CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Analysis of defaced Indian websites Year-2006

by

S. S. Sarma and Garima Narayan

Department of Information Technology
Ministry of Communications and Information Technology
Government of India

Issue Date: March 31, 2007

Index

1. Introduction

Web Defacement is the term applied to the unauthorized modification of a website. Other terms may be used i.e web jacking, vandalism, cyber graffiti and so on. Web defacement occurs when an intruder maliciously alters a webpage by inserting or substituting provocative or offending data.

The primary objective of this paper is to present the detailed statistical analysis of defaced Indian websites during year 2006. In the year 2006 a total of 5211 Indian websites were defaced , on an average of about 14 websites per day.

CERT-In has published statistics of Indian website defacement for the first half of the year 2006 vide white paper CIWP-2006-02. This paper discusses the statistics for the complete year 2006.

2. Distribution of defaced domains

This paper attempts to present an overview of defacement activities targeted against Indian web sites. The domains included for analysis are

- Top level domains (*.com, .net, .org and .edu*) and
- Country code top level domain – ccTLD (*.co.in, .net.in, .gov.in, .org.in, .nic.in, .ac.in, .ernet.in and .res.in*).

Figure 1 shows the segregation of defacement for the year 2006 on six month basis. In the second half of the year 2006 significant increase in Indian website defacement was noticed.

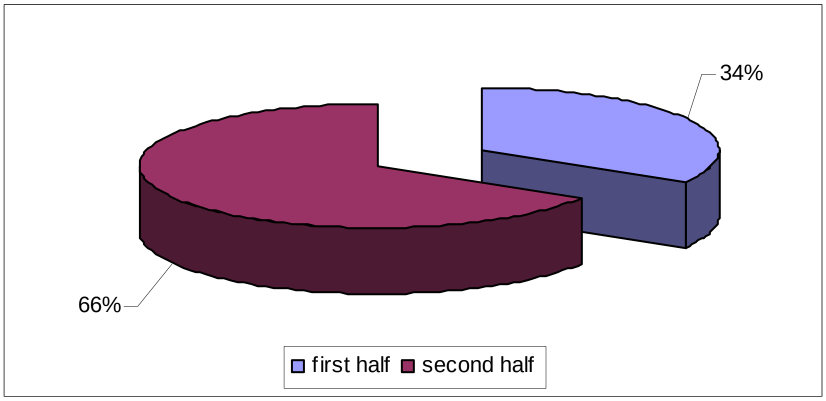

Figure 1: Distribution of defacement

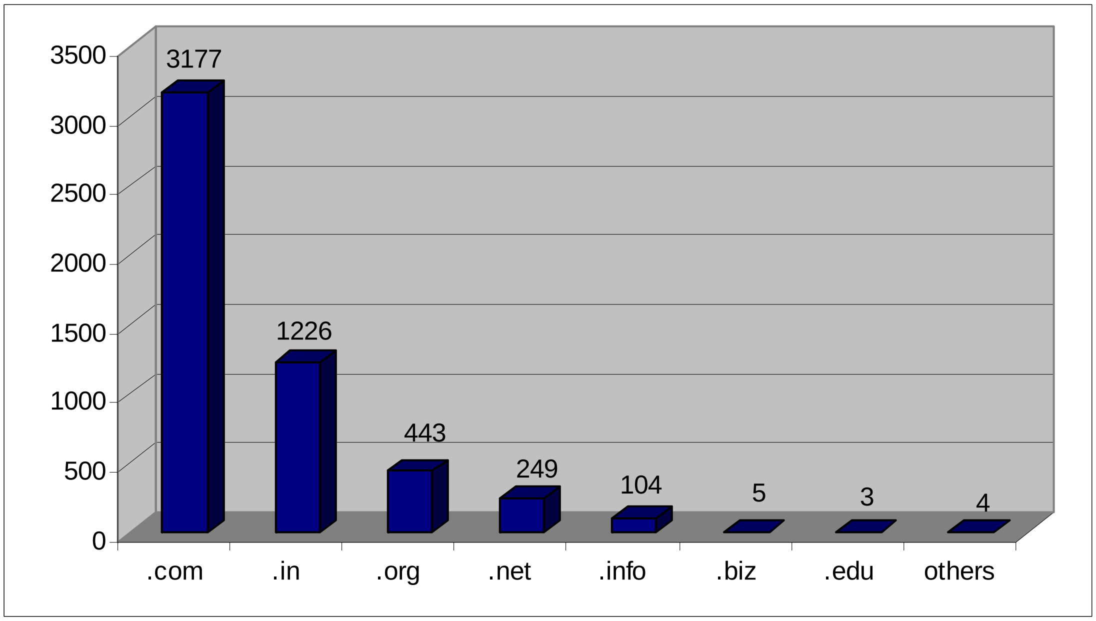

Figure 2 : Distribution of Defaced Domains

Figure 2 and 3 shows the Distribution of the total Indian website defacement.

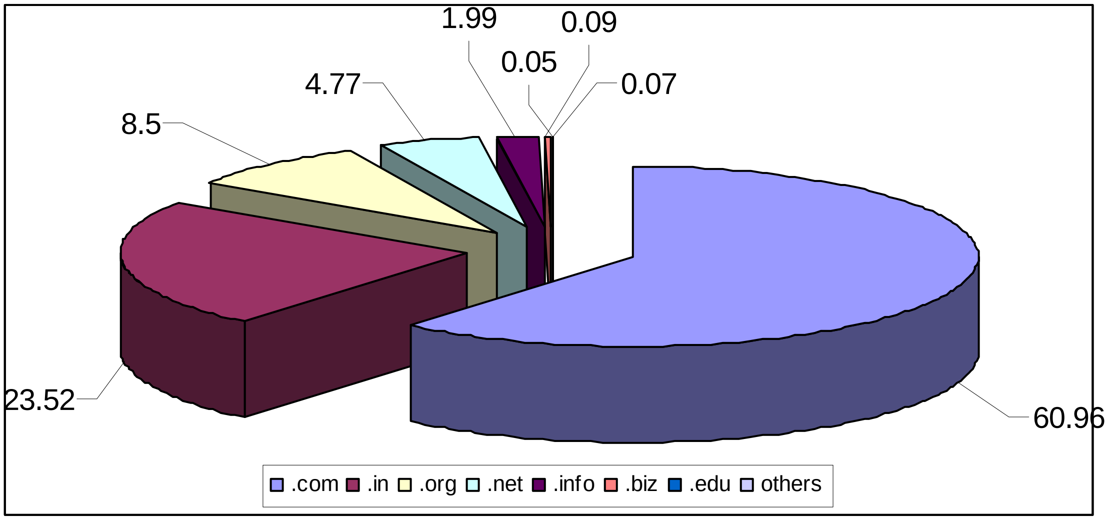

Figure 3: % Distribution of Defaced Domains

In the year 2006 in all 5211 Indian websites were defaced. Out of these, 60.96% were *.com* domain websites and 23.52% were *.in* domain websites. The statistics shows the increase in the *.in* domain defacement in comparison to previous year. *.in* domain defacements were second largest in the year 2006. In the year 2006 *.com* and *.org* domains has received less defacement in comparison to year 2005.

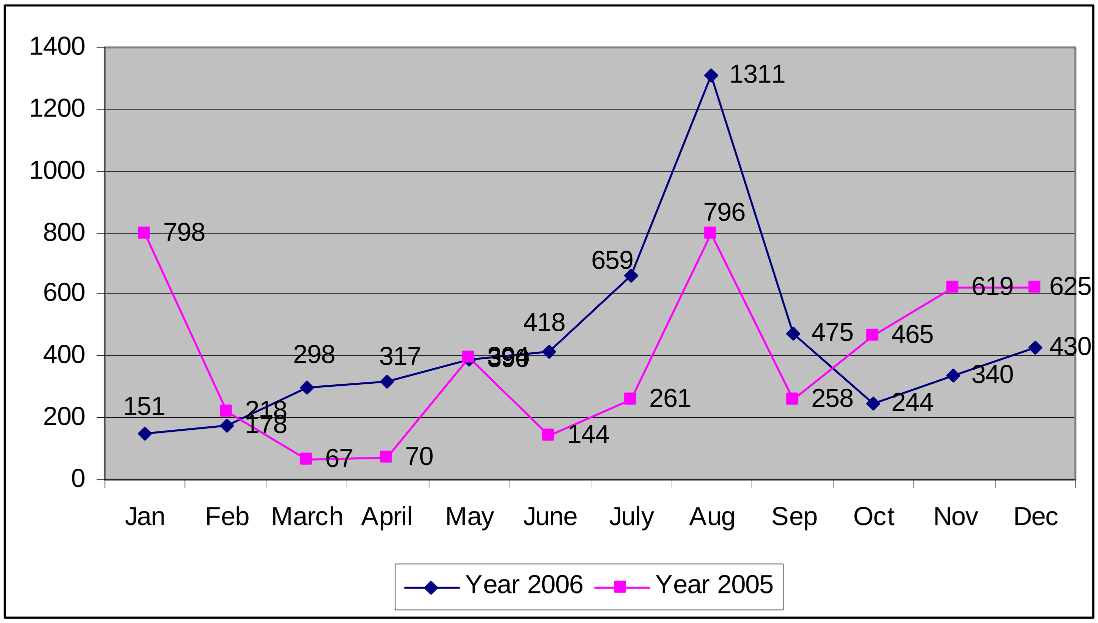

Figure 4: Comparison with year 2005 data

Figure 4 shows the month wise comparison of the Indian website defacements in year 2005 and 2006. In the month of August unusual increase has been noticed in the year 2005 as well as in the year 2006. In the year 2006 total 1311 defaced Indian websites were tracked. Highest number of defacements were on 14th August 2006, one day before the Independence day 15th August 2006.

2.1 Distribution of defaced domains by second level ccTLD

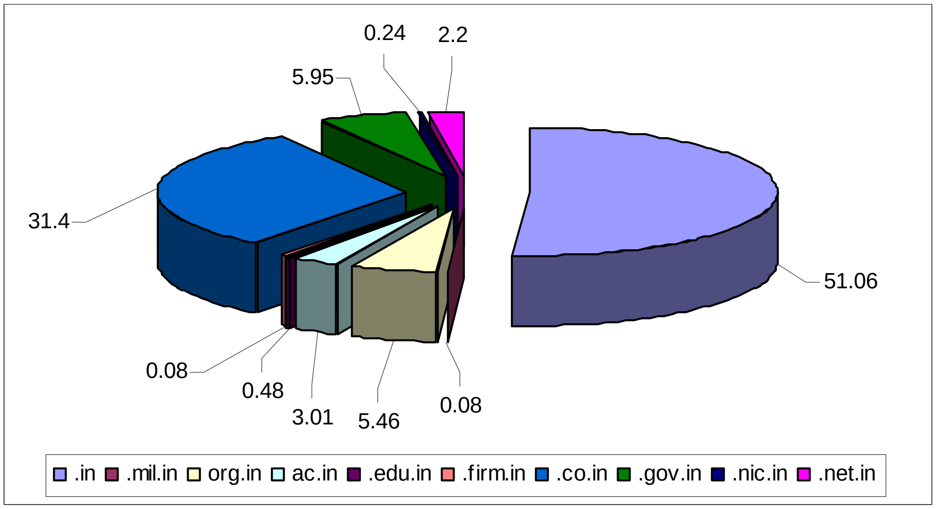

Figure 5 : Distribution of Defaced Domains by ccTLD

Figure 5 shows the distribution of defacements under *.in* domain. In total, 1226 Indian websites under *.in* domain were defaced during year 2006. 51.06% defacement was on *.in* domain, 31.4% defacements were on *.co.in* domain and 5.95% share goes to *.gov.in* domain.
In the year 2006, 278 websites under *.in* domain were defaced in the first half (Jan-June) and rest 948 were defaced in the second half (July – Dec). The statistics shows defacers were more active in the second half of the year 2006.

It may be noted that the websites under *.in* domain are not only hosted in India but they may also be hosted outside India or registered by persons residing outside India.

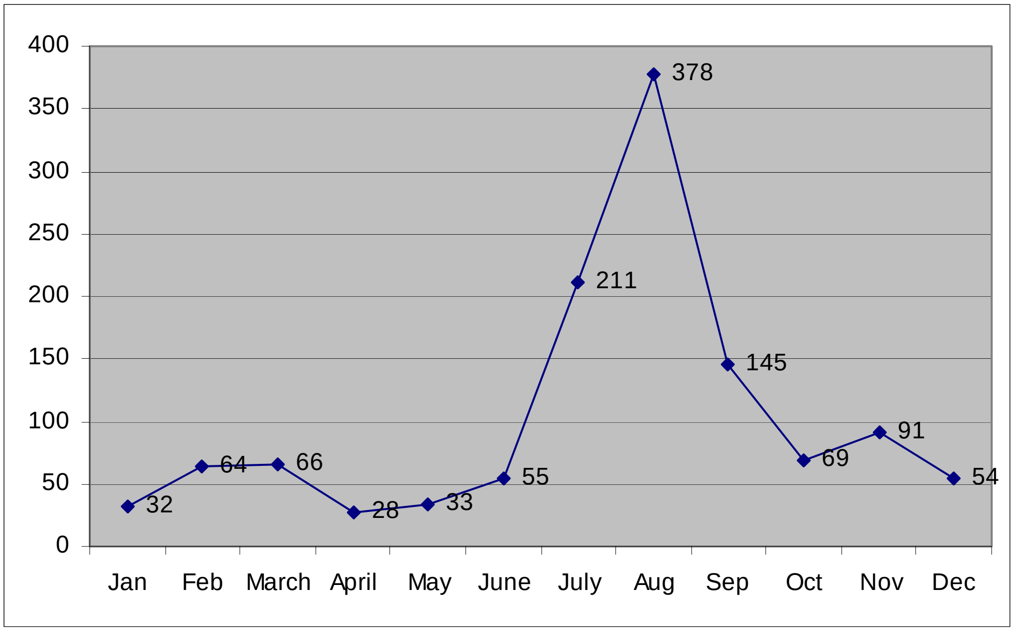

Figure 6: Month wise .in ccTLD defacement

Figure 6 shows month wise defacement on *.in* domain. In the month of August, most number of *.in* domain websites were defaced, i.e., 378 websites were defaced in a single month which is more than the total *.in* domain defacement in the first half of the year 2006 and total *.in* domain defacements in the year 2005.

2.2 Sector wise Defacement

Figure 7 shows the Sector wise defacements in ccTLD. Statistics show higher defacements in commercial sector, it is 85% of all the ccTLD defacement.

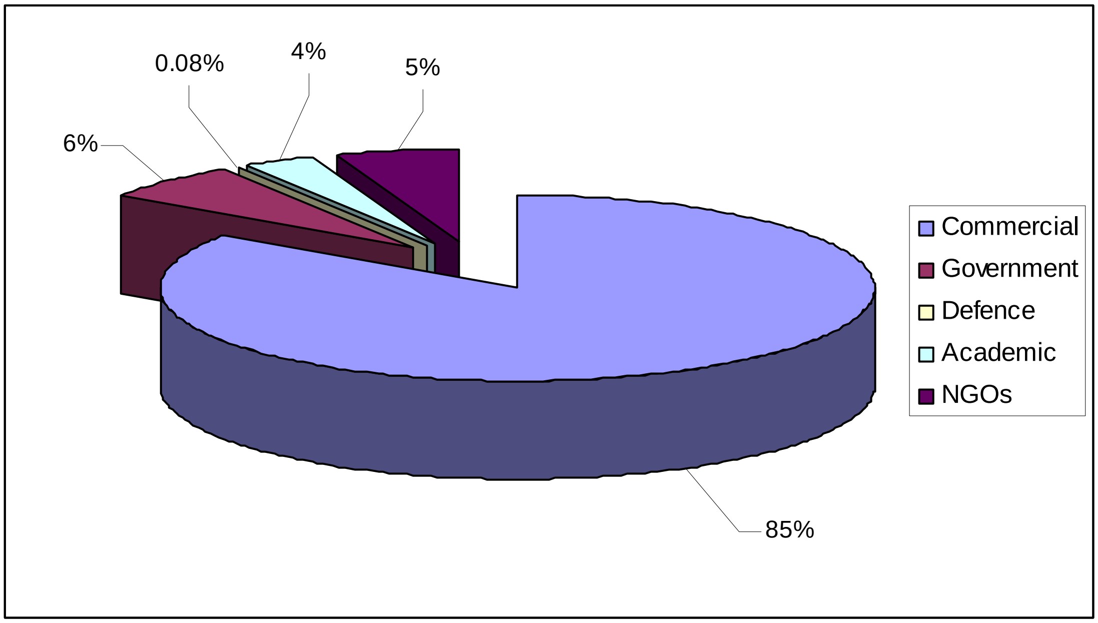

Figure 7: Sector wise Defacement

3. Time Line of Defacements

3.1. Defacements by year

Figure 8 shows the year wise *.in* domain defacement. Significant increase has been noticed in the *.in* defacements. In the year 2006, 1226 Indian websites under *.in* domain were defaced. This is highest in 6 years. It is even more than the sum of the previous five years defacements. This increase may also indicate higher number of websites being registered in .in domain in recent years.

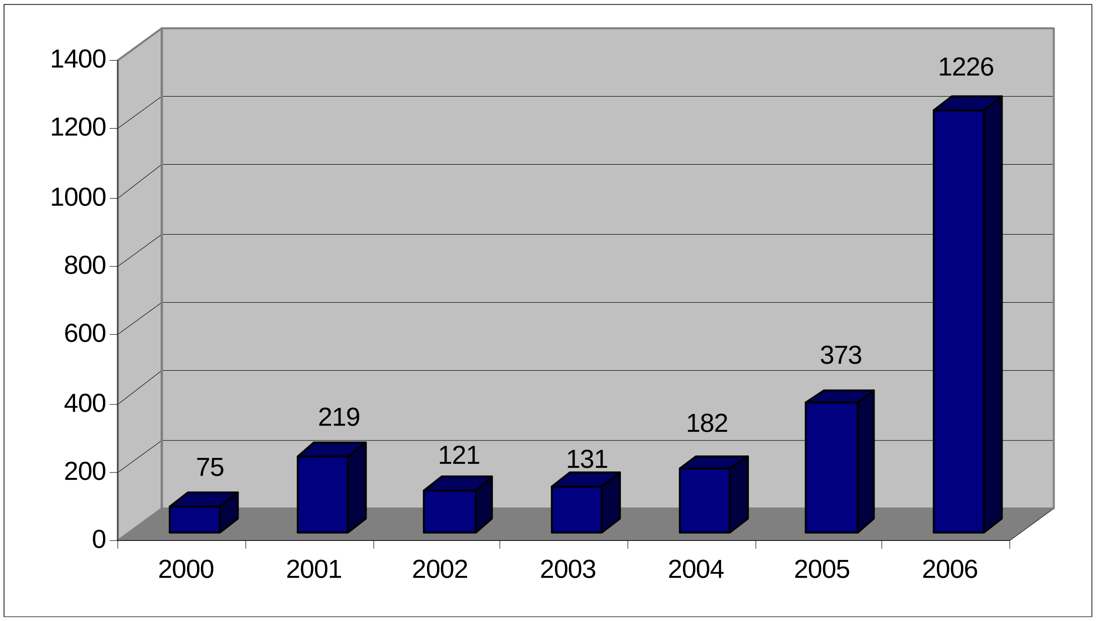

Figure 8: .in defacements year wise

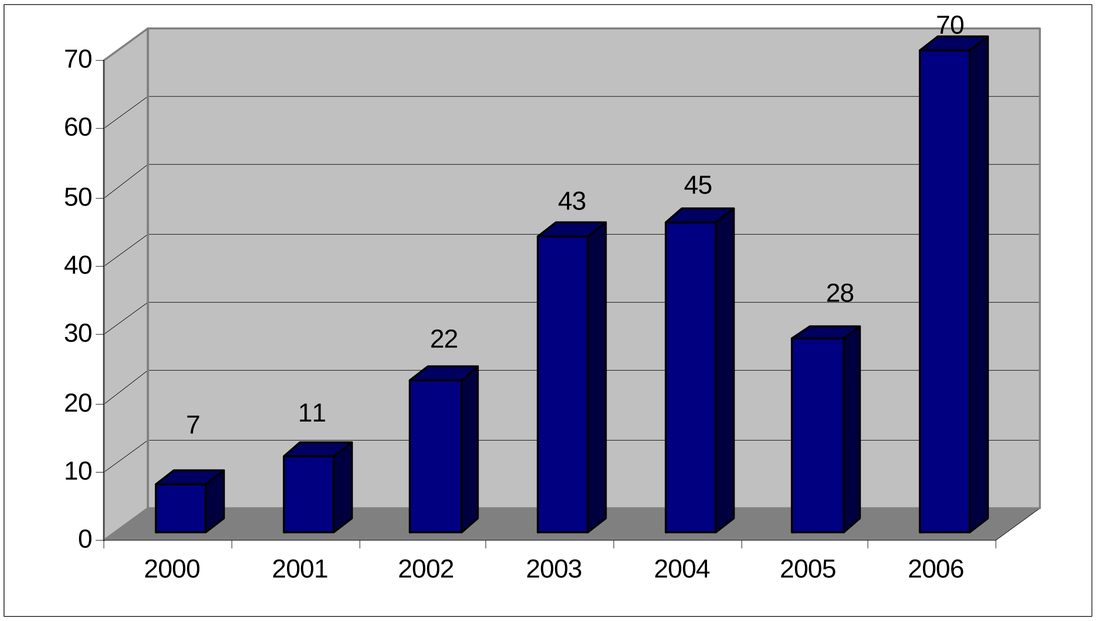

Figure 9: .gov.in defacement year wise

Figure 9 shows the year wise .gov.in defacement. In the year 2006, 70 Indian government websites were defaced. In the month of February, websites of Government of Punjab were targeted and in the month of November, Government of Rajasthan websites were targeted. All the Government of Rajasthan websites were hosted on the same server and were defaced at very short intervals of one or two days. Some of these Websites were:

http://janmitra.gov.in//delta.htm
http://rajirrigation.gov.in/delta.htm
http://rajcmrelief.gov.in/images/delta.htm
http://rajshiksha.gov.in/images/delta.htm
http://rajtaxboard.gov.in/delta.htm
http://rajdst.gov.in/delta.htm

All the above websites were defaced by “DeltahackingSecurityTEAM” and were hosted in US at the time of defacement.

3.2. Highest Defacements in a single day

Table 1 Shows the Highest defacement on a single day in the first half of year 2006.

S.No.	Date	No. of Defacements
1	8/14/2006	320
2	3/27/2006	227
3	5/25/2006	189
4	12/14/2006	188
5	8/5/2006	155
6	9/20/2006	134
7	9/5/2006	130
8	5/28/2006	123
9	4/6/2006	118
10	7/27/2006	103

Table 1: Highest Defacement on a single Day

It is been observed that all the defacements on a single day were mass defacements and done mostly by the same defacer Group.

Indian websites received the highest defacement on a single day on 14/8/2006, one day before the Independence Day. 320 Indian websites were defaced on that day; it was a mass defacement on the IP 69.64.33.17 in which 319 websites was defaced by hacker group CyberLords. Second and third highest defacements on a single day were done by the hacker's group LORD. In the mass defacement of 27/03/06 on the IP 216.185.43.165, the site of CENTRAL INLAND FISHRIES RESEARCH INSTITUTE, BARRACKPORE, WEST BENGAL was defaced.

4. Hacker wise Defacements

4.1 Top Defacers TLD wise

Table 2 shows the top 10 TLD defacers in the first half of the year 2006.

S.No	Defacer	No.of websites	Percentage of total TLD defacement
1	LORD	434	8.32
2	CyberLord	388	7.44
3	yusufislam	340	6.52
4	Devil-X	194	3.72
5	aLpTurkTegin	183	3.51
6	kardeshackerlar	176	3.37
7	G00DY S3CURITY TEAM	176	3.37
8	b4d_m00d	133	2.55
9	crackers_child	128	2.45
10	ssh-2	127	2.43

Table 2: Top Defacers TLD wise

Top defacer group on Indian website defacements was LORD; LORD defaced 434 websites in the year 2006, and in which 424 was in the first half of the year 2006. All the defacements done by

LORD was on Win 2003 server. LORD is a Turkish hacker group. CyberLord had been a very active hacker group in the year 2006. All the defacement on the eve of Independence Day was done by CyberLord, it is also a Turkish hacker group and has defaced websites on Windows machines as well as on Linux machines. Two Indian government websites were targeted by the defacer group in the month of august *http://suratmunicipal.gov.in/* and *http://cgwborissa.gov.in/.* In the month of July and August hacker group yusufislam, another Turkish Hacker was very active and defaced 61 websites under .in domain.

4.2 Top Defacer ccTLD wise

Table 3 shows the Top defacers of ccTLD.

S.No.	Defacer	No. of Sites
1	crackers_child	103
2	CyberLord	70
3	yusufislam	58
4	LORD	50
5	EL_MuHaMMeD	46
6	G00DY S3CURITY TEAM	43
7	kardeshackerlar	41
8	ihtilal.org	38
9	ssh-2	36
10	DeltahackingSecurityTEAM	32

Table 3: Top Defacer ccTLD wise

5. Operating System wise Defacement

Figure 10 shows the operating system wise defacement statistics. In the the year 2006 windows been the most targeted operating system. In total defacements of 5211, 2918 defacements were on Windows systems (Win NT, Win 2000, Win 2003).

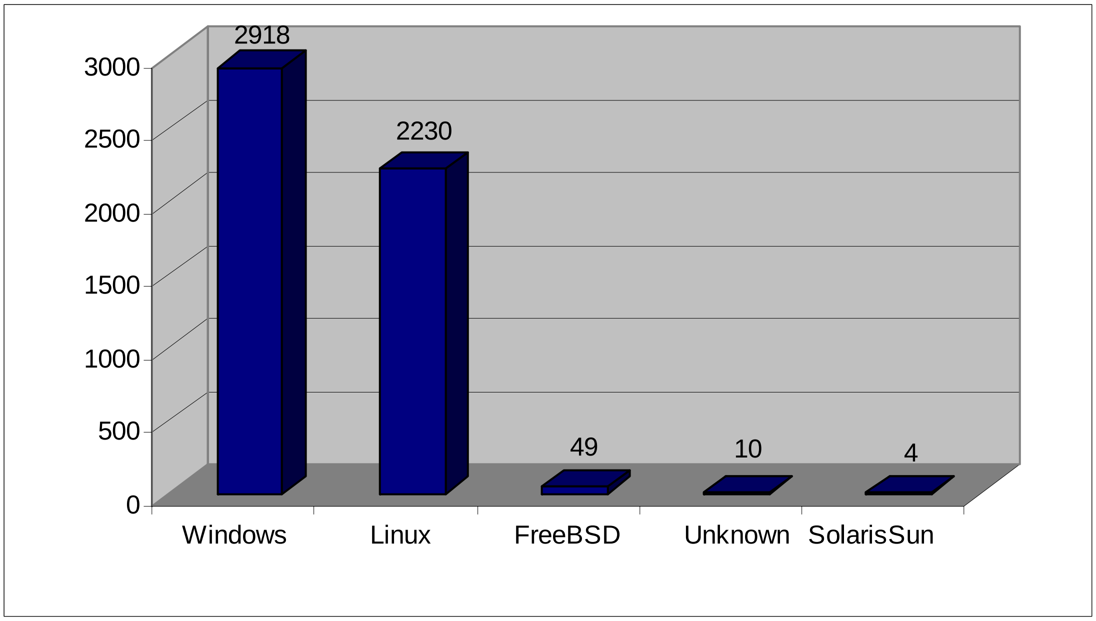

Figure 10: Defacement Operating System wise

5.1 Domain Wise Operating System Defacement

Table 4 shows the Operating system wise defacement on TLD's.

	.com	.in	.org	.net	edu	.info	.biz
Windows	1853	631	227	154	3	35	5
Linux	1293	569	214	90	0	69	0
FreeBSD	23	22	1	4	0	0	0
Solaris	6	2	1	0	0	0	0
Unknown	2	2	0	1	0	0	0

Table 4: Operating system TLD wise

Figure 11 shows the domain defacement operating system wise. In each domain windows have the most no. of defacements.

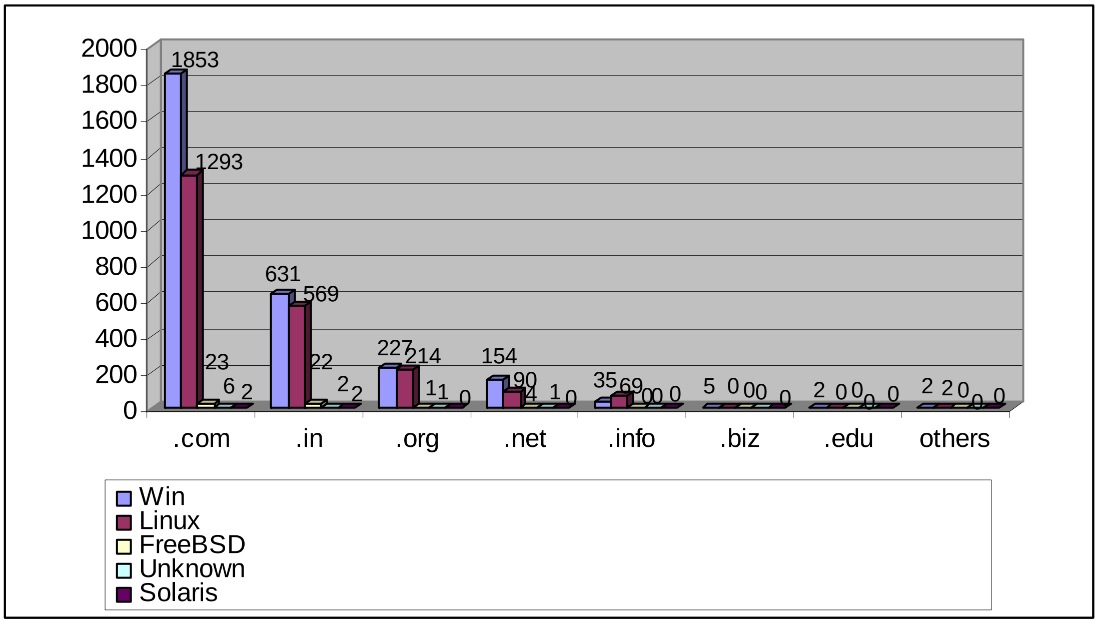

Figure 11: Domain wise Operating System Defacement

It has been observed that the Indian websites defaced in year 2006 were mostly hosted on the Windows machine.

6. Defacement by Networks

6.1 Most Targeted Networks

Table 5 shows the most targeted networks. Among the Indian ISPs, VSNL received the most no of attacks.

S. No.	ISP	No. of Websites	Country
1	TPIS NETBLOCK	443	US, some range in India
2	THE PLANET	438	USA, some range in India
3	VSNL IN	345	IN
4	S4Y1 NET	323	US
5	AOTECH	229	US
6	IANA NETBLOCK	228	US
7	FORTRESSITX	209	US
8	CW NETBLOCK	192	US
9	PEER1 SERVERBEACH	166	US
10	SOFTLAYER NETBLOCK	156	US

Table 5 : Most Targeted Networks

It has been observed that the large number (61%) of Indian websites defaced in year 2006 was hosted outside India. Table 6 shows the Indian ISP which have received the major defacement during year 2006.

S. No.	ISP	No. of Websites
1	VSNL	345
2	NET4	134
3	Spectrum	75

Table 6 : Most Targeted Indian Networks

6.2 Most Targeted IP

Table 7 lists the most defaced IPs in the first half of the year 2006.

S.No.	Defaced IP	No. Of Websites	ISP
1	69.64.33.17	320	S4Y1-NET(US)
2	216.185.43.165	228	AOTECH-NETBLK01(US)
3	67.19.173.228	195	NETBLK-THEPLANET-BLK-11 (US)-----THEPLANET-BLK-11 (IN)
4	64.92.173.50	185	SAVVIS (US)
5	70.86.75.178	173	NETBLK-THEPLANET-BLK-13(US)-----THEPLANET-BLK-13 (IN)
6	70.86.129.59	164	NETBLK-THEPLANET-BLK-13(US)----THEPLANET-BLK-13 (IN)
7	70.86.46.178	163	NETBLK-THEPLANET-BLK-13 (US)-------- THEPLANET-BLK-13 (IN)
8	64.34.166.12	162	PEER1-BLK-08 (US)
9	203.199.113.30	135	VSNL-IN
10	67.19.231.146	121	NETBLK-THEPLANET-BLK-11 (US)----- THEPLANET-BLK-11 (IN)

Table 7: Most Targeted IPs

7. Commonly used Website Defacement techniques

Web Defacement is the term applied to the unauthorized modification of a website. Other terms may be used i.e web jacking, vandalism, cyber graffiti and so on. Web defacement occurs when an intruder maliciously alters a webpage by inserting or substituting provocative or offending data.

Web defacement is a significant and major threat to business developing an online presence. Defacement of a website can detrimentally affect the credibility and reputation of the organization as a whole. Unlike other attack cases where the hacker hides his activities, in defacement incident, the major goal of the hacker is to gain publicity by demonstrating the weakness of the existing security measures.

Web defacement can range from simple graffiti designed to demonstrate the hacker's ability to enter a system to subversive convert sabotage aimed at fraud or theft. The motivation for defacing website can likewise vary from mischievous entertainment to criminal gain.

An important and often overlooked aspect of web design is web security. Securing a website is an extremely important step in maintaining data integrity and availability of resource.

The vulnerabilities which are often used by the attacker to deface a website are discussed in the following paragraphs:

Cross Site Scripting (CSS) is a common vulnerability in website design. The most common form of this style of attack is done in message boards and forms. It essentially exploits improper validation of forms and malicious code not being detected in message boards.

A Cross site scripting is caused by the failure of a web based application to validate user supplied input before returning it to the client system. "Cross Site" refers to the security restriction that the client browser usually places on data (i.e. cookies, dynamic content attributes, etc.) associated with web site. By causing the victim's browser to execute injected code under the same permissions as the web application domain, an attacker can bypass the traditional Document Object Model (DOM) security restriction which can result not only in cookie stealing but also in phishing, web defacement etc.

Websites that handle error incorrectly are also at risk. One form of hacking is to cause errors which give the hacker an opportunity to get inside the web server and perform malicious activities such as web defacement. When a hacker finds a site that has inappropriate error handling, he seizes the opportunity and cause continual errors until he finds a vulnerability to exploit and gain higher privileges.

Obtaining User names and passwords is a very popular and effective technique used by hackers to break into a website and deface it. Hackers use the information gathering techniques to retrieve the information.

If the hacker has a username, he can try to guess the password by going through a list of popular or default choices or by using intelligent guesses. Social engineering is also commonly used by hackers to gather sensitive information. After the hacker is logged on to the system, he tries to escalate his privileges i.e. obtain system administrator privileges. To do this, hacker does some additional information gathering such as the exact version and patch level of the operating system, the versions of software packages installed on the machine, and services and processes enabled etc. Using this information he accesses well known web sites and easily locates hacks that exploit vulnerabilities existing in the software installed. When these exploits are executed on the machine, the hacker ends up gaining privileged access rights and actually controls the machine. At this stage, he can simply change any page of the website.

HTTP smuggling and Response Splitting attacks are also very popular among hackers for defacing a website.

7.1 Significant Web Server/ Web Application Vulnerabilities

In the year 2006, web servers running on windows server were highly exploited. Vulnerabilities which have been exploited on different systems are listed below:
Windows

- Microsoft Windows Embedded Web Fonts Code Execution Vulnerability
  CERT-In Vulnerability Note CIVN-2006-03
  CVE-2006-0010
  Jan 10, 2006

- Windows Media Player Plug-in EMBED Element Buffer Overflow
  CERT-In Vulnerability Note CIVN-2006-13
  CVE-2006-0005
  February 15, 2006

- Microsoft Windows Explorer COM Object Handling Vulnerability
  CERT-In Vulnerability Note CIVN-2006-32
  CVE-2006-0012
  April 12, 2006

- Microsoft Windows ART Image Handling Buffer Overflow
  CERT-In Vulnerability Note CIVN-2006-45
  CVE-2006-2378
  June 14, 2006

- Microsoft JScript Memory Corruption Vulnerability
  CERT-In Vulnerability Note CIVN-2006-46
  CVE-2006-1313
  June 14, 2006

- TCP/IP Remote Code Execution Vulnerability
  CERT-In Vulnerability Note CIVN-2006-54
  CVE-2006-2379
  June 14, 2006

- Microsoft .NET Framework Application Folder Information Disclosure Vulnerability
  CERT-In Vulnerability Note CIVN-2006-63
  CVE-2006-1300
  July 12, 2006

- Microsoft Windows Server Service Buffer Overrun Vulnerability
  CERT-In Vulnerability Note CIVN-2006-75
  CVE-2006-3439
  August 09, 2006

- Windows Kernel Privilege Elevation Vulnerability
  CERT-In Vulnerability Note CIVN-2006-82
  CVE-2006-3444
  August 09, 2006

- Microsoft Windows GDI Kernel Structures Handling Vulnerability
  CERT-In Vulnerability Note CIVN-2006-113
  CVE-2006-5758
  November 07, 2006

- Microsoft Windows workstation Service Memory Corruption Vulnerability
  CERT-In Vulnerability Note CIVN-2006-117
  CVE-2006-4691
  November 15, 2006

- Microsoft XML Core Services XMLHTTP ActiveX Control Code Execution Vulnerability
  CERT-In Vulnerability Note CIVN-2006-112
  CVE-2006-5745
  November 15, 2006

IIS

- Microsoft Internet Information Services (IIS) 5.x
  Microsoft IIS Malformed URL Potential Denial of Service Vulnerability
  2005-12-19

- Microsoft Internet Information Services ASP Code Buffer Overflow
  CERT-In Vulnerability Note CIVN-2006-64
  CVE-2006-0026
  CVE-2006-6578
  CVE-2006-6579
  2006-07-11

Linux

- Linux Kernel "proc/base.c" Userspace Interaction Local
  Privilege Escalation Vulnerability
  CVE-2006-3626

- Multiple Linux Kernel SCTP vulnerabilities
  CERT-In AdvisoryCIAD-2006-25

- Linux Kernel Unspecified "init_timer()" Security Issue
  CVE-2006-5749

- Linux Kernel "ip_summed" Memory Corruption Vulnerability
  CVE-2006-6333

- Linux Kernel "do_coredump" Function Security Bypass and File Manipulation Vulnerability
  CVE-2006-6304

PHP

- PHP unserialize() Array Creation Integer Overflow vulnerability
  CERT-In Vulnerability Note CIVN-2006-104
  CVE-2006-4812
  October 12, 2006

- PHP-Nuke "modules/News/index.php" SQL Injection Vulnerabilities
  CERT-In Vulnerability Note CIVN-2006-122
  November 29, 2006

Apache

- Apache mod_imap "Referer" Cross-Site Scripting Vulnerability
  CVE-2005-3352
  2005-07-26

- Apache 2 mod_ssl Denial of Service Vulnerability
  CVE-2005-3357
  2006-01-06

- Apache Tomcat Directory Listing Denial of Service
  CVE-2005-3510
  2005-11-03

- Apache "mod_rewrite" Remote Off-By-One Buffer Overflow Vulnerability
  CERT-In Vulnerability Note CIVN-2006-74
  CVE-2006-3747

- Apache XSS vulnerability
  CVE-2006-3918

- Apache Mod_TCL Remote Format String Vulnerability
  CERT-In Vulnerability Note CIVN-2006-106
  CVE-2006-4154

- Apache mod_auth_kerb "der_get_oid()" Off-By-One Vulnerability
  CERT-In Vulnerability Note CIVN-2006-120
  CVE-2006-5989

- Apache mod_imap "Referer" Directive Cross Site Scripting Vulnerability
  CERT-In Vulnerability Note CIVN-2006-21
  CVE-2005-3352

Cross Site scripting Vulnerabilities

- Cross-site Scripting FrontPage Server Extensions Vulnerability
  CVE-2006-0015
  CERT-In Vulnerability Note CIVN-2006-34
  April 12, 2006

- Microsoft .NET Framework 2.0(ASP.NET 2.0) Cross-Site Scripting Vulnerability
  CERT-In Vulnerability Note CIVN-2006-95
  CVE-2006-3436

- Cross-site scripting (XSS) vulnerability in phpMyAdmin
  CVE-2006-3388

8. Errata

Primarily the data has been collected from defacement mirror website [Ref. 2] and the accuracy of this analysis is thus dependent on the data available on the defacement mirror.

9. References

1. Analysis of Defaced Indian websites under .in ccTLD
   www.cert-in.org.in/knowledgebase/whitepapers/CIWP-2004-01.pdf
   www.cert-in.org.in/knowledgebase/whitepapers/CIWP-2005-03.pdf

www.cert-in.org.in/knowledgebase/whitepapers/ciwp-2006-01.pdf
www.cert-in.org.in/knowledgebase/whitepapers/ciwp-2006-02.pdf

2. www.zone-h.org

10. List of Figures

11. List of Tables