Phishing & Anti-Phishing: A Review

Disha D N, Rachana N B, Kumari Deepika, Nidhi Shri G

***Abstract*— With the advent of internet, various online attacks have been increased and among them the most popular attack is phishing. This paper surveys the literature on Phishing Attacks and Anti-Phishing.**

Phishing is a form of Social Engineering Technique used to deceive users. Social networking is one of the most popular Internet activities, with about millions of users from around the world. The time spent on sites like Facebook, e-mail and instant messaging is constantly increasing at an impressive rate. At the same time, users populate their online profile with a plethora of information which aims at providing a complete and accurate representation of themselves. Attackers may duplicate a user's online presence in the same or across different social networks and, therefore, fool other users into forming trusting social relations with the fake profile. By abusing that implicit truss transferred from the concept of relations in the physical world, they can launch phishing attacks, harvest sensitive user information, or cause unfavorable repercussions to the legitimate profile's owner.

***Index Terms*— Phishing, E-mail Phishing, URL Obfuscation, Mobile Phishing, Anti-Phishing.**

I. INTRODUCTION

Phishing is the attempt to acquire sensitive information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing emails may contain links to websites that are infected with malware [1]. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake used to deceive users, and exploits the poor usability of current web security technologies [2]. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and you should not use the same passwords anywhere on the internet [3].

The current paper is organized as follows: Section II to V details the types of phishing attacks. Section VI to VII presents the anti-phishing techniques for phishing detection and prediction. Section VIII details the websites to report for phishing attacks. Finally, Section IX Summaries the paper.

Manuscript received December 23, 2014.

Disha D N, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054

Rachana N B, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054

Kumari Deepika, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054

Nidhi Shri G, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054

A. HOW DOES PHISHING WORK

Phishing scams are set up to look as legitimate and as genuine as possible by creating an email and web page that is almost identical to an official email and website of a trusted organization, or by injecting untrusted data within an existing authentic website. The email sent by the phishers will include a link to what appears to be an "official" website, which is actually a fake site operated by the attacker. Once you have visited this website, any information you enter on the web page will be collected by the phisher and may be used fraudulently for whatever purpose the phisher has in mind. From beginning to end, the process involves

i Planning: A phisher decides which business to target and determines how to obtain email addresses for the customers of that business. They often use the same mass mailing and address collection techniques as spammers.

ii Setup: Once they know which business to spoof and who their victims are, the phisher creates methods for delivering the message and collecting the data. Most often, this involves email addresses and a web page.

iii Attack: This is the step people are most familiar with the phisher sends a phony message that appears to be from a reputable source.

iv Collection: The phisher records the information victims enter into web pages or popup windows.

v Identity Theft and Fraud: The phisher uses the information they have gathered to make illegal purchases, or otherwise commit fraud.

If a phisher wishes to coordinate other attacks, he will evaluate the successes and failures of the completed scam and begin the cycle again. Phishing scams often take advantage of software and security weaknesses on both the client and server sides [4], but even the most high-tech phishing scams work like old fashioned con jobs, in which a hustler convinces his mark that he's reliable and trustworthy[5].

II. E-MAIL PHISHING

Phishing emails are messages designed to fool the recipient into handing over personal information, such as login names, passwords, credit card numbers, account credentials, social security numbers etc. Fraudulent emails harm their victims through loss of funds and identity theft. They also hurt Internet business, because people lose their trust in Internet transactions for fear that they will become victims of fraud [6].

A. Different forms of e-mail Phishing

i Generic Greeting Phishing emails are usually sent in large batches. To save time, Internet criminals use generic names like "First Generic Bank Customer" so they don't have to type all recipients' name out and send emails one by one. If you don't see your name be suspicious [5].

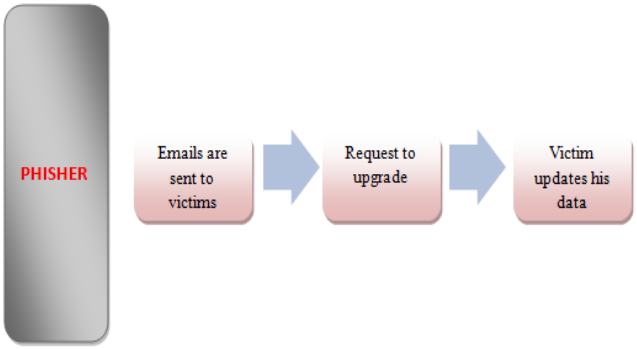

Fig 1: Phishing Process

ii Forged Link: Even if a link has a name you recognize somewhere in it, it doesn't mean it links to the real organization. By rolling your mouse over the link you can see if it matches what appears in the email. If there is a discrepancy, it is advised not to click on the link. iii Requests Personal Information: The main purpose of sending a phishing email is to trick you into providing your personal information. If you receive an email requesting your personal information, it is probably a phishing attempt. iv Sense of Urgency: Internet criminals want you to provide your personal information immediately. They do this by making you think something has happened that requires you to act fast. The faster they get your information, the faster they can move on to another victim [8].

v Poor Spelling: is also a very reliable indication that the email is not authentic.

B. Phishing stages

Phishing attacks involve several stages

i The attacker obtains E-mail addresses for the intended victims. These could be guessed or obtained from a variety of sources.

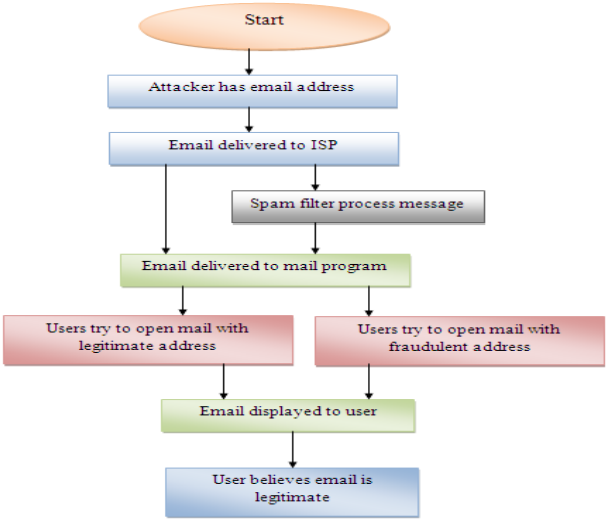

Fig 2: Phishing Stages

ii The attacker generates an E-mail that appears legitimate and requests the recipient to perform some action.

iii The attacker sends the E-mail to the intended victims in a way that appears legitimate and obscures the true source. Depending on the content of the E-mail, the recipient opens a malicious attachment, completes a form, or visits a web site.

iv The attacker harvests the victim's sensitive information and may exploit it in the future [9].

The phishing attack starts with an E-mail to the intended victims. The attacker creates the E-mail with the initial goal of getting the recipient to believe that the E-mail might be legitimate and should be opened. Attackers obtain E-mail addresses from a variety of sources, including semi-random generation, skimming them from Internet sources, and address lists that the user believed to be private. Spam filtering can block many of the phishing Emails.

If the institution whose customers are being phished regularly uses authenticated E-mail (such as PGP or S/MIME), the recipient may notice that the E-mail does not have a valid signature, thereby stopping the attack. Once the E-mail is opened by the user, the E-mail contents have to be sufficiently realistic to cause the recipient to follow the directions in the Email [10][11].

III. URL OBFUSCATION PHISHING ATTACKS

URL Obfuscation phishing attack misleads the victims into thinking that a link and/or website displayed in their web browser is legitimate. This phishing attack tends to be technically simple but highly effective. There are several methods for obfuscating the URL like bad domain name or misspelled domain name, friendly login URL, shortened URL, using IP address, encoded URL.

A. General Steps for URL Obfuscation Phishing Attack

Generally, the URL Obfuscation phishing attacks perform with the following four steps:

i First of all, the phisher have to make an obfuscated URL website to lure the victims, and that URL and website must be seems as legitimate one.

ii Then, that obfuscated URL is attached to the lots of spoofed e-mails and sends to the number of users. That e-mail will convince the victim to click on that URL.

iii If the victim clicks on that obfuscated URL and visits that website, it convince the victim to provide the financial information of some confidential data.

iv Phisher then acquires some entered data or information, and later it can be misused by phisher.

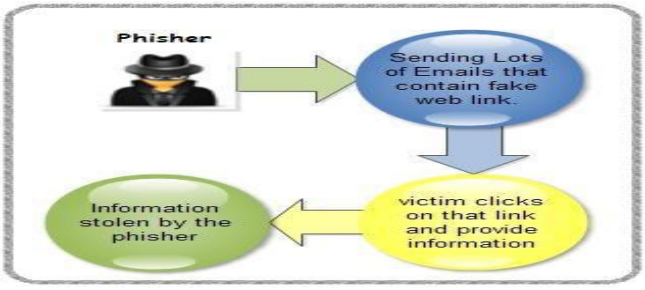

Fig 3: URL Based Phishing Steps

B. Existing Methods for URL Obfuscation Phishing Attack

URL Obfuscation is a type of phishing attacks, in this attack the obfuscated URL used instead of real URL to dupe the victims. There are several methods used for obfuscating the URL.

i Bad domain name or Misspelled domain name

One of the most trivial obfuscation methods is through the purposeful registration and use of bad domain name. Consider the financial site Real Bank has registered the domain name realbank.com and associated customer transactional site http://onlinebanking.realbank.com. The attacker could set up

any of similar domain name to obfuscate the real destination host. Like,
http://realbankS.com
http://realbamk.com http://onlinebanking.realbankS.com
http://onlinebanking.realbamk.com

Fig 4: Misspelled domain name.

ii Shortened URLs

A shortened URL is short URL, which minimize the length and the complexity of web based application URL's. It is redirected to the targeted URL. Shortened URL is a combination of service site and unique number. The phisher may use these free services to obfuscate the true destination. Such as,
http://tinyurl.com,
http://bitly.com
http://goo.gl

iii Host name Obfuscation or Using IP address*:*

In host name obfuscation method the host name can also be obfuscated by replacing it with the IP address of the same domain name. A phisher may wish to use the IP address as part of a URL to obfuscate the host and possibly bypass the content filtering system or hide the destination from the end user.

For example: the IP address for the obfuscated URL http://realbankS.com is 173.193.212.4. Then the above URL will be obfuscated such as http://173.193.212.4/. Most commonly the dotted IP address is used by the phisher to obfuscate the URL. Like instead of our misspelled domain name realbankS.com we have use the IP address 173.193.212.4. There are the other formats also available for the IP address such as dot less IP address in decimal, dotted IP address in octal, dotted IP address in hexadecimal, dot less IP address in hexadecimal.

Fig 5: IP address for the obfuscated URL

iv Friendly Login URL

Many web browsers allows for the URLs that contain authentication information such as username and password. The general format is url://username:password@hostname/path. So, by using this facility the attackers may proxy the username and password field for targeted organization.

For example: following URL sets the username = onlinebanking and password = realbank.com and the destination hostname is realbankS.com. So, the URL looks like
http://onlinebanking:realbank.com@realbankS.com/fakepage.php. Through the above URL, user thinks that they are visiting the legitimate onlinebanking of realbank.com site. But truly they are visiting the fake page of realbankS.com. That fake page will resemble to realbank.com.

v Encoded URL Obfuscation

In this method, phisher obfuscate the URL using encoding schemes. It is trivial for the phisher to obfuscate the true nature of URL using the encoded schemes [12][13].

IV. MOBILE PHISHING

Different types of phishing attack on mobile devices are Bluetooth phishing, Short Message Service (SMS) phishing and Voice over IP Phishing or known as vishing [14][15].

Fig 6: Ways of Mobile device phishing attack

A. Different Forms of Phishing Attacks

i Bluetooth

The Bluetooth phishing attack works when user connects to the Wi-Fi hotspot. Attacker can steal the data when the user connects to the Wi-Fi.

ii Vishing

The potential victim receives a message, often generated by speech synthesis, indicating that suspicious activity has taken place in a credit card account, bank account, mortgage account or other financial service in their name. The victim is told to call a specific telephone number and provide information to "verify identity" or to "ensure that fraud does not occur." If the attack is carried out by telephone, caller ID spoofing can cause the victim's set to indicate a legitimate source, such as a bank or a government agency.

Vishing is difficult for authorities to trace, particularly when conducted using VoIP. Furthermore, like many legitimate customer services, vishing scams are often outsourced to other countries, which may render sovereign law enforcement powerless.

Consumers can protect themselves by suspecting any unsolicited message that suggests they are targets of illegal activity, no matter what the medium or apparent source. Rather than calling a number given in any unsolicited message, a consumer should directly call the institution named, using a number that is known to be valid, to verify all recent activity and to ensure that the account information has not been tampered with.

iii Mobile Web Application

Another attack used successfully is to forward the client to a bank's legitimate website, then to place a popup window requesting credentials on top of the website in a way that it appears the bank is requesting this sensitive information [16].

iv SMS Phishing(SMishing)

SMS phishing attempts occur when cell phone user is the recipient of a message acknowledging receipt of an unknown purchase. To terminate bogus purchases and avoid monthly or daily charges, consumers are directed to phishing websites. Unknowingly, customers go directly to the website, allowing hackers to access personal cell phone information. SMS phishing has become increasingly prevalent on social website networks, such as Facebook. SMS Phishing is a way of performing identity theft, as the inadvertently downloaded malware captures and transmits all of the stored cellphone data, including stored credit card details, names, addresses and other data, like password details for email accounts, which, when opened, increase the vulnerability of online banking and other accounts. The malware can then cover its tracks by wiping the phone clean, including all call records, causing repeated rebooting or similar odd behavior rendering the phone unusable. Thus, the original phishing attack is easily unnoticed by the user. Viruses and phishing scams are far reaching to all types of digital devices. Wise consumers should choose their products according to available product security software and data recovery technologies.

v Wi-Fi Phishing attack scenario

The new Wi-Fi phishing variant is a more sophisticated version of the Evil Twin attack that hit the Internet in January. In Evil Twin, also known as the AP (access point) phishing scam, an attacker poses as a legitimate hot spot and tricks victims into connecting to the hacker's laptop or handheld device, according to Air Defense [1]. Once the victim connects, the attacker can attempt to coerce the user into revealing personal and confidential information.

To avoid becoming victims of the latest scam, Air Defense recommends that wireless users take several security steps. When accessing their accounts at hot spots, users should enter passwords only into Web sites that include a Secure Sockets Layer key at the bottom right of the Web browser. Users should also avoid hot spots where it's difficult to tell who is connected, such as at hotels and airport clubs. Hot spots should only be used for Web surfing and not for making online purchases or any other transactions where account numbers or passwords are needed, the company said.

Users should also turn off or remove their wireless cards from their computers when they aren't accessing a hot spot to prevent others from accessing their machines, the company said. Users are also encouraged not to use unsecured applications such as e-mail or instant messaging while at hot spots. All patches for personal firewall and security software should also be continuously updated [2].

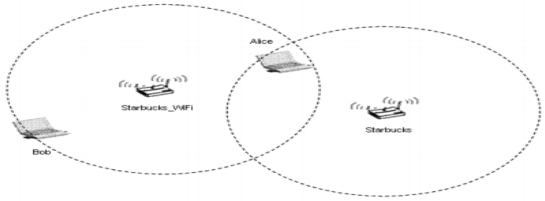

Fig 7: Wi-Fi Phishing Attack Scenario

V. ANTI-PHISHING TECHNIQUES

Anti-Phishing is the method employed in order to detect and prevent the Phishing attack. Anti Phishing prevent user from giving user credentials. Phishing attacks are the most popular form of cybercrime in the 21st century. The media regularly reports lists of organizations whose customers became victim to phishing attacks. Phishing scams increase in quality and quantity every day. phishing frequently leads to real financial losses. In this paper we have describe the methods to avoid them. Some techniques works on emails, some on mobile device, some works on attributes of web sites and some on URL of the websites [17].

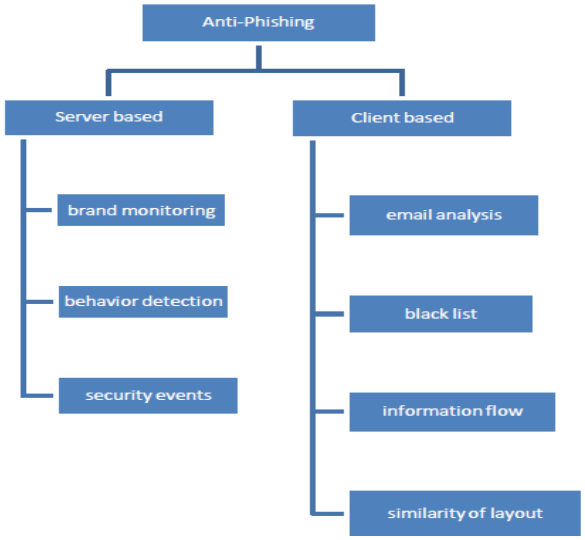

Fig 8: Anti-phishing Techniques

A. Server Based Anti-phishing

These techniques are implemented by service providers (ISP, etc) and are of following types

i Brand Monitoring: Cloning online websites to identify "clones" which are considered phishing pages. Suspected websites are added to centralized "black list".

ii Behavior Detection: for each customer, a profile is identified (after a training period) which is used to detect anomalies in the behavior of users.

iii Security Event Monitoring: security event analysis and correlation using registered events provided by several sources (OS, application, network device) to identify anomalous activity or for post mortem analysis following an attack or a fraud.

B. Client Based Anti-phishing

These techniques are implemented on user's end point through browser plug-ins or email clients and are of following types

i Email based analysis: email based approaches typically use filters and content analysis. If trained regularly, Bayesian filters are actually quite effective in intercepting both spamming and phishing e-mails.

ii Black Lists: black lists are collection of URLs identified as malicious. The black-list is queried by the browser at run time whenever a page is loaded. If the currently visited URL is included in the black list, the user is advised of the danger otherwise the page is considered legitimate.

iii Information flow: information flow solutions are based on the premise that while a user can be easily fooled by URL obfuscation or a fake domain name, a program will not run. Antiphish is an example of this type of technique which keeps track of sensitive information that the user enters into web forms, raising an alert if something is considered unsafe.

iv Similarity of layouts: most advanced techniques try to distinguish a phishing page from a legitimate page by comparing their visual similarities. DOM-Antiphish

computes the similarity value extracting the DOM-tree of the considered web pages.

v DOM-Antiphish description: when a password associated with certain domain is reused on another domain the system compares layout of current page with the page where the sensitive information was originally entered. For the comparison, DOM trees of the original webpage and the new one are checked. If the system determines that both trees are same in appearance, then phishing attack is assumed.

Table. 1: Phishing Example

Legitimate web page	Phishing Web page
<html>	<html>
<body>	>
HELLO	 HELLO
</body>	</body>
</html>	</html>
Legitimate DOM tree	Phishing DOM Tree

VI. PHISHING PROTECTION BEST PRACTTICES

BOTNETS: In today's business and consumer computing paradigm, an emerging tool for various malicious activities is the botnet. Botnets networks of compromised machines infected with malicious programs have been identified as a leading cause for phishing, a serious form of spam.

Bots: A BOT, short for robot is an automated software program that operates as an agent for a user or another program, or alternatively, simulates human activity. On the Internet, the most ubiquitous bots more commonly known as spiders or Web crawlers are legitimate programs that access Web sites and collect content for search engine databases. Bots have also been created to verify stock quotes or compare prices on shopping-based Web sites. Other bots such as knowbots and chatterbots have been used in a variety of legitimate ways.

However, bots are increasingly used for malicious purposes; these are known as IRC (Internet Relay Chat) bots. This type of BOT is created when a computer virus or worm installs a backdoor program such as a Trojan horse (a malicious program disguised as, or embedded within, legitimate software) or a drive-by downloader (which exploits Web browsers, e-mail clients, or operating system bugs to download malware without requiring any user intervention) that leaves a PC Internet port open. The MyDoom (2004) and SoBig (2003) email worms, for example, employed this tactic. The infected machines subsequently become available for future activation. A hacker then searches for infected PCs with open ports. Once located, the hacker installs the bot program onto their hard drives. The bot then typically connects to Internet Relay Chat to listen for commands, and the controller (a malicious third party) can unleash the effects of the bot by sending a single command to those machines. Bots can also be formed when their creators embed malware on Web pages; creators commonly use pornography, celebrity, Web hosting, or social networking Web sites for this purpose. Users unknowingly download the malware either by clicking on links containing the code or, worse, simply by visiting a URL. Businesses and consumers can protect themselves from the devastating effects of phishing due to botnet activities in two ways: educating themselves about phishing techniques and employing technology solutions that combat phishing [18].

VII. REPORT PHISHING

Whenever user finds a particular webpage as spam one he can report the phishing on following websites. Businesses and consumers can file phishing reports with the following organizations.

Anti-Phishing Working Group http://www.antiphishing.org
Digital-Phishnet http://www.digitalphishnet.org/
Federal Trade Commission http://www.consumer.gov/idtheft/
Internet Crime Complaint Centre (a joint project of the FBI and the National Collar Crime Centre)
http://www.ic3.gov
Trend Micro Anti-Fraud Unit antifraud@support.trendmicro.com.[10]-[7].

VIII. CONCLUSION

In this paper we have looked at different types of phishing attacks and anti-phishing methods. Phishing is a critical issue now a day. Several methods used in this attacks and several mechanism works against this attacks but still there are some challenges which needs to be considered. So, there is likelihood to overcome these drawbacks and try to make a solid algorithm that may cover maximum phishing attacks.

ACKNOWLEDGEMENT

This work is supported by the Management of MSRIT, Dr. K G Srinivas, HOD, Computer Science and Engineering Department. Our special thanks to Dr. Monica R Mundada, Associate Professor. Dept. of CSE, MSRIT, Bangalore.

REFERENCES

[1]http://www.thepinoyonline.com/facebook-phishing-attack/
[2]http://mashable.com/category/phishing/
[3]http://www.google.com/Technical_papers\Phishing Wikipedia, the free encyclopedia.html
[4]http://webtoolsandtips.com/uncategorized/detecting-phishing-scam-emails/
[5] Globalsign White Paper, "The Detection and Prevention of Phishing Attacks",www.globalsign.co.uk, www.globalsign.eu
[6] Noor Ghazi M .et, "Detection Phishing Emails Using Features Decisive Values", Volume 3, Issue 7, July 2013, .pp 257 ISSN: 2277 128X
[7]Anti-Phishing Working Group, http://www.antiphishing.org.
[8]https://www.phishtank.com/what_is_p hishing.php
[9] Atul M. Tonge , Surbhi R. ChaudhariInternational Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013, pp.68,ISSN: 2229-5518
[10] Jyoti Chhikara et al., "Phishing & Anti-Phishing Techniques: Case Study", Volume 3, Issue 5, May 2013, .pp 458-464, ISSN: 2277 128X
[11] Angelo P.E et al., "A Layout Similarity Based Approach For Detecting Phishing Pages". IEEE Conference on Security and Privacy in Communication Networks, Nice, France, September 2007.
[12] Prof. Debalina Nandy et al., "URL Obfuscation Phishing and Anti-Phishing: A Review", Vol. 4, Issue 1(Version 1), January 2014, pp.339-340, ISSN: 2248-9622
[13] U.Naresh et al. "Intelligent Phishing Website Detection and Prevention System by Using LInkGuard Algorithm" International journal for scientific research ,Volume.14 Issue.3, sep-oct 2013 pp.28-36,ISSN:2278-8727
[14] A.P.Felt and D.Wagner, "Phishing On Mobile Devices", 2011

[15]O. Salem, et al., "Awareness Program and AI based Tool to Reduce Risk of Phishing Attacks," in Computer and Information Technology (CIT), 2010 IEEE 10th International Conference on, 2010, pp.1418-1423.

[16] Cik Feresa Mohd Foozy, et al., "Phishing Detection Taxonomy for mobile device", International Journal of Computer Science Issues, Vol. 10, Issue 1, No 3, January 2013,ISSN : 1694-0784 pp.340-341

[17] Gaurav et al. "Anti-Phishing Techniques: A Review", International Journal of Engineering Research and Applications, Mar-Apr 2012, Vol. 2, Issue 2, ISSN: 2248-9622, pp.350-355

[18] "Man sentenced for "botnet" attack on hospital," The Mercury News, August 25, 2006. http://www.mercurynews.com/mld/mercurynews/news/local/states/california/northern_california/15364273.html

Disha D N, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054

Rachana N B, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054

Kumari Deepika, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054

Nidhi Shri G, M Tech-1ST Sem, Dept. of CSE, M S Ramaiah Institute of Technology, Bangalore-560054