CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Analysis of Phishing Incidents Year-2006

By

Anil Sagar and Rashmi Singh

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

Issue Date: March 30, 2007

CONTENTS

1. Introduction

Phishing is a fraudulent activity to acquire personal information of a user like bank account number, user name, password, credit card details, etc by using social engineering techniques. In a typical phishing attack, a phisher sends convincing emails to thousands of users and provides a hyperlink in the message. When a user clicks on the hyperlink, the request is sent to an exact replica of a bank/financial institution website asking for the sensitive information like user name, password, credit card details etc. When innocent user enters the information, the data is immediately sent to the phishers who thereby uses this information to transfer money .

In other phishing techniques, the phishers may perform malware attack to compromise sensitive data. The DNS-based attack also known as Pharming may divert a user to a fraudulently hosted phishing website. It has been observed that number of phishing attacks and their sophistication has increased dramatically in the past few months.

According to Gartner survey, the financial losses from phishing attacks have raised to more than $2.8 billion in the year 2006.

The phishing attacks generally span across multiple countries and involve organized criminal groups.

Countermeasures to phishing attacks involve action at the user level and bank/financial institution/organization level. The phishing techniques and countermeasures are given in CERT-In Whitepaper "**Phishing Attacks and Countermeasures"** [CIWP-2005-03]

This document provides the trend of phishing attacks occurred in the year 2006. It provides details on the incidents analyzed, targeted sectors and brands hijacked etc.

The phishing incidents described in this document are those in which either the phishing websites are hosted in India or domain registrant belongs to India. The phished brand such as bank or financial institution mostly belongs to foreign countries.

2. Incidents Reported to CERT-In.

2.1 Trend of Phishing Incidents

In the year 2006 a total of 335 phishing incidents have been reported to CERT-In by various national and international agencies. On an average 28 incidents [Figure 2] were reported in a month. The figure [Figure 1] shows that maximum phishing incidents were reported in the month of May. There was progressive increase of phishing incidents in the second half of the year.

SL No	Month	Number of Incidents Reported
1	January	14
2	February	23
3	March	18
4	April	38
5	May	53
6	June	29
7	July	25
8	August	31
9	September	29
10	October	30
11	November	22
12	December	23

Table 1**:** Phishing Incidents Reported: Month-Wise

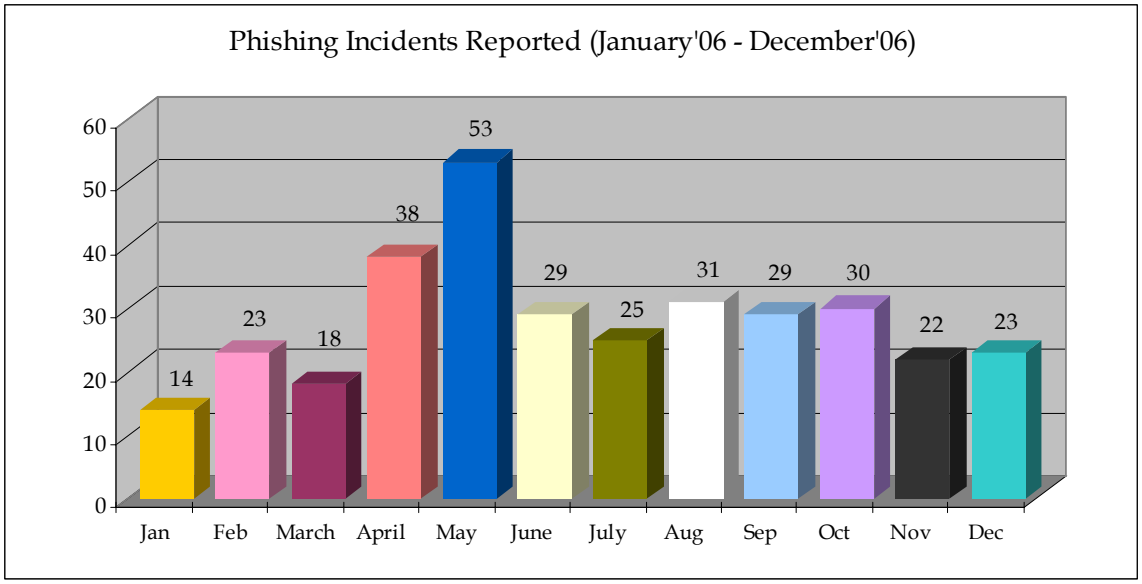

Figure 1: Phishing Incidents Reported: Month-Wise

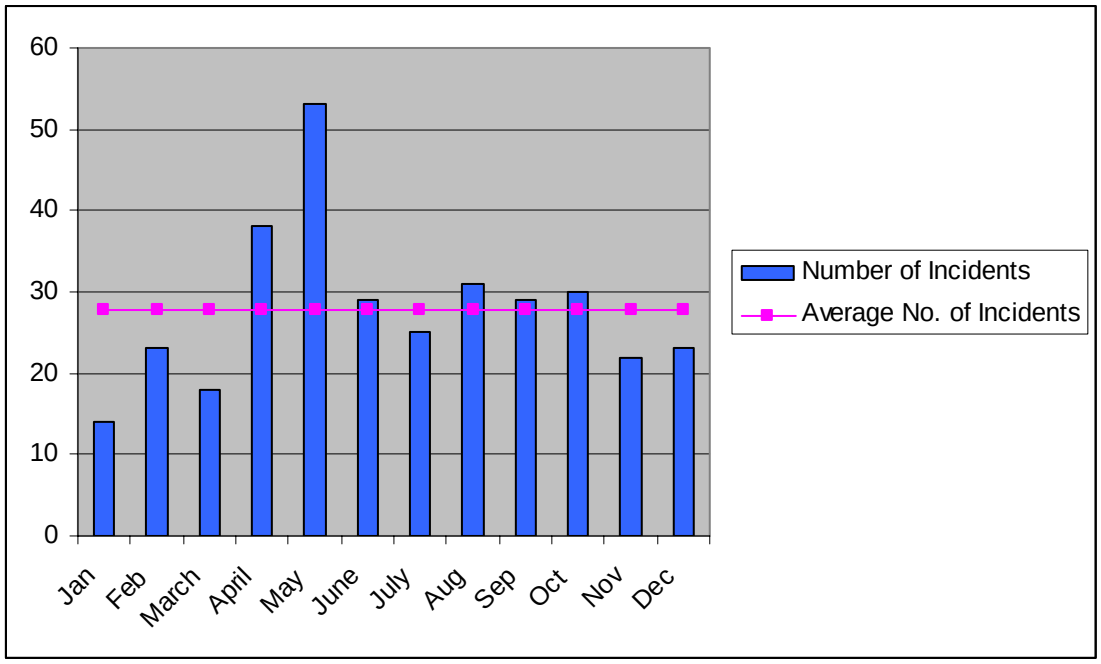

Figure 2: Average number of Phishing Incidents Reported

2.2 Number of unique Phishing URLs

In a phishing incident, the phisher provides phishing URLs to redirect users onto phishing websites. However in a single phishing incident multiple unique phishing URLs could be involved. It has been observed that in the last six months of 2006, 576 of unique phishing URLs were reported to CERT-In. This is an increase in 94% over the 297 unique phishing URLs reported in the first half of 2006 [Figure 3]

SL No	Month	Number of unique Phishing URLs
1	January	14
2	February	28
3	March	26
4	April	61
5	May	124
6	June	44
7	July	67
8	August	61
9	September	64
10	October	101
11	November	198
12	December	85

Table 2: Monthly Unique Phishing URLs Reported

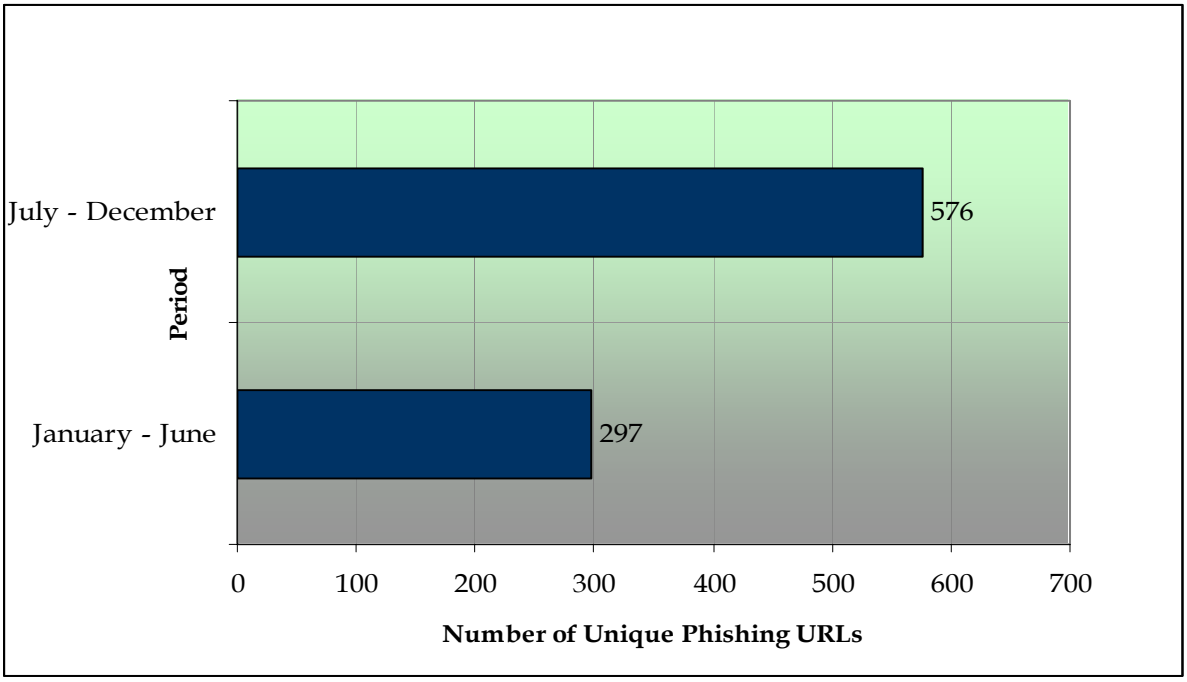

Figure 3: Trend of Unique Phishing URLs Reported

In the month of November there were 198 [Figure 4] unique phishing URLs reported, the highest number of active phishing URLs during last half of 2006. However for the first half of 2006, May month has encountered highest number with 124 phishing URLs. Both of which is contributing major part of total 873 unique active phishing URLs reported to CERT-In.

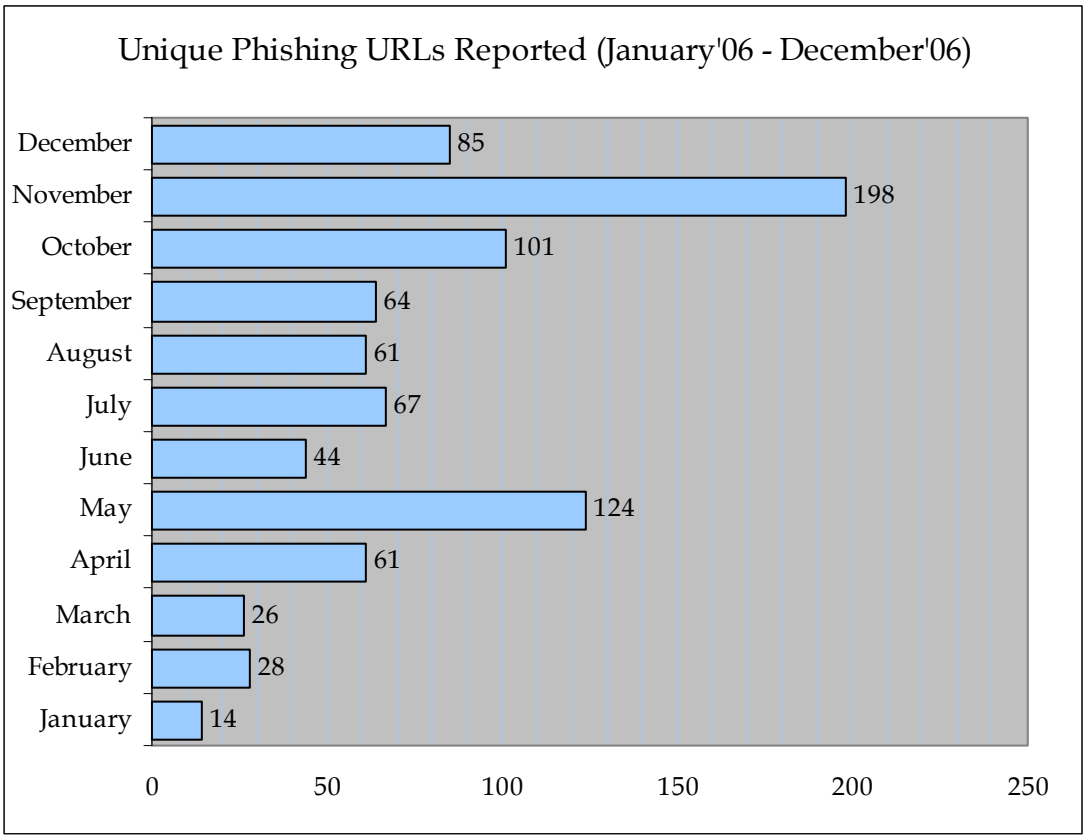

Figure 4: Monthly Unique Phishing URLs Reported

2.3 Ports used by Phishing URLs

The phishing URLs connects through a port to a phishing website. Most of the phishing incidents reported used TCP Port 80, which is the default port for *http* web protocol for the attack. It constitutes 96% of the total phishing URLs [Figure 5]. TCP Port 84 is reported with other most targeted port used in attack [Figure 5.1]

SL No	TCP Port No	Number of Phishing URLs
1	80	838
2	84	18
3	8081	6
4	8880	3
5	180	3
6	8000	2
7	40	1
8	89	1
9	7640	1

Table 3: Ports used by Phishing URLs

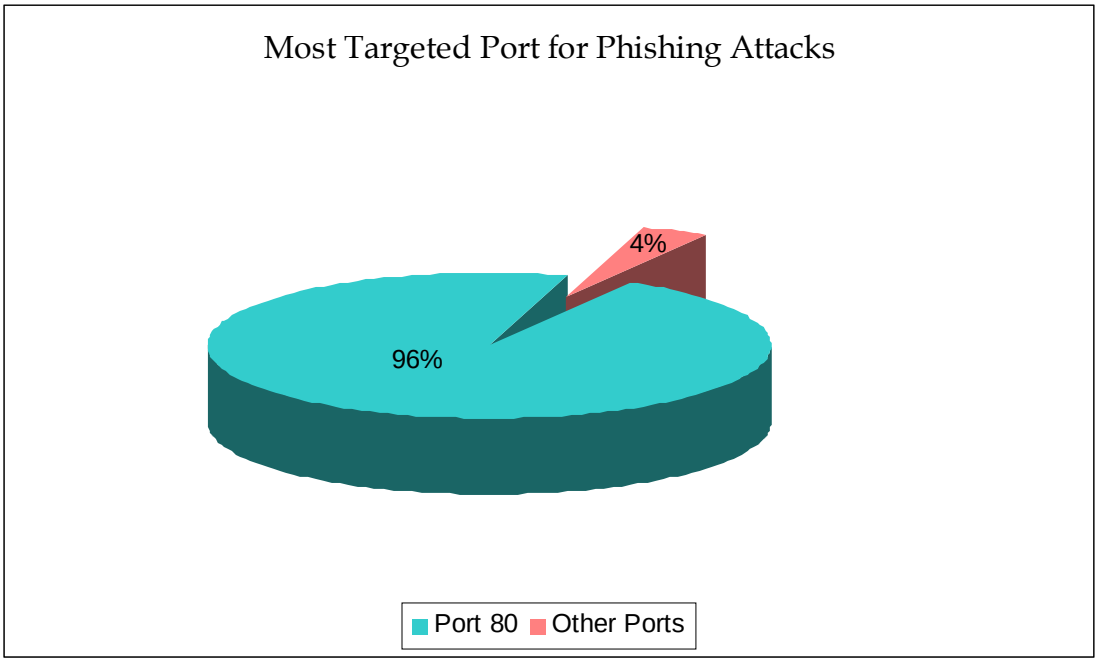

Figure 5: Most Targeted Port

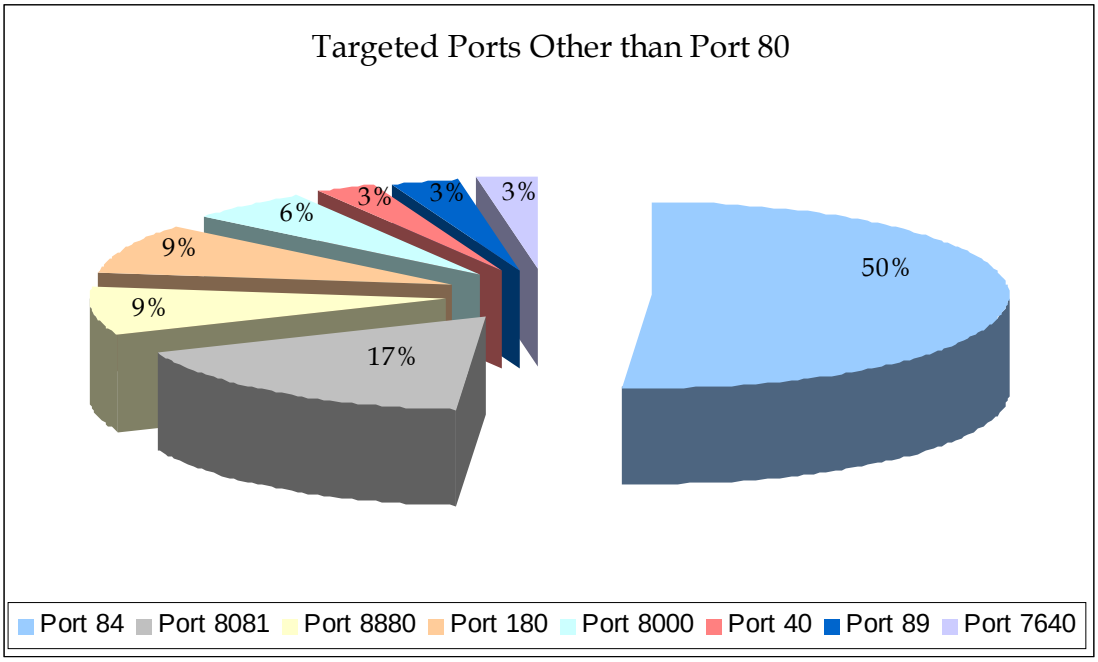

Figure 5.1: Other Targeted Ports

2.4 Targeted Sectors

The most widespread phishing attack reported is carried out against e-commerce sector which includes online retailers, auction sites, etc. It is accounting for 76%. The second most targeted sector is financial services which include banks, financial institutions, etc accounting for 24 % [Figure 6] of the total number of incidents reported in the year 2006.

Among the attacks against financial services sector 9% of targeted brands belongs to country India.

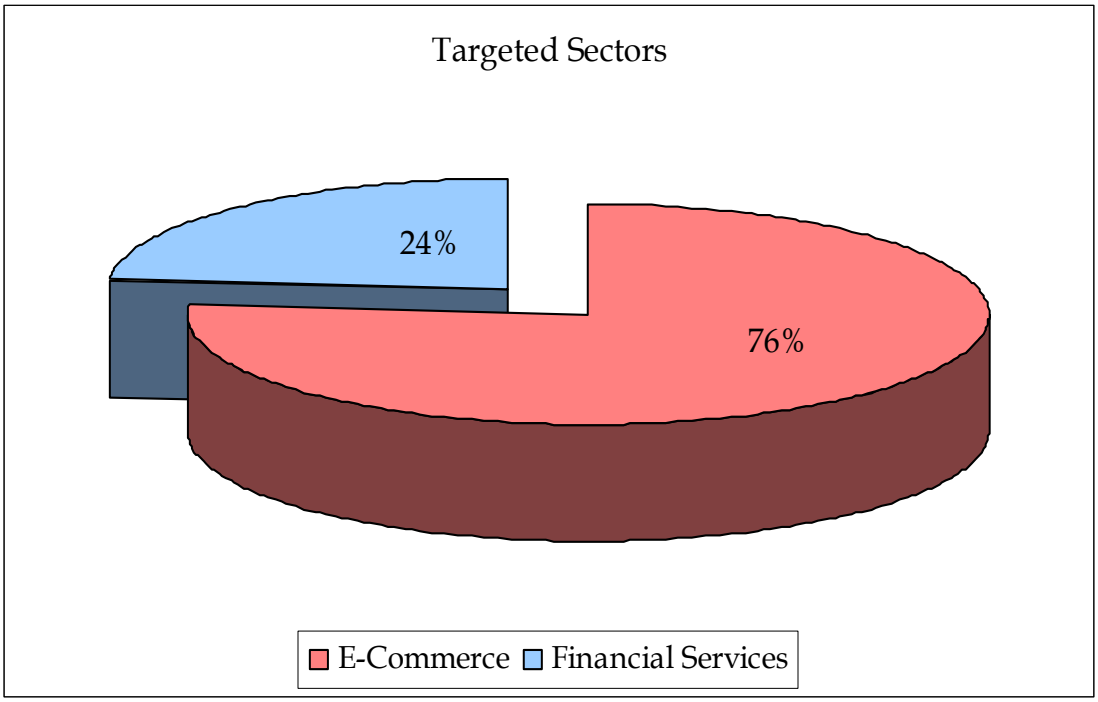

Figure 6: Targeted Sectors

It has been noticed that Phishing incidents reported in the last half of the year 2006 is showing shift in targeted sectors landscape particularly in financial services sector. Phishers are now on the move to target small financial sectors that are not popular. It gives the attacker more time to remain active in the cyber space and make the attack more successful.

2.5 Brands Hijacked

The November 2006 has witnessed large number of brands being hijacked by the phishers with 23 [Figure 7]. Small Banks and Credit Unions have been phished by the attackers during the last half of the year.

SL No	Month	Number of Brands Hijacked
1	January	7
2	February	6
3	March	5
4	April	2
5	May	4
6	June	3
7	July	7
8	August	6
9	September	8
10	October	10
11	November	23
12	December	9

Table 4. Brands Hijacked: Month-Wise

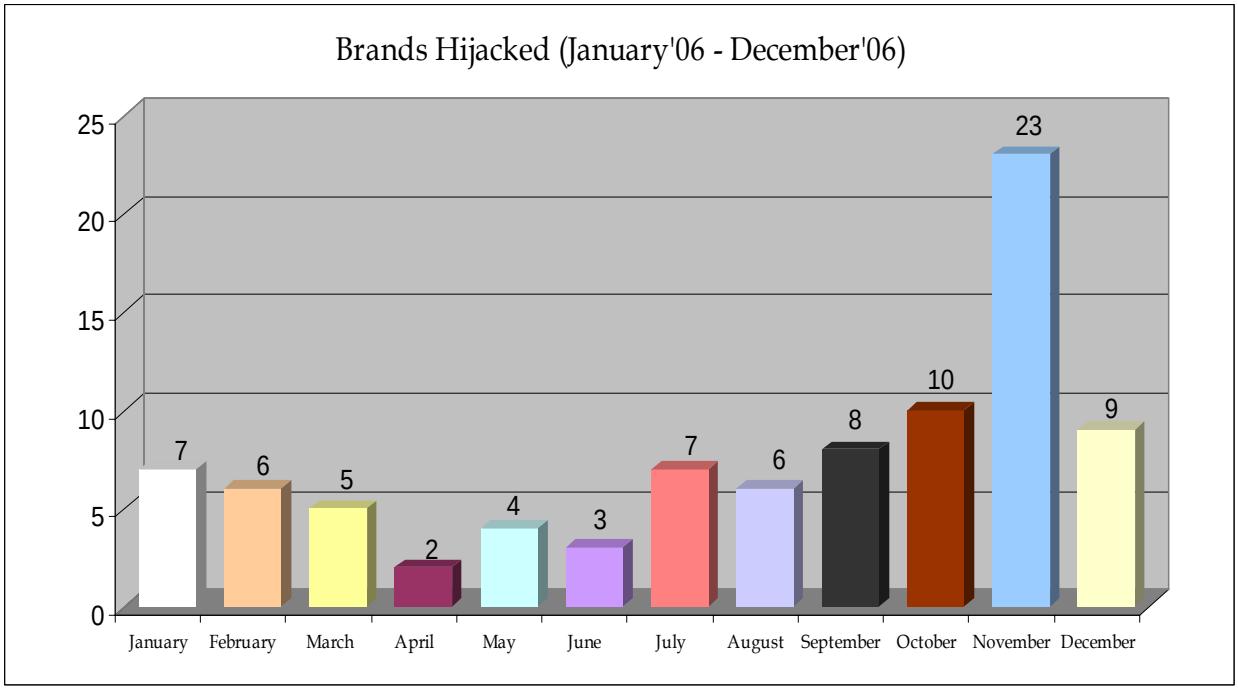

Figure 7: Brands Hijacked: Month-Wise

2.6 Country of Brands hijacked

Large number of brands hijacked belongs to the country United States. 93% of hijacked brands are from USA. While 2% belongs to INDIA and AUSTRALIA each [Figure 8]

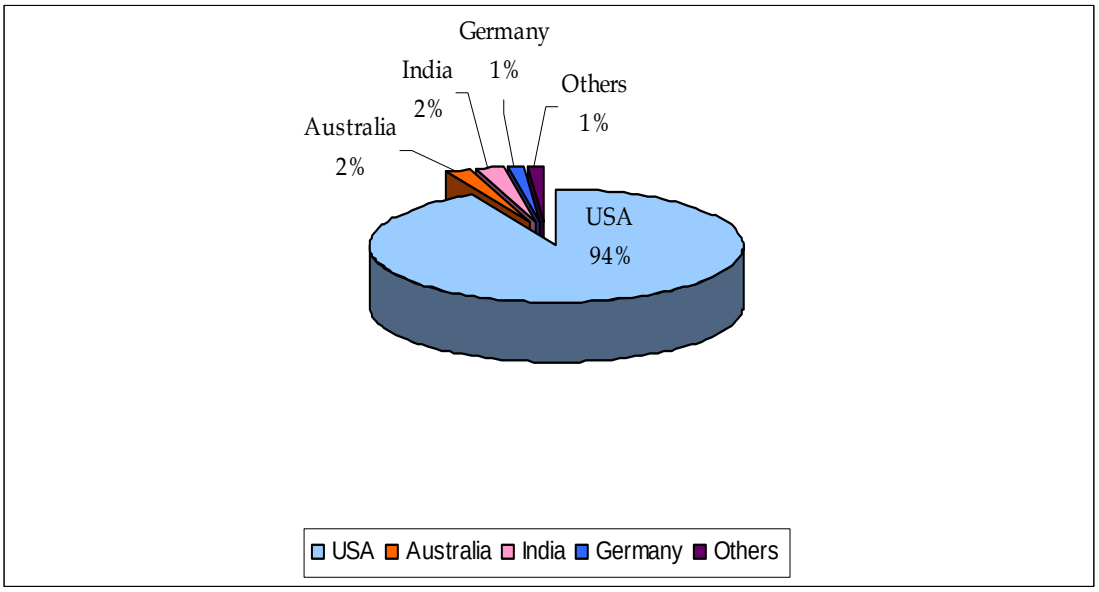

Figure 8: Brands Hijacked: Country-Wise

2.7 Phishing URLs with Top Level Domain (TLD)

The analysis of phishing URLs indicates that *.com* is the most popular top level domain (TLD) for hosting the phishing website [Figure 9]

SL No	Top Level Domain	Number of Phishing URLs
1	.com	135
2	.in	36
3	.org	16
4	.net	12
5	.edu	7
6	.ro	4
7	.biz	1
8	.tw	1

Table 5: Phishing URLs with Top Level Domain (TLD)

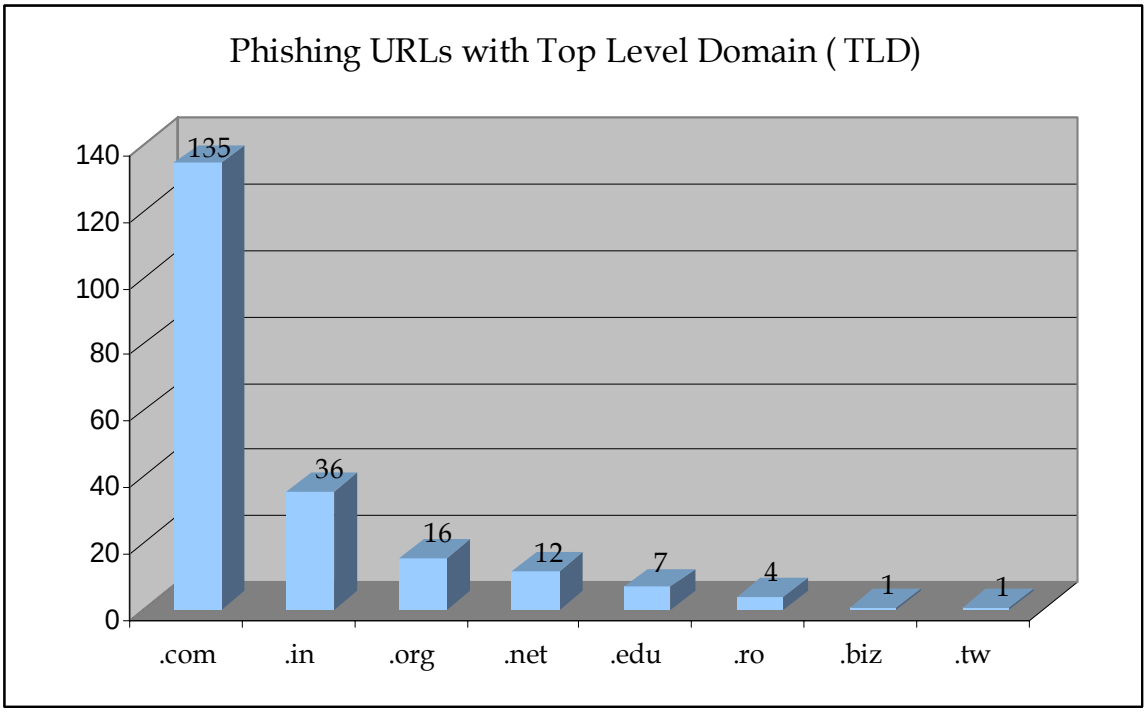

Figure 9: Phishing URLs with Top Level Domain (TLD)

.in is reported with highest country specific TLD hosting phishing page.
While ROMANIA and TAIWAN are the other country specific TLD (.ro and .tw) found hosting phishing page.

2.8 Use of Phishing Toolkits

It has been observed that phishing toolkits are being used by the phishers to hijack multiple brands. CERT-In was reported with such kind of incident which has used the phishing toolkit to host multiple brands phishing sites on a single machine. One such example of phishing toolkit is "Rock Phish Kit".

2.9 Exploitation of vulnerabilities to carry out phishing attacks

The phishers compromise internet hosts for the purpose of hosting phishing websites by exploiting vulnerabilities in the operating system and application software. There are vulnerabilities in the client software like web browsers and mail user agents which are exploited during the phishing attacks. The details of the vulnerabilities discovered in various operating systems, application software and client software in the year 2006 are available on CERT-In website
[http://cert-in.org.in].

3 Countermeasures

- Deploy an Enterprise security model that combines intrusion detection, firewall, antivirus and vulnerability management systems for maximum protection against malicious code and other threats.

- Keep up-to-date security patches and update release for Operating System.

- Keep up-to-date security patches and update release for application software.

- Keep up-to-date Antivirus and Antispyware signatures to protect against latest malware spreading in the wild.

- Do not click on a link embedded within any suspicious email, especially if the email requests personal information. Instead start a new internet session and type the Web address of the link into the address bar to ensure that you are now in the legitimate website.

- Do not disclose any personal or financial information in a response to any email. Instead contact your financial institution/ Bank for the authentication of received e-mail.

- Use anti-phishing toolbar/browser to get early detection of phishing websites.

- Follow Security Best Practices.

4. Reporting of Phishing Incidents

The phishing incidents pertaining to Indian scenario can be reported to CERT-In Incident Response Help Desk

Email: incident@cert-in.org.in

Phone: +91-11-24368572
Fax : +91-1800-11-6969

Postal Address:
Indian Computer Emergency Response Team (CERT-In)
Department of Information Technology
Ministry of Communications & Information Technology
Government of India
Electronics Niketan
6, CGO Complex, Lodhi Road,
New Delhi - 110 003
India

And also report the incident to the concerned bank/financial institution.

5. List of Figures

6. List of Tables