CERT-In

Indian Computer Emergency Response Team

Handling Computer Security Incidents

Analysis of Defaced Indian websites under .in ccTLD

By

Sabyasachi Chakrabarty and Basudev Saha

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

Index

1. Introduction

Recently there has been a noticeable rise of cyber crime in different forms, ranging from information theft/modification to launching denial of service attacks. Among the different form of cyber attacks, defacement of websites has become popular among the hackers/ hacker groups. These defacements are carried for different motives including fun, political, revenge or just proving their competency.

With the global rise in cyber terrorism activity, Indian websites have also been similarly affected and have been the targeted by many attackers, some of them being opportunist while some have targeted specific sites/domains.

There are many web sites that keep track and mirror global defacements through active submission from the hackers. The website www.zone-h.org is one of the most popular and comprehensive web defacement mirroring site.

A statistical analysis has been presented in this paper for the defaced Indian websites. This analysis has been done for .in ccTLD (country code top level domain). The ccTLDs have been created by Internet Assigned Numbers Authority (IANA), which has now been superseded by ICANN. The second level domains under Indian .in ccTLD are co.in, firm.in, ac.in, res.in, gov.in, mil.in, net.in, in, org.in, ind.in and gen.in

Besides the Indian sites hosted under the .in ccTLD, many other Indian organizations use generic Top Level Domains (TLDs) like .com, .net, .org, etc. Determining the Indian websites hosted under the generic TLDs and gathering the data is rather difficult, especially for the old defaced sites. This analysis of Indian websites has therefore been confined to only the .in ccTLD sites.

An analysis of Indian defacements was carried out earlier by Mr.K N Srijith (www.srijith.net), but the analysis was limited in scope and covered defacements till 2002.

2. Data analysed

The defacements of websites under Indian Country Code Top Level Domain (ccTLD) **.in** have been analyzed. The range of the data obtained for analysis dates from **1998 to Sept 20th, 2004.**

According to the figures published by NCST on their website, the total .in ccTLD registered domains is **6430**. Majority of this number comprises of .co.in domains. However, this number doesn't include the sub-domains under nic.in and ernet.in.

3. Sources of Data

Defacement mirrors hold data on worldwide defacements. This is usually obtained through reports by the hackers/hacker-groups, which are then verified by the defacement mirrors.

The data for this analysis of defacement of **.in ccTLD** sites was obtained from the leading defacement mirrors. These include

www.zone-h.org,
mirror.delta5.com.br
www.attriton.org
www.safemode.org

All the .in ccTLD defacement records from zone-h.org were first collected. Later records from mirror.delta5.com.br and attriton.org were added to the list for analysis while taking due care that no duplicate records were added. Though attriton.org no longer mirrors defacement, they still archive the old data of defaced .in ccTLD sites. Defacement records on two more sites safemode.org and aldas.de were not accessible. However, the records of defaced Indian sites on safemode.org & aldas.de were available on srijith.net.

A total of **667** defacement records have been found under the .in ccTLD.

4. Analysis

4.1. Distribution of defaced domains by second level ccTLD

The analysis of the defaced Indian **.in ccTLD sites** reveals that the domain **.co.in** had the most number of defacements.

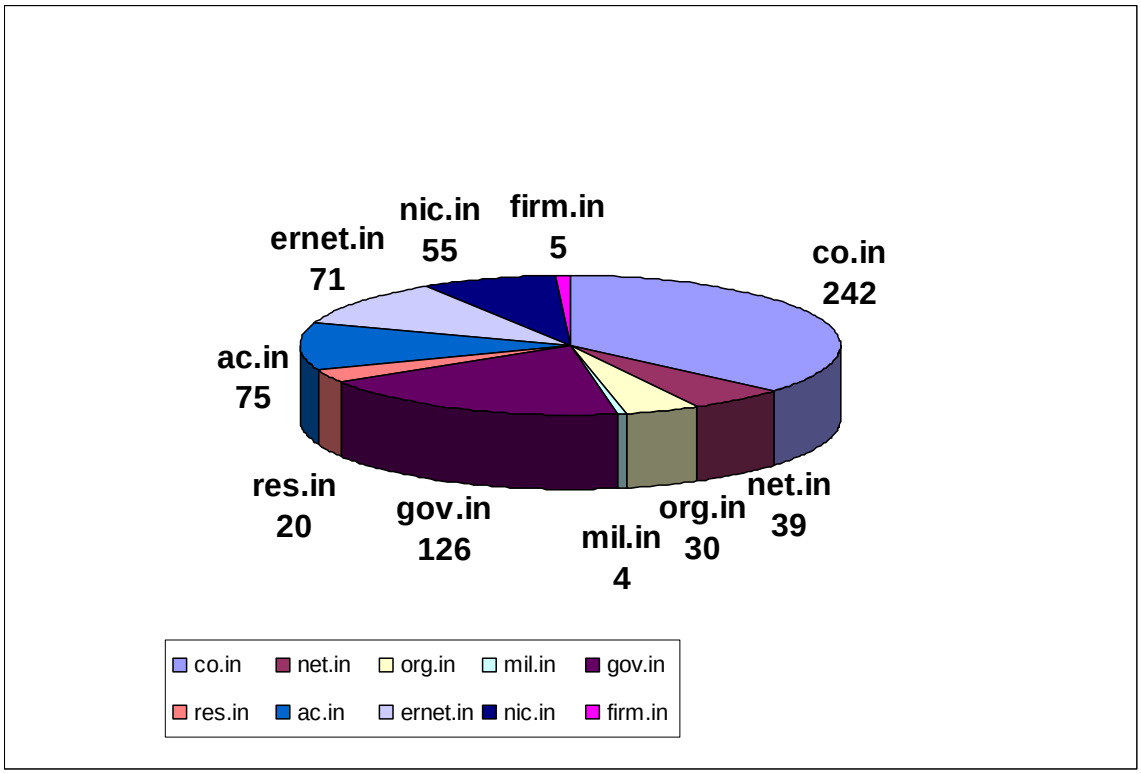


fig. 1

The domain **.co.in** had 242 defacements which is more than 36 % of the total defacements. It was also almost twice the number of **.gov.in** sites defaced.

Domain	co.in	gov.in	ac.in	ernet.in	nic.in	net.in	org.in	res.in	Firm.in	mil.in
Number	242	126	75	71	55	39	30	20	5	4
Percentage of the Total Defacements	36.28	18.89	11.24	10.64	8.25	5.85	4.50	3.00	0.75	0.60

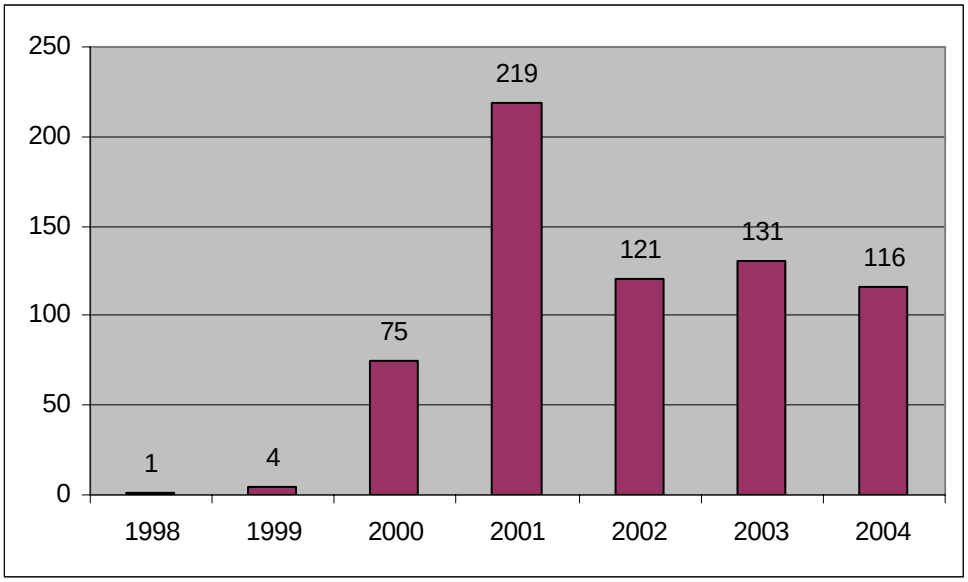
fig. 2

4.2. Defacements Time distribution

4.2.1. Defacements by year

The number of **.in ccTLD** sites defaced was highest in the year 2001, when 219 sites were defaced. More than 33 % of the .in ccTLD sites defaced till date was in the year 2001. This

was a sharp increase of more than three times, than in the year 2000. It decreased in the year 2002 and seems to be stabilized around the level of 2002, as shown in fig 3.



	1998	1999	2000	2001	2002	2003	2004
Sites defaced	**1**	**4**	**75**	**219**	**121**	**131**	**116**
Percentage of total defaced sites	**0.15**	**0.60**	**11.24**	**32.83**	**18.14**	**19.64**	**17.39**

fig: 3 : .in defacements Year wise

However, there has been an increase in the number of **.gov.in** sites being defaced every year. From only one site defaced in 1999, it increased to 43 in 2003. There is likely to be an increase in **.gov.in** sites defaced this year too, as 42 **.gov.in** sites have already been defaced this year.

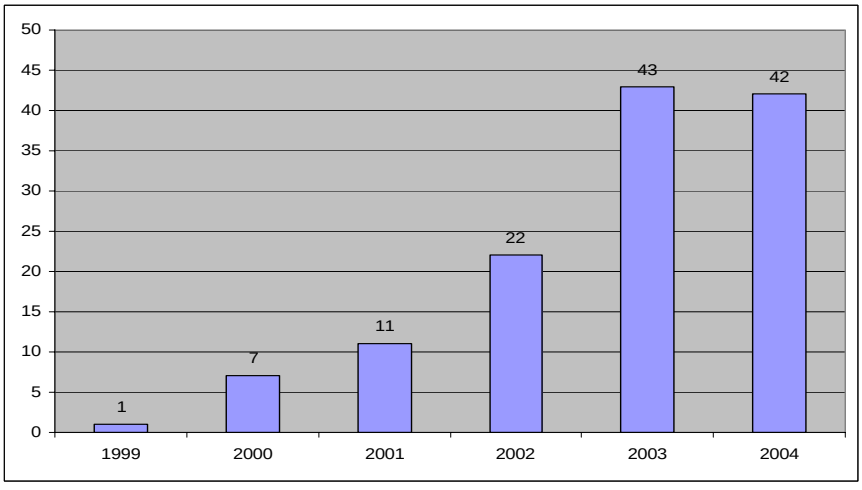


fig: 4: .gov.in defacements Year wise

4.2.2. Defacements by month, year-month

The fig. 5 details the cumulative month-wise defacements for all the years. The month of April seems to have the highest number of defacements, while August had the second highest number of defacements.

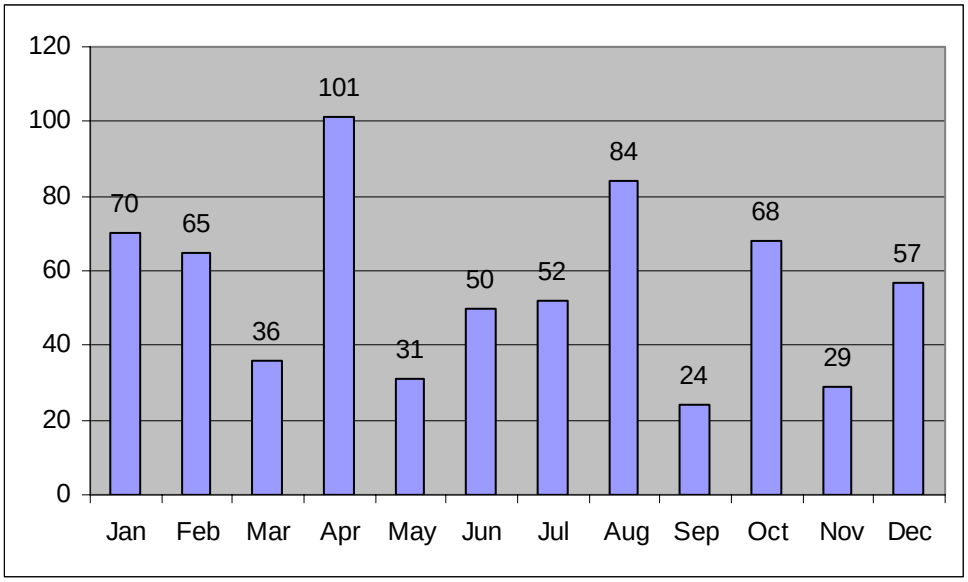


fig5: .in defacements Month wise cumulative

The month wise defacements over the years is as shown in fig 6. The month of September seems to be consistently least active.

	1998	1999	2000	2001	2002	2003	2004
Jan	**0**	**0**	**0**	**35**	**13**	**6**	**16**
Feb	**0**	**0**	**2**	**11**	**0**	**3**	**49**
Mar	**0**	**1**	**5**	**14**	**7**	**3**	**6**
Apr	**0**	**0**	**2**	**34**	**36**	**24**	**5**
May	**0**	**0**	**2**	**10**	**6**	**11**	**2**
Jun	**1**	**0**	**0**	**16**	**10**	**6**	**17**
Jul	**0**	**0**	**5**	**16**	**19**	**8**	**4**
Aug	**0**	**0**	**18**	**25**	**4**	**27**	**10**
Sep	**0**	**0**	**3**	**7**	**6**	**1**	**7**
Oct	**0**	**1**	**20**	**25**	**14**	**8**	**-**
Nov	**0**	**0**	**2**	**6**	**0**	**21**	**-**
Dec	**0**	**2**	**16**	**20**	**6**	**13**	**-**

fig:6 .in defacements Month wise

The highest number of defacements in a single month of a particular year occurred in Feb 2004, when 49 .in ccTLDs defacements took place.

4.2.3. Highest Defacements in a single day

The highest number of defacements of .in cc.TLD sites occurred on 5th February 2004. There were 27 defacements on that day. The second highest was on 1st February, when there were 15 defacements.

	Date	Defacements
1	5/2/2004	27
2	1/2/2004	15
3	22/4/2001	14
4	1/4/2002	10
5	30/6/2004	10

Fig:7: .in defacements

The highest defacement of .in cc.TLD sites on 5th February 2004 was a mass defacement on NET4 network. Some of the sites defaced on 5th February were rpcb.gov.in, atimysore.gov.in, sonatech.ac.in, psgim.ac.in, jnec.ac.in, stellar.co.in, vdc.co.in.

	Date	Defacements
1	30/06/2004	10
2	1/4/2002	6
3	10/10/2002	4
4	6/2/2004	3
5	13/11/2003	3

Fig:8: .gov.in defacements

The highest number of defacements of **.gov.in** sites in a single day occurred on 30th June 2004. 10 sites were defaced on that day. Some of the sites defaced were newsletter.gujarat.gov.in, bisag.gujarat.gov.in, btm.gujarat.gov.in Infact, all the sites defaced were of the **.gujarat.gov.in** domain and were hosted on the GNFC network.

4.3. Hacker wise defacements

4.3.1. Top Hackers, % of defacement

More than 150 hacker/hacker groups have been responsible for defacing Indian websites. The hackers/hacker groups responsible for the highest number of .in ccTLD defacements are shown in fig.9

Defacer	Number of defacements	Percentage of Total .in ccTLD Defacements
AIC	97	14.54
Silver Lords	57	8.55
GForce Pakistan	41	6.15
FBH	37	5.55
powHACK	31	4.65
TimeOut	18	2.70
WFD	17	2.55
TheBuGz	14	2.10
m0r0n and nightman	13	1.95
TechTeam	13	1.95

Fig:9 : .in defacements hacker wise

The group AIC (Anti India Crew) has defaced the most number of .in ccTLD sites.. They were responsible for around 15 % of the total .in ccTLD sites defaced. The other top defacers are Silver Lords, G-Force Pakistan and FBH (Federal Bureau of Hackers). In fact, the top 4 defacers together were responsible for more than 35% of the total defacements. Interestingly, the members of the top four hacker groups are said to be predominantly from Pakistan.

The break up of the .in ccTLD sites defaced by the top five hacker groups is shown in fig. 10.

	.co.in	.gov.in	.org.in	.net.in	.nic.in	.ac.in	.ernet.in	.res.in
AIC	26	10	7	7	14	13	15	5
Silver Lords	30	1		3	6	3	12	1
Gforce Pakistan	6	2		4	12	4	9	4
FBH	16	13	1	2		4		1
powHACK	13	16	1			1		

Fig:10 : .in defacements hacker by second level domain

The group powHACK has the highest number of defacements for the **.gov.in** domain, as shown in fig. 11

Defacer	Number of defacements	Percentage of total gov.in defacements
powHACK	**16**	**12.60**
FBH	**13**	**10.24**
Fatal Error	**12**	**9.45**
AIC	**10**	**7.87**
DarkBicho	**4**	**3.15**
GhostIRC	**4**	**3.15**
TheBuGz	**4**	**3.15**
Abunasar	**3**	**2.36**
Gantep	**2**	**1.57**
Gforce	**2**	**1.57**

Fig:11 : gov.in defacements hacker wise

Figures 10 and 11 reveal:

- Except powHACK, all other groups have defaced more .co.in sites than .gov.in sites
- The group FBH and powHACK have not defaced any site in the **nic.in** or **ernet.in** domain.
- The group GForce Pakistan seems to have targeted .nic.in sites as they have defaced **.nic.in** sites more than any other domain. However, the maximum no of **nic in** sites have been defaced by AIC.
- The most number of **gov.in** sites have been defaced by powHACK.. The groups powHACK and FBH seemed to have targeted the **gov.in** & .**co.in** domains and not any other domain.
- Silver Lords seems to have primarily targeted the **.co.in** domain

4.3.2. Hackers activity across the years

	AIC	Silver Lords	Gforce	FBH	powHACK
1998	0	0	0	0	0
1999	0	0	0	0	0
2000	0	0	36	0	0
2001	32	56	5	0	0
2002	43	1	0	3	0
2003	4	0	0	34	23
2004	18	0	0	0	8

Fig:12: .in defacements hacker/year distribution

The defacement activity of .in ccTLD sites by the hacker groups across the years is shown in fig 12. The hacker group AIC has been consistently attacking .in sites since 2001 and is still active. However, other groups have been active for particular period of 2 years.

4.4. Defacement by domain and Network

4.4.1. Most redefaced second/third level Domain

The top ten most re-defaced second/third level .in ccTLD domain are shown in fig 13. The most redefaced second level/third level .in ccTLD domain was railnet.gov.in. It was redefaced 16 times. The sites affected were er.railnet.gov.in, ircot.railnet.gov.in, irpmu.railnet.gov.in and nfr.railnet.gov.in

No.	Second level Domain	Redefacements
1	railnet.gov.in	16
2	ushacomm.co.in	6
3	caddcentre.co.in	5
4	ap.gov.in	4
5	cherrysoft.co.in	4
6	dtegoa.gov.in	4
7	ecrtenders.gov.in	4
8	ernet.in	3
9	vdc.co.in	3
10	aiims.ac.in	2

Fig: 13: .in re-defacements

4.4.2. Most targeted network

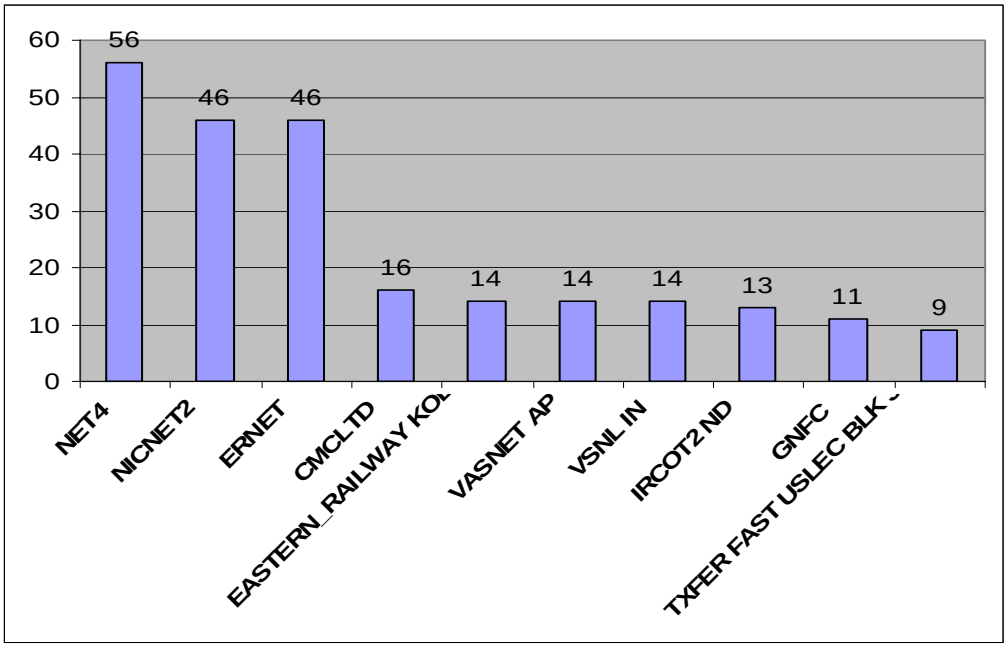


Fig:14 : .in defacements by network

The figure 14, details the networks affected by the defacement of .in ccTLD sites. It reveals that NET4 network is the most defaced, followed by ERNET and NICNET. It is also observed that 34 of the 46 defacements in the ERNET network involved the iisc.ernet.in sub domain.

4.4.3. Network defacements Year wise

	NIC	NET4	ERNET	EASTERN_RAILWAY	CMC LTD	IRCOT
1998	0	0	0	0	0	0
1999	1	0	0	0	0	0
2000	8	0	8	0	0	0
2001	18	3	28	0	0	0
2002	17	1	9	2	12	3
2003	1	7	1	11	4	7
2004	1	45	0	1	0	3

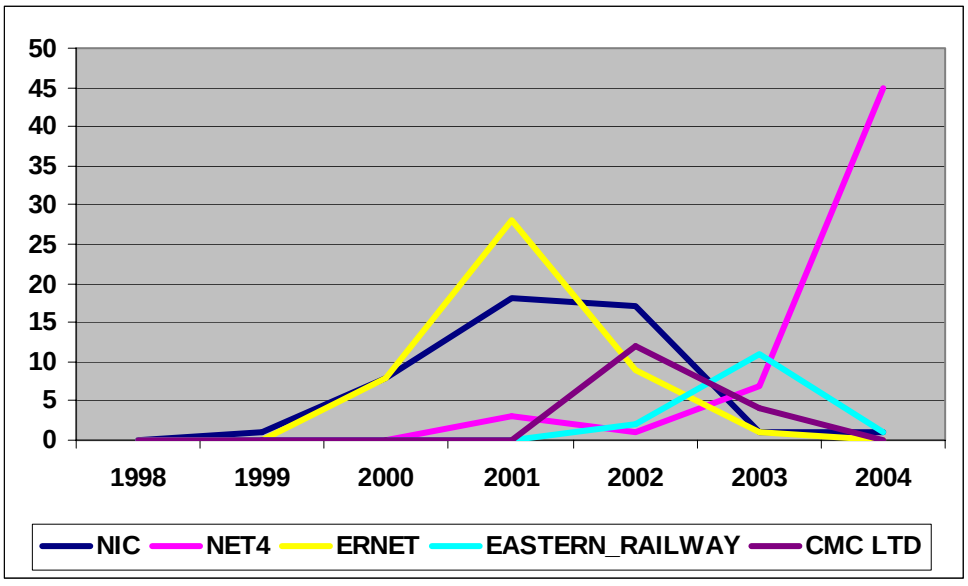


Fig: 15: .in defacements by network/year

The year wise defacements of some of the networks reveal that most of the defacements for the ERNET and NIC occurred before the year 2003. The networks seemed to have been secured after 2002 and as a result only one **.nic.in** site was defaced in 2003 and one in 2004. Similarly only one .ernet.in site was defaced in 2003 and none yet in 2004.

In contrast, the network NET4 had a sharp rise in defacements over the years. They had only 3 defacements in 2001, 1 in 2002, 7 in 2003 and already 45 defacements this year.

4.4.4. Most Defaced IP

The top 10 defaced IPs is shown in fig. 16. An IP wise highest defacement table is given. It includes mass defacements

No.	IP	Defacements	Network	Some Domains Hosted
1	202.71.129.55	28	NET4	ecrtenders.gov.in stellar.co.in
2	203.197.214.100	16	CMCLTD	airportsindia.org.in cbec.gov.in
3	202.4.160.9	14	VASNET AP	cpc.co.in karavalicollege.ac.in
4	203.163.160.35	11	GNFC	gujarat.gov.in
5	203.197.220.169	10	IRCOT2 ND	ircot.railnet.gov.in
6	202.71.129.116	9	NET4	worldcourier.co.in
7	203.200.107.145	9	AIIMS3 ND	aiims.ac.in
8	203.200.167.51	8	EASTERN_RAILWAY KOL	er.railnet.gov.in
9	202.71.144.146	7	NET4	caddcentre.co.in
10	207.235.6.88	7	RACKSPACE3 6 23	seacom.co.in

Fig: 16 : .in defacements by IP

IPs of the network NET4 appears twice in the list of top 10 defaced IPs. The NET4 IP 202.71.129.55 had suffered a mass defacement on 5th February 2004 which affected 14 sites.

As shown in Fig 17, for the .gov.in sites, the most defaced IP belonged to GNFC. However, IPs of Indian Railways networks EASTERN_RAILWAY KOL and IRCOT2 ND appear thrice in the top ten. The IP of NET4 network appears twice in the list of top ten defaced .gov.in IPs. Interestingly, a US based network TXFER FAST USLEC BLK 3 also appears in the list of top ten defaced .gov.in IPs.

No.	IP	Defacements	Network	Some Domains hosted
1	203.163.160.35	11	GNFC	gujarat.gov.in gidc.gov.in
2	203.197.214.100	10	CMCLTD	cbec.gov.in servicetax.gov.in epfindia.gov.in
3	203.197.220.169	10	IRCOT2 ND	irpmu.railnet.gov.in ircot.railnet.gov.in
4	203.200.167.51	8	EASTERN_RAILWAY KOL	er.railnet.gov.in
5	202.71.129.55	6	NET4	ecrtenders.gov.in
6	216.187.93.129	6	NET4	dtegoa.gov.in
7	203.200.167.52	5	EASTERN_RAILWAY KOL	nfr.railnet.gov.in
8	203.122.59.194	4	SPECTRA IDC NET	surveyofindia.gov.in
9	203.199.178.41	4	APTS3 HYD	ipr.ap.gov.in
10	207.106.22.27	4	TXFER FAST USLEC BLK 3	dop.rajasthan.gov.in

Fig: 17: gov.in defacements by IP

4.5. Defacement by Hosting Country

The fig 18 details the hosting of **.in** websites country-wise. 470 of .in sites were hosted in India, while 58 sites were hosted in US, 8 sites were in Canada, 6 in Australia, 3 in European Union while 1 each in UK and Singapore. Hosting details of some of the old defacements were not available.

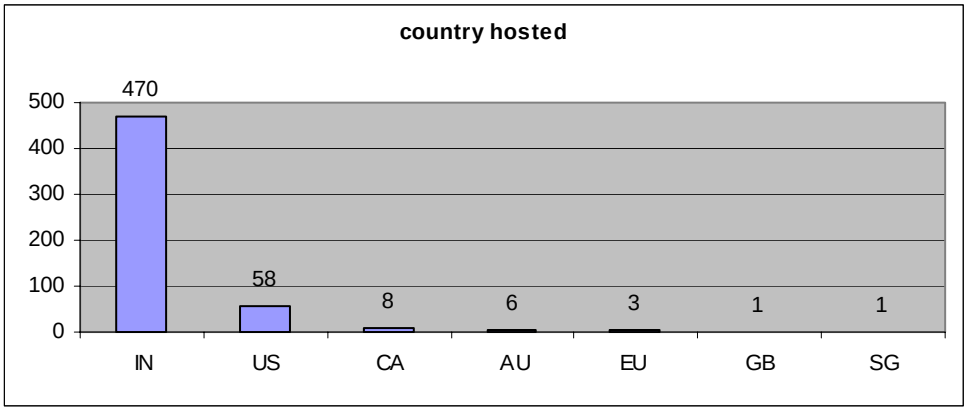


Fig: 18: .in defacements by hosting country

The figure 19 shows the details of .gov.in sites hosted country-wise. In the .gov.in sites, 101 were hosted in India, 8 in USA and 7 in Canada. It is interesting to note some .gov.in sites are hosted abroad and and have been defaced .

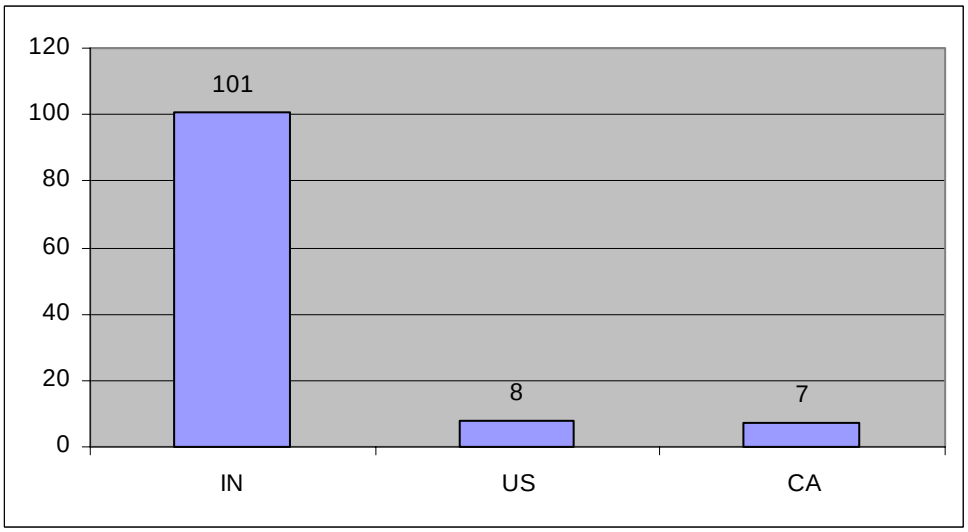


Fig: 19: gov.in defacements by hosting country

4.6. Hosting Platform

The fig 20 details the hosting platforms on which .in sites were hosted. The windows (all versions) had the highest number of defacements in comparison to other platforms.

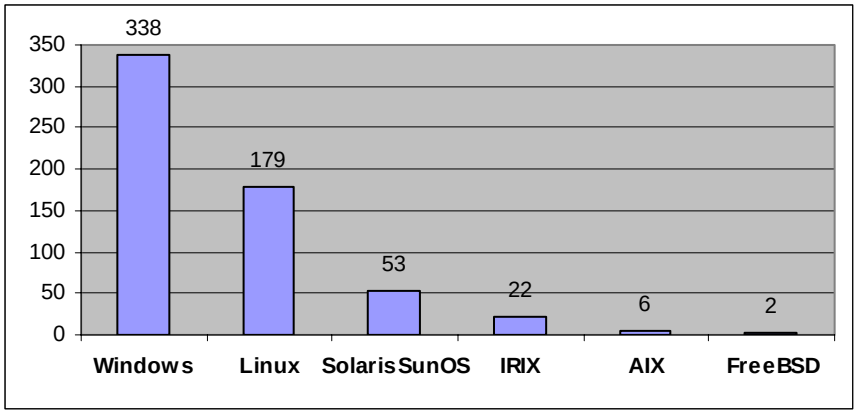


Fig: 20: .in defacements by platform

The fig 21 details the hosting platforms on which .gov.in sites were hosted. Here too, windows had the maximum number of defacements

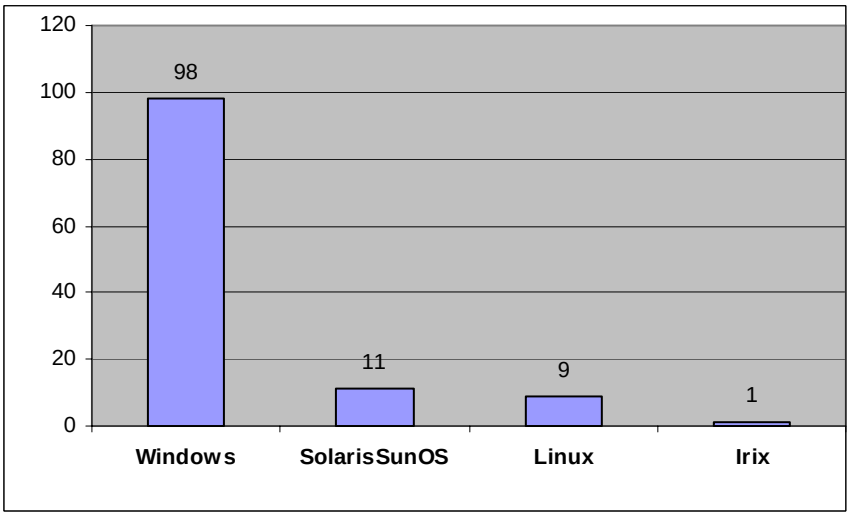


Fig: 21: gov.in defacements by platform

.

5. Errata

Data regarding some sites are presently not available as some of the domains no longer exist.

6. References

1. www.zone-h.org
2. www.attrition.org
3. mirror.delta5.com.br
4. www.srijith.net
5. www.dnsstuff.com
6. www.safemode.org
7. domain.ncst.ernet.in
8. whois.domain.ncst.ernet.in