CERT-In

Indian Computer Emergency Response Team

Enhancing Cyber Security in India

Analysis of Phishing Incidents Year-2007

By

Anil Sagar & Rashmi Singh

Department of Information Technology
Ministry of Communications and Information Technology
Government of India

Issue Date: April 30,2008

CONTENTS

1. Introduction

'Phishing' is a term derived from *'fishing'*, in which the fish catcher puts a bait to catch fishes. Similarly in today's cyber world bad people use various techniques to lure innocent internet users and acquire their personal information.

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 (website link) in the e-mail 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 the user enters the information, the data is immediately sent to the phisher who thereby uses this information to transfer money from the user's account. *Phishing*, thus, is a form of profit- oriented malicious activity, uses spoofed emails to lead consumers to counterfeit websites that are designed to trick users into divulging account names and passwords.

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.

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

According to Gartner survey, financial losses due to *phishing* attacks have raised to more than $3.2 billion in the year 2007.

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

This document provides the trend of *phishing* attacks reported to CERT-In during the year 2007. It provides details on the incidents analyzed, targeted sectors, brands hijacked, etc.

The *phishing* incidents described in this document falls into below mentioned criteria.

- *Phishing* website hosted in India.
- Domain registrant belonged to India.
- Domain registrar belonged to India.
- *Phishing* domain hosted on '.in' namespace.

Incidents analyzed by CERT-In indicates that the *phished* brand such as bank or largely financial institution, belongs to foreign countries.

The trend also shows that *phishing* incidents of Indian financial institutions have increased in the year 2007.

2. Incidents Reported to CERT-In

1.1. Trend of *Phishing* Incidents

In the year 2007 a total of 392 *phishing* incident were reported to CERT-In by various national and international agencies. On an average 32 *phishing* incidents were reported in a month. The figure [Figure 1] shows that maximum *phishing* incidents were reported in the month of January.

SL No	Month	Number of Incidents Reported
1	January	46
2	February	33
3	March	33
4	April	27
5	May	32
6	June	27
7	July	33
8	August	31
9	September	32
10	October	39
11	November	30
12	December	29

Table 1. *Phishing* Incidents Reported by Month -2007

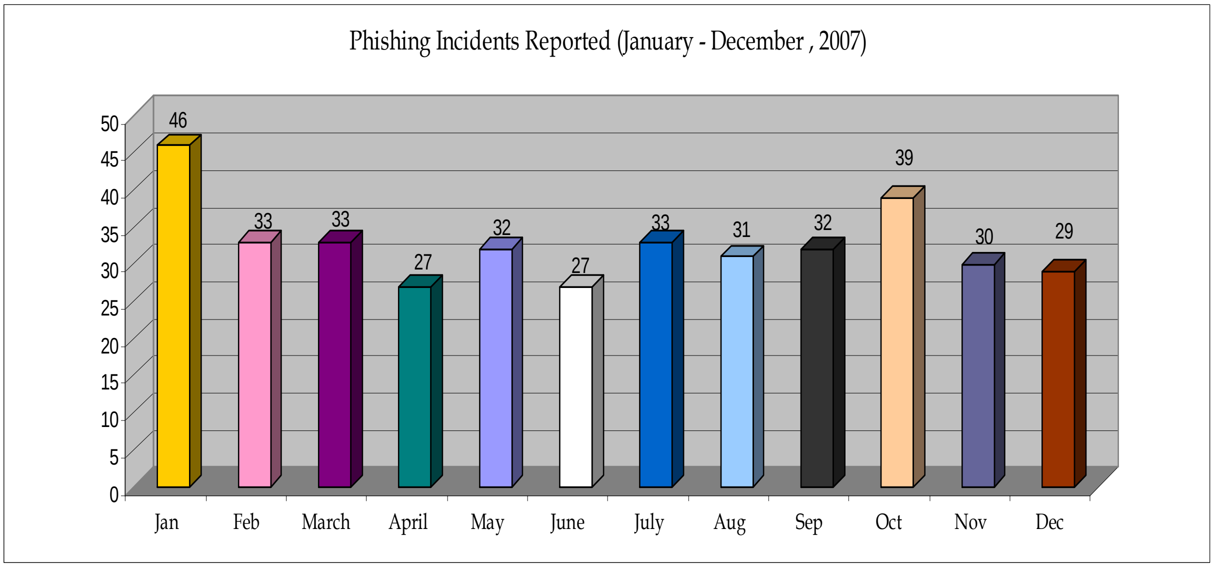

Figure 1: *Phishing* Incidents Reported by Month

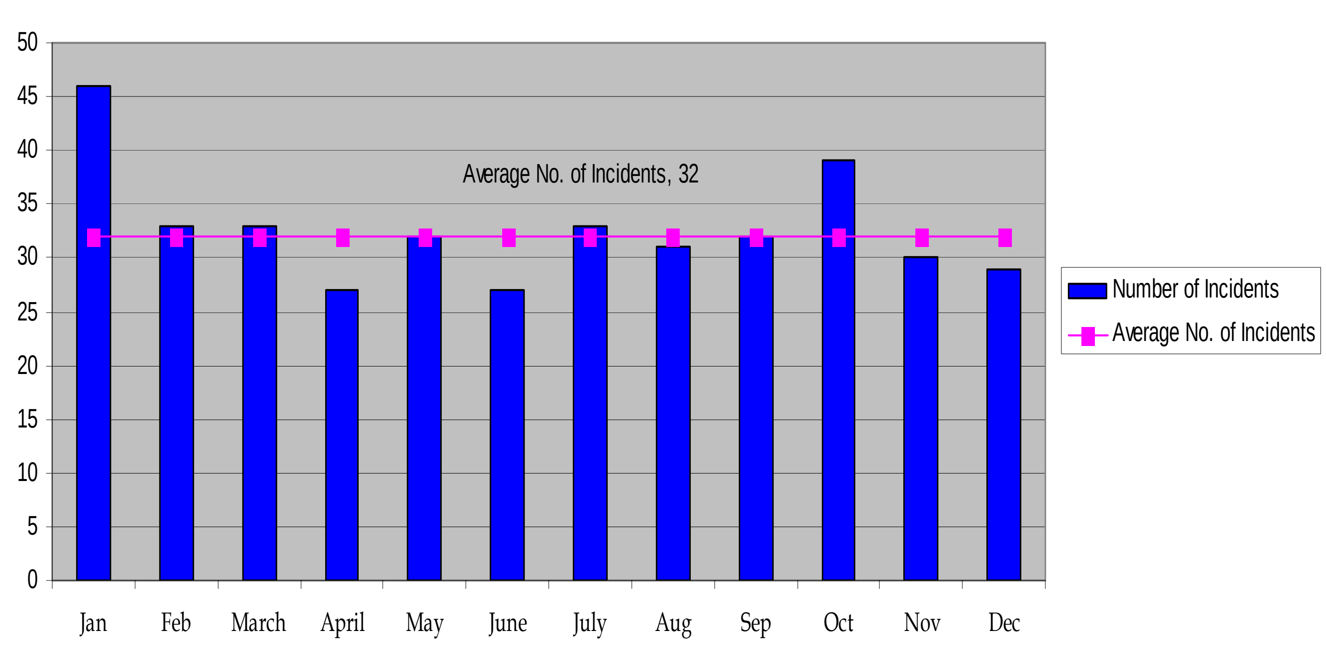

Figure 2: Average number of *Phishing* Incidents Reported

SL No.	Month	Number of Incidents Reported Year 2006
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 2. *Phishing* Incidents Reported by Month-Year 2006
(Source: CIWP-2007-01, Analysis of *Phishing* Incidents year-2006)

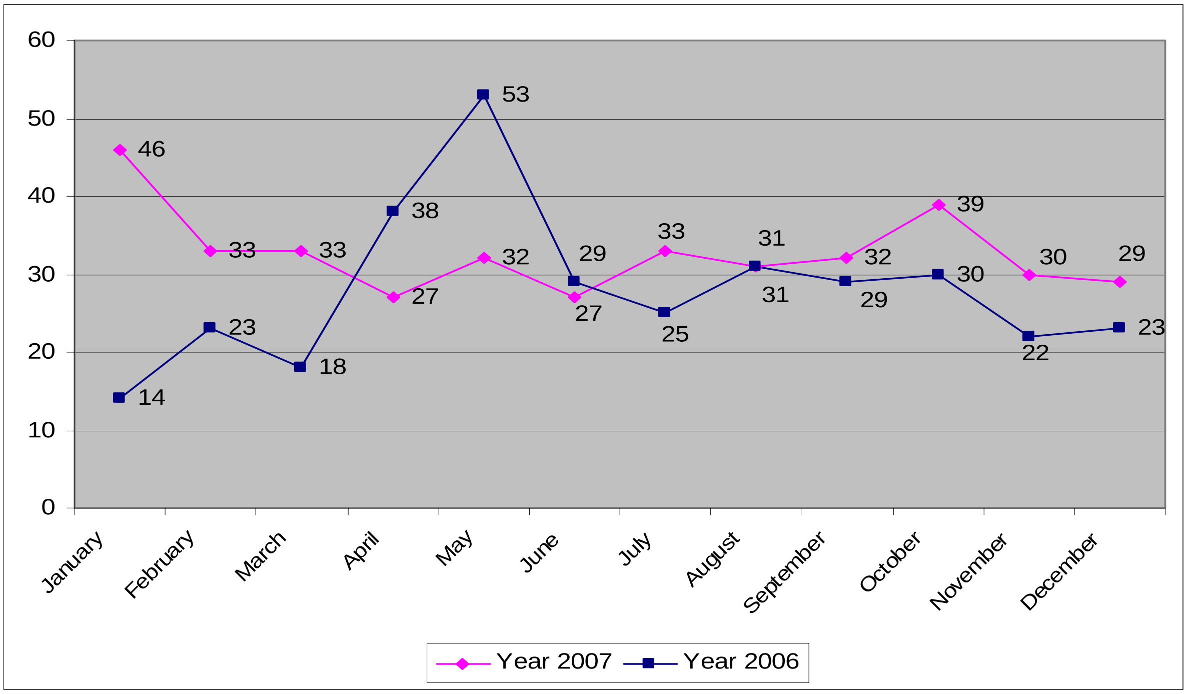

Figure 3: Comparison of *Phishing* Incidents Year 2006 - 2007

1.2. Number of unique *phishing* URLs

In a *phishing* incident, the phishers provide *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 during the year 2007, CERT-In received 957 reports of unique *phishing* URLs. This is an increase in 10% over the 873 unique *phishing* URLs reported in the year 2006 [Figure 4].

SL No	Month	Number of unique *Phishing* URLs
1	January	145
2	February	89
3	March	87
4	April	65
5	May	82
6	June	58
7	July	66
8	August	82
9	September	58
10	October	87
11	November	81
12	December	57

Table 3. Monthly Unique *Phishing* URLs reported

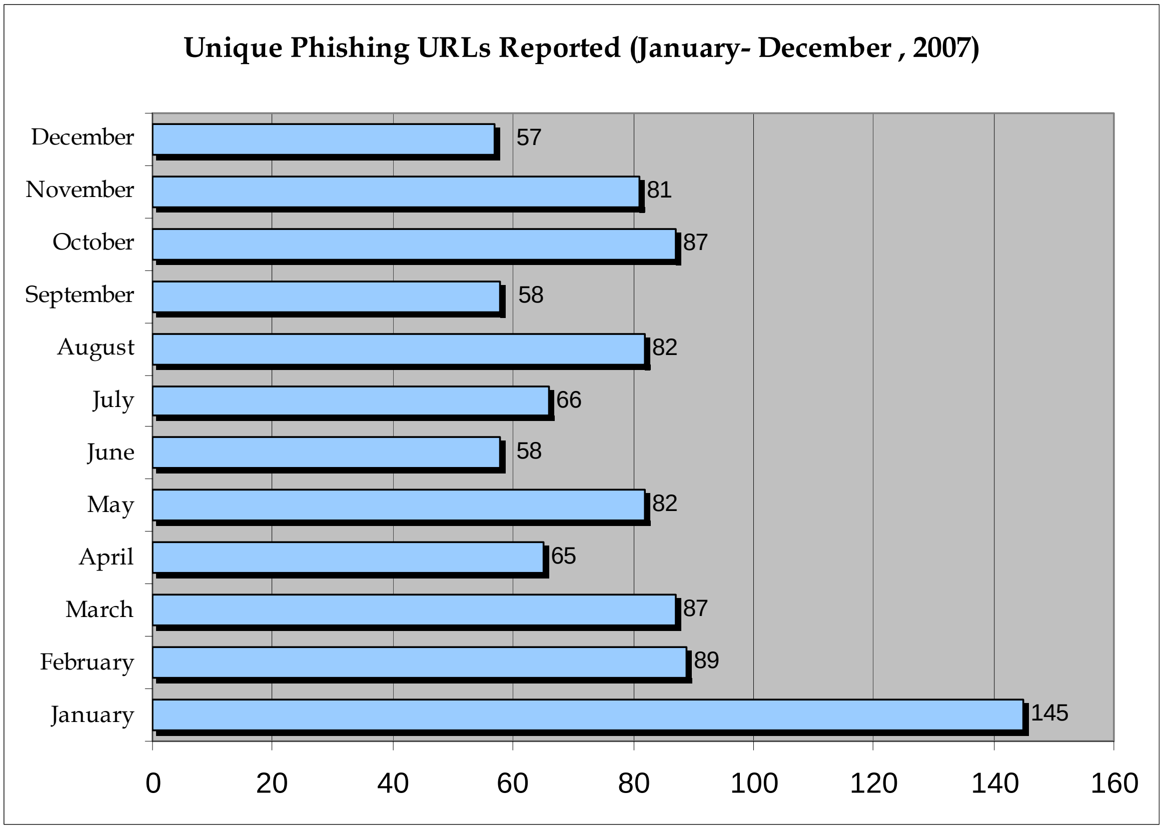

Figure 4: Monthly Unique *Phishing* URLs Reported

In the month of January there were 145 unique *phishing* URLs reported, the highest number of active *phishing* URLs during first half of 2007. However for the second half of 2007 October month has encountered highest number with 87.

This increase in unique *phishing* URLs is contributed due to increased "Rock Phish" incidents, hosting of multiple *phishing* websites on a single domain during the year 2007 as compared to 2006.

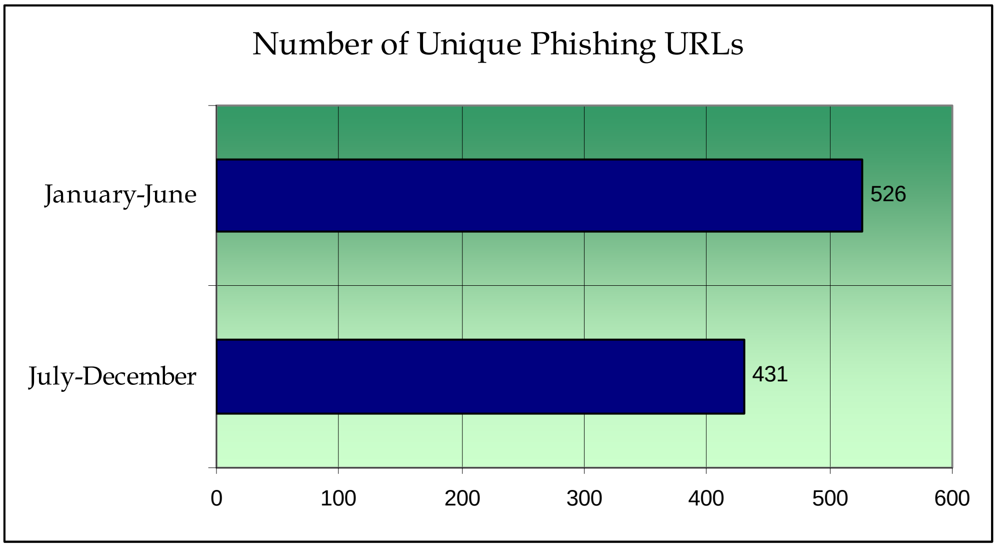

Figure 5: Trend of Unique *Phishing* URLs reported

2.3 *Phishers* are moving down mark

In the beginning, *phishers* only used large brand name financial institutions or online retailers to target consumers. Now *phishers* are expanding their targets to smaller financial institutions that consumers feel will be less likely to be affected.

2.4 Ports used by *Phishing* URLs

The *phishing* URLs connects through a port to a *phishing* website. Most of the *phishing* incidents reported used Port 80 which is the default port for *http* web protocol. This is in the continuation to the trend seen during the year 2006.
It constitutes 96% of the total *phishing* URLs [Figure 6] and Port 84 is reported with 2%, the second most popular Port for the attack. Some different ports are also seen this year, as used by *phishing* URLs.

SL No	Port No	Number of *Phishing* URLs
1	80	917
2	84	14
3	82	8
4	81	8
5	3219	4
6	8080	2
7	8082	2
8	86	1
9	7640	1

Table 4. Ports used by *Phishing* URLs

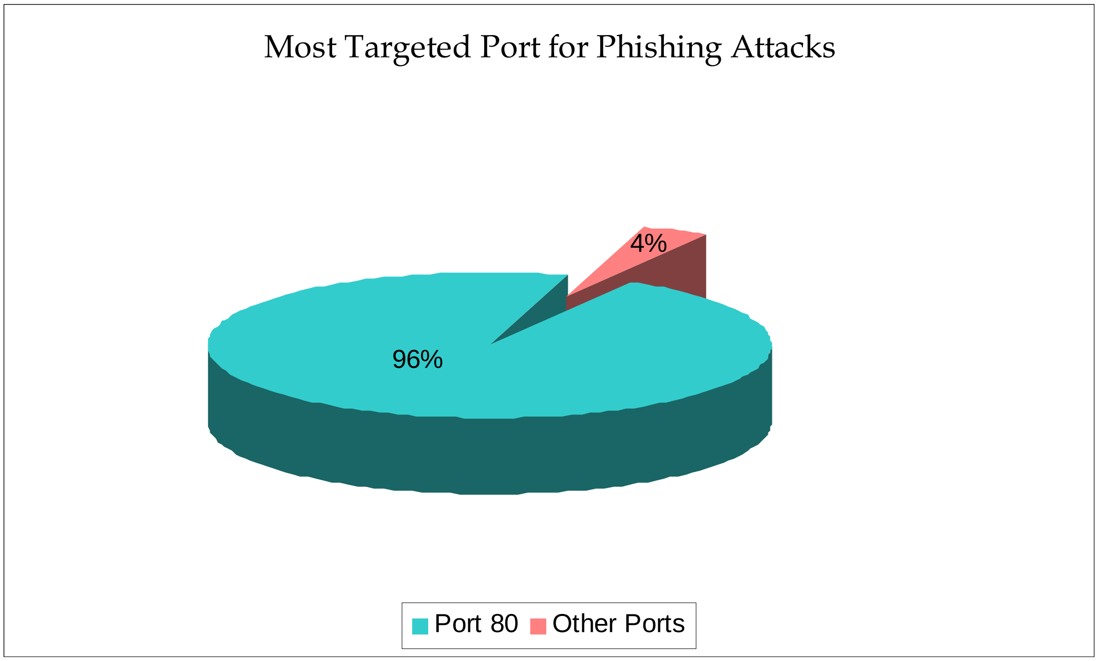

Figure 6: Most Targeted Port

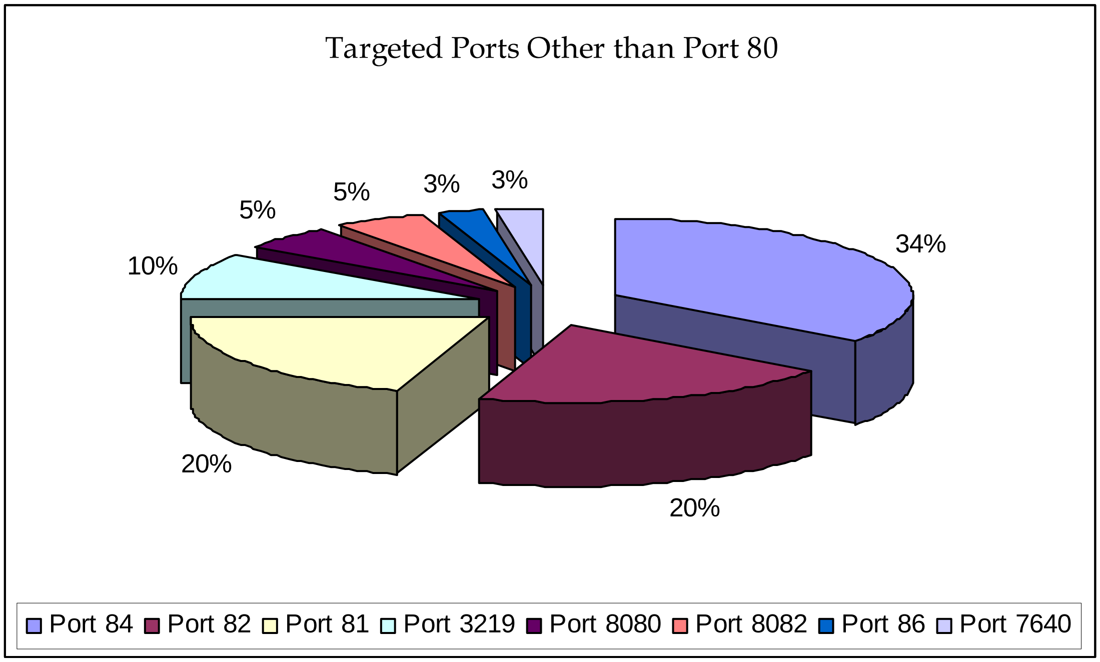

Figure 6.1: Ports targeted other than *Port* 80

2.5 Targeted Sectors

There is a significant increase in *phishing* attacks against financial services in the year 2007. 47% of the targeted attacks have been carried out against financial services sector as compared to 24% in the last year. CERT-In has observed increase of 27% from the last year 2006. More number of Banks, Credit Unions and Financial Institutions of different countries were on the target in the year 2007. However 51% of the targeted attacks were carried out against e-Commerce sector and remains the favorite sector for the *phishers*.

Among the attacks against financial services sector, 12% of targeted brands belonged to country India. This is an increase of 3% over the last year (2006).
Some other sectors which include Government Sector were also seen on the *phishers* target.

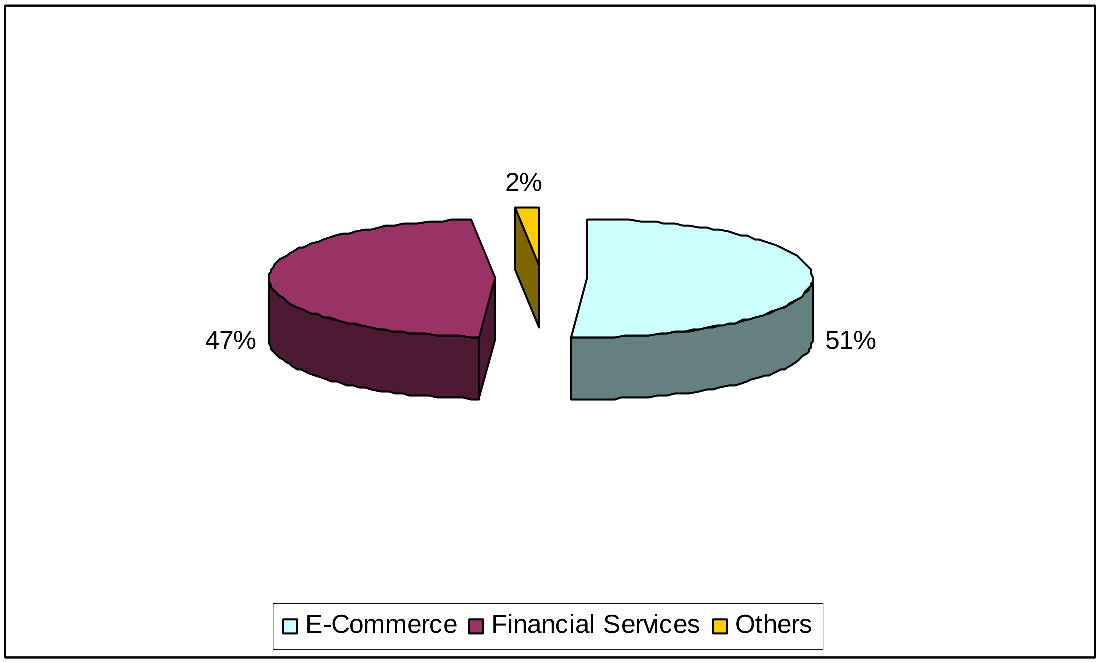

Figure 7: Targeted Sectors

2.6 Brands Hijacked

Month January 2007 has witnessed large number of brands being hijacked by the *phishers,* in total 12 brands [Figure 8]. Various well-known Banks from different countries, Small Banks and Credit Unions particularly of USA have been phished by the attackers during the year.

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

Table 5. Brands Hijacked: Month-Wise

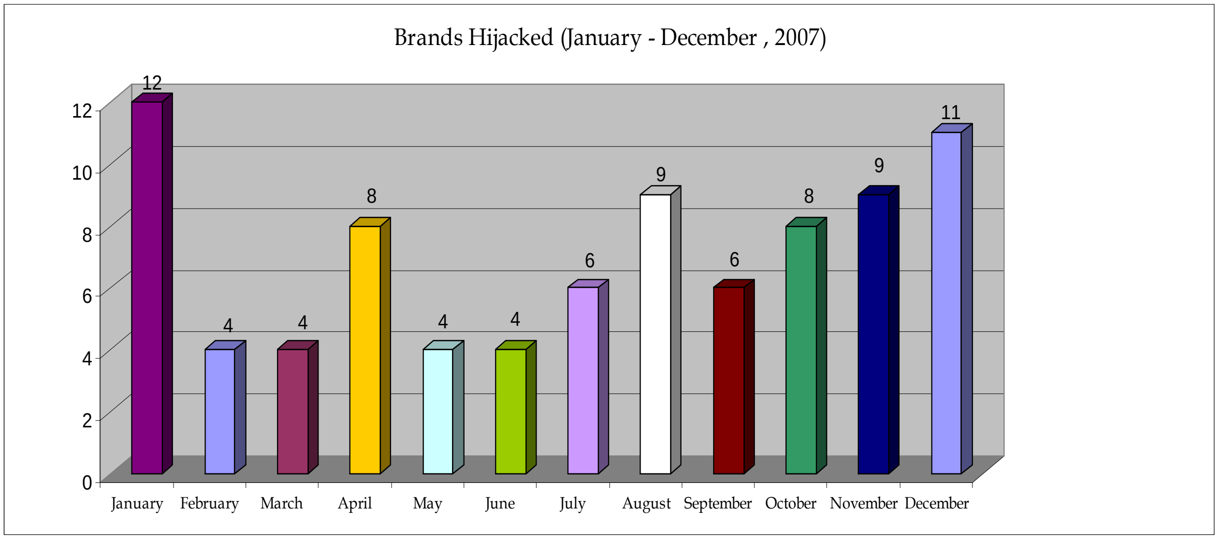

Figure 8: Brands Hijacked: Month -Wise

2.7 Country belonging of Brands hijacked

Large number of brands hijacked belongs to the country United States, USA. 80% of hijacked brands are from USA. While 15% belongs to India and 2% belongs to Italy [Figure 9]. 3% belonged to other countries.

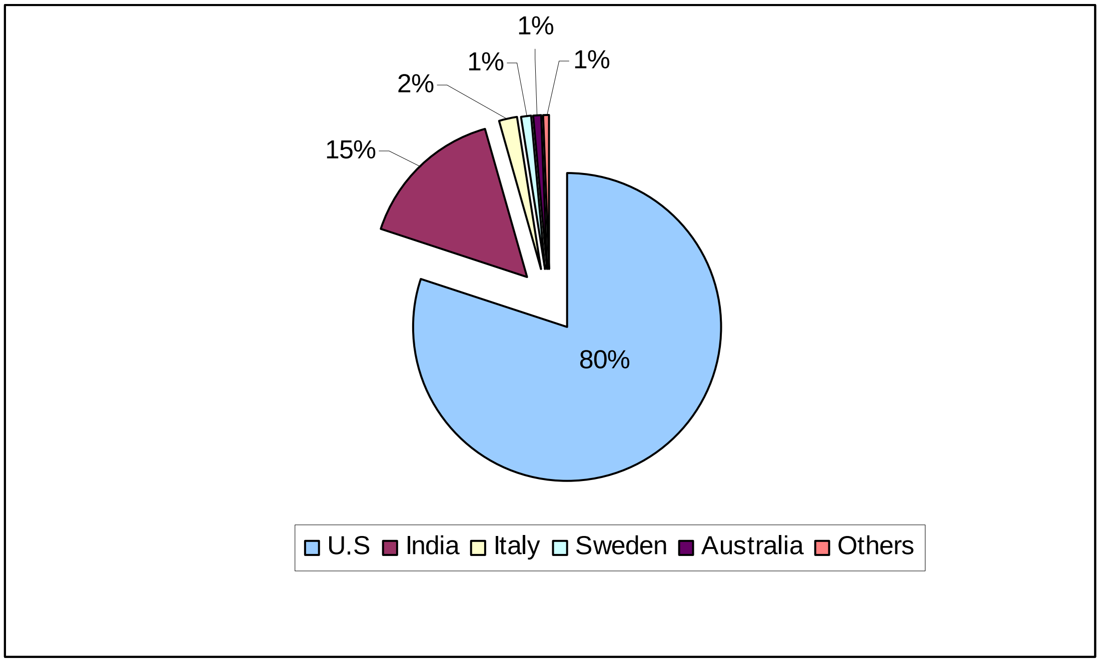

Figure 9: Brands Hijacked: Country-Wise

2.8 *Phishing* URLs with Top Level Domain (TLD)

The analysis of *phishing* URLs indicates that *.com* is the most popular top level domain (TLD) for the *phishers* [Figure 10]. This is again the continuation of trend as seen in the last year (2006).

SL No	Top Level Domain	Number of *Phishing* URLs
1	.com	215
2	.in	66
3	.net	17
4	.org	10
5	.uk	7
6	.edu	5
7	.br	5

8	.eu	4
9	.mobi	1
10	.info	1
11	.biz	1
12	.cn	1
13	.de	1

Table 6. *Phishing* URLs with Top Level Domain (TLD)

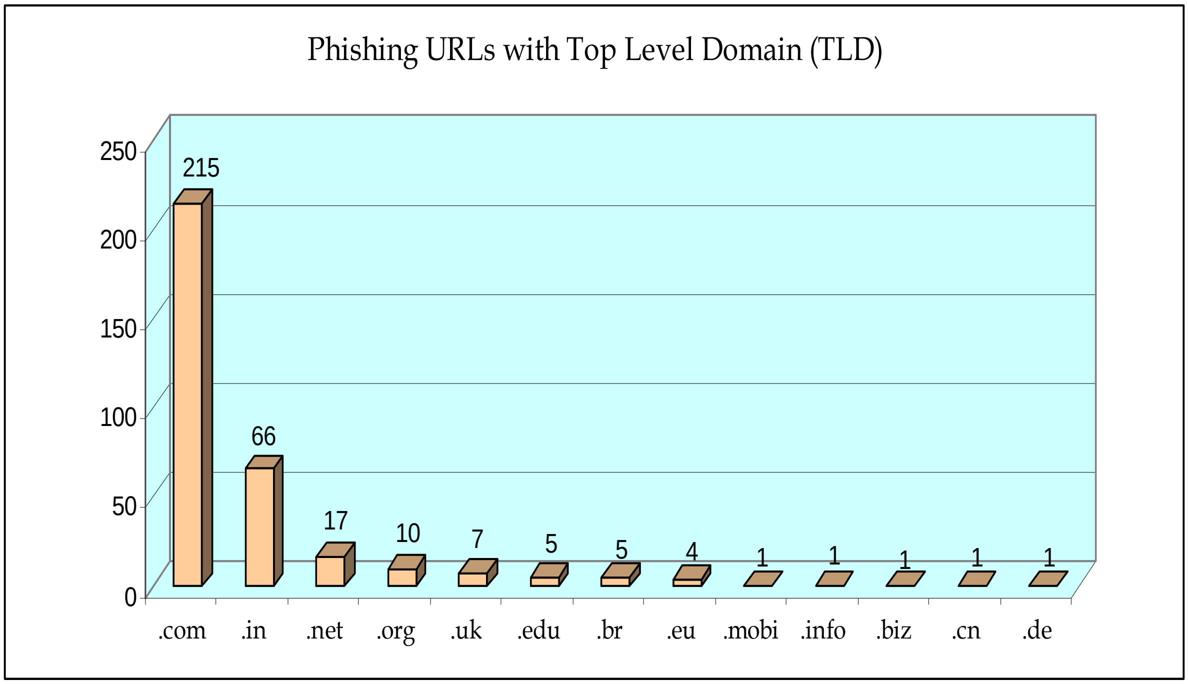

Figure 10: *Phishing* URLs with Top Level Domain (TLD)

.in is reported with highest country specific TLD hosting *phishing* page.
While UK, BRAZIL, CHINA and DENMARK are the other country specific TLDs (.uk,.br,.cn,.de) found hosting *phishing* page.

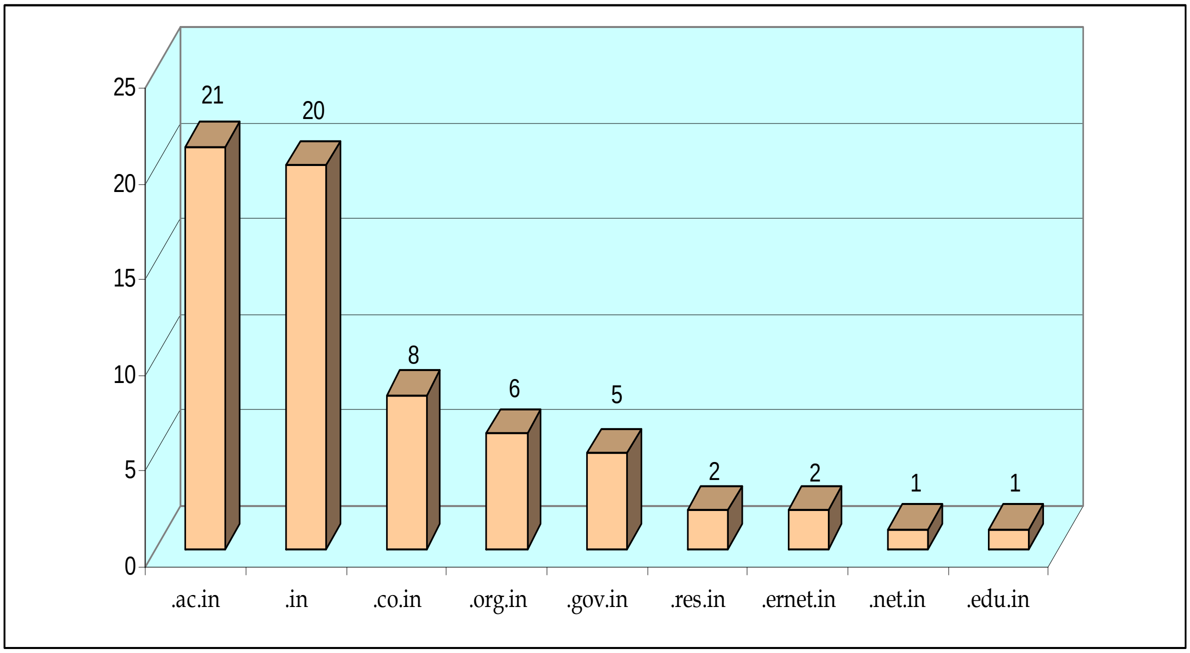

Figure 10.1: Distribution of *Phishing* URLs hosted on *.in* Domain.

The most targeted domain under **'.in'** ccTLD is **'.ac.in'**, amounting to 31.8% and next is ***'.in'*** amounting to 30% of total domains under **'.in'** ccTLD.

2.9 Use of *Phishing* Toolkits and Fast Flux DNS

Even with users' awareness growing, sophistication of *phishing* threats continues to plague consumers.

CERT-In has observed new trends and developments in *phishing* techniques adopted by the *phishers* to launch *phishing* attacks during the year 2007.

1. *Phishing* attacks are accelerating and becoming more surreptitious.

2. Attacks are morphing: *Phishing* threats started as emails that lead one to counterfeit Websites. Now, the threat also includes *phishing*-based Trojans and Malware like key logging system -- which run in the background intercepting a user's account information and reporting it back to the criminals without the user's knowledge. Year's most active malware 'Storm BOT' is being used to perform *phishing* attacks on some financial institutions/banks.

3. Fast flux *phishing* is observed as an emerging trend this year. Fast-flux DNS allows to point the DNS to multiple sites, so that when one goes offline, the others are used. *Phishers* adopted this technique to host fraudulent domains on fast flux DNS. With this technique a single *phishing* domain is served by multiple geographically distributed IP addresses, which increases the survivability of *phishing* domains.

4. There is also increase in *Rock Phish* incidents which employed "*Rockphish*" toolkit, during the year 2007 as compared to year 2006. Again *Rock Phish* domains serve longer survivability. *Phishing* kits such as ***Metafisher*** is also seen to launch *phishing* attacks.

2.10 Vulnerability exploitation 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 also exploited during the *phishing* attacks. The details of the vulnerabilities discovered in various operating systems, application software and client software in the year 2007 are available on CERT-In website.
[http://www.cert-in.org.in].

3. Countermeasures

The *phishing* threats will worsen as criminals target smaller financial institutions, launch more personalised attacks and intrude consumer's systems. On the brighter side consumers can thwart *phishers* by adopting a combination of security measures from their email browsers and financial service providers.

There are various countermeasures needs to be taken at user level, organization level, financial institution and industry level. These countermeasures are discussed in detail in CERT-In Whitepaper "*Phishing* Attacks and Countermeasures" [CIWP-2005-03]. Some of the important countermeasures are described below:

1. Enterprises should deploy an Enterprise security model that combines intrusion detection, firewall, antivirus and vulnerability management systems for maximum protection against malicious code and other threats.
2. ISPs, email service providers and browser vendors should install anti-spam filters that prevent *phishing* messages hitting user's mail box. They

should provide toolbars and enhancement that block consumers from visiting *phishing* websites.

3. Keep up-to-date security patches and update release for Operating System.
4. Keep up-to-date security patches and update release for application software.
5. Keep up-to-date Antivirus and Antispyware signatures to protect against latest malware spreading in the wild.
6. Do not click on a link embedded within any potentially 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.
7. The enterprises should protect their own brands from being used in *phishing* attacks by subscribing to *anti-phishing* solution.
8. 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.
9. The enterprises dealing with consumer financial accounts should protect their accounts from *phishing* and other malware attacks through stronger user authentication and transaction verification.
10. Follow Security Best Practices.

4. Reporting of Phishing Incidents

Phishing incidents pertaining to Indian scenario can be reported to ***CERT-In Incident Response Help Desk.*** As well as concerned bank/financial institution**.**

CERT-In Incident Response Help Desk
Email: incident@cert-in.org.in
Phone: +91-11-24368572
Fax : +91-11-24368546

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

5. List of Figures

6. List of Tables