ORISSA COMPUTER APPLICATION CENTRE
Technical Directorate of I.T. Department, Government of Orissa

Our Ref.No.OCAC-TE-1/2010-3024 Dated 23 -07-2011

From

Shri Manoj Kumar Pattanik, OAS-I(JB)
General Manager (Admn.)

To

The Under Secretary,
Deptt. of IT,
Govt. of Orissa

Sub: CERT-In Security Guidelines received from Govt. of India

Ref: Our Letter No. OCAC-TE-1/2010-751, dated 21-03-11
Your Letter No. 1730/IT, dated 05-07-11 and No. 433/IT, dated 05-02-11

Sir,

In inviting a reference to the subject cited above, I am directed to draw a reference to the Letter DO No. 2(5)-2010-CERT-In, dated 8-06-11 received from DG, CERT-In, MCIT, GOI, New Delhi indicating therein the summary of web site defacements for the months of March & April, 2011 indicating the attack trends, methodologies, vulnerabilities, suggested counter measures and the guidelines recommending best practices to be followed by systems administrators / web site administrators etc. to secure the web applications and web servers , available in the guidelines page of CERT-In website. Web Server Security Guidelines, Securing IIS 7.0 Web Server Guidelines, Guidelines for Auditing and Logging etc. is available in the following URL.

http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW01

The said letter may kindly be communicated to all Departments and Organisations in the domain of the State Govt. to follow the best practices for securing the web applications and web servers, remain vigilant about signs of such attacks and share the said information and experience with OCAC & CERT-In, take appropriate measures for protecting their system & network, and also

(411)

239

GOVERNMENT OF ORISSA
DEPARTMENT OF INFORMATION TECHNOLOGY

* * *

No 1730 /IT
IT-VI-31/2011(Pt.)

Bhubaneswar Dtd. 07-11
Dated

From

Shri Tuladhar Bhoi, OFS-I (JB)
AFA-cum-Under Secretary to Government

9310
OCAC
Technical Directorate of IT Deptt. Govt. of Orissa
05 JUL 2011
RECEIVED
BY

To

The General Manager (Admn.)
Orissa Computer Application Centre (OCAC),
Bhubaneswar

Sub: CERT-In Security Guidelines received from the Government of India.

Sir,

In enclosing a copy of the D.O. letter No.2(5)/2011-CERT-In dtd 6.7.11 alongwith its enclosures received from the Director General, MCIT, DIT, Government of India on the above subject, I am directed to request you to please take appropriate follow up action under intimation to this Department.

6.7.11
2058
(1750)
Dgn (Ucrt)

Yours faithfully,

AFA-cum-Under Secretary to Government

SKM, Sir
Put up in file
12-7-11

3.3 Details of Mass Defaced IPs during March 2011

S No.	IP	ISP Name	Defacer	OS	WebServer	ISP Location	No. Of Sites
1	216.151.174.22	CYBERCON	HEXBOOT3R	Linux	Apache	CA	503
2	173.233.65.99	TURNKEY-INTERNET	TeaMp0isoN	Linux	Apache	US	145
3	174.122.92.189	THEPLANET-AS	1923Turk	Linux	Apache	US	28

Table 3: Mass Defaced IPs

4. Defacement by Networks

4.1 Most Targeted Networks

It has been observed that most (98%) of Indian websites defaced were hosted outside India.

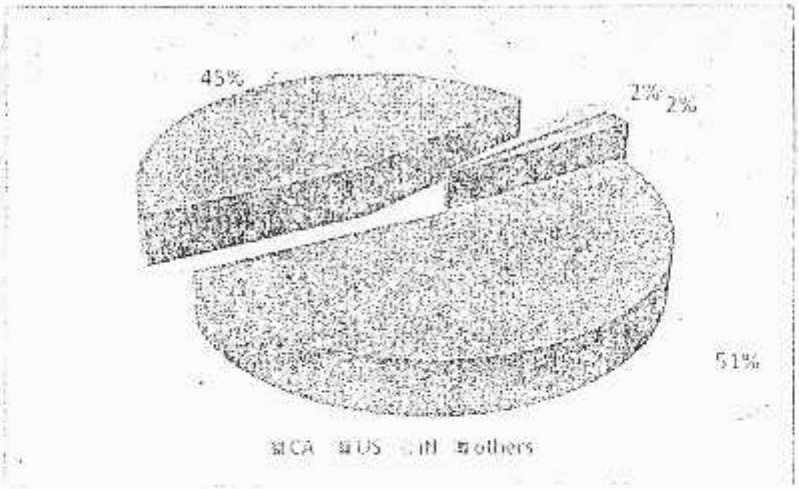

Figure 5: Defaced website hosting country-wise

6. Suggested Countermeasures

- Apply appropriate updates/patches at the OS and application level regularly.
- Validate and sanitize all user input, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks.
- Enable and maintain logs of different devices and servers and maintain the same for all the levels.
- Conduct auditing for web application & configuration settings of web server periodically.
- Periodically check the web server directories for any malicious/unknown web shell files and remove as and when noticed.
- Use an application firewall to controls input, output, and/or access to the web application.
- Install a good antivirus and keep it updated and running.
- The following CERT-In security guidelines may be referred :
  - Web Server Security Guidelines
    http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guideline CISG-2004-04
  - Securing IIS 7.0 Web Server Guidelines
    http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guides CISGu-2010-01
  - Guidelines for Auditing and Logging
    http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guideline CISG-2008-01

S. Mallik

to track detect and mitigate these cyber attacks. The Departments may be advised to get their web sites security-audited by authorized auditors empanelled with Govt. of India for the said purpose. If required, CERT-In may be contacted for necessary advice and guidance.

The security related circulars, guidelines, documents etc. shall be made available on the Govt. web site (www.orissa.gov.in) as well as OCAC web site (www.ocac.in)

This is for kind information and necessary action.

Yours faithfully,

27.7.11

General Manager (Admn.)

Encl : As above

C.C : 1. SIO, NIC, Bhubaneswar for kind information and necessary action.

2. Director, STPI for kind information and necessary action.

3. Director, OeSL for favour of information and necessary action.

4. Mrs. Sarathi Mallick, SSE, OCAC, placed at IT Centre, Secretariat (To upload the security related documents or provide related links to IT Dept. page of Govt. web site immediately after confirming the same from officials of CERT-In)

5. Mrs. S. Mohanty, SSE, OCAC (To upload the security related documents or provide related links to OCAC web site immediately)

A DY NO 2504 (IT) 21.6.11 1238
CSI 21.6.11

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
सूचना प्रौद्योगिकी विभाग
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन)
इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्प्लेक्स, नई दिल्ली-110003
Government of India
Ministry of Communications and Information Technology
Department of Information Technology
Indian Computer Emergency Responce Team (CERT-in)
Electronics Niketan, 6, C.G.O. Complex, New Delhi-110003
Tel. : 24368544, Fax : 24366806 E-mail : grai@mit.gov.in

Director General

D.O.No. 2(5)/2011-CERT-In

8.06.2011

Dear Shri Gupta,

CERT-In is tracking defacement of Indian websites on regular basis. A total of 981 & 1526 Indian websites were defaced by various defacers during the month of March & April 2011 respectively. Similarly 217 & 244 number of websites have been compromised and links to malicious websites were planted on these sites during corresponding months. Summary of website defacements depicting domain-wise and network-wise break-up of the websites defaced, top defacers and vulnerabilities which are largely exploited is attached.

In view of growing attacks on websites, you are requested to advise website administrators to follow best practices to secure web applications and web servers.

The following CERT-In security guidelines may be referred:

- Web Server Security Guidelines
  http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guideline CISG-2004-04
- Securing IIS /7.0 Web Server Guidelines
  http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guides CISGu-2010-01
- Guidelines for Auditing and Logging
  http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guideline CISG-2008-01

With regards,

Yours sincerely,

(Gulshan Rai)

Encl: As above

Shri Debendra Nath Gupta, IAS
Comm. & Secretary IT,
Information Technology Deptt.
Orissa Computer Application Centre Building,
Jayadev Vihar, Bhubaneswar-751001, Orissa

237

15

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of
Website Defacements
April 2011

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

CONTENTS

CERT-In Defacements Summary April 2011

1. Introduction

This report summarizes Indian website defacements during April 2011. In all 1526 Indian websites were defaced during the month of April 2011 against 981 defacements in March 2011.

2. Distribution of defaced domains

The defaced domains include:

- Top level domains TLDs (.com, .net, .org, .edu .biz and .info) and
- Country code top level domain – ccTLDs (.co.in, .net.in, .gov.in, .org.in, .nic.in, .ac.in, .edu.in and .res.in).

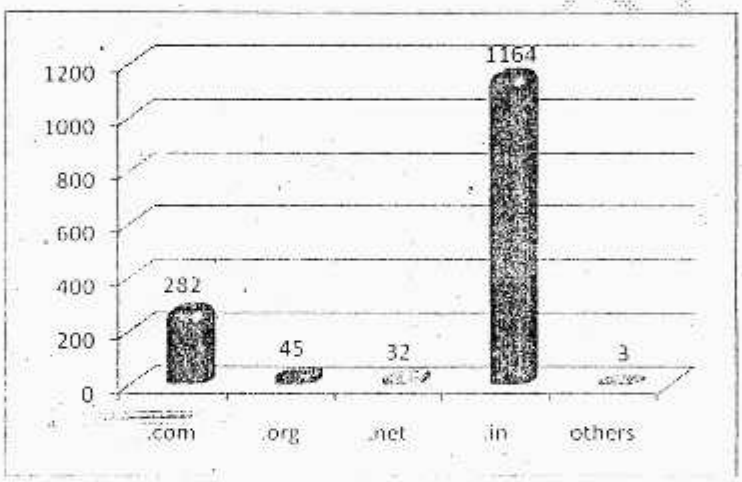

Figure 1: Distribution of Defaced Domains (TLDs)

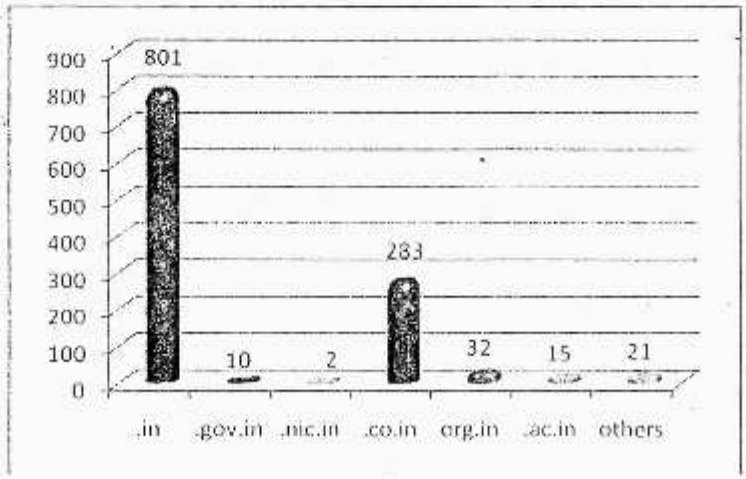

Figure 2: Distribution of Defaced Domains (ccTLDs)

CERT-In Defacements Summary April 2011

1. Introduction

This report summarizes Indian website defacements during April 2011. In all 1526 Indian websites were defaced during the month of April 2011 against 981 defacements in March 2011.

2. Distribution of defaced domains

The defaced domains include:

- Top level domains TLDs (.com, .net, .org, .edu .biz and .info) and
- Country code top level domain – ccTLDs (.co.in, .net.in, .gov.in, .org.in, .nic.in, .ac.in, .edu.in and .res.in).

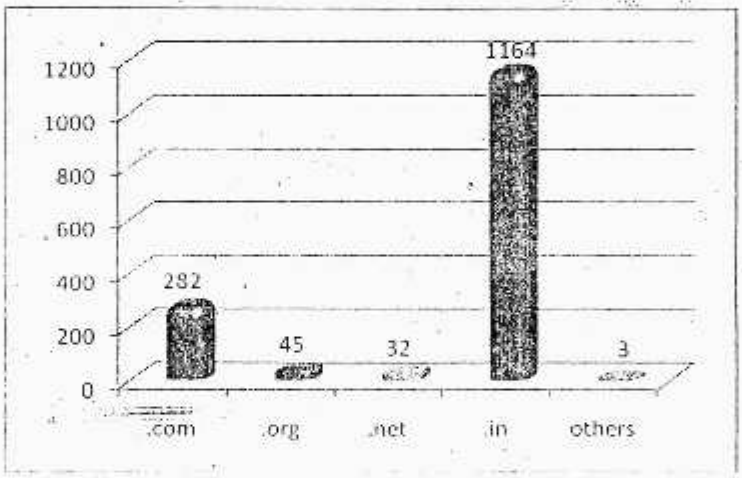

Figure 1: Distribution of Defaced Domains (TLDs)

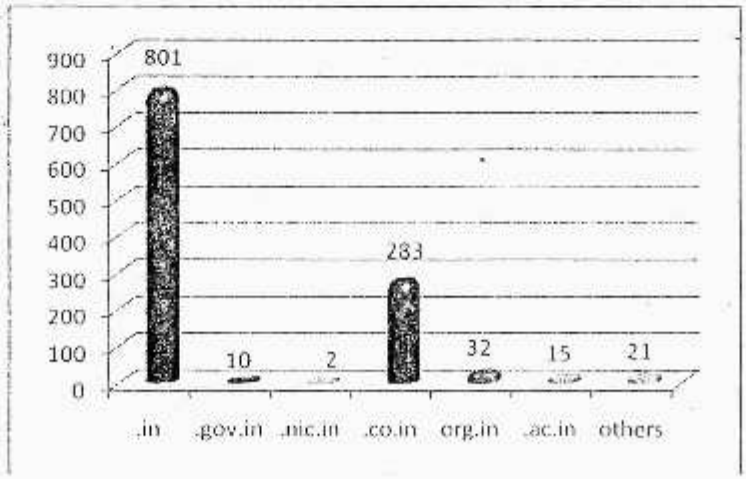

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of April 2011 a total of 1526 Indian websites were defaced. Out of theses 76% websites were on .in domain and 19% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

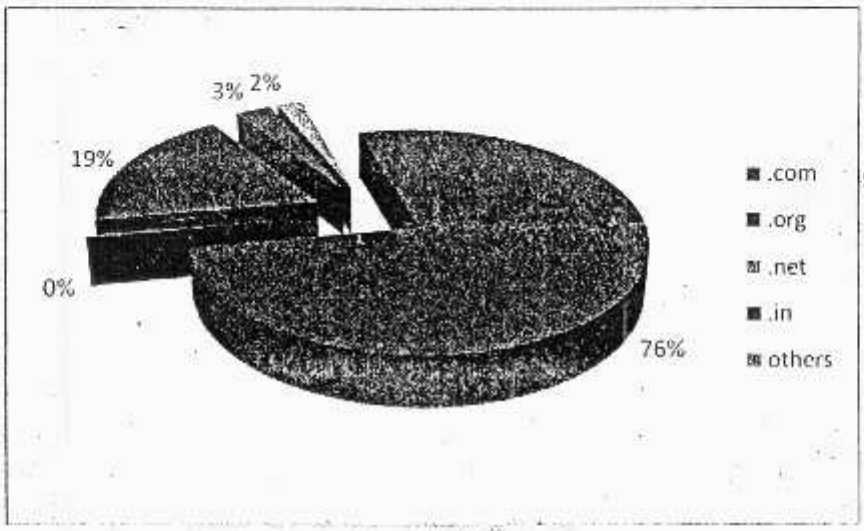

Figure 3. % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 1164 defaced websites, 69% were in .in domain, 24% in .co.in and 1% in .gov.in domains.

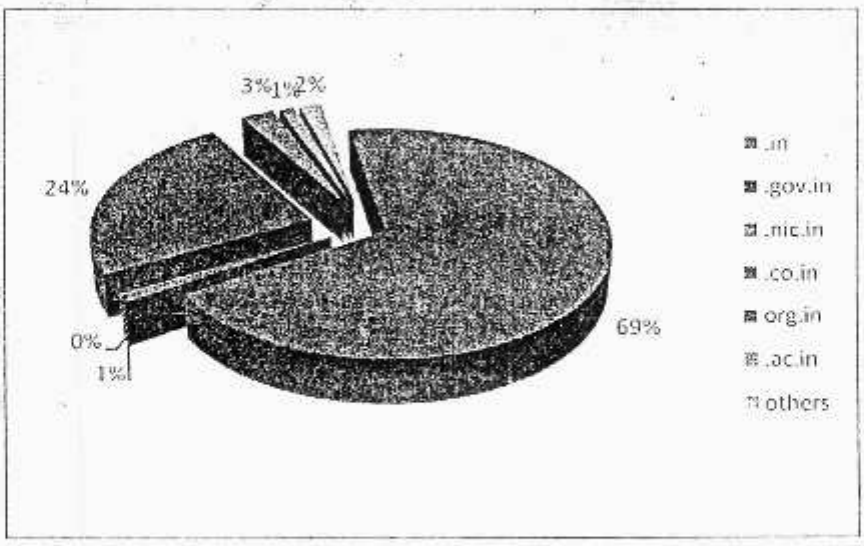

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (TLDs)

Table 1 shows Top Defacers (TLD) wise in April 2011

S.No	Attacker Name	Number of websites
1	PakH3X0r	109
2	1923Turk	92
3	TeaM HITMAN HaCkEr	25
5	C37HUN	17
6	Hidden Pain	16
7	iskorpitx	14
8	DEATH_K1NG	8
9	INNOCENT HACKER	7
10	Mr.PaPaRoSSe	7

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

Table 2 shows Top Defacers (ccTLD) wise in April 2011.

S.No	Attacker Name	Number of websites
1	1923Turk	183
2	iskorpitx	138
3	HEXB00T3R	83
5	IslamiC GhostS TeaM	66
6	ZCompany Hacking Crew	55
7	DEATH_K1NG	49
8	PakH3X0r	42
9	TeaM HITMAN HaCkEr	33
10	alex_owners	33

Table 2: Top Defacers ccTLD wise

3.3 Details of Mass Defaced IPs during April 2011

S No.	IP	ISP Name	Defacer	OS	WebServer	ISP Location	No. Of Sites
1	66.96.205.133	Network Operations Center	1923Turk	Linux	Apache	US	76
2	65.98.11.154	FortressITX	HEXB00T3R	Linux	Apache	US	72
3	174.132.224.210	ThePlanet	PakH3X0r	Win 2003	IIS/6.0	US	70
4	206.212.241.34	COLOSTORE	IslamiC GhostS TeaM	Linux	Apache	US	64
5	75.126.141.28	SoftLayer	ZCompany Hacking Crew	Win 2003	IIS/6.0	US	50

Table 3: Mass Defaced IPs

4. Defacement by Networks

4.1 Most Targeted Networks

It has been observed that most (93%) of Indian websites defaced were hosted outside India.

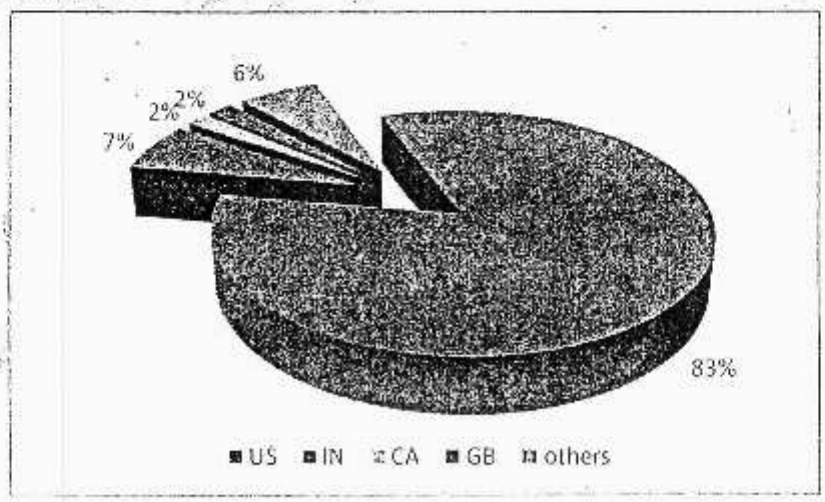

Figure 5. Defaced website hosting country-wise

5. Attack Trends

5.1 Attack Methodologies

Attack methodologies which are generally used to deface a website are:

- Attacks against the administrator/user (password stealing/ sniffing)
- Shared mis-configurations
- File Inclusion
- SQL Injection
- Web shell uploading
- Access credentials through Man in the Middle attack
- FTP Server Intrusion
- Web Server Intrusion
- DNS attack through cache poisoning
- Remote administrative panel access through brute forcing
- SSH server Intrusion
- RPC Server intrusion
- Telnet Server intrusion

5.2 Vulnerabilities

The Vulnerabilities which are largely exploited for the defacements

- SQL injection vulnerability in the Maian Media Silver (com_maianmedia) component for Joomla! (CVE-2010-4739)
- SQL injection vulnerability in the JExtensions JE Auto (com_jeauto) component for Joomla! (CVE-2010-4720)
- Multiple cross-site scripting (XSS) vulnerabilities in the Back End in Joomla! (CVE-2010-2535)
- Cross-site scripting (XSS) vulnerability in Microsoft SharePoint Server 2007 (CVE-2010-0817)
- SQL injection vulnerability in the Yannick Gaultier sh404SEF component for Joomla! (CVE-2010-4404)
- Multiple Vulnerabilities in Microsoft products : Windows Server 2008, 2003 & Windows Vista (CIAD-2010-0064)
- Microsoft Internet Information Services(IIS) Authentication Memory Corruption Arbitrary Code Execution Vulnerability (CIVN-2010-153)
- Apache 'mod_isapi' Memory Corruption Vulnerability (CIVN-2010-70)
- Apache HTTP Server Request Header Information disclosure Vulnerability (CIVN-2010-71)

8) 230

6. Suggested Countermeasures

- Apply appropriate updates/patches at the OS and application level regularly.
- Validate and sanitize all user input, and present error messages that reveal little or no useful information to the user to prevent SQL injection attacks.
- Enable and maintain logs of different devices and servers and maintain the same for all the levels.
- Conduct auditing for web application & configuration settings of web server periodically.
- Periodically check the web server directories for any malicious/unknown web shell files and remove as and when noticed.
- Use an application firewall to controls input, output, and/or access to the web application.
- Install a good antivirus and keep it updated and running.
- The following CERT-In security guidelines may be referred :
  - Web Server Security Guidelines
    http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guideline CISG-2004-04
  - Securing IIS /7.0 Web Server Guidelines
    http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guides CISGu-2010-01
  - Guidelines for Auditing and Logging
    http://www.cert-in.org.in/s2cMainServlet?pageid=GUIDLNVIEW02&refcode=Guideline CISG-2008-01

229

9

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements March 2011

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

CONTENTS

CERT-In Defacements Summary March 2011

1. Introduction

This report summarizes Indian website defacements during March 2011. In all 981 Indian websites were defaced during the month of March 2011 against 1012 defacements in February 2011.

2. Distribution of defaced domains

The defaced domains include:

- Top level domains TLDs (.com, .net, .org, .edu .biz and .info) and
- Country code top level domain – ccTLDs (.co.in, .net.in, .gov.in, .org.in, .nic.in, .ac.in, .edu.in and .res.in).

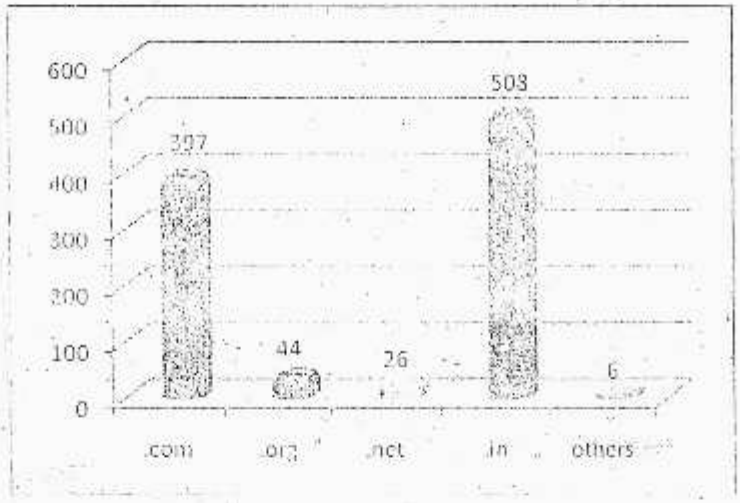

Figure 1: Distribution of Defaced Domains (TLDs)

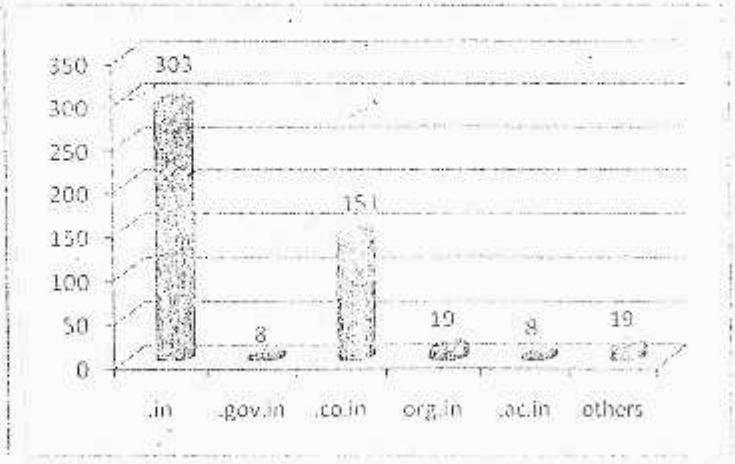

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of March 2011 a total of 981 Indian websites were defaced. Out of theses 52% websites were on .in domain and 40% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

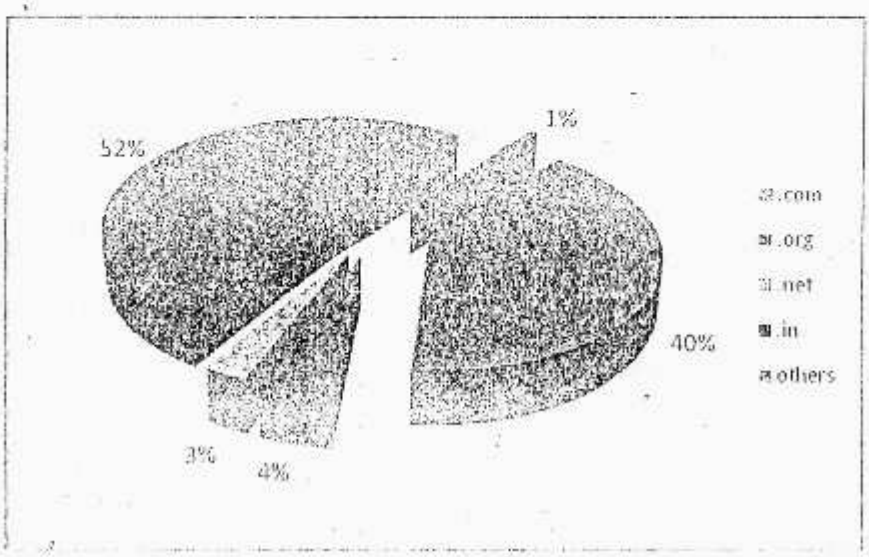

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 508 defaced websites, 60% were in .in domain, 30% in .co.in and 1% in .gov.in domains.

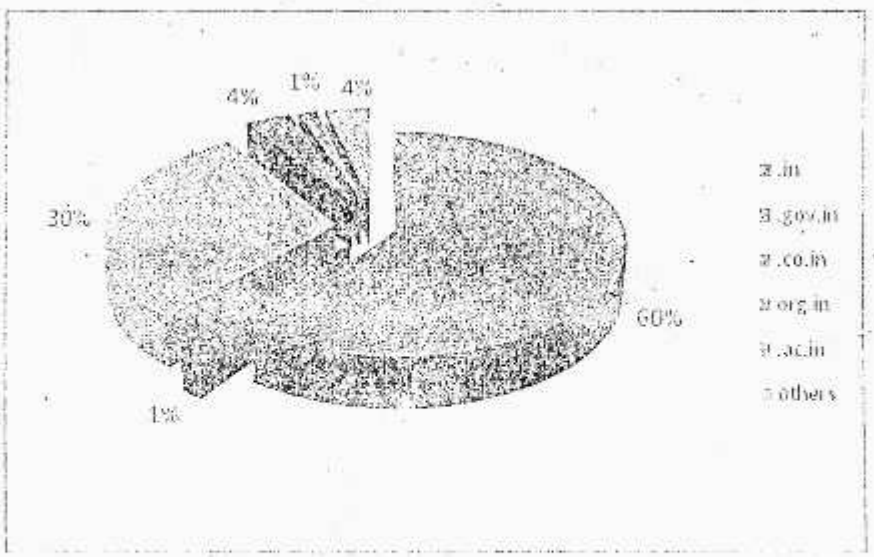

Figure 4: % Distribution of Defaced Domains (ccTLDs)

4) 226

2.1 Percentage Distribution of defaced domains

In the month of March 2011 a total of 981 Indian websites were defaced. Out of theses 52% websites were on .in domain and 40% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

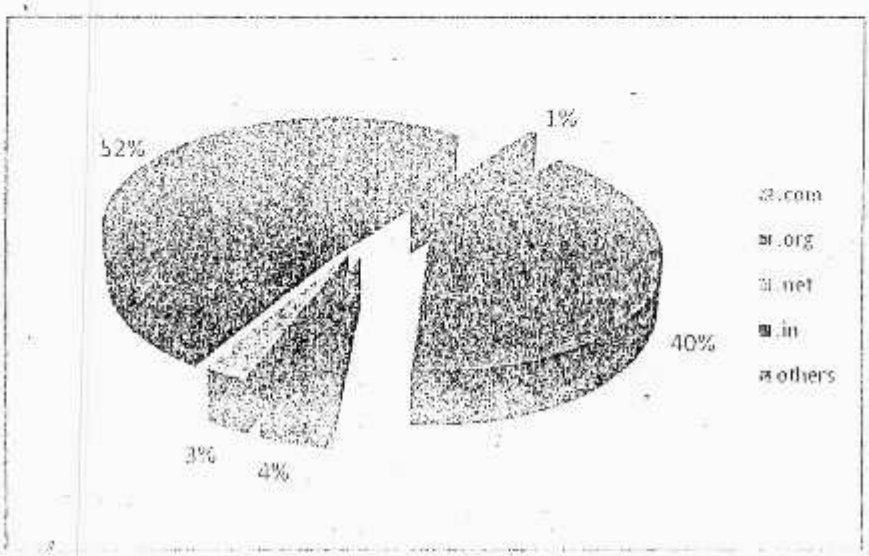

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 508 defaced websites, 60% were in .in domain, 30% in .co.in and 1% in .gov.in domains.

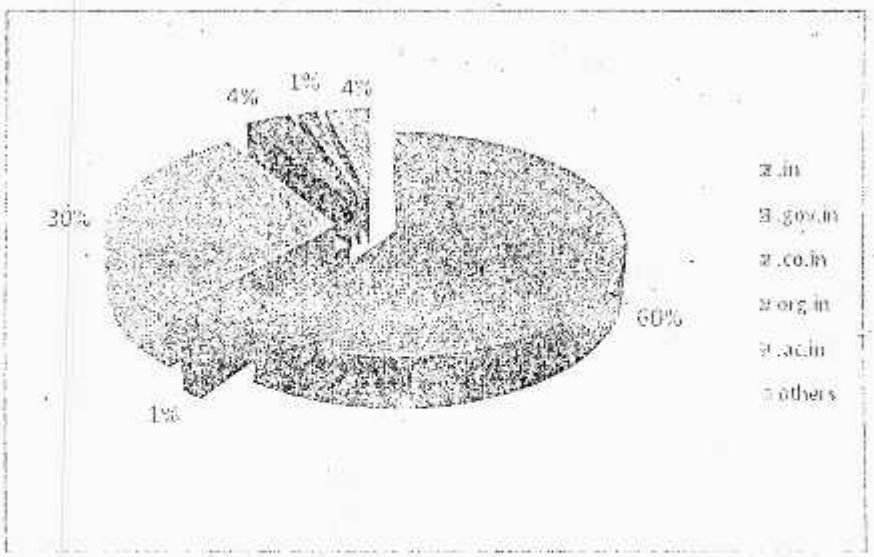

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (TLDs)

Table 1 shows Top Defacers (TLD) wise in March 2011

S.No	Attacker Name	Number of websites
1	HEXB00T3R	301
2	TeaMp0isoN	53
3	1923Turk	47
5	iskorpitx	14
6	s-man	13
7	ZCompany Hacking Crew	7
8	bhierien	5
9	hacked by Wx	3
10	TeaM MosTa	3

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

Table 2 shows Top Defacers (ccTLD) wise in March 2011.

S.No	Attacker Name	Number of websites
1	HEXB00T3R	206
2	1923Turk	95
3	TeaMp0isoN	92
5	iskorpitx	22
6	ZCompany hacking crew	9
7	TechnicaL	8
8	INNOCENT HACKER	7
9	DeltahackingSecurityTEAM	5
10	bhierien	5

Table 2: Top Defacers ccTLD wise

3.3 Details of Mass Defaced IPs during March 2011

S No.	IP	ISP Name	Defacer	OS	WebServer	ISP Location	No. Of Sites
1	216.151.174.22	CYBERCON	HEXBOOT3R	Linux	Apache	CA	503
2	173.233.65.99	TURNKEY-INTERNET	TeaMp0isoN	Linux	Apache	US	145
3	174.122.92.189	THEPLANET-AS	1923Turk	Linux	Apache	US	28

Table 3: Mass Defaced IPs

4. Defacement by Networks

4.1 Most Targeted Networks

It has been observed that most (98%) of Indian websites defaced were hosted outside India.

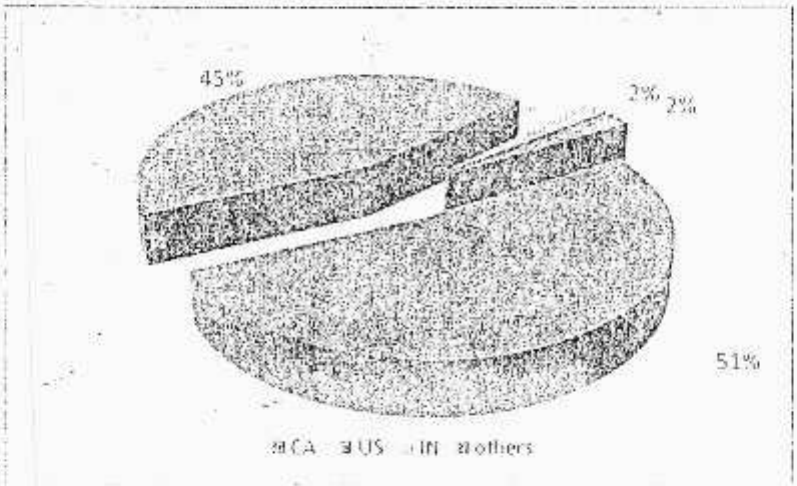

Figure 5: Defaced website hosting country-wise