CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of
Website Defacements
December 2011

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

327

CONTENTS

CERT-In Defacements Summary December 2011

1. Introduction

This report summarizes Indian website defacements during December 2011. In all 2087 Indian websites were defaced during the month of December 2011 against 1651 defacements in November 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).

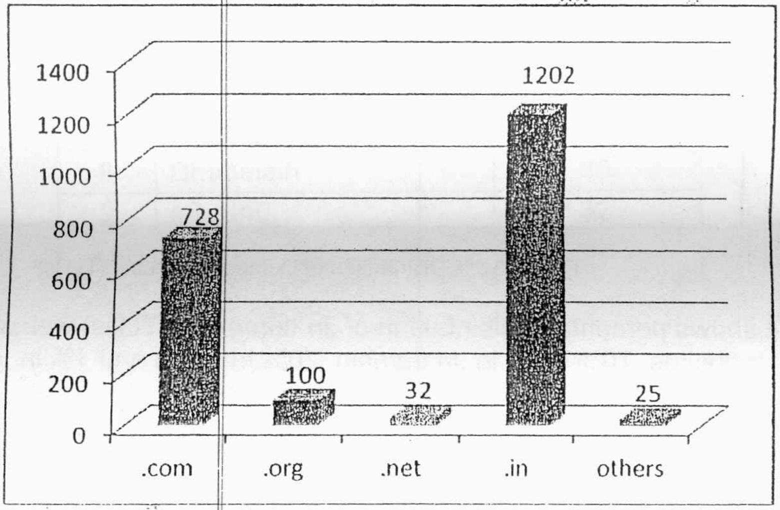

Figure 1: Distribution of Defaced Domains (TLDs)

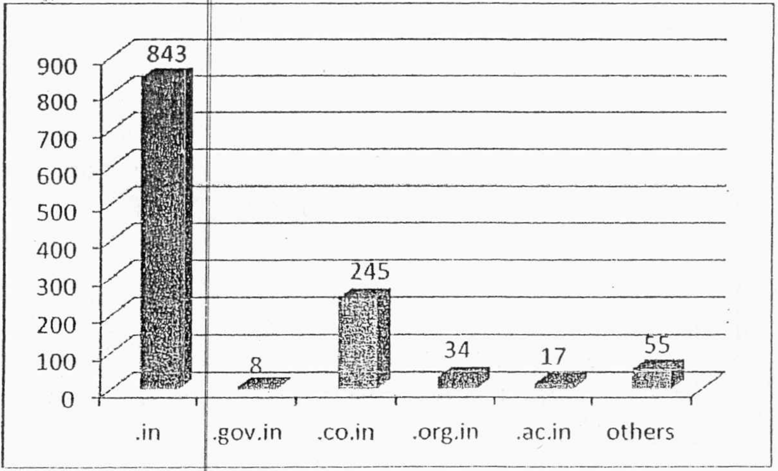

Figure 2: Distribution of Defaced Domains (ccTLDs)

B25

2.1 Percentage Distribution of defaced domains

In the month of December 2011 a total of 2087 Indian websites were defaced. Out of these 58% websites were on .in domain and 35% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

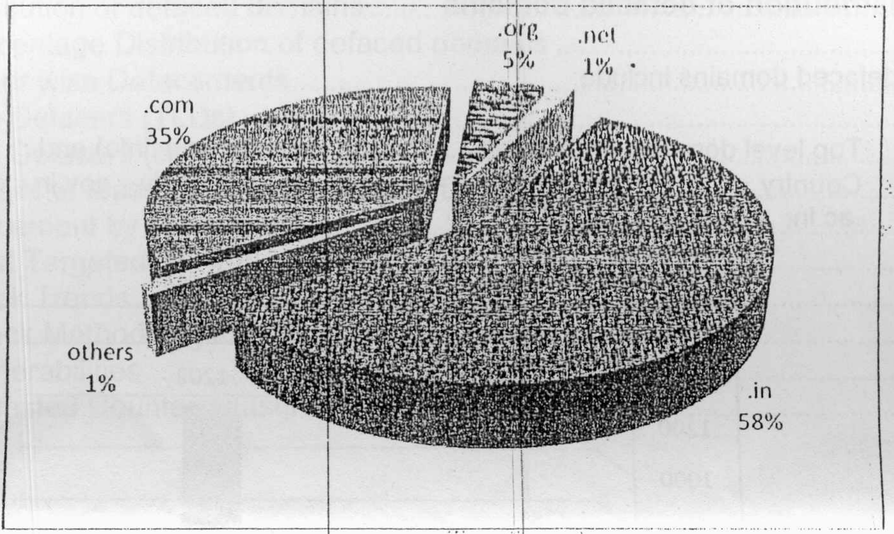

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 1202 defaced websites, 70% were in .in domain, 20% in .co.in and 1% in .gov.in domains.

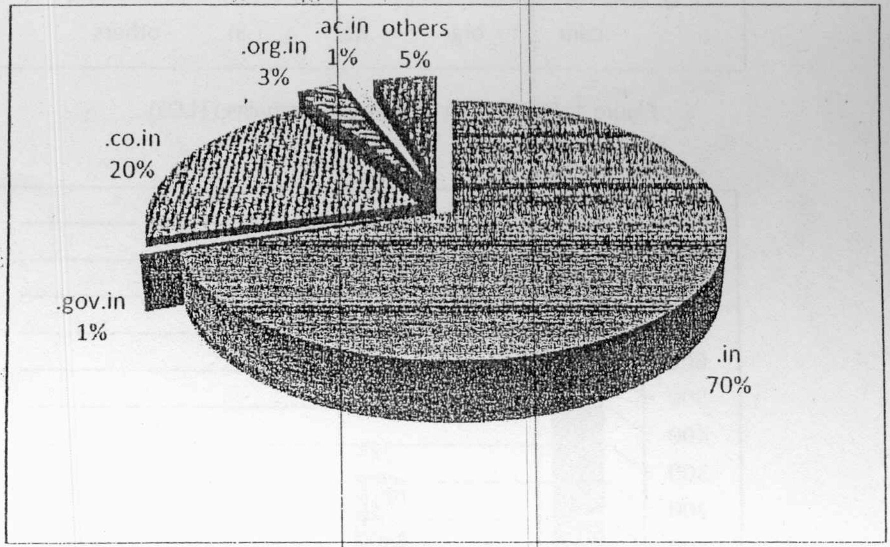

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (TLDs)

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

S.No	Attacker Name	Number of websites
1	Pakleets	264
2	Hidden Pain	82
3	Th3 K!LL3r Dz	80
4	Niruda	68
5	aBu.HaliL501	50
6	Tn_Scorpion	37
7	mr.mash3l	35
8	Dr.abolalh	33
9	pSyCh0	32
10	TheHackersArmy	27

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

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

S.No	Attacker Name	Number of websites
1	Pakleets	178
2	Cyber-Crystal	106
3	aBu.HaliL501	94
4	TheHackersArmy	79
5	Th3 K!LL3r Dz	65
6	Hmei7	47
7	Hidden Pain	42
8	BriscO-Dz	31
9	J|nX	29
10	Niruda	29

Table 2: Top Defacers ccTLD wise

32-3

3.3 Details of Mass Defaced IPs during December 2011

S No.	IP	ISP Name	ISP Location	Defacer	OS	WebServer	No. of Sites
1	174.36.228.38	SOFTLAYER	US	Pakleets	Linux	Apache	192
2	69.73.173.58	GNAXNET	US	aBu.HaliL501	Linux	Apache	174
3	72.52.166.134	LIQUID-WEB-INC	US	Th3 KILL3r Dz	Linux	Apache	158
4	184.173.91.104	SOFTLAYER	US	Pakleets	Linux	Apache	132
5	173.248.143.44	WEHOSTSITESCOM	US	Hidden Pain	Linux	Apache	111
6	64.120.179.138	NOC	US	TheHackersArmy	Linux	Apache	74
7	68.67.77.60	GORACK	US	Dr.abolalh	Linux	Apache	55

Table 3: Mass Defaced IPs

4. Defacement by Networks

4.1 Most Targeted Networks

It has been observed that most (96%) of Indian websites defaced were hosted outside India.

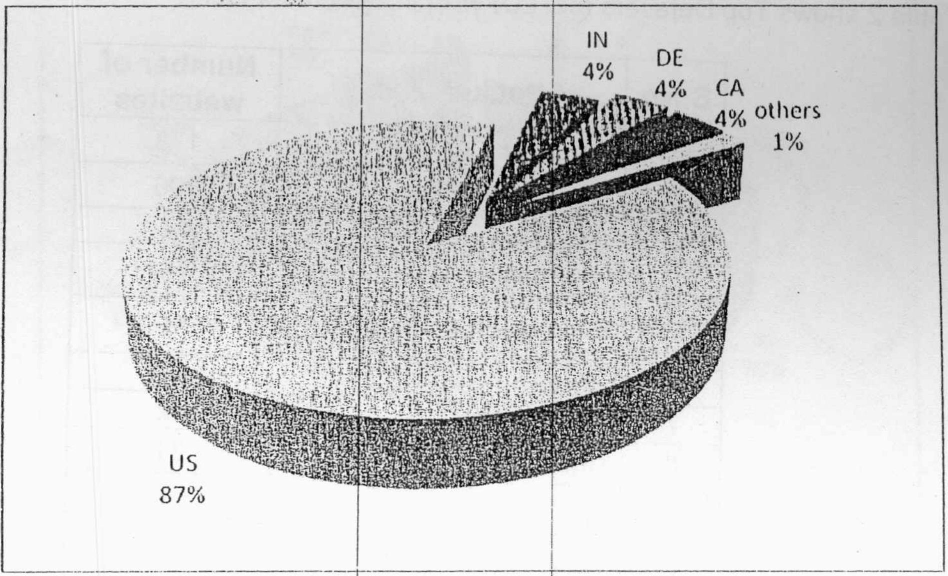

Figure 5: Defaced website hosting country-wise

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 JS Calendar component for Joomla! (CVE-2010-4795)
- SQL injection vulnerability in the Maian Media Silver component for Joomla! (CVE-2010-4739)
- Multiple cross-site scripting (XSS) vulnerabilities in Joomla! (CVE-2011-2710, CVE-2011-2509)
- Multiple cross-site scripting (XSS) vulnerabilities in the Back End in Joomla! (CVE-2010-2535)
- Cross-site scripting (XSS) vulnerability in the Petition Node module for Drupal (CVE-2011-4560)
- SQL injection vulnerability in Drupal Translation Management module 6.x before 6.x-1.21 (CVE-2011-1663)
- Authentication bypass vulnerabilty in phpMyAdmin (CVE-2010-4481)
- Vulnerabilities in Microsoft SharePoint Could Allow Elevation of Privilege (CIVN-2011-0152)
- 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)

321

- Apache Tomcat HTTP DIGEST Authentication Vulnerability (CIVN-2011-0169)
- Apache HTTP Server Request Header Information Disclosure Vulnerability (CIVN-2010-71)

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