344

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements May 2012

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

CONTENTS

1. Introduction

This report summarizes Indian website defacements during May 2012. In all 3015 Indian websites were defaced during the month of May against 1689 defacements in April 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).

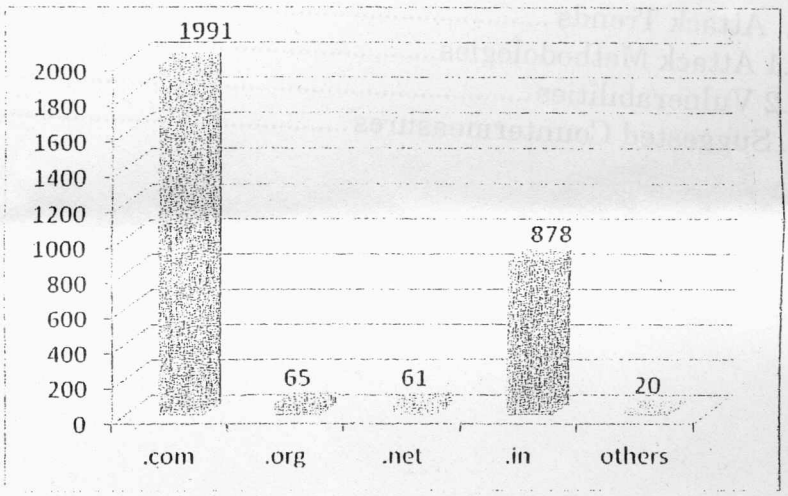

Figure 1: Distribution of Defaced Domains (TLDs)

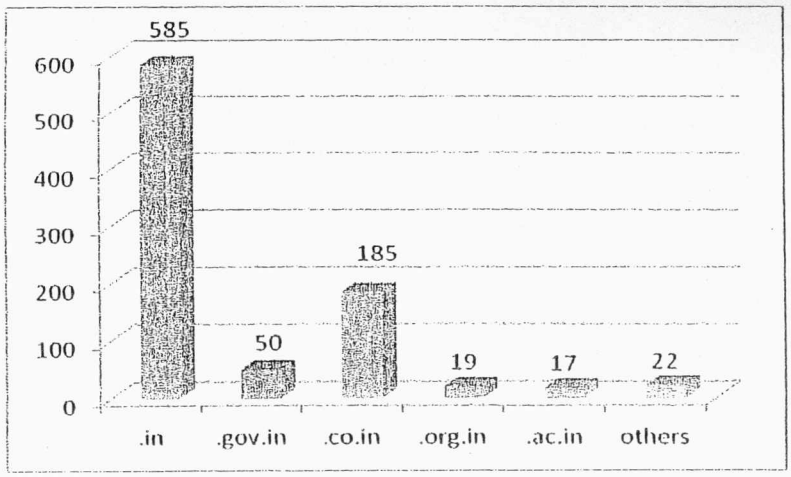

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of May 2012 a total of 3015 Indian websites were defaced. Out of these 29% websites were on .in domain and 66% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

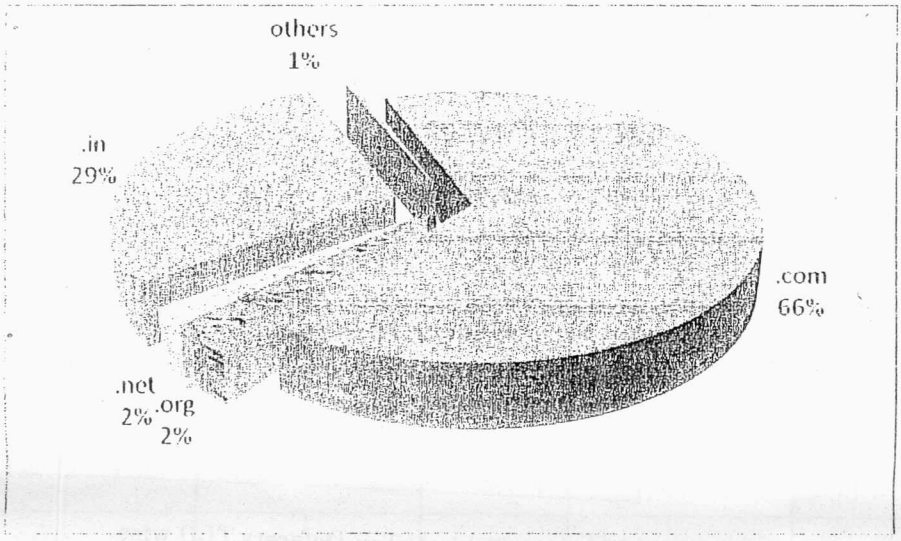

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 878 defaced websites, 67% were in .in domain, 21% in .co.in and 6% in .gov.in domains.

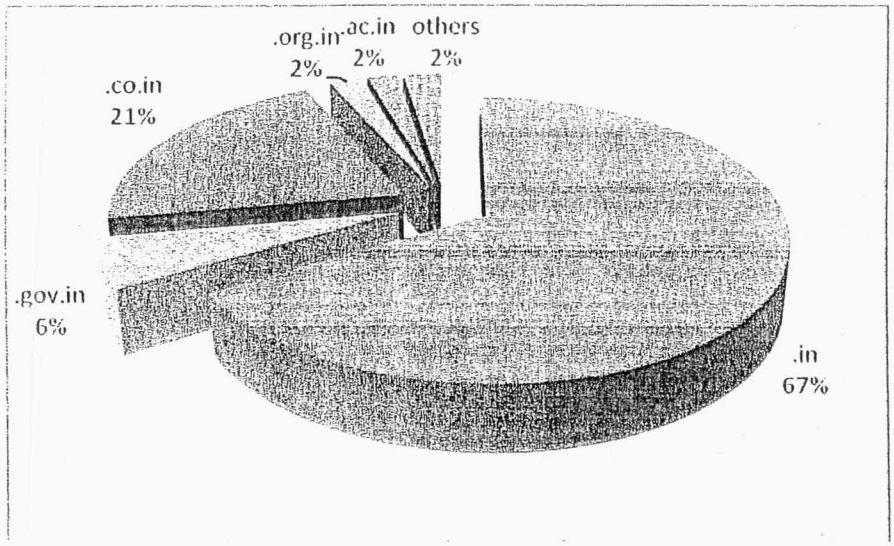

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (Total)

S.No	Attacker Name	Number of websites
1	Bangladesh Cyber Army	971
2	Ne0-h4ck3r	302
3	ZCompany Hacking Crew	295
4	Golden_Boy	135
5	hatrk	104
6	w3bdrill3r	92
7	TheHackersArmy	91
8	3xp1r3	86
9	BD BLACK HAT	68
10	Dbuzz	66

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

S.No	Attacker Name	Number of websites
1	Ne0-h4ck3r	96
2	Bangladesh Cyber Army	64
3	SA3D HaCk3D	59
4	ZCompany Hacking Crew	53
5	BD BLACK HAT	34
6	3xp1r3	31
7	Dbuzz	31
8	TiGER-M@TE	28
9	Anonymous	23
10	BADI	17

Table 2: Top Defacers ccTLD wise

3.3 Details of Mass Defaced IPs during May 2012

S No.	IP	ISP Name	ISP Location	Defacer	OS	WebServer	No. Of Sites
1	202.65.135.26	CtrlS Datacenters	IN	Bangladesh Cyber Army	Linux	Apache	900
2	74.86.216.243	SoftLayer	US	ZCompany Hacking Crew	Win 2003	IIS/6.0	255
3	216.45.55.175	OC3 Networks	US	Ne0-h4ck3r	Linux	Apache	139
4	176.9.67.146	Hetzner	DE	Golden_Boy	Linux	Apache	132
5	72.11.139.25	OC3 Networks	US	Ne0-h4ck3r	Linux	Apache	125
6	216.12.221.130	SoftLayer	US	w3bdrill3r	Win 2003	IIS/6.0	85
7	173.192.106.219	SoftLayer	US	The HackersArmy	Linux	Apache	85
8	184.154.125.250	SingleHop	US	hatrk	Linux	Apache	69
9	118.67.248.188	Net4India	IN	Dbuzz	Linux	Apache	66
10	184.154.21.218	SingleHop	US	hatrk	Linux	Apache	62

Table 3: Mass Defaced IPs

4. Defacement by Networks

4.1 Most Targeted Networks

It has been observed that most (82%) of Indian websites defaced were hosted outside India.

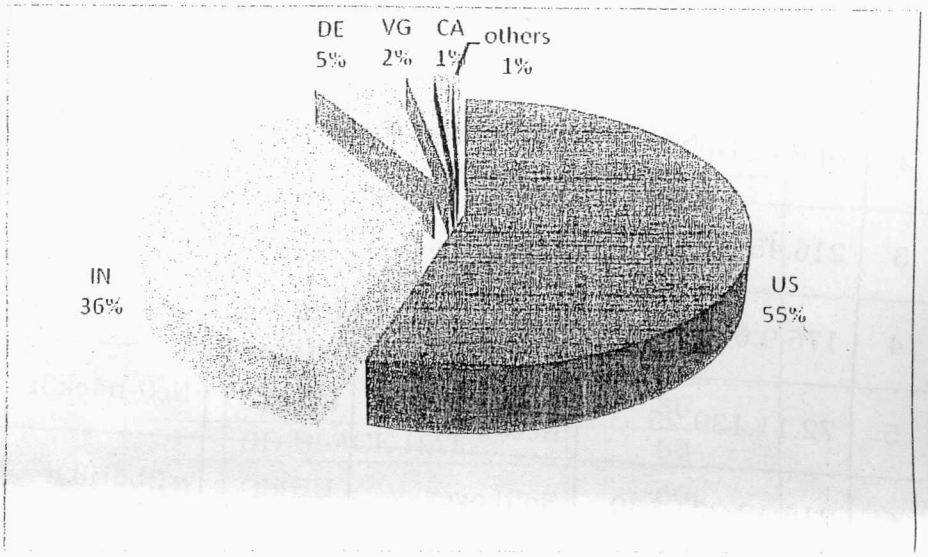

Figure 5: Defaced website hosting country-wise

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)
- Multiple SQL injection vulnerabilities in Vik Real Estate component 1.0 for Joomla! (CVE-2011-4823)
- SQL injection vulnerability in the JS Calendar component for Joomla! (CVE-2010-4795)
- 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-2011-4560)
- 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 from the Knowledgebase Section:
  - Web Server Security Guidelines
  - Securing IIS /7.0 Web Server Guidelines
  - Guidelines for Auditing and Logging