CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements February 2012

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

310

CONTENTS

1. Introduction

This report summarizes Indian website defacements during February 2012. In all 2460 Indian websites were defaced during the month of February 2012 against 1425 defacements in January 2012.

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).

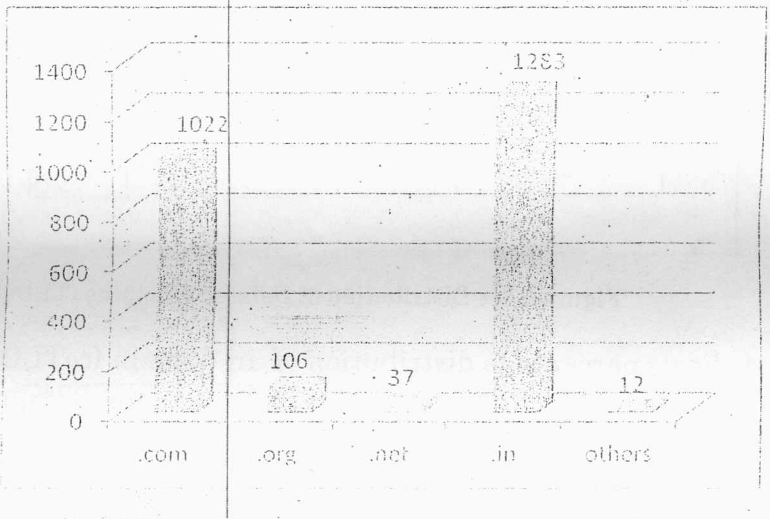

Figure 1: Distribution of Defaced Domains (TLDs)

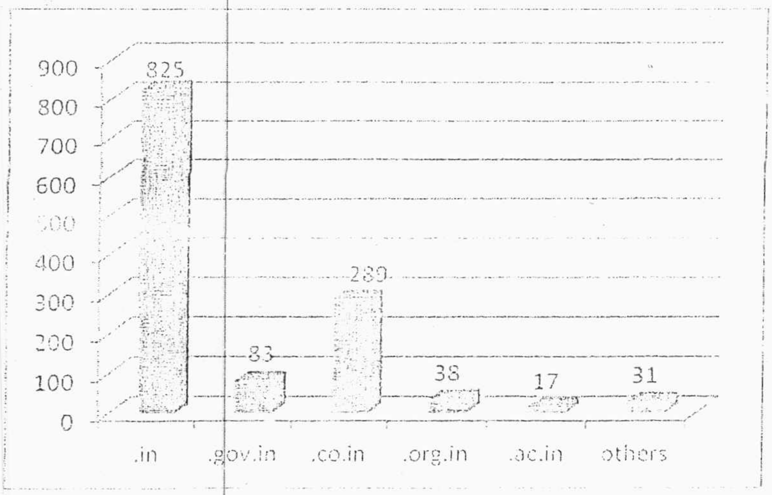

Figure 2: Distribution of Defaced Domains (ccTLDs)

308

2.1 Percentage Distribution of defaced domains

In the month of February 2012 a total of 2460 Indian websites were defaced. Out of these 52% websites were on .in domain and 41.5% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

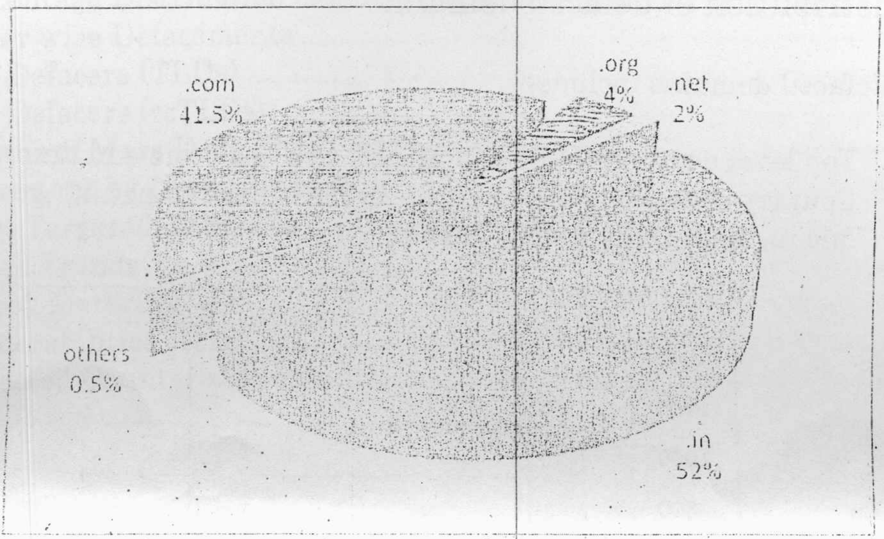

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 1283 defaced websites, 64% were in .in domain, 23% in .co.in and 7% in .gov.in domains.

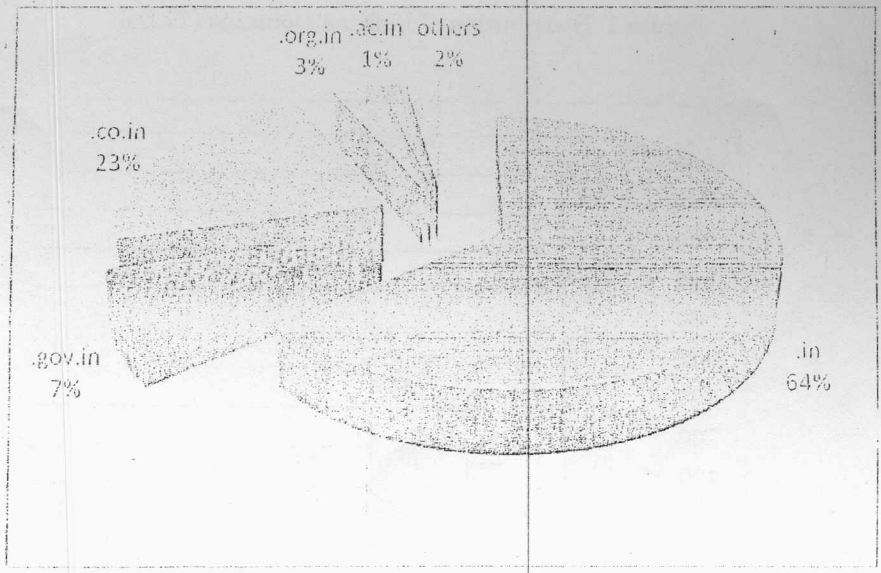

Figure 4: % Distribution of Defaced Domains (ccTLDs)

307

3. Hacker wise Defacements

3.1 Top Defacers (TLDs)

S.No	Attacker Name	Number of websites
1	H4x0rL1f3	248
2	ZCompany Hacking Crew	178
3	SM00K0 HaCkEr	135
4	AL.MaX HaCkEr	122
5	Bangladesh Cyber Army	111
6	kinG oF coNTroL	101
7	MrWanz	99
8	k1r4	50
9	DR-MTMRD	36
10	Tariq SQL	32

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

S.No	Attacker Name	Number of websites
1	H4x0rL1f3	145
2	AL.MaX HaCkEr	112
3	kinG oF coNTroL	73
4	ZCompany Hacking Crew	69
5	Bangladesh Cyber Army	89
6	Dm4r aLsuLMi	49
7	Hmei7	45
8	MrWanz	45
9	DR-MTMRD	43
10	sksking	42

Table 2: Top Defacers ccTLD wise

304

Co

- Multiple Vulnerabilities in Microsoft products : Windows Server 2008, 2003 & Windows Vista (CIAD-2010-0064)
- Apache Tomcat HTTP DIGEST Authentication Vulnerability (CIVN-2011-0169)

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