320

CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Summary of Website Defacements January 2012

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

CONTENTS

1. Introduction

This report summarizes Indian website defacements during January 2012. In all 1425 Indian websites were defaced during the month of January 2012 against 2087 defacements in December 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).

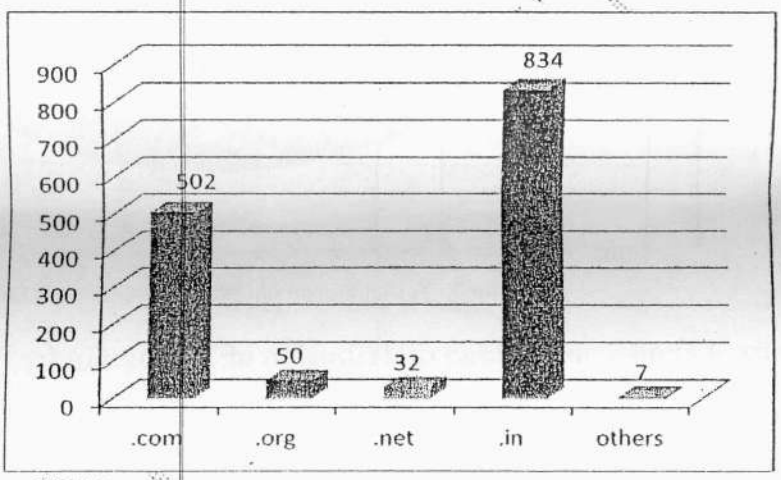

Figure 1: Distribution of Defaced Domains (TLDs)

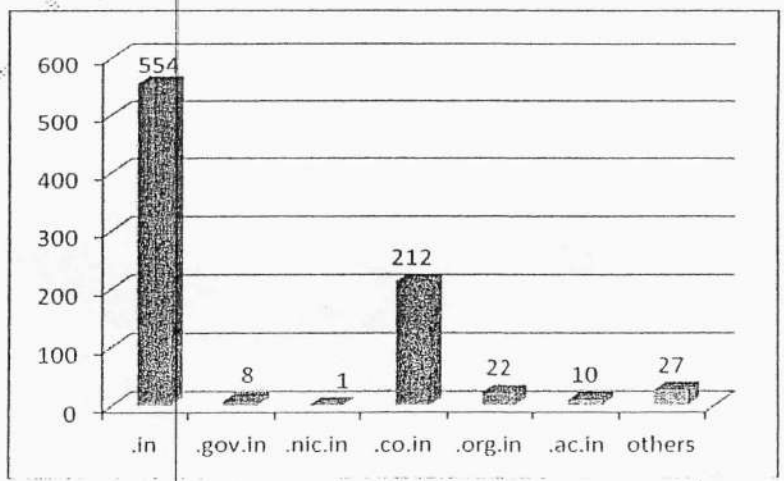

Figure 2: Distribution of Defaced Domains (ccTLDs)

2.1 Percentage Distribution of defaced domains

In the month of January 2012 a total of 1425 Indian websites were defaced. Out of these 58.5% 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).

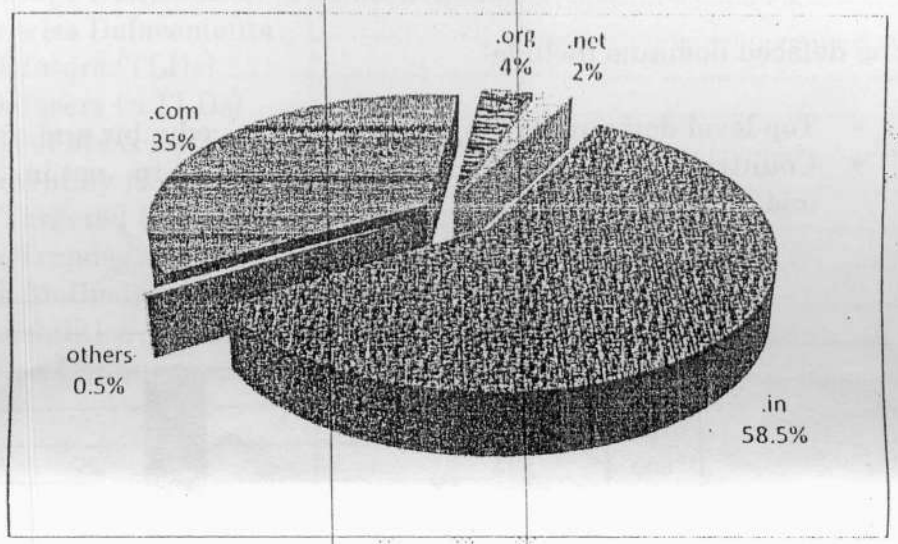

Figure 3: % Distribution of Defaced Domains (TLDs)

Figure 4 shows percentage distribution of .in domain (ccTLDs) websites. Out of the 834 defaced websites, 67% were in .in domain, 25% in .co.in and 1% in .gov.in domains.

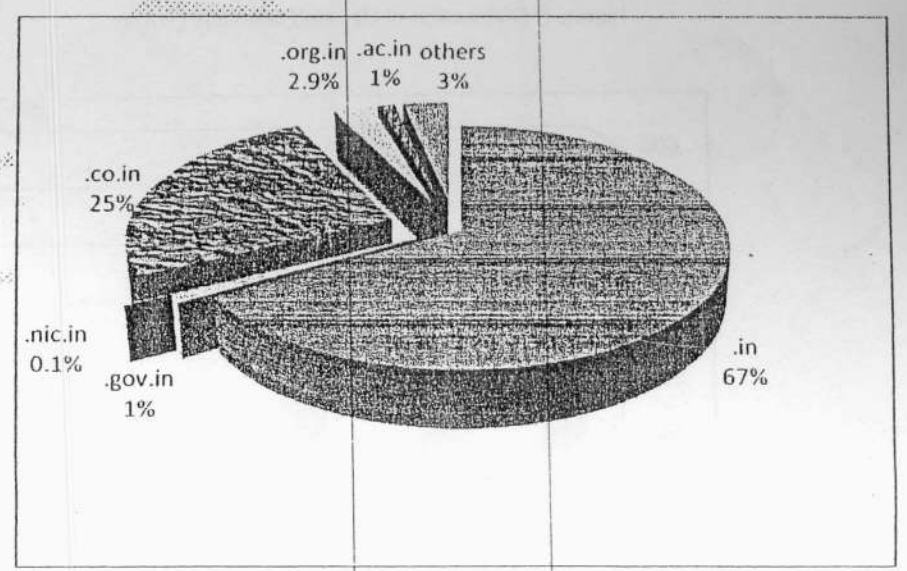

Figure 4: % Distribution of Defaced Domains (ccTLDs)

3. Hacker wise Defacements

3.1 Top Defacers (TLDs)

Table 1 shows Top Defacers (TLD) wise in January 2012

S.No	Attacker Name	Number of websites
1	PakH3X0r	237
2	Muslim Liberation Army	219
3	nO IOv3	29
4	BY DRISS	26
5	Bazzooka	20
6	TheHackersArmy	10
7	H4x0rL1f3	8
8	Pakistan Net Army	8
9	bogel	7
10	isyanqar	7

Table 1: Top Defacers TLD wise

3.2 Top Defacers (ccTLDs)

Table 2 shows Top Defacers (ccTLD) wise in January 2012.

S.No	Attacker Name	Number of websites
1	Ne0-h4ck3r	112
2	H4x0rL1f3	105
3	PakH3X0r	79
4	KiLLerMiNd	45
5	1923Turk	44
6	Muslim Liberation Army	44
7	Hmei7	24
8	BY DRISS	23
9	bogel	21
10	S@D H@cK3r	20

Table 2: Top Defacers ccTLD wise

3.3 Details of Mass Defaced IPs during January 2012

S No.	IP	ISP Name	ISP Location	Defacer	OS	WebServer	No. of Sites
1	50.23.226.200	SoftLayer	US	PakH3X0r	Win 2003	IIS/6.0	310
2	216.12.216.18	THEPLANET	US	Muslim Liberation Army	Win 2003	IIS/6.0	261
3	118.67.248.163	NET4INDIA	IN	Ne0-h4ck3r	Win 2008	IIS/7.0	107
4	184.173.179.200	SoftLayer	US	H4x0rL1f3	Linux	Apache	106

Table 3: Mass Defaced IPs

4. Defacement by Networks

4.1 Most Targeted Networks

It has been observed that most (88%) of Indian websites defaced were hosted outside India.

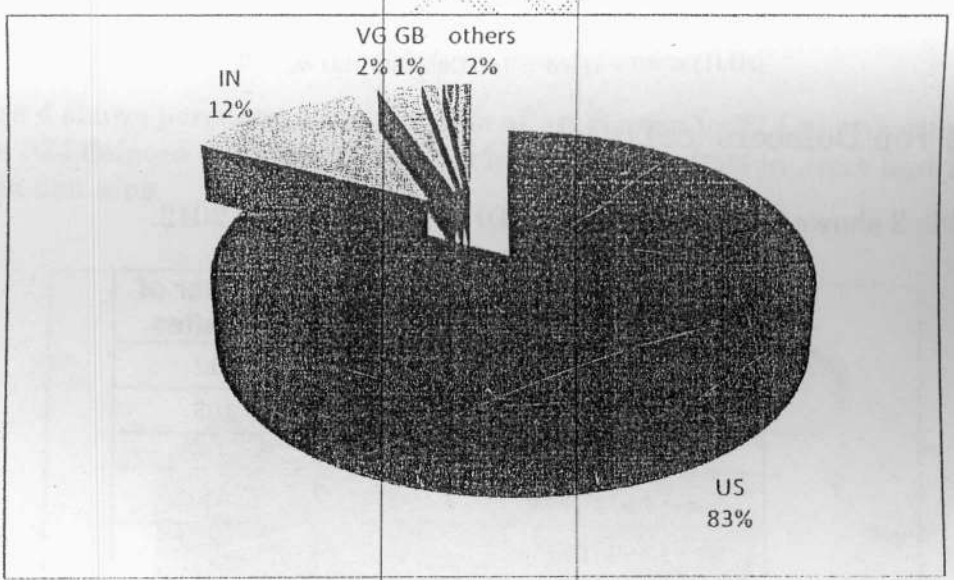

Figure 5: Defaced website hosting country-wise

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)
- 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)

- 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

CONFIDENTIAL

भारत सरकार
संचार एवं सूचना प्रौद्योगिकी मंत्रालय
सूचना प्रौद्योगिकी विभाग
भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन)
इलेक्ट्रॉनिक्स निकेतन, 6, सी.जी.ओ. कॉम्प्लेक्स, नई दिल्ली-110003
Government of India
Ministry of Communications and Information Technology
Department of Information Technology
Indian Computer Emergency Responce Team (CERT-in)
Electronics Niketan, 6, C.G.O. Complex, New Delhi-110003
Tel. : 24368544, Fax : 24366806 E-mail : grai@mit.gov.in

D.O No. 2(7)/2012-CERT-In

20.04.2012

Dear Shri Mohapatra,

CERT-In is tracking defacement of Indian websites on regular basis. A total of 2460 & 2486 Indian websites were defaced by various defacers during the month of February & March 2012 respectively. Similarly 475 & 296 number of websites have been compromised and links to malicious websites were planted on these sites during corresponding months. Summaries of monthly website defacements depicting domain-wise and network-wise break-up of the websites defaced, top defacers and vulnerabilities which are largely exploited are attached.

In view of growing attacks on websites, you are requested to advise website administrators to follow best practices to secure web applications and web servers.

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

With regards,

Yours sincerely,

(Gulshan Rai)

Encl: As above

Shri Pradipta Kumar Mohapatra,IAS
Commissioner cum Secretary,
IT Department
OCAC, N-1/7-D, Acharya Vihar,
Bhubaneswar-751001
Orissa