was featured prominently on the university's website.

[\[More\]](#)

#### **Report: Turkish hackers breached U.S. Army servers**

[Source:<http://news.cnet.com/>] 29 May 2009

Hackers based in Turkey penetrated two U.S. Army Web servers and redirected traffic from those Web sites to other pages, including one with anti-American and anti-Israeli messages, according to a report in InformationWeek.

The hackers, who go by the group name "m0sted," breached a server at the Army's McAlester Ammunition Plant in Oklahoma on January 26 and a server at the U.S. Army Corps of Engineers' Transatlantic Center in Winchester , Va. , on September 19, 2007 , the report said.

Investigators believe an SQL injection attack was used to exploit a vulnerability in Microsoft's SQL Server database in order to gain access to the servers.

[\[More\]](#)

#### **PC-pwning infection hits 30,000 legit websites**

[Source: <http://www.theregister.co.uk>] 29 May 2009

A nasty infection that attempts to install a potent malware cocktail on the machines of end users has spread to about 30,000 websites run by businesses, government agencies and other organizations, researchers warned.

The infection sneaks malicious javascript onto the front page of websites, most likely by exploiting a common application that leads to a SQL injection, said Stephan Chenette, manager for security research at security firm Websense. The injected code is designed to look like a Google Analytics script, and it uses obfuscated javascript, so it is hard to spot.

The malicious payload silently redirects visitors of infected sites to servers that analyze the end-user PC. Based on the results, it attempts to exploit one or more of about 10 different unpatched vulnerabilities on the visitor's machine. If none exist, the webserver delivers a popup window that claims the PC is infected in an attempt to trick the person into installing rogue anti-virus software.

The rogue anti-virus software uses polymorphic techniques to constantly alter its digital signature, allowing it to evade detection by the vast majority of legitimate anti-virus programs. Because it uses obfuscation, the javascript is also hard to detect by antivirus programs and impossible to spot using Google searches that scour the web for a common string or variable.

[\[More\]](#)

#### **Phishing For Phishing For Twitter Popularity**

[Source: <http://blog.trendmicro.com/>] 28 May 2009

As many as 13,000 Twitter users have been affected by a new "worm-like" phishing attack that feeds on some members' desire to gain more followers. The said scam dupes

users into forking over their account names and passwords using a Web site called "Twittercut."

When they click on the link, they are redirected to a fraudulent Twitter Web site that asks them for their account name and password. Once the needed login details are entered, the site sends similar messages to all of the affected users' followers, along with links to a paid dating service.

The messages are said to have started from an account called @twittercut, which had been disabled. But then the tweets continued to come, this time from a new account called @tweetcut. The latter is now also inoperative.

The site operators at TwitterCut denied phishing allegations and announced that they were shutting the site down.

"According to several social network blog sites, TwitterCut has been the bud of several rumors," they said on a message on their site. "Our website and its programmers can assure you that these rumors are not true and that TwitterCut is simply a Twitter train that was a work in progress!"

[\[More\]](#)

#### **Seminal password tool rises from Symantec ashes**

[Source: <http://www.theregister.co.uk/> 27 May 2009]

More than three years after Symantec unceremoniously pulled the plug on L0phtcrack, the seminal tool for auditing and cracking passwords is back with a set of new capabilities.

L0phtcrack 6 is available from the same team of hackers who introduced it to the world a decade ago. The program was pulled from the market in late 2005 shortly after it was acquired by Symantec, presumably because its offensive capabilities didn't fit in with the company's portfolio of defensive products and services.

While programs like John the Ripper and Cain and Abel in many ways filled the void, L0phtcrack is credited with bringing awareness about password strength to the masses.

"It was one of the few tools that you could use to do password cracking that looked legitimate at the time," said HD Moore, founder of the Metasploit project. "It became fairly common for not only the pen testers and the assessment folks to use but also very common for system administrators to use to audit the passwords of their systems."

[\[More\]](#)

#### **FBI and US Marshals laid low by mystery virus**

[Source:<http://www.theregister.co.uk/>] 22 May 2009

A mystery viral infection forced the FBI and US Marshals Service to pull the plug on parts of their respective computer networks .

A spokesperson for the US Marshals Service explained that it had disconnected some of its computers from the wider Justice Department systems, as a precaution against spreading the as yet unidentified malware further. Access to internal email and the internet is being restricted at both the FBI and Marshals service while techies try to identify the precise cause of the problem.

Both government agencies stress that only unclassified systems are affected by the issue and that operations are proceeding as normal, despite the computer hiccup. Each is downplaying possible fears that the breach might lead to the compromise of sensitive data.

[\[More\]](#)

#### **BitDefender launches 'suck it and see' free anti-virus scanner**

[Source: <http://www.theregister.co.uk/> 21 May 2009]

Romanian anti-virus firm BitDefender has begun offering a free version of its anti-virus scanner software to consumers.

Similarly cut-down versions of BitDefender's anti-phishing and chat encryption software are also being offered at no charge to home users.

The launch of free editions of its security suites is designed to increase BitDefender's visibility in a crowded marketplace and to tempt users into evaluating its products. It's not designed as an alternative to paid-for antivirus software packages not least because it lacks some of the protection found in comparable free editions of anti-virus packages from AVG and Avast, for example.

BitDefender Free Edition is an on-demand virus scanner which omits real-time protection against viruses or other forms of malware. Users wanting anything beyond vanilla virus scanning and removal are advised to use a standard antivirus product, such as BitDefender Antivirus 2009 (or comparable suites from Symantec, Panda, Trend Micro, Kaspersky et al.)

Bogdan Dumitru, BitDefender's CTO , explained: "BitDefender Free Edition is perfect for users who want to quickly scan and disinfect a PC, even if they are already using an anti-malware solution."

BitDefender Anti-Phishing Free Edition provides browser-based protection from phishing fraud by blocking access to malicious web sites. The tool is compatible with IE and Firefox. BitDefender Chat Encryption allows users to share encrypted message via Yahoo! Messenger or Windows Live Messenger providing both parties are running BitDefender's IM scrambling software.

[\[More\]](#)

#### **D-Link router's CAPTCHA flawed, WPA passphrase retrieved**

[Source: <http://blogs.zdnet.com/>] 19 May 2009

It took only a week for the researchers at SourceSec to find a flaw in the CAPTCHA implementation of D-Link's recently introduced CAPTCHA in its routers, originally aimed to prevent DNS changing malware from automatically achieving its objective.

According to SourceSec, the flawed implementation allows an attacker/malware to retrieve the router's WPA passphrase with user-level access only, and without even a properly solved CAPTCHA. Moreover, a combination of a simple Javascript code using anti-DNS pinning doesn't even require the attacker to have malware installed on the router, instead, the attack can be triggered by visiting a web site.

Here's how the attack works:

- Malware loads the router's index page and glean the salt generated by the router
- The malware uses the salt to generate a login hash for the D-Link User account (blank password by default)
- The malware sends the hash to the post\_login.xml page
- The malware sends a request to the wifisc\_add\_sta.xml page, activating WPS
- The attacker uses WPSpy to detect when the victim's router is looking for WPS clients, and connects to the WiFi network using a WPS -capable network card

[\[More\]](#)

#### **Gumblar Google-poisoning attack morphs**

[Source: <http://www.theregister.co.uk/>] 19 May 2009

A Web attack that poisons Google search results is getting worse, according to security researchers.

The attack first relies on compromising normally legitimate website and planting malicious scripts. US CERT reports that stolen FTP credentials are reckoned to be the main technique in play during this stage of the attack but poor configuration settings and vulnerable web applications might also play a part.

Surfers who visit compromised websites are exposed to attacks that rely on well-known PDF and Flash Player vulnerabilities to plant malware onto Windows PCs.

This malware is designed to redirect Google search results as well as to swipe sensitive information from compromised machines, according to early findings from ongoing analysis.

The SANS Institute's Internet Storm Centre (ISC) adds that the attack has been around for some time but has intensified over recent days. Initially the malware was served up onto vulnerable Windows clients from the website gumblar.cn, which has been offline since Friday. A second domain - martuz.cn - has taken over this key role in the attack, ISC reports.

[\[More\]](#)

#### **Kaspersky Lab Neutralizes New Variant of the Sinowal Rootkit**

[Source: <http://usa.kaspersky.com/>] 18 May 2009

Kaspersky Lab, a leading developer of Internet threat management solutions that protect against all forms of malicious software, has implemented detection and treatment for a new variant of a unique MBR rootkit, Sinowal. The new variant of Sinowal, a malicious program that is capable of hiding its presence in the computer system by infecting the Master Boot Record (MBR) on the hard drive, was detected at the end of March 2009. Over the last month Sinowal has been actively spreading from a number of malicious sites that use the Neosploit exploit toolkit.

Kaspersky Lab analysts have been monitoring the Sinowal bootkit since early 2008; however the new variant came unexpectedly. Unlike earlier versions, the new modification, Backdoor.Win32.Sinowal has these features:

- It penetrates much deeper into the system to avoid being detected
- A stealth method that hooks into device objects at the operating system's lowest level
- Sinowal conceals the payload's activities, which are designed to steal user data and various account details
- It can penetrate a system through a vulnerability in Adobe Acrobat and Reader, which allows a maliciously rigged PDF file to plant malware on a system without the user's knowledge.

This is the first time cybercriminals have used such sophisticated technologies. It also explains why no antivirus products could treat computers infected or even detect the new Sinowal modification when it first appeared. Implementing detection and treatment for Sinowal has been one of the toughest jobs facing antivirus researchers.

[\[More\]](#)

#### **56th variant of the Koobface worm detected**

[Source: <http://blogs.zdnet.com/>] 15 May 2009

Researchers from PandaLabs are reporting on the detection of the 56th variant of the Koobface worm (Boface.BJ.worm), spreading across Facebook, Tagged, Friendster, MySpace, MyYearBook, Fubar.com, Hi5 and Bebo since May, 2008.

According to the company, the growth of Koobface related infections is as high as 1,200% since the first time it was detected over an year ago, where almost 40% of the infections based in the U.S, with the growth trend also confirmed by Microsoft's Malware Protection Center .

What the cybercriminals have changed this time is the template, the use of an Ukrainian web site hosting service, and the "missing" fake codec, which upon execution is not only converting the infected PC into a hosting provider part of the campaign, but is also pushing scareware, **liveantimalwareproscanner .com** and **live-antimalware-scanner .com** in particular.

[\[More\]](#)

#### **UC Berkeley computers hacked, 160,000 at risk**

[Source: <http://news.cnet.com/>] 08 May 2009

Hackers broke into the University of California at Berkeley 's health services center computer and potentially stole the personal information of more than 160,000 students, alumni, and others, the university announced.

At particular risk of identity theft are some 97,000 individuals whose Social Security numbers were accessed in the breach, but it's still unclear whether hackers were able to match up those SSNs with individual names, Shelton Waggener, UCB's chief technology officer, said in a press conference.

The attackers accessed a public Web site and then bypassed additional secured databases stored on the same server. In addition to SSNs, the databases contained health insurance information and non-treatment medical information, such as immunization records and names of doctors patients had seen. No medical records (i.e. patient diagnoses, treatments, and therapies) were taken, as they are stored in a separate system, emphasized Steve Lustig, associate vice chancellor for health and human services.

[\[More\]](#)