1352

MOS

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements April 2012

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

CONTENTS

1. Introduction

This report summarizes Indian website defacements during April 2012. In all 1689 Indian websites were defaced during the month of April against 2486 defacements in March 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).

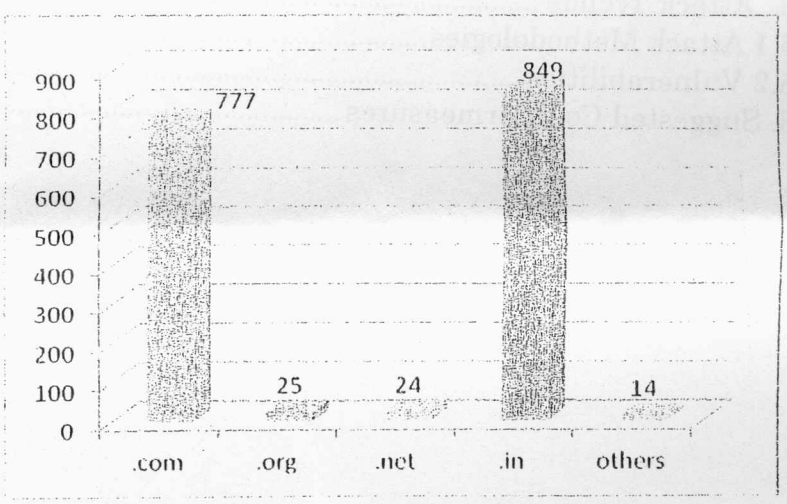

Figure 1: Distribution of Defaced Domains (TLDs)

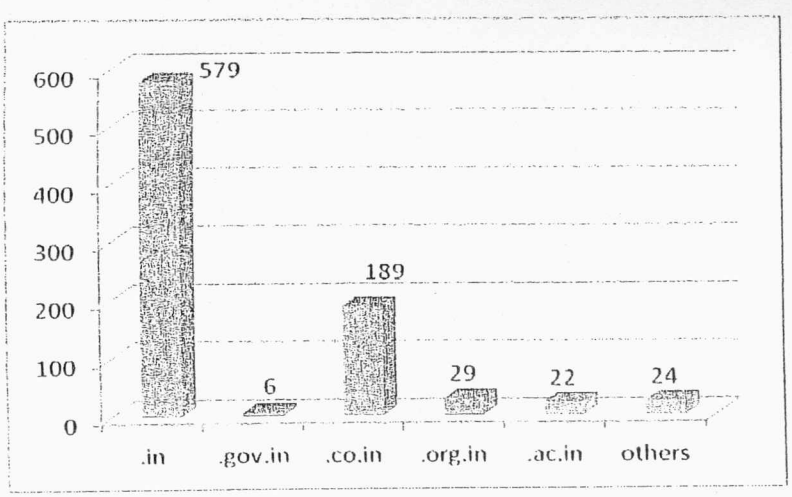

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of April 2012 a total of 1689 Indian websites were defaced. Out of these 50% websites were on .in domain and 46% websites were on .com domain. Figure 3 shows the percentage distribution of defaced site in top level domains (TLDs).

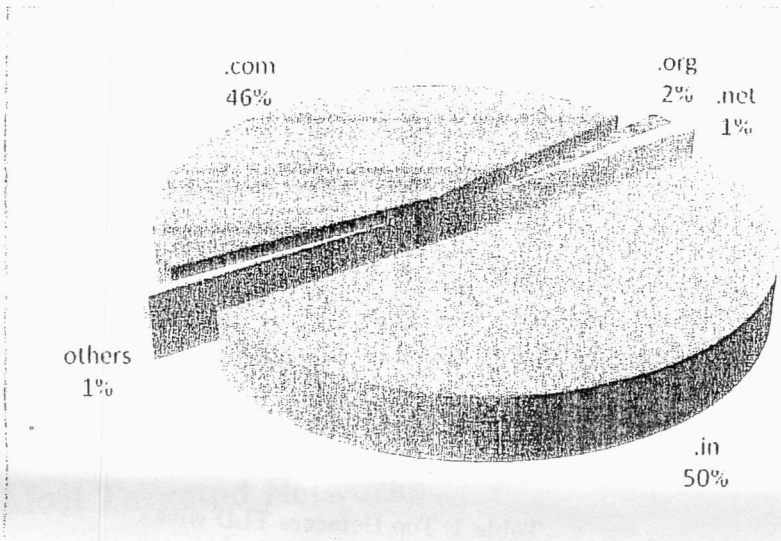

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 849 defaced websites, 68% were in .in domain, 22% in .co.in and 1% in .gov.in domains.

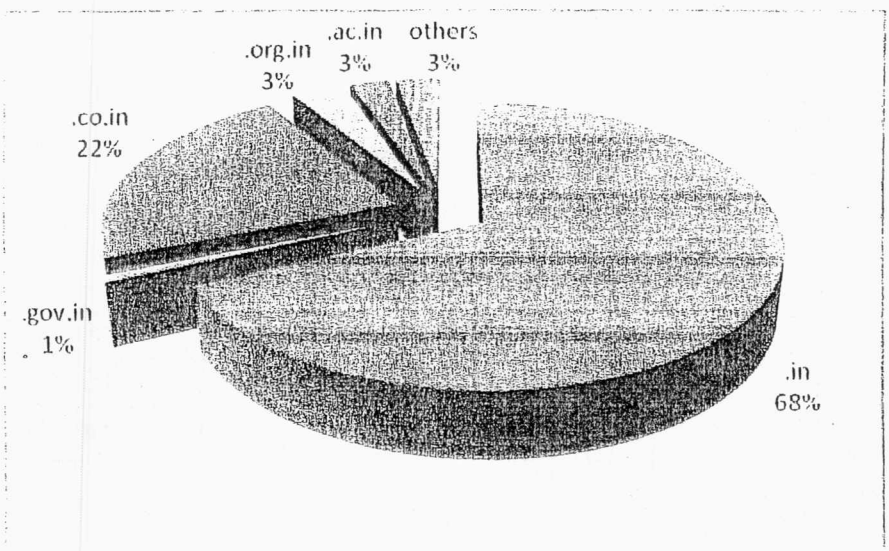

Figure 4: % Distribution of Defaced Domains (ccTLDs)

348

3. Hacker wise Defacements

3.1 Top Defacers (Total)

S.No	Attacker Name	Number of websites
1	TiGER-M@TE	439
2	HTC 28 DZ	195
3	3xp1r3	140
4	3rry com3y	113
5	Bangladesh Cyber Army	103
6	Th3 K!LL3r Dz	85
7	MrWanz	63
8	FL1T0X_Dz	62
9	wlhaan hacker	52
10	ArTiN	50

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

S.No	Attacker Name	Number of websites
1	TiGER-M@TE	378
2	HTC 28 DZ	58
3	1923Turk	47
4	3xp1r3	34
5	Th3 K!LL3r Dz	29
6	FL1T0X_Dz	22
7	Armadillo.DZ	16
8	Bangladesh Cyber Army	15
9	Hidden Pain	15
10	ZoRRoKiN	14

Table 2: Top Defacers ccTLD wise

3.3 Details of Mass Defaced IPs during April 2012

S No.	IP	ISP Name	ISP Location	Defacer	OS	WebServer	No. Of Sites
1	72.11.141.91	OC3 Networks	US	HTC 28 DZ	Linux	Apache	273
2	182.18.141.154	CtrlS Datacenters	IN	3xp1r3	Linux	Apache	203
3	204.93.160.150	Server Central Network	US	TiGER-M@TE	Win 2008	IIS/7.0	89
4	202.65.135.26	CtrlS Datacenters	IN	Bangladesh Cyber Army	Linux	Apache	87
5	204.93.167.28	Server Central Network	US	TiGER-M@TE	Win 2008	IIS/7.0	70
6	8.22.201.18	GORACK	US	wlhaan hacker	Linux	Apache	51

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.

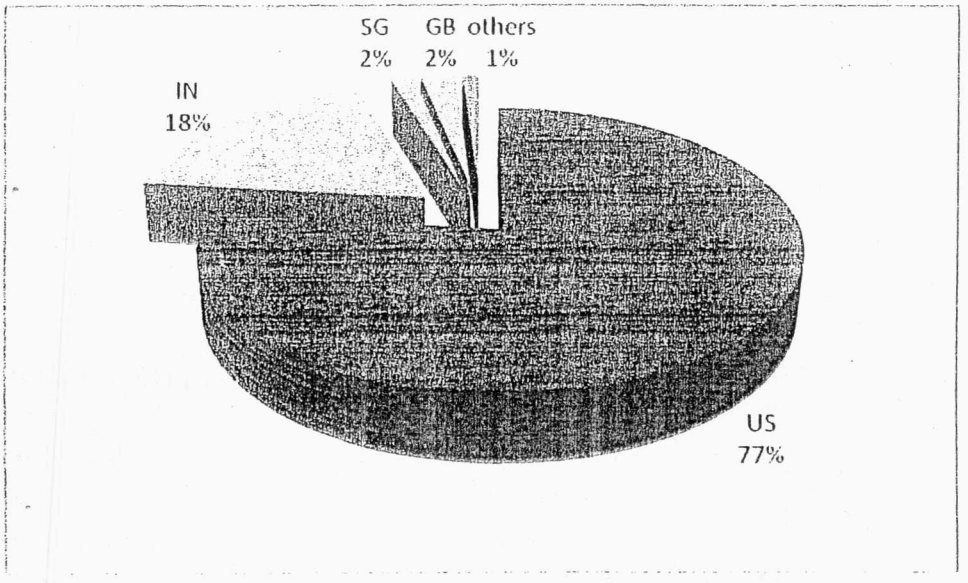

Figure 5: Defaced website hosting country-wise

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 Knowlegdebase Section:
  - Web Server Security Guidelines
  - Securing IIS /7.0 Web Server Guidelines
  - Guidelines for Auditing and Logging