CERT-In
Indian Computer Emergency Response Team
Enhancing Cyber Security in India

Analysis of defaced Indian websites Year-2006(till June)

By

Garima Narayan

Department of Information Technology
Ministry of Communications and Information Technology
Govt. of India

Index

1. Introduction

The primary objective of this paper is to present the detailed statistical analysis of defaced Indian websites during first half of year 2006. This paper is an extension to the earlier white papers "Analysis of Defaced Indian websites under .in ccTLD [Ref.1]. The data used in this analysis has been collected primarily from defacement mirror: zone-h [Ref.2].

2. Distribution of defaced domains

The primary objective of the paper is to give 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).

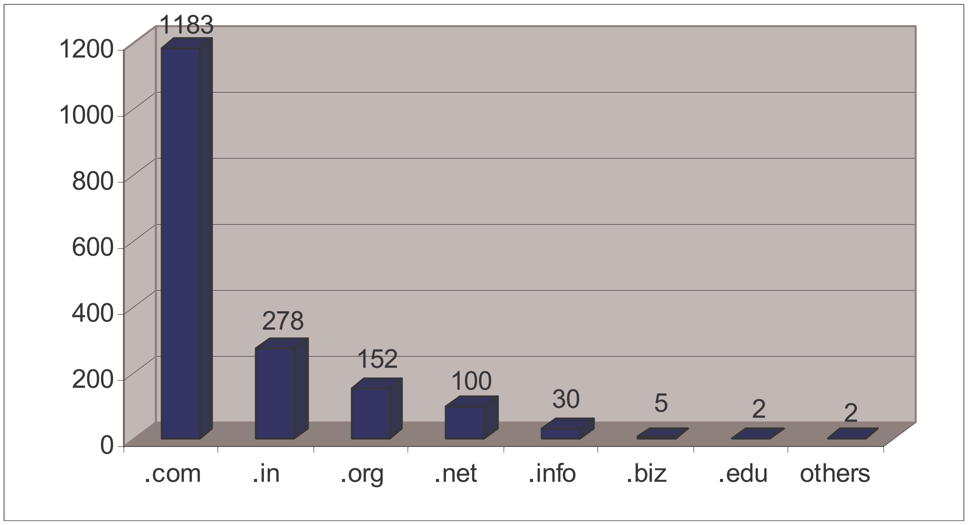

Figure 1: Distribution of Defaced Domains

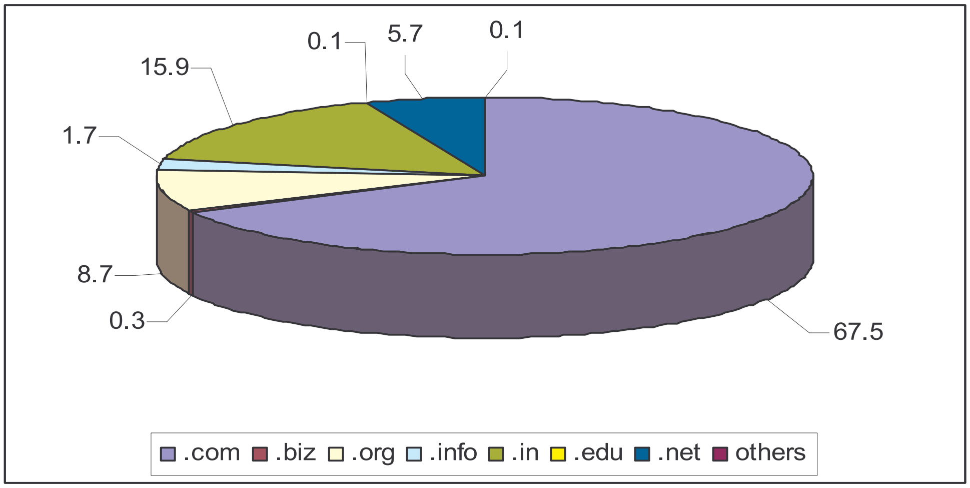

Figure 2: Distribution of Defaced Domains

In the first half of year 2006 total 1752 indian websites were defaced. 67.5 % were .com domain websites and 15.9% were .in domain websites. the statistics shows the increase in the .in domain defacement in comparison to previous year .in domain defacement. In year 2005 total 373 .in domain websites were defaced but 278 .in websites were defaced only in first half of the year 2006.

2.1 Distribution of defaced domains by second level ccTLD

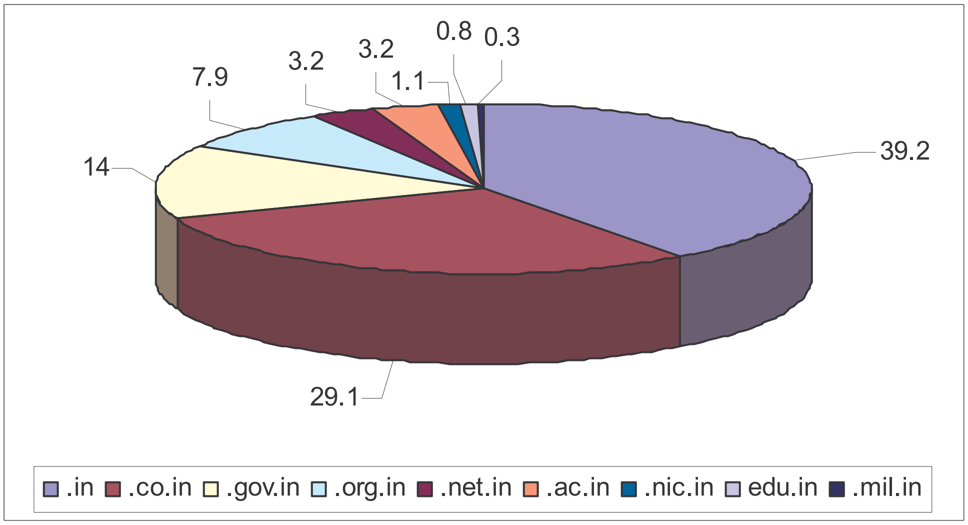

Figure 3: Distribution of Defaced Domains by ccTLD

In the first half of year 2006 increase in .gov.in websites defacement has been observed. 39 .gov.in sites were defaced in the first half of year 2006 which is 15.1 % of total .in domain defacement. 109 .in and 81 .co.in websites were defaced in this period.

2.2 Sector wise Defacement

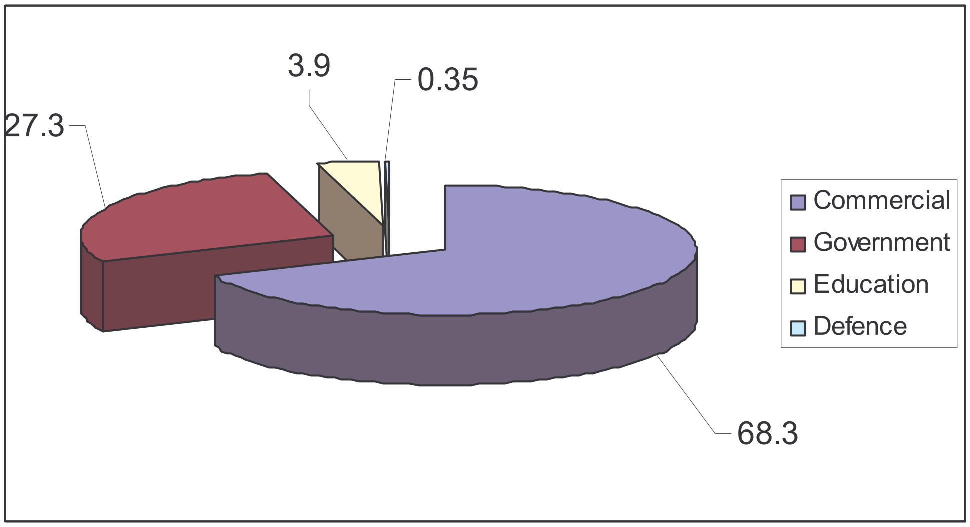

Figure 4 : Sector wise Defacement

Figure 4 shows the Sector wise defacement in ccTLD defacement. Statistics show a high no of defacement in commercial sector, it is 68.3% of all the ccTLD defacement. Government sector also has a big share, it is 27.3 % of all ccTLD defacement.

3. Time Line of Defacements

3.1. Defacements by year

Statistics shows an increase in the .in domain defacements. Only in the first half of the year 2006 total 278 .in websites were defaced in which major defacements were on the commercial Indian websites.

Figure 5 shows the year wise .in domain defacement. Drastic increase has been noticed in the .in defacements.

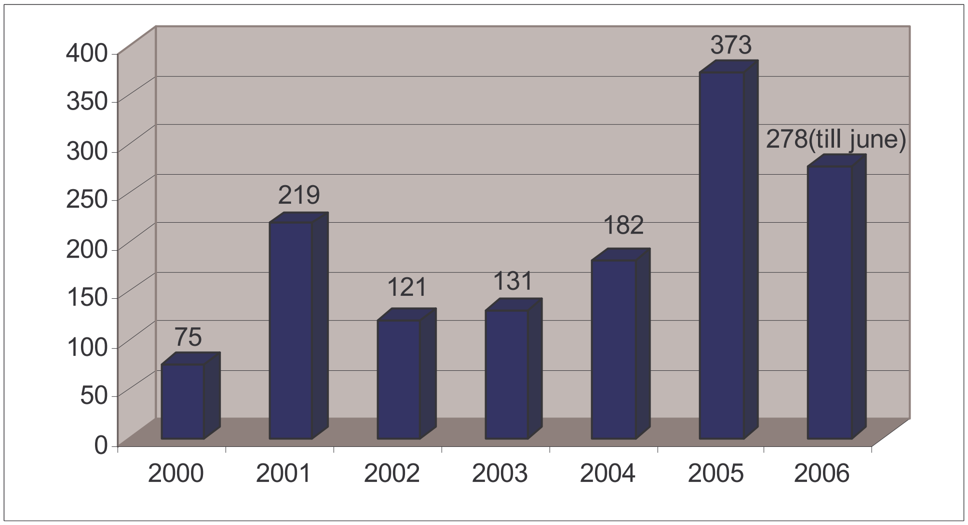

Figure 5: .in defacements year wise

Figure 6 shows the .gov.in defacements year wise. Only in the first half of the year 2006 42 .gov.in websites were defaced. The statistics of year 2005 shown decrease in the .gov.in defacements in comparison to year 2003 and 2004 but an increase in the .gov.in defacements has been observed in the year 2006.

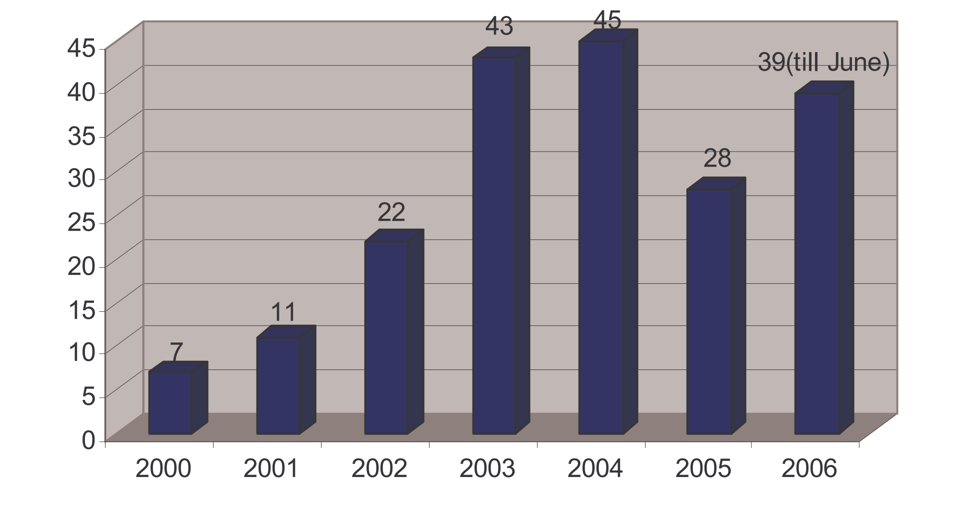

Figure 6:.gov.in defacement year wise

In these 39 .gov.in sites 27 sites were of Punjab government on a single day. nisd.gov.in were defaced two times in the first half of year 2006(http://ncdap.nisd.gov.in/webchat/choice.php, nice.nisd.gov.in/webchat/choice.php). another major defacements on http://www.aponline.gov.in/apportal/index.asp and //www.orissatourism.gov.in/mdoc/4index.htm .

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	3/27/2006	227
2	5/25/2006	189
3	5/28/2006	123
4	4/6/2006	118
5	4/8/2006	101
6	1/30/2006	54
7	2/6/2006	48
8	6/16/2006	45
9	6/20/2006	43
10	6/6/2006	42

Table 1: Highest Defacement on a single Day

Highest defacement observed on 27th March 2006, a total of 227 websites were defaced on this day followed by 189 websites on 25th May and 123 websites on 28th may. The defacement on

27th march includes 51 .in websites defacement. Major .in sites defaced on this day were http://www.cifri.gov.in/LORD.asp. all the defacement on the 27th March was done by LORD defacer group, it was a mass defacement on the IP belongs to a US based ISP. On 25th May it was also a mass defacement on a IP belongs to Millioncolors Hyderabad.

Figure 7 shows the websites defaced on 27th march 2006.

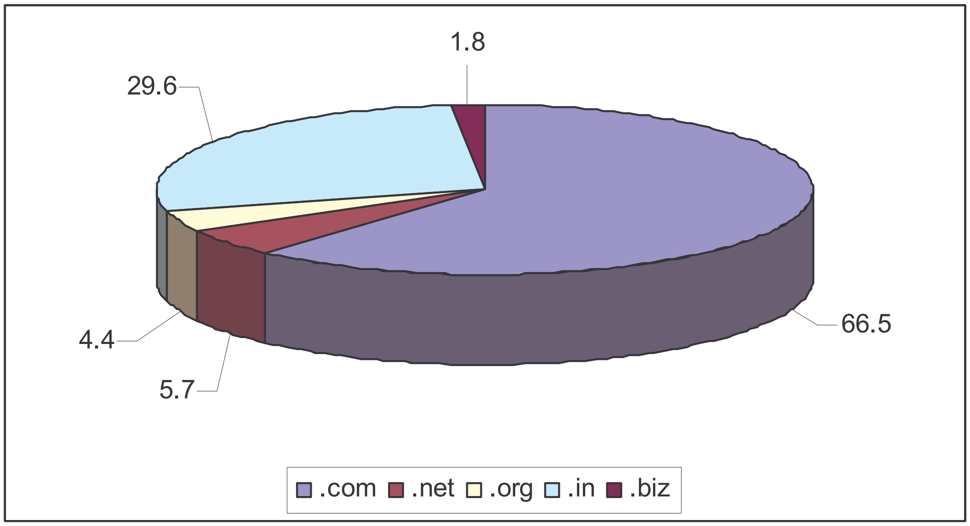

Figure 7: Defacement on 27/3/2006

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	424	24.2
2	aLpTurkTegin	177	10.1
3	b4d_m00d	133	7.6
4	Cyber-Warrior TIM	85	4.8
5	Xarnuz	78	4.4
6	IRANIAN BOYS BLACK HAT	52	3
7	eno7	46	2.6
8	DeltahackingSecurityTEAM	45	2.5
9	Lady_Lara	36	2
10	Mirim	35	1.9

Table 2: Top Defacers TLD wise

24.2 % of the total defaced sites were defaced by LORD defacer group. This is a Turkish defacer group and has been very active in the year 2006. this group leaves the message "HACKED BY LORD **Turkish Hacker"** on the defaced website. aLpTurkTegin is also a Turkish hacker. All the defacement done by b4d_m00d Hacker group was on a single day(6th April 2006). It was a mass defacement on an IP belongs to Videsh Sanchar Nigam Ltd. Most of the defacer group leaves message on the defaced websites praising them selves and mentioning about the website's security weaknesses. Some defacer group wants to spread messages among public (pro Islam).

4.2 Top Defacer ccTLD wise

Table 3 shows the Top defacers of ccTLD.

S.No.	Defacer	No. of Sites
1	LORD	50
2	eMP3R0r TEAM	28
3	aLpTurkTegin	23
4	DeltahackingSecurityTEAM	18
5	Xarnuz	17

Table 3: Top Defacer ccTLD wise

Figure 8 Shows the defacement by LORD hacker group on the Indian domains. All the websites of Indian domain defaced by LORD hacker group were on Win 2003 Operating System.

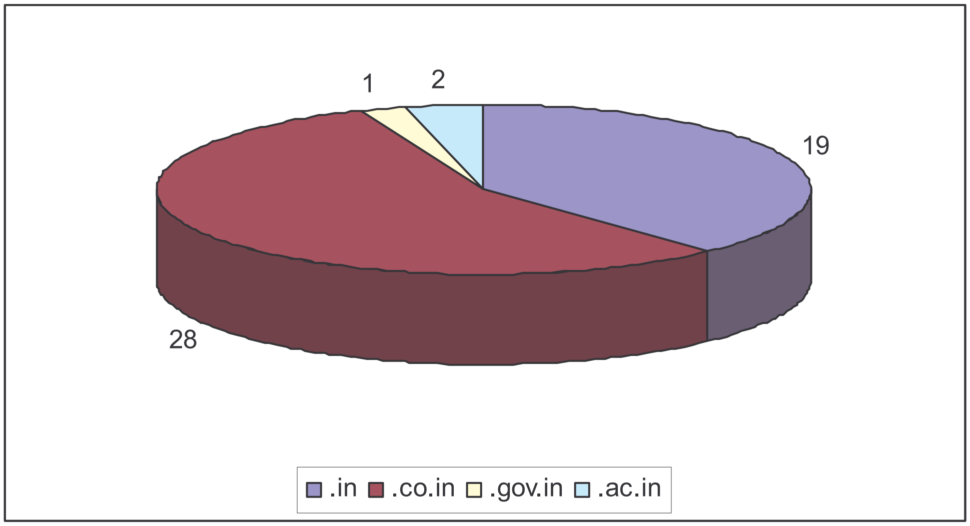

Figure 8: ccTLD defacement by LORD

4.3 Hackers Operating System Wise

Table 4 shows the Defacer's profile Operating System wise. A large number of the Indian websites defaced in the first half of the year 2006 were on Win 2003 server. In the first half of the year 2006 defacer group LORD defaced 24% of the total defaced websites, all were on win 2003.

	Win	Linux	Solaris	Others
LORD	424	0	0	0
aLpTurkTegin	177	0	0	0
b4d_m00d	0	133	0	0
Cyber-Warrior TIM	85	0	0	0
Xarnuz	78	0	0	0
IRANIAN BOYS BLACK HAT	52	0	0	0
eno7	49	0	0	0
DeltahackingSecurityTEAM	42	4	0	0
Lady_Lara	36	0	0	0
Mirim	35	0	0	0

Table 4: Defacer's profile Operating System wise

Figure 11 shows the defacement on windows operating system hacker wise.

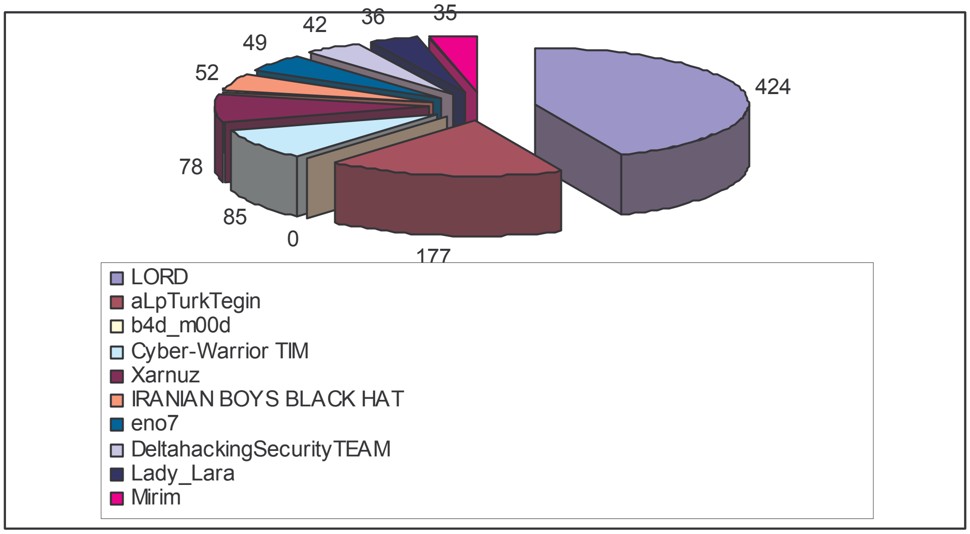

Figure 11: Windows Operating System Defacement Hackers wise

Figure 12 shows defacements on Linux operating system hackers wise.

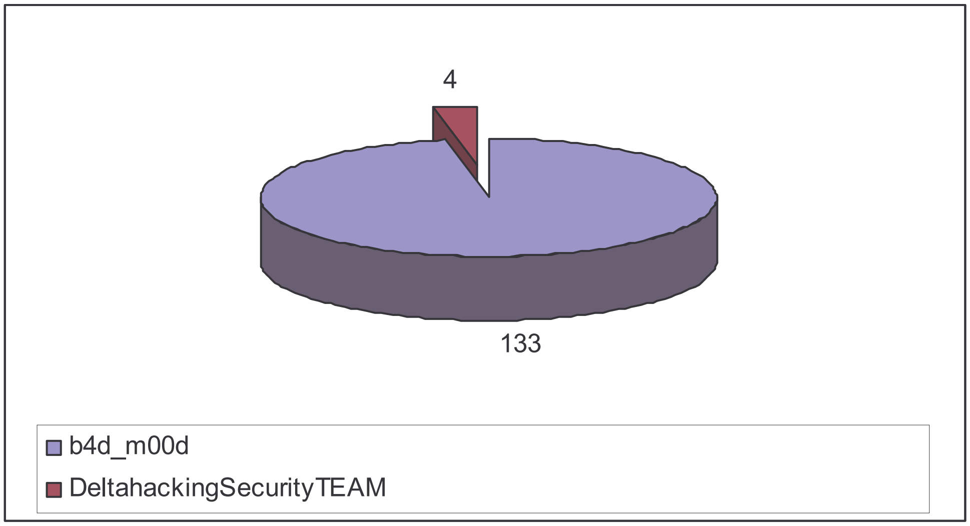

Figure 12: Linux Operating system Defacement Hackers wise

5. Operating System wise Defacement

Figure 9 shows the operating system wise defacement statistics. In the first half of the year 2006 windows been the most defaced operating system. In total of 1752 defacement 1397 defacement were on windows systems (Win 2000, Win 2003).

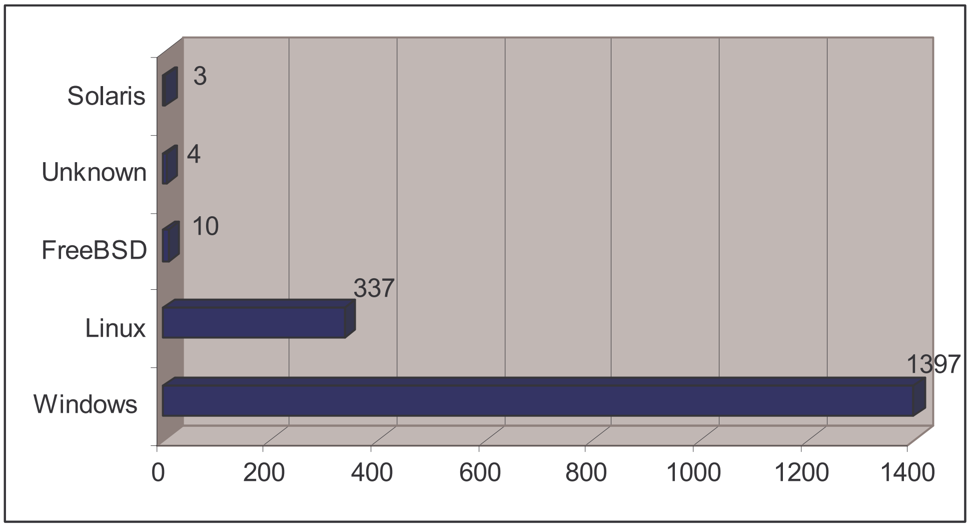

Figure 13: Defacement Operating System wise

5.1 Domain Wise Operating System Defacement

Table 5 shows the Operating system wise defacement on TLD's.

	.com	.in	.org	.net	edu	.info	.biz
Windows	949	211	123	84	3	21	5
Linux	226	62	26	14	0	9	0
FreeBSD	8	2	0	1	0	0	0
Solaris	1	2	0	0	0	0	0
Unknown	1	1	0	1	0	0	0

Table 5: Operating system TLD wise

Figure 10 shows the domain defacement operating system wise. In each domain windows have the most no. of defacements.

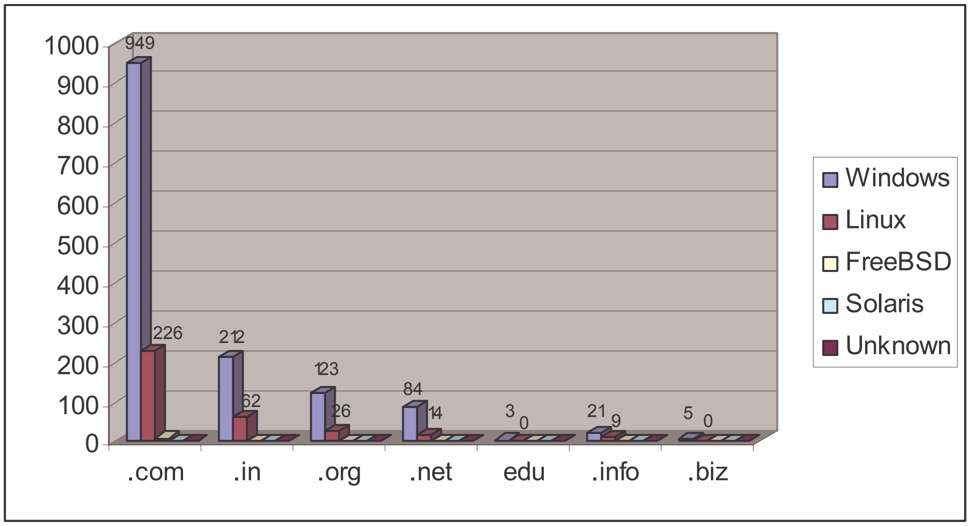

Figure 14: Domain wise Operating System Defacement

6. Defacement by Networks

6.1 Most Targeted Networks

Table 4 shows the most targeted networks. Among the Indian ISPs VSNL received the most no of attacks.

S. No.	ISP	No. of Websites
1	THE PLANET	388
2	AOTECH	227
3	VSNL IN	183
4	YIPS WEBWERK	149
5	NET4	127
6	NOC4HOSTS	93
7	HIVEL BLK	67
8	IANA NETBLOCK	52
9	Spectrum	46
10	EVRY BLK	43

Table 6: Most Targeted Networks

Figure 13 shows the different domains defaced on the VSNL network. Three Indian government sites which were defaced in the first half of year 2006 were hosted on VSNL. Websites are: http://www.fmc.gov.in, http://www.er.railnet.gov.in, http://www.ieg.gov.in/chiluvuru

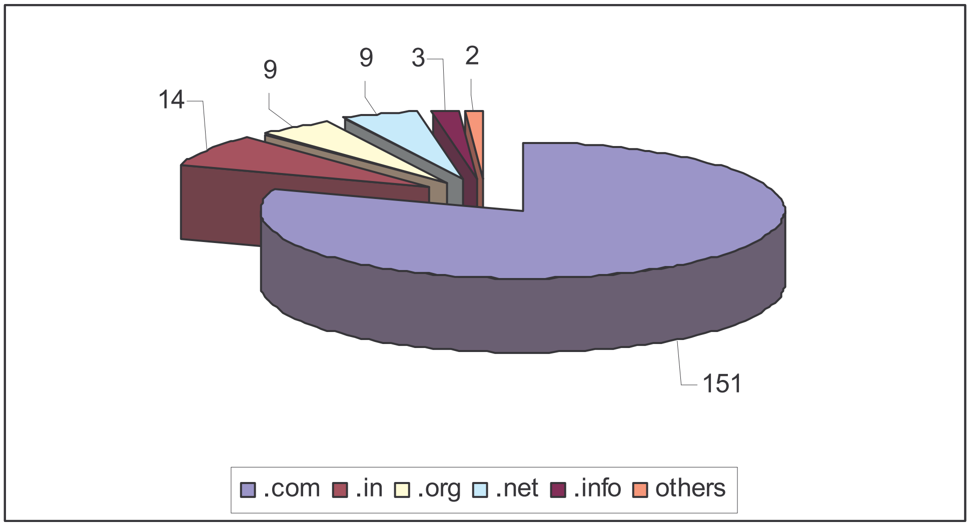

Figure 15: Defacement on VSNL Network

6.2 Most Targeted IP

Table 5 lists the most defaced IPs in the first half of the year 2006.

S.No.	Defaced IP	No. Of Websites	ISP
1	216.185.43.165	228	AOTECH
2	67.19.173.228	186	THEPLANET

3	203.199.113.30	135	VSNL-IN
4	66.7.148.132	118	YIPES-BLK2
5	70.86.129.59	112	THEPLANET
6	70.86.46.178	78	THEPLANET
7	66.96.85.70	67	HIVEL-BLK1
8	202.71.136.92	50	NET4
9	204.15.132.217	45	NDCHOST-204.15.132.0
10	202.146.192.145	40	SPECTRUM

Table 7: Most Targeted IPs

7. Website Defacements

Most defacements result from hackers using prefabricated exploits to gain administrative control of the target system and then replacing the Web pages hosted on the system with their own version. On certain rare occasions, Web site defacement occurs in quite an unusual manner. The attacker may not have had an opportunity to gain any sort of user-level privileges on the target system but was able to take advantage of poorly written Web scripts or poorly configured Web servers to carry out the defacement.
To gain administrative control on the targeted system hackers uses the exploit code related to vulnerability of web servers or of operating system on which web server is running.

In the first half of the year 2006, web servers running on windows server were highly exploited. Vulnerabilities which have been exploited for windows are listed below:

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

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

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

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

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

- TCP/IP Remote Code Execution Vulnerability

CVE-2006-2379
CIVN-2006-54
June 14, 2006

Vulnerabilities related to web servers which have been exploited are listed below:

Apache

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

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

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

IIS

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

Cross site Scripting is also a widely used method of defacing a website. According to this method, an attacker finds some cross site scripting vulnerability on the web server software and attempt to execute scripts or other system commands on the vulnerable system running the target web server. Vulnerabilities related to Cross Site Scripting which could have been exploited are listed below.

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

Vulnerabilities related to scripting languages such as PHP could also be used for website defacement. CERT-In has issued virus alert related to worms which were exploiting the vulnerabilities in PHP.

- Net-Worm.Linux.Mare.d
  February 22, 2006

8. Errata

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
2. www.zone-h.org

10. List of Figures

11. List of Tables