# CERT-In

**Indian Computer Emergency Response Team**
***Enhancing Cyber Security in India***

# Analysis of defaced Indian websites Year-2005

By

Ashish Gairola and Garima Narayan

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

Issue Date: July 15th, 2006

## Index

## 1. Introduction

The primary objective of this paper is to present the detailed statistical analysis of defaced Indian websites during year 2005. This paper is an extension to the earlier white papers "Analysis of Defaced Indian websites under .in ccTLD" [Ref.1]. This paper emphasizes on the defacement trends of the year 2005. 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).

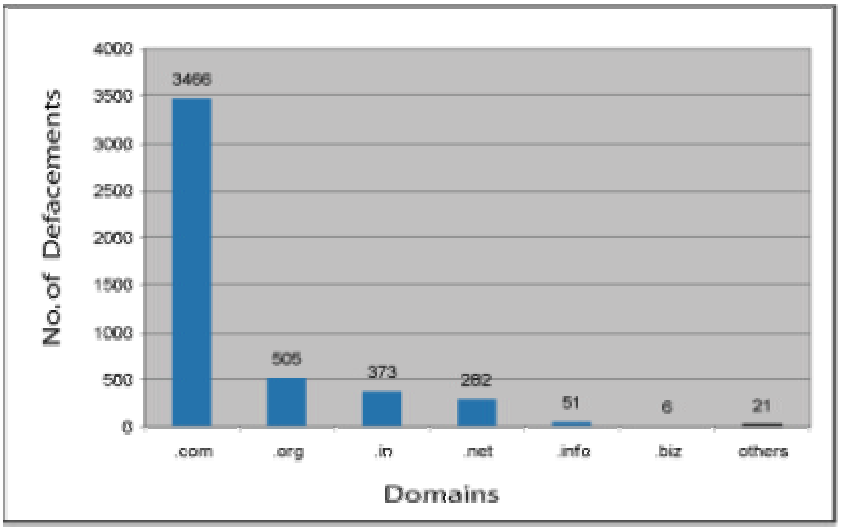


Figure 1: Distribution of defaced domains

| Domain | .com | .org | .in | .net | .info | .biz | .edu | .name |
|---|---|---|---|---|---|---|---|---|
| Number | 3466 | 505 | 373 | 262 | 51 | 6 | 2 | 7 |
| Percentage of the Total defacements | 74.18 | 10.80 | 7.98 | 5.60 | 2.33 | 0.12 | 0.04 | 0.14 |

Table 1: Distribution of defaced domains

On analyzing the defacement statistics of year 2005, it was observed that there is a growth in the number of sites defaced during the previous years. The total no of sites defaced in 2005 were 4715 compared to 1131 in 2004. The domain .com had 3466 defacements which is more than 70% of the total defacements. It was almost nine times the number of .in defacements.

### 2.1 Distribution of defaced domains by second level ccTLD

| Domain | co.in | .ac.in | .gov.in | .ernet.in | .nic.in | .net.in | .org.in | .firm.in | .mil.in |
|---|---|---|---|---|---|---|---|---|---|
| Number | 136 | 31 | 28 | 2 | 5 | 3 | 8 | 5 | 1 |
| Percentage of the Total defacements | 38 | 8 | 9 | 1 | 1 | 1 | 2 | 1 | 1 |

Table 2: Distribution of defaced domains by ccTLD

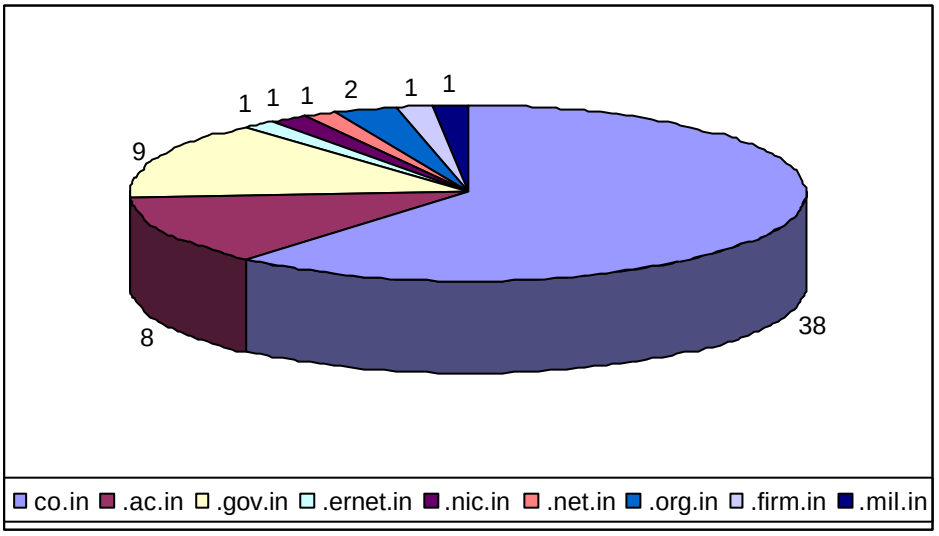


Figure 2: Distribution of defaced domains by ccTLD

The total numbers of defaced .in domains were 373, with the domain .co.in having the highest no. of defacements among the 2nd level domains followed by .ac.in and .gov.in. It was more than 38% of the total defacements. It was more than four times the number of .gov.in sites defaced in 2005.

## 3. Time Line of Defacements

### 3.1. Defacements by year

It has been observed that there is a sharp growth in the number of .in sites defaced during the previous year. The total number of .in sites defaced in 2005 were 373.

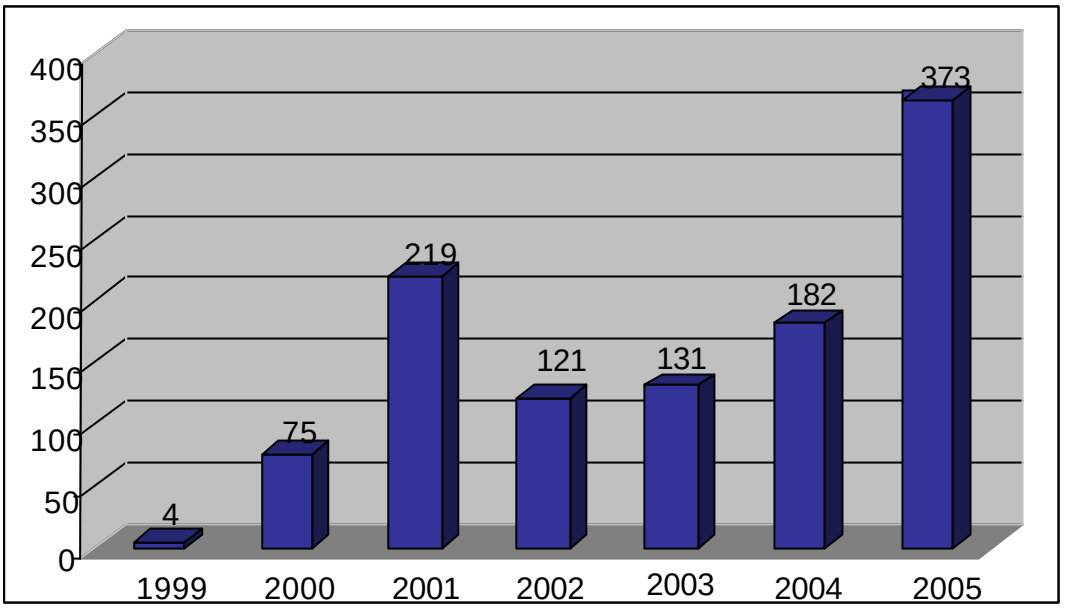


Figure 3: .in defacements Year wise

| Year | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 |
|---|---|---|---|---|---|---|---|
| Sites defaced | 4 | 75 | 219 | 121 | 131 | 182 | 373 |
| Percentage of total defaced sites | 0 | 7 | 20 | 11 | 12 | 17 | 33 |

Table 3: .in defacements Year wise

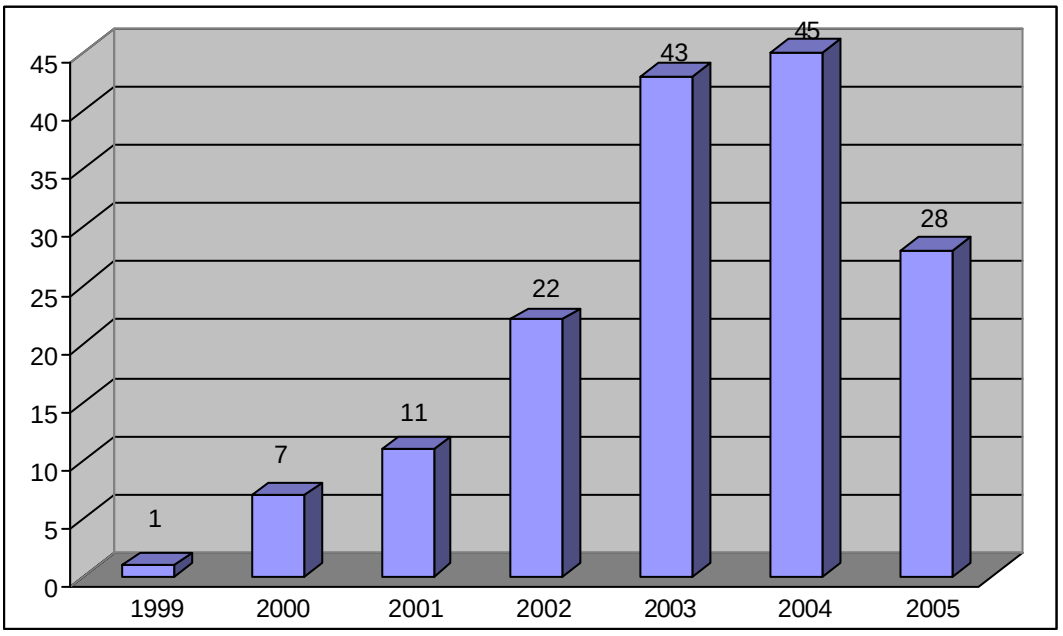


Figure 4: .gov.in defacements Year wise

| | 1999 | 2000 | 2001 | 2002 | 2003 | 2004 | 2005 |
|---|---|---|---|---|---|---|---|
| Sites defaced | 1 | 7 | 11 | 22 | 43 | 45 | 28 |
| Percentage of total defaced sites | 1 | 4 | 7 | 14 | 27 | 28 | 19 |

Table 4: .gov.in defacements Year wise

It was also observed that the total number of defaced .gov.in sites are less in 2005 compared to 2004, the figure 4 shows it is 70% in the comparison of previous year. In 2004 defaced .gov domain numbers were 45 compared to 28 in 2005.

### 3.2. Defacements by month

The figure 5 details the month-wise defacements in all top level domains. The month of January had the highest number of defacements followed by August, December and November, while March had the least number of defacements.

The figure 6 shows the month wise .in domain defacement.

The maximum number of .in domains defaced in the month of December, the total number of websites defaced during this month were 83. The second highest numbers of domains defaced during the month November were 52. The major domains defaced during these months were http://www.mapit.gov.in, http://www.lepakshihandicrafts.gov.in, http://madhyapradeshtourism.gov.in and http://www.pibtvm.gov.in

The highest numbers of defacements in .gov.in domain were 5 in the month of April and August each, while January, October and December 4 .gov.in websites defaced in each month. The major domains defaced during these months were http://www.fmc.gov.in, http://www.rajstamps.gov.in, http://www.wbseb.gov.in, http://www.nisd.gov.in, http://www.mapit.gov.in,

Some .gov.in sites such as http://www.rajrevboard.gov.in, http://www.rajstamps.gov.in and http://www.icf.gov.in were redefaced during 2005. The most redefaced website was http://www.rajstamps.gov.in. This website was defaced three times in year 2005.

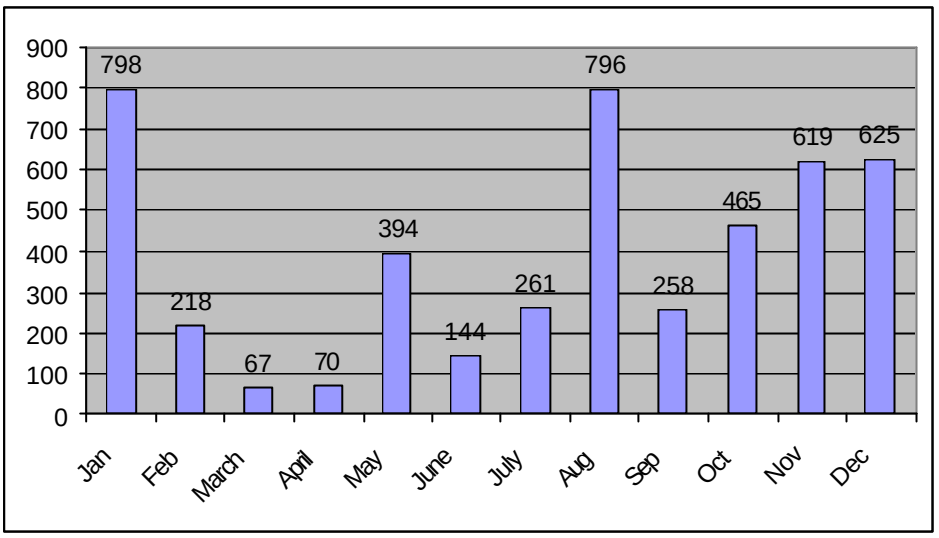


Figure 5: Top Level Domain defacements Month wise

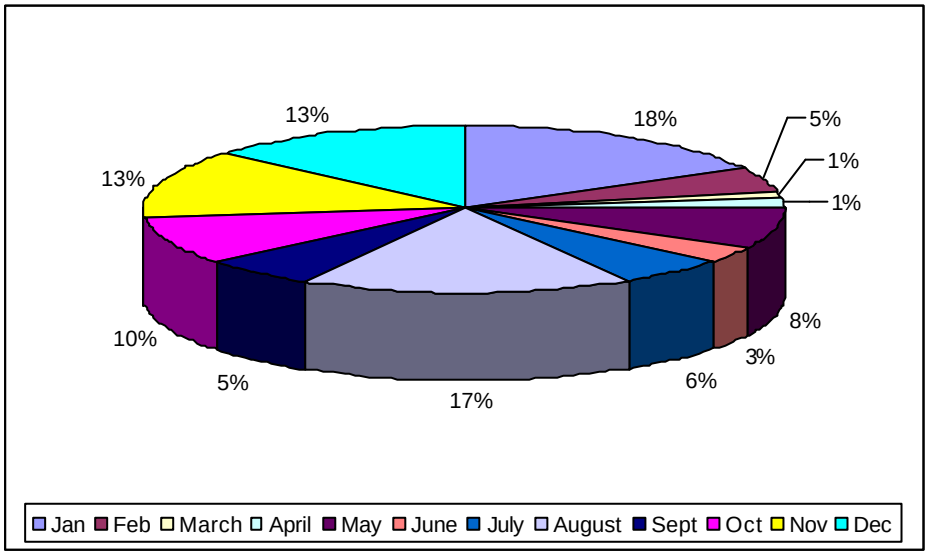


Figure 6: .in defacement month wise

### 3.3. Highest Defacements in a single day

Table 5 shows highest defacement in a single day. The highest number of defacements of Indian website occurred on 2nd January 2005. There were 225 number of domain defaced on that day followed by 208 domains on 19th January, 2005.

| S. No. | Date | Defacements |
|---|---|---|
| 1 | 2nd January, 2005 | 225 |
| 2 | 19th January, 2005 | 208 |
| 3 | 3rd August, 2005 | 194 |
| 4 | 4th August, 2005 | 165 |
| 5 | 12th January, 2005 | 162 |
| 6 | 22nd January, 2005 | 126 |

Table 5: Highest No of domains defacements on single day

The Highest number of defacements of .in sites in a single day is 22nd November 2005. In total 41 websites were defaced on that day. It was a mass defacement on US based YIPS network. The second highest number of defacements on a single day occurred on 12th December 2005 having 40 websites on TATA-IN network, Third highest number of defacements on a single day was on 23 October, 2005 total 14 websites on US based HURRICANE Network.

The highest number of defacements of .gov.in sites in a single day occurred on 8th August 2005, 4 sites were defaced on that day. Defaced websites were http://www. nisd.gov.in, http://www.ncdap.nisd.gov.in, http://www.nice.nisd.gov.in and http://www. nicp.nisd.gov.in. These website were hosted on Reliance Infocom Ltd Network.

## 4. Hacker wise Defacements

### 4.1 Top Hackers

In 2005 the Iranian defacer group *Delta hacking Security Team* defaced most of the TLD domains. A total of 690 websites were defaced by this group which is around 15% of the total websites defacements during the year. The IRANIAN BOYS BLACK HAT and batistuta defaced 13% and 7% of domains of the total number of website defacement during one year respectively.

The break up of total number of websites defaced by the top ten hacker groups is shown in Table 6.

| Defacer | Number of defacements | Percentage of Total TLD Defacements |
|---|---|---|
| Delta hacking SecurityTEAM | 690 | 15 |
| IRANIAN BOYS BLACK HAT | 605 | 13 |
| batistuta | 345 | 7 |
| WHACKERZ | 320 | 7 |
| put4z0 | 268 | 6 |
| nEt^DeViL | 256 | 5 |
| M@TRiX | 166 | 4 |
| Iskorpitx | 161 | 3 |
| 23Erdem | 142 | 3 |
| Ejder | 140 | 3 |

Table 6: Total number of defacements hacker wise

### 4.2 Profile of hackers: Domain wise

The domain wise profile of top 10 hackers is shown in Table 7.

| Defacer | Domain | | | | | | |
|---|---|---|---|---|---|---|---|
| | .com | .in | .net | .org | .edu | .info | .biz |
| DeltaHackingSecurityTEAM | 509 | 50 | 39 | 87 | 1 | 4 | |
| IRANIAN BOYS BLACK HAT | 466 | 44 | 41 | 48 | | 6 | |
| batistuta | 253 | 3 | 25 | 52 | | 6 | 6 |
| WHAKERZ | 186 | 6 | 17 | 17 | | 2 | 2 |
| put4z0 | 211 | 24 | 14 | 18 | | 1 | |
| nEt^DeViL | 193 | 14 | 13 | 30 | | 4 | 2 |
| M@TRiX | 164 | 1 | 1 | | | | |
| Iskorpitx | 85 | 52 | 2 | 19 | 1 | 2 | |
| 23Erdem | 107 | 6 | 10 | 15 | | 2 | 2 |
| Ejder | 101 | 3 | 10 | 22 | | 2 | 2 |

Table 7:Domain wise: Hacker Profile

### 4.3 .in Defacements: Hacker wise

In 2005 under .in domain defacements, the Delta Hacking Security Team group has the highest number of defacements, followed by iskorpitx, put4z0 and IRANIAN BOYS BLACK HAT. The Delta Hacking Security Team defaced a total number of 59 domains, iskorpitx defaced 53 domains and put4z0 and IRANIAN BOYS BLACK HAT defaced 49 domains each.

| Defacer | Number of defacements | Percentage of total .in defacements |
|---|---|---|
| DeltahackingSecurityTEAM | 59 | 16 |
| Iskorpitx | 53 | 14 |
| put4z0 | 49 | 13 |
| IRANIAN BOYS BLACK HAT | 49 | 13 |
| OXIN | 31 | 8 |
| nEt^DeViL | 15 | 4 |
| D.O.M | 10 | 3 |

Table 8: .in defacements hacker wise

The highest number of the defacements of .gov.in sites was done by XTech Inc Group having total 4 websites followed by the other group batistuta. The Batistuta defaced 3 websites. Some of the common domains defaced by these groups are nisd.gov.in, chittoor.ap.gov.in, ceobihar.eci.gov.in etc.

### 4.4 Profile of Hackers: Operating System wise

The operating system wise profile of hackers is shown in Table 9.

| Defacer | Operating System | | | | Total |
|---|---|---|---|---|---|
| | Win 2000 | Win 2003 | Win NTx | Linux | |
| Delta Hacking Security TEAM | 153 | 536 | | | 689 |
| IRANIAN BOYS BLACK HAT | 181 | 419 | | | 419 |
| Batistuta | 131 | 10 | 204 | | 345 |
| WHAKERZ | 229 | 1 | | | 230 |
| put4z0 | 90 | 110 | | 67 | 267 |
| nEt^DeViL | | | | 256 | 256 |
| M@TRiX | 2 | | 162 | | 164 |
| Iskorpitx | 11 | 140 | | 9 | 160 |
| 23Erdem | 111 | 31 | | | 142 |
| Ejder | 139 | 1 | | | 140 |

Table 9: Hackers profile: Operating System Wise

## 5. Defacement by domain and Networks

### 5.1. Most Targeted Networks

The VSNL network had the highest no of defacements, as shown in Table 10. It had total of 548 defacements during the year 2005.

| Network | Number of defacements | Percentage of total defacements |
|---|---|---|
| VSNL-IN | 548 | 14.190 |
| Spectrum | 529 | 11.322 |
| NET4 | 302 | 6.464 |
| EXATT TECHNOLOGIES | 142 | 3.039 |

Table 10: Most targeted Indian Networks

Under .in defacements VSNL network had the highest no of defacements followed by EXATT Technologies, as shown in Table 11. It had 40 defacements comprising more than 30% of the total .in ccTLD defacements of the year 2005.

| Network | Number of .in defacements | Percentage of total defacements |
|---|---|---|
| VSNL-IN | 40 | 11.049 |
| EXATT TECHNOLOGIES | 10 | 2.762 |
| NET4 | 7 | 1.933 |
| Spectrum | 2 | 0.552 |

Table 11: Number of .in defacements on Indian Networks

### 5.2. Most Defaced IPs

The most defaced IPs are given in Table 12. The network Spectrum had the highest no of defacements. It had 493 defacements comprising more than 10% of the total defacements of the year 2005. Other networks are THEPLANET and HURRICANE.

| No. | Defaced IP | No of sites defaced | Network |
|---|---|---|---|
| 1 | 202.146.192.145 | 493 | Spectrum |
| 2 | 67.19.238.148 | 426 | THEPLANET |
| 3 | 69.93.103.60 | 268 | THEPLANET |
| 4 | 64.62.254.61 | 256 | HURRICANE |
| 5 | 202.71.128.215 | 225 | NET4 |
| 6 | 67.19.132.90 | 211 | THEPLANET |
| 7 | 207.106.22.74 | 137 | WEB WERKS |
| 8 | 202.63.160.38 | 136 | EXATT TECHNOLOGIES |
| 9 | 203.199.107.181 | 130 | VSNL-IN |
| 10 | 202.54.10.77 | 126 | VSNL IN |

Table 12: Number of defacements on Single IP

The most defaced Indian IPs are shown in Table 13. The network Spectrum had the highest number of defacements followed by NET4 and EXATT Technologies

| No. | Defaced IP | No of sites defaced | Network |
|---|---|---|---|
| 1 | 202.146.192.145 | 493 | Spectrum |
| 2 | 202.71.128.215 | 225 | NET4 |
| 3 | 202.63.160.38 | 136 | EXATT TECHNOLOGIES |
| 4 | 203.199.107.181 | 130 | VSNL-IN |
| 5 | 202.54.10.77 | 126 | VSNL IN |

Table 13: Most defaced Indian IPs

### 5.3. Defacement by Hosting Country

The Figure 7 shows, hosting of defaced websites worldwide. The maximum no. of defaced websites were hosted in US. Table 14 shows the total numbers of defaced websites hosted in US were 2034, around 40% of the total defacement. 2265 numbers websites were hosted in India, while 142 hosted in Australia, rest were hosted in the EU, CH, DE and FR etc which got defaced.

| No. | Hosting Country | Defacement | |
|---|---|---|---|
| 1 | US | 2034 | 43.5 |
| 2 | India | 2265 | 48.5 |
| 3 | Australia | 142 | 3.1 |
| 4 | EU | 118 | 2.5 |

Table 14: Number of defacements by Hosting Country

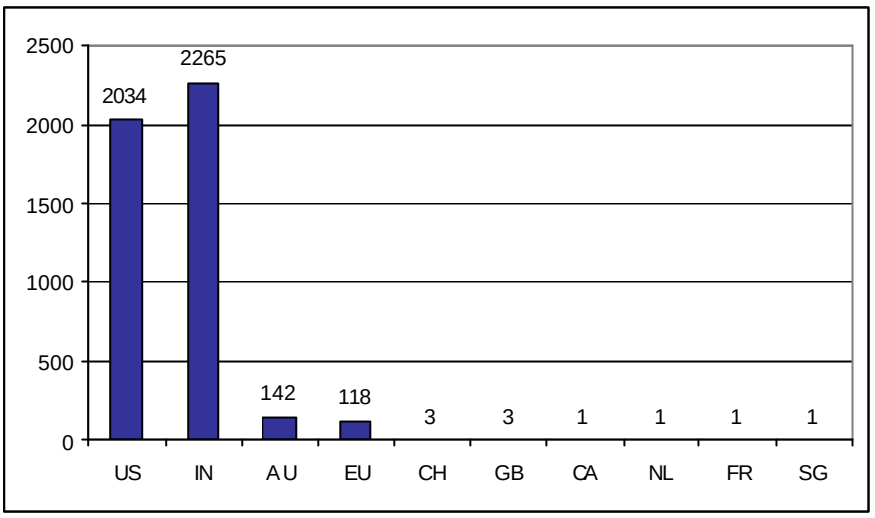


Figure 7: .in defacements by hosting country

Figure 8 details the hosting of .in defaced websites in various countries. In total defaced 178 .in sites were hosted in India, while 164 sites in US, 6 in Australia and 5 each in EU, Denmark and Great Britain.

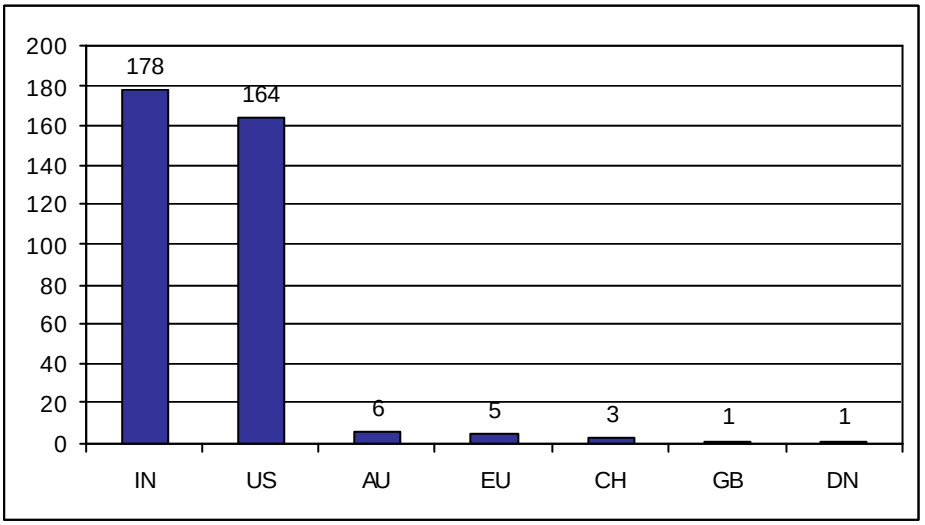


Figure 8: .in defacements by hosting country

## 5.4 Defacements: Sector wise

Table 15 shows the .in domain defacements in various sectors. 64 % commercial sites has been defaced in second level domain.

| Sector | No of Defacements |
|---|---|
| Commercial | 141 |
| Acadamic | 33 |
| Government | 36 |
| Non profit Organization | 8 |
| Defence | 1 |

Table 15 : Defacements: Sector wise

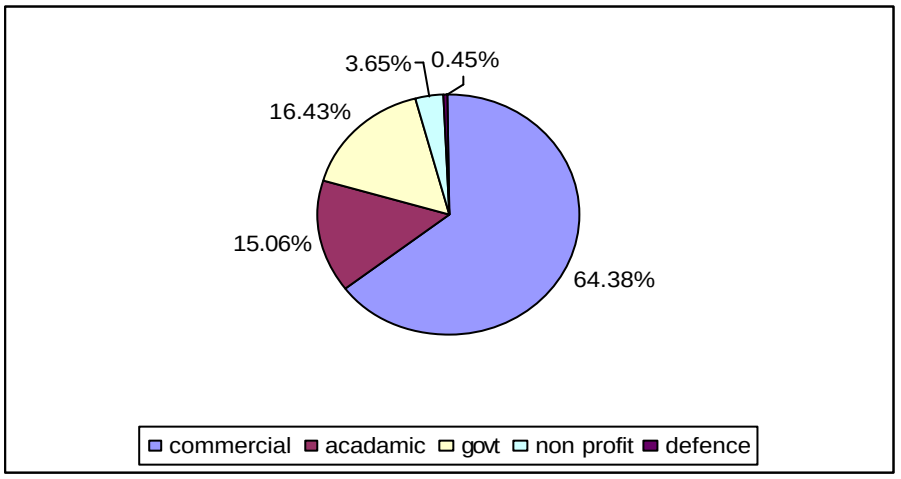


Figure 9: Defacement: Sector wise

## 6. Hosting Platform

Figure 10 shows the most defaced websites in 2005 were hosted on Windows platform. Total number of websites hosted on windows were 3768 which includes Win 2003 1768 websites, Win 2000 1463 websites and Win NT9x 537 websites. The second highest were hosted on Linux platform, the total numbers are 782 followed by Solaris and FreeBSD. 104 websites were hosted on miscellaneous platforms such Compaq Tru64, MacOS and Unix etc. The defacement statistics indicate that higher level of defacements were on Windows servers during the period.

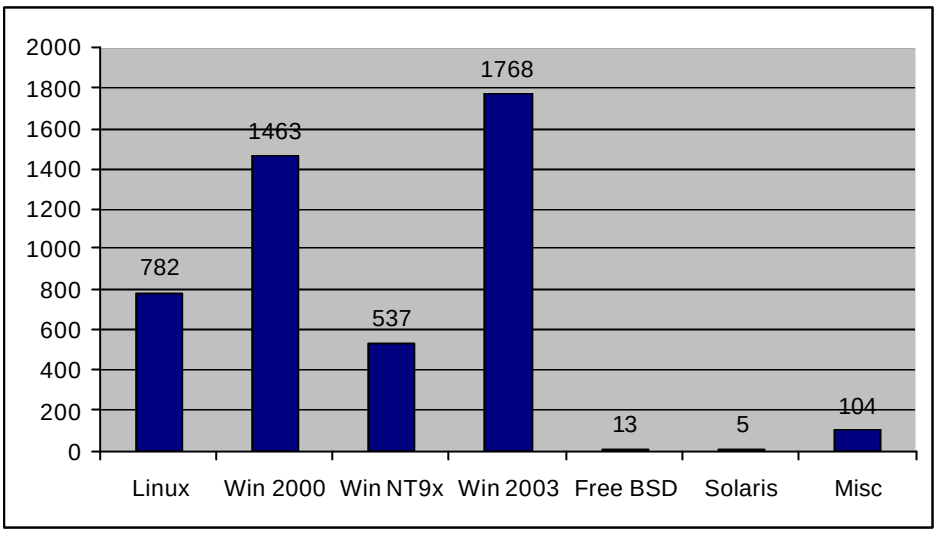


Figure 10: defacements by hosting platform

## 6.1 .in defacement by Platform

The figure 11 details the hosting platforms on which defaced .in sites were hosted. The statistics indicate Windows 2003 had the highest number of defacements for .in ccTLD followed by Windows 2000 and Linux servers. The total numbers of websites hosted on windows family servers were 312 while Linux had 60 websites.

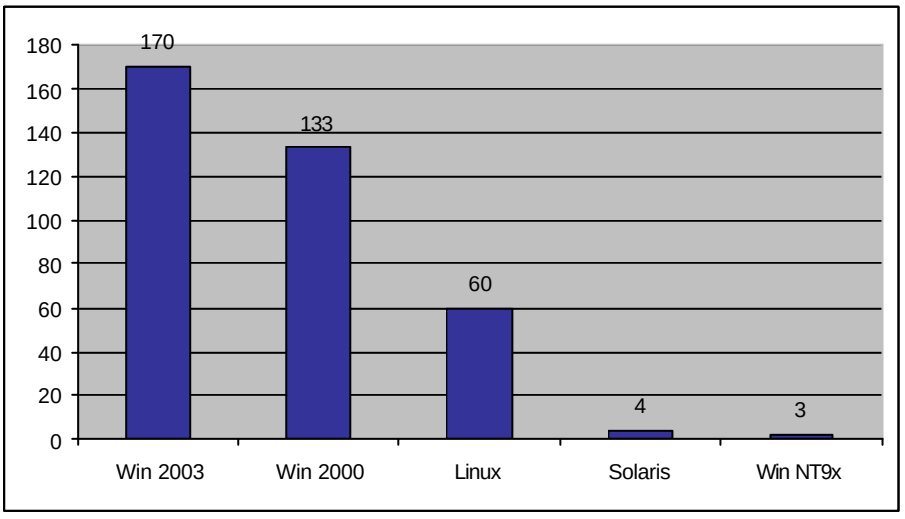


Figure 11: .in defacements by platform

### 6.2 TLD Operating System wise defacements

Table 16 shows the number of defaced websites which were hosted on prominent operating systems such as Win 2000, Win 2003 and Linux.

| Domain | Operating system | | | | Total |
|---|---|---|---|---|---|
| | Win 2000 | Win 2003 | Win NT9x | Linux | |
| .com | 1097 | 1275 | 420 | 574 | 3366 |
| .in | 166 | 212 | 9 | 94 | 481 |
| .net | 80 | 99 | 26 | 50 | 255 |
| .org | 126 | 202 | 73 | 86 | 487 |
| .info | 18 | 19 | 6 | 11 | 54 |
| .biz | 6 | | 4 | 7 | 17 |
| .edu | | 4 | | 1 | 5 |

Table 16 : TLD Operating System Wise

## 7. 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.

## 8. 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
2. www.zone-h.org
3. www.dnsstuff.com

## 9. List of Figures

## 10. List of Tables