303

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements March 2012

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

CONTENTS

1. Introduction

This report summarizes Indian website defacements during March 2012. In all 2486 Indian websites were defaced during the month of March against 2460 defacements in February 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).

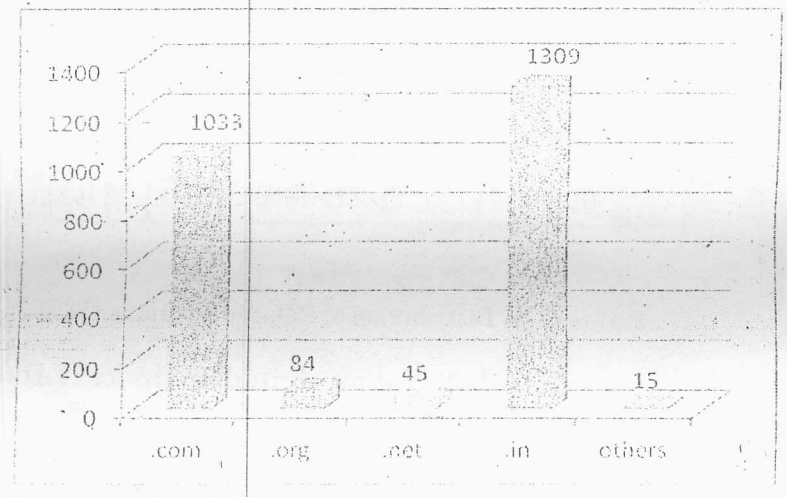

Figure 1: Distribution of Defaced Domains (TLDs)

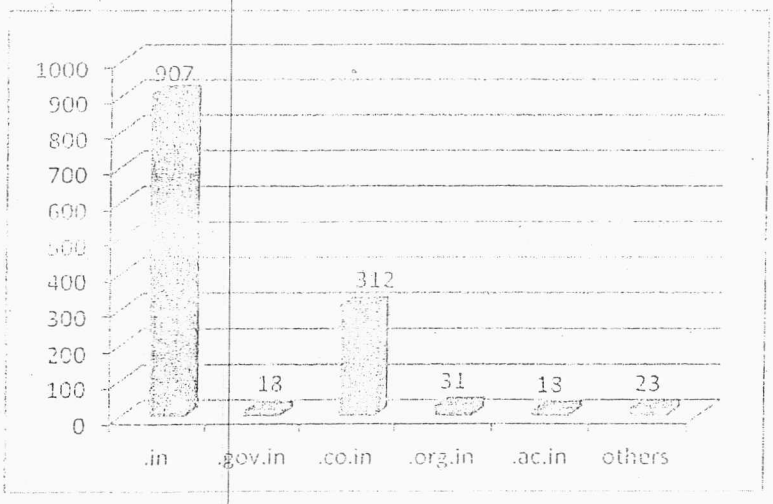

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of March 2012 a total of 2486 Indian websites were defaced. Out of these 52.5% websites were on .in domain and 42% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

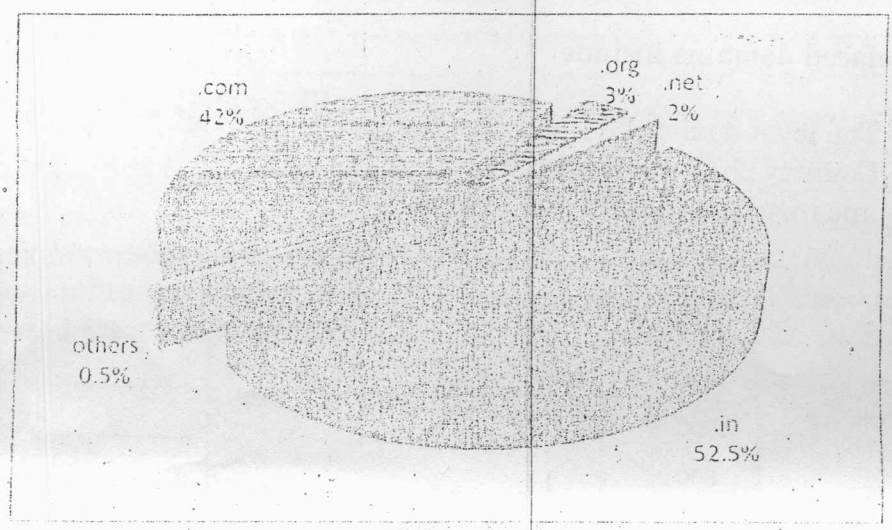

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 1309 defaced websites, 69% were in .in domain, 24% in .co.in and 2% in .gov.in domains.

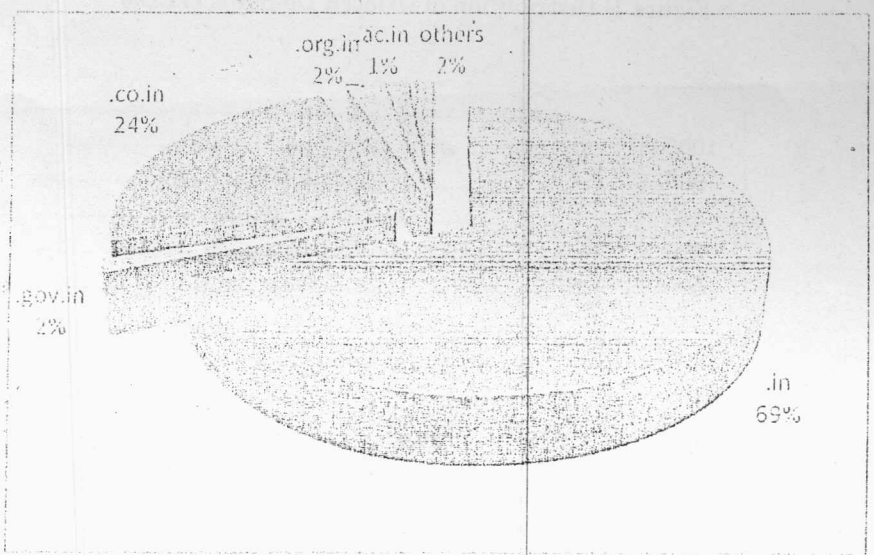

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (TLDs)

S.No	Attacker Name	Number of websites
1	Muslim Liberation Army	396
2	w3bdrill3r	207
3	hamadascorpion	146
4	DR-MTMRD	84
5	PCA-Master	73
6	Bozkurt97	56
7	MrWanz	43
8	Bangladesh Cyber Army	38
9	indramayu cyber	37
10	GiRl-RiD3r-H3x()r	28

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

S.No	Attacker Name	Number of websites
1	Hmei7	245
2	Muslim Liberation Army	234
3	PCA-Master	75
4	hamadascorpion	71
5	w3bdrill3r	61
6	Bangladesh Cyber Army	45
7	TheHackersArmy	45
8	DR-MTMRD	42
9	GiRl-RiD3r-H3x()r	38
10	3xp1r3	29

Table 2: Top Defacers ccTLD wise

3.3 Details of Mass Defaced IPs during March 2012

S No.	IP	ISP Name	ISP Location	Defacer	OS	WebServer	No. Of Sites
1	174.37.211.193	SOFTLAYER	US	Muslim Liberation Army	Win 2003	IIS/6.0	442
2	118.67.248.123	NET4INDIA	IN	Hmei7	Win 2008	IIS/7.0	277
3	208.43.91.92	SOFTLAYER	US	PCA-Master	Linux	Apache	150
4	111.118.178.177	CYFUTURE-AS-IN	IN	hamadascorpion	Linux	Apache	142
5	69.167.151.224	LIQUID-WEB-INC	US	Muslim Liberation Army	Win 2003	IIS/6.0	135
6	98.131.164.2	ECOMMERCE	US	w3bdrill3r	Linux	Apache	98

Table 3: Mass Defaced IPs

4. Defacement by Networks

4.1 Most Targeted Networks

It has been observed that most (78%) of Indian websites defaced were hosted outside India.

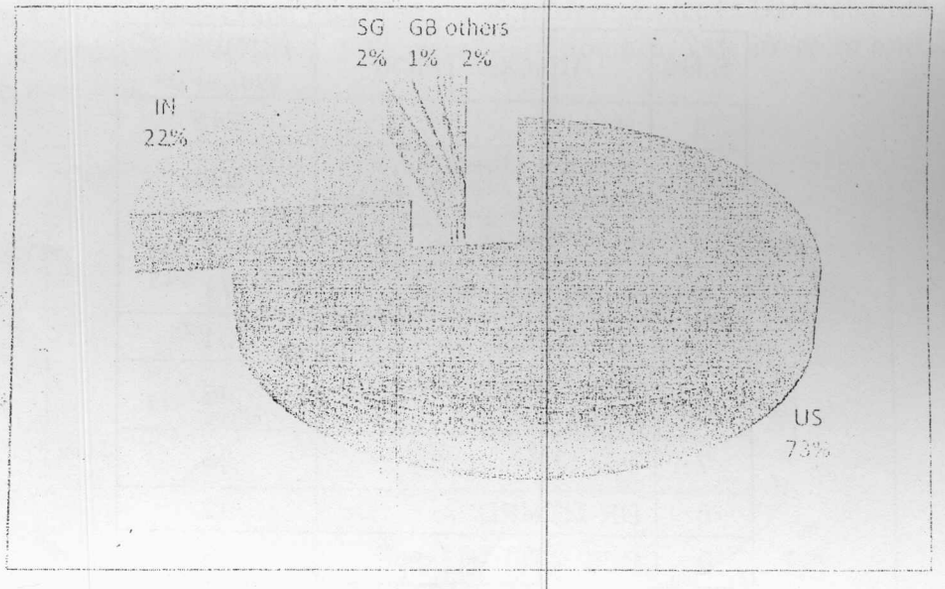

Figure 5: Defaced website hosting country-wise

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

- XSS vulnerability in D-Mack Media Currency Converter module in Joomla! (CVE-2012-1018)
- 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)
- Cross-site scripting (XSS) vulnerability in the Petition Node module for Drupal (CVE-2011-4630)
- SQL injection vulnerability in Drupal Translation Management module 6.x before 6.x-1.21 (CVE-2011-1663)
- Multiple cross-site scripting (XSS) vulnerabilities in phpMyAdmin (CVE-2012-0914)
- 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)
- 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

S. Mallick