National Conference on Recent Advances in Computer Science and IT (NCRACIT)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 1 | ISSN : 2456-3307

Phishing Attacks and It's Various Defences

Surbhi Sharma[1], Deo prakash[2]

[1]M.Tech, Dept. of computer science, Shri Mata Vaishno Devi University, J&K, India
[2]Asst. Professor, Dept. of computer science, Shri Mata Vaishno Devi University, J&K, India
surbhisharma684@gmail.com[1]

ABSTRACT

Phishing is primarily a venture executed by cybercriminals to gain access to the important information of the users viz. passwords, emails, bank details, corporate stats, etcetera to swindle them. Phishing is somehow related to fishing in a lake, but here instead of capturing a fish, phishers try to steal the information of the unsuspected users. It is predominantly carried through by spamming some fancy trending but fallacious emails which catches the eye of the users and if they proceed into enquiring about it by entering the page and filling in their credentials as asked by the page, they fall into the trap and suffer at the hands of the phishers. Purpose of this disquisition is to identify the various deceiving techniques being exercised by the phishers to purloin the crucial information of their victims. I will also discuss how we can detect various phishing attacks and prevent them from harming you.

Keywords: Phishing; Phishers ; AOI accounts; Deceptive; key loggers ; Ransomware

I. INTRODUCTION

Phishing is an act of stealing person's information electronically. It is typically done via email and the information stolen is conventionally the usernames, passwords and other sensitive information such as personal credentials, credit card, and banking information. The attacker tricks the victim by serving vague information, ending up in deceiving the stooge and obtaining the confidential information in a way that he the target is unaware of the fact that his information has been abducted. The phisher actually plays a very cunning game with a target to obtain confidential information. The attacker takes advantage of the helping nature of the people and their weakness to procure the confidential information. The term phishing was coined in 1996 by a group of hackers who hacked into AOL user's accounts by scamming their passwords. These hackers were using email alerts to set up hooks into the ocean of internet users hoping that they take the bait so that they can fish their passwords and gain access to their accounts to loot or ask for ransom for sensitive information. Eventually, this trend became so popular among hackers that they began using AOL accounts as currency and training for hacking software. They commonly used HTML tag found in all chat transcripts to acquire information which referred to stolen accounts, credit cards or illegal activities in order to print the AOL chat filtering system from detecting illegal activity. Today cyber crime is a huge problem for individual, society and even in matters of national security. Merely in the last decade, hundreds and thousands of credit cards have been abducted millions of social security numbers and healthcare records have been compromised. Not only this, even nuclear centrifuges have been hacked. Cyber criminals use the most common trick to send a large amount of spam email in an attempt to trick people into sharing their sensitive personal information. This is called a phishing scam. In other words, a phishing scam is when you receive a trustworthy appearing email asking you to login, in case you click to login you are taken to the fake website. If you still continue to login anyway then possibly you are in serious trouble. Hackers can then use your login credentials to access your real accounts to steal the information or maybe even to steal your money.

II. CLASSIFICATIONS OF PHISHING

Generally, a social engineering attack is when someone tries to trick you into doing something which could have adverse consequences for like downloading malicious software or sharing personal information such as username and password of important accounts or credit card details. Social engineering attacks are typically executed through emails, adverts or websites that look similar to the sites that you already use. Social engineering emails look like they are from a legitimate source such as a bank or authentic service provider but they are not. In this section, we will be discussing various phishing attacks.

A. Deceptive Phishing

Deceptive means "Misleading". Deception has been present since the ancient times. In philosophy, some of these notable people have regarded skepticism to be a product of deception. Decepting a person can lead control over his or her information would evolve by utilizing different digital media. Deceptive phishing approach is also known as link manipulation approach. Deceptive phishing utilizes a broadcasting methods such as instant messages and the messages contain instructions or links which require the recipient to provide information like account details, fictitious account charges, etc. When a user clicks on the deceptive link it redirects the user to the other fake website which appears similar to the recognized source viz. Bank, online shopping website [2].

B. Malware Based Phishing Attack

Malware based phishing involves running a malicious software by attaching it to emails or other web services which may exploit computer vulnerability of the target. In malware phishing, the attacker spams an email with an attachment containing a malware. When that malware file is opened, it becomes active and executes its detrimental task. After that it becomes easy for the attacker to perform unauthorized activities like transferring funds, accessing users private information etc[3].

C. Search Engine Phishing

In this phishers create a fake websites with attractive or pleasing offers and append legally with the search engines. The user come across these websites while searching for their desired products and are being fooled into giving up their information.

D. Web Based Delivery

Web based delivery is also known as MAN-IN-THE-MIDDLE. In this type of phishing, the phisher resides in between the original web site and the user. During the transaction is being executed between the real website and the user the phisher very smartly traces the details. As the user continues to pass the information it is all gathered by the phisher and then used for his personal benefits.

E. Key Logger Phishing

In Key logger's phishing, a malware is made handy to identify inputs from the keyboard and the information is then retrieved by the hacker from this malware via internet[4].

III. DETECTION AND PREVENTION FROM PHISHING ATTACKS

In order to prevent Phishing attack we must first spot it. According to a survey it's being estimated that 156 million Phishing emails are being sent every day, and out of these 16 million Phishing mails get through the protection software (Anti-Phishing tools), 8 million infected mails are opened, 800,000 links are being clicked and 80,000 people fall for the scam and give away their personal information's or details. So it becomes quiet important that one must have knowledge to detect these scams and prevent it. So here we are going to discuss how to spot and prevent Phishing attacks.

A. Preventing Users From Becoming Victim Of Such Attacks:

Under these prophylaxis measures spotting techniques are reckoned. This section lays special emphasis on unearthing phishing attacks so that the phishing along with the masterminds behind it can be easily detected and removed.

B. Spot And Block Phishing Website

One of the challenging tasks is determining the illegitimate and dubious websites because they look almost alike the legit ones but when noticed carefully a minute loop can be discovered. These errors are so minute that a user generally fails to make out, hence, lands up duped. With a little attention these can be differentiated on the basis of few selected features such as URL, domain identity etc. In URL based detection following things should be given attention to like the IP address, length of URL, presence of any suffix or prefix in the URL or "@" sign in the URL. These features can be used to find out whether the website is a phish or legit. Following are the simple steps to check whether the website address is genuine or not:

Step1. Check if the URL has IP address or not, if it does then it is a phish site or otherwise it is good to proceed with.

Step2. Check if there is any prefix or suffix associated with the URL, if yes then it is not a licit website otherwise yes.

Step3. Check for "@" sign if it is present then it is a phishing site or else sound.

Step4. Check for the length of the URL, usually phishers use long URL to hide suspicious content. If the length of the URL is less than or equal to 54 characters then there is nothing to worry about. But, if the length of the URL exceeds 54 characters then the website is a phishing website. For example;

Genuine website email:

https://www.facebook.com/

https://accounts.google.com/

https://www.snapdeal.com/

Spam website email:

https://www.faceboook.com/

https://accounts.google1.com/

https://www.snaapdeal.com/

C. Preventing Man-in-the-Middle Attack.[3]

These kind has caused the loss of millions of dollars worldwide. As we already know that in Man-in-the-Middle attack the hacker places himself in between two authentic communicating parties so the hacker try to hack the communication between the two parties either by DNS spoofing, ARP poisoning or through email phishing. In a executed Man-in-the-Middle attack the communicating parties may have no idea that there communication is being watched over. So one can prevent this Man-in-the-Middle attack through three ways as discussed below

- VPN (Virtual Private Network)

VPN broadens one's private network across a public network. With the help of VPN we can protect our sensitive data when we are browsing over a public networks like public Wi-Fi and also on secure websites where we don't want them to know our location or IP address. When we join a VPN our connection gets encrypted and secure by making us anonymous online preventing the hackers to monitor your communication. It is being creating by building a virtual point-to-point connection by the use of a dedicated connection.

- Proxy Server with Data Encryption

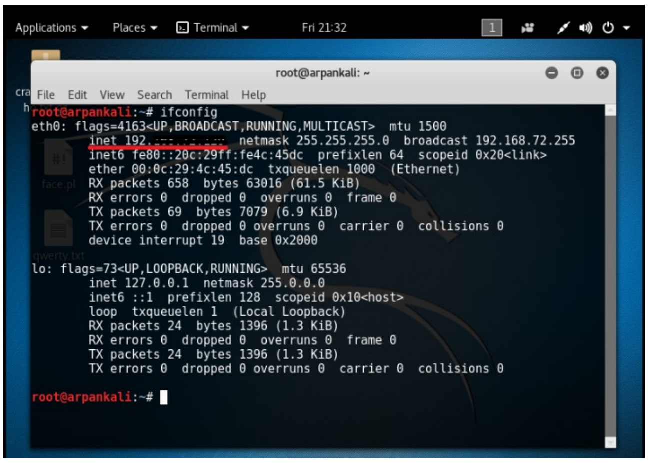
It uses reliable and secure proxy server and encrypt the transmission between the communicating parties. One can use software's like Open VPN, Tor Browser, I2P Hide My IP.

IV.PRACTICAL IMPLEMENTATION OF PHISHING ATTACKS

In this section, we are going to show how we can execute phishing attack through an example. We will be using Kali Linux to demonstrate these examples. Note the shown examples are for the education purpose only.

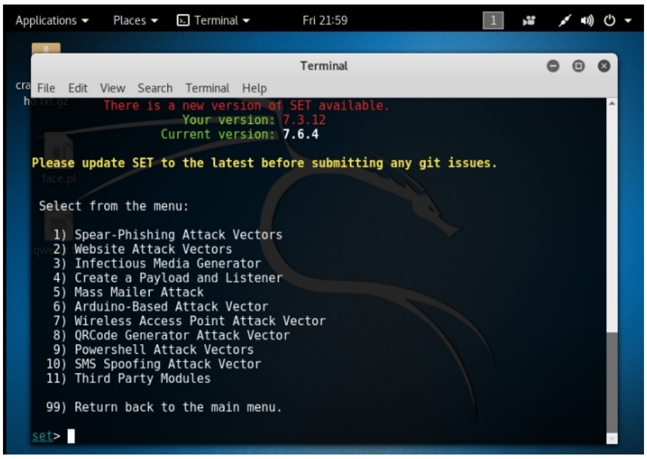
Phishing attack using Social Engineering Toolkit[6]. Social engineering toolkit or SET is a toolkit provided under the Kali Linux. Kali Linux is distribution of the Linux Operating System dedicated toward the penetration testing. Social engineering toolkit or SET is a toolkit provided under the Kali Linux. Kali Linux isdistribution of the Linux Operating System dedicated toward the penetration testing. So to do this following steps are involved:

a) First open Kali Linux followed by opening Terminal. Type the command "ifconfig" to get our IP address because that's the place where we want to send the data. The underlined inet is our IP addresses so next copy the IP address.

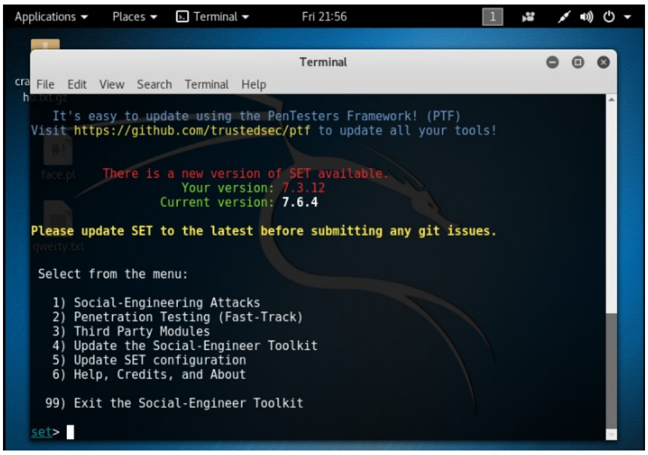


```
root@arpankali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 192.[redacted]  netmask 255.255.255.0  broadcast 192.168.72.255
        inet6 fe80::20c:29ff:fe4c:45dc  prefixlen 64  scopeid 0x20<link>
        ether 00:0c:29:4c:45:dc  txqueuelen 1000  (Ethernet)
        RX packets 658  bytes 63016 (61.5 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 69  bytes 7079 (6.9 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0
        device interrupt 19  base 0x2000

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1  (Local Loopback)
        RX packets 24  bytes 1396 (1.3 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 24  bytes 1396 (1.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@arpankali:~#
```

b) Now open SET by clicking Applications >> Social Engineering Tools >> Social Engineering Toolkit or open terminal and then type se-toolkit and hit enter. We will see a list of options and out of those we have to choose "Social Engineering Attacks" to do this press 1 and hit enter.

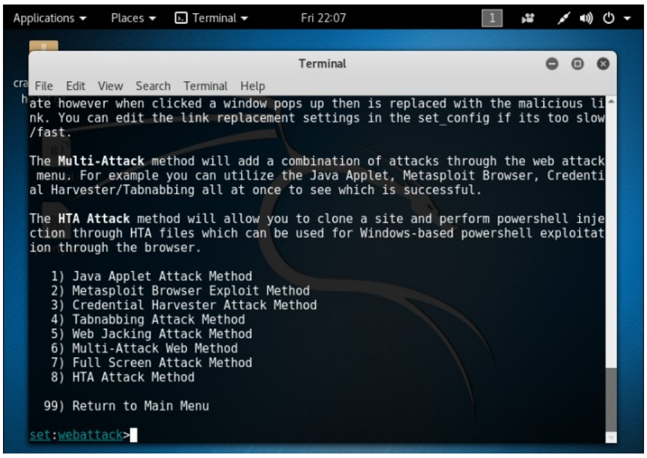


```
  There is a new version of SET available.
                    Your version: 7.3.12
               Current version: 7.6.4

Please update SET to the latest before submitting any git issues.

 Select from the menu:

   1) Spear-Phishing Attack Vectors
   2) Website Attack Vectors
   3) Infectious Media Generator
   4) Create a Payload and Listener
   5) Mass Mailer Attack
   6) Arduino-Based Attack Vector
   7) Wireless Access Point Attack Vector
   8) QRCode Generator Attack Vector
   9) Powershell Attack Vectors
  10) SMS Spoofing Attack Vector
  11) Third Party Modules

  99) Return back to the main menu.

set>
```

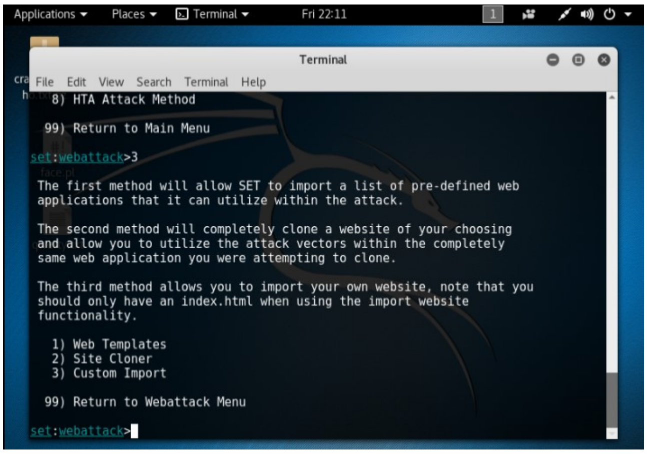


```
   It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

  There is a new version of SET available.
                    Your version: 7.3.12
               Current version: 7.6.4

Please update SET to the latest before submitting any git issues.

 Select from the menu:

   1) Social-Engineering Attacks
   2) Penetration Testing (Fast-Track)
   3) Third Party Modules
   4) Update the Social-Engineer Toolkit
   5) Update SET configuration
   6) Help, Credits, and About

  99) Exit the Social-Engineer Toolkit

set>
```

c) Select "Website Attack Vectors" by pressing 2 and hit enter. Under it select "Credential Harveseter Attack Method" by pressing 3 and hit enter. Since we are going to clone the Facebook website select "Site Cloner" option by typing 2 and hit enter.

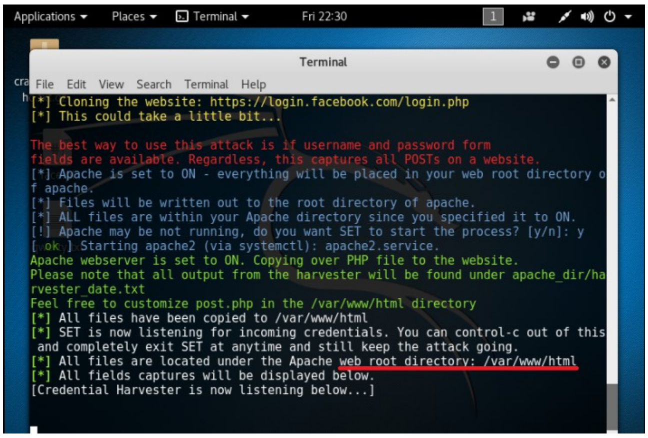


```
ate however when clicked a window pops up then is replaced with the malicious li
nk. You can edit the link replacement settings in the set_config if its too slow
/fast.

The Multi-Attack method will add a combination of attacks through the web attack
 menu. For example you can utilize the Java Applet, Metasploit Browser, Credenti
al Harvester/Tabnabbing all at once to see which is successful.

The HTA Attack method will allow you to clone a site and perform powershell inje
ction through HTA files which can be used for Windows-based powershell exploitat
ion through the browser.

   1) Java Applet Attack Method
   2) Metasploit Browser Exploit Method
   3) Credential Harvester Attack Method
   4) Tabnabbing Attack Method
   5) Web Jacking Attack Method
   6) Multi-Attack Web Method
   7) Full Screen Attack Method
   8) HTA Attack Method

  99) Return to Main Menu

set:webattack>
```



```
  8) HTA Attack Method

 99) Return to Main Menu

set:webattack>3

The first method will allow SET to import a list of pre-defined web
applications that it can utilize within the attack.

The second method will completely clone a website of your choosing
and allow you to utilize the attack vectors within the completely
same web application you were attempting to clone.

The third method allows you to import your own website, note that you
should only have an index.html when using the import website
functionality.

  1) Web Templates
  2) Site Cloner
  3) Custom Import

 99) Return to Webattack Menu

set:webattack>
```

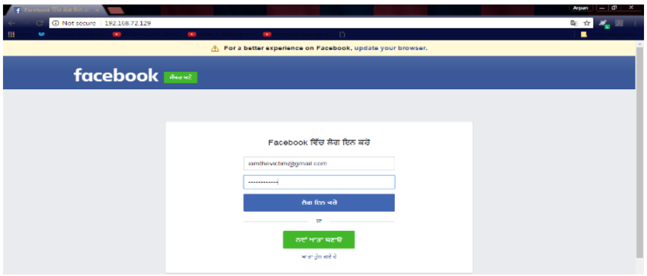
d) Now paste your IP address as told in step “a” and hit enter. Now it will ask for the URL you want to clone, as we want to clone Facebook so type http://www.facebook.com.Now it would start cloning the website it could take a while. After cloning the website it will show you the path were all the information is going to be stored. So the attack is live now and we are ready to go.



```
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] Apache is set to ON - everything will be placed in your web root directory o
f apache.
[*] Files will be written out to the root directory of apache.
[*] ALL files are within your Apache directory since you specified it to ON.
[!] Apache may be not running, do you want SET to start the process? [y/n]: y
[ ok ] Starting apache2 (via systemctl): apache2.service.
Apache webserver is set to ON. Copying over PHP file to the website.
Please note that all output from the harvester will be found under apache_dir/ha
rvester_date.txt
Feel free to customize post.php in the /var/www/html directory
[*] All files have been copied to /var/www/html
[*] SET is now listening for incoming credentials. You can control-c out of this
 and completely exit SET at anytime and still keep the attack going.
[*] All files are located under the Apache web root directory: /var/www/html
[*] All fields captures will be displayed below.
[Credential Harvester is now listening below...]
```

e) Now you can send this IP address to the victim through Facebook, Gmail or by any other mean but note this technique will only work when you and the victim are over the same network.

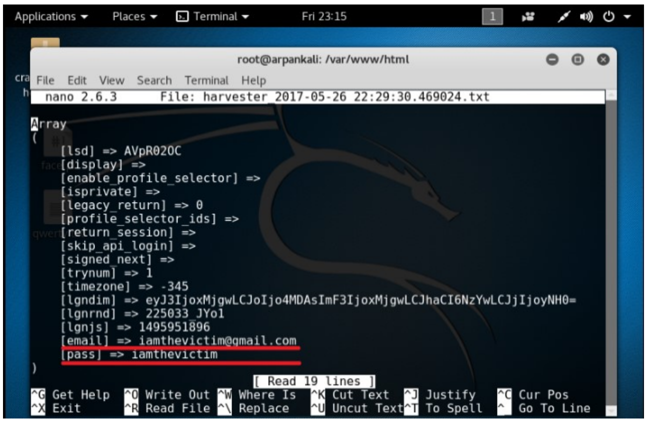
f) Now when the victim will open the link the following page will openand the victim enters his username say iamthevictim@gmail.com and password “iamthevictim” and the press login. The information will be send to the directory file of the Phisher and the victim will be the directed to the original Facebook login page. On opening the root directory file we can see the username and the password entered by the victim.


Not secure | 192.168.72.129

For a better experience on Facebook, update your browser.

Facebook ਵਿੱਚ ਲੌਗ ਇਨ ਕਰੋ

iamthevictim@gmail.com


Applications
Places
Terminal
Fri 23:15
root@arpankali: /var/www/html
File Edit View Search Terminal Help

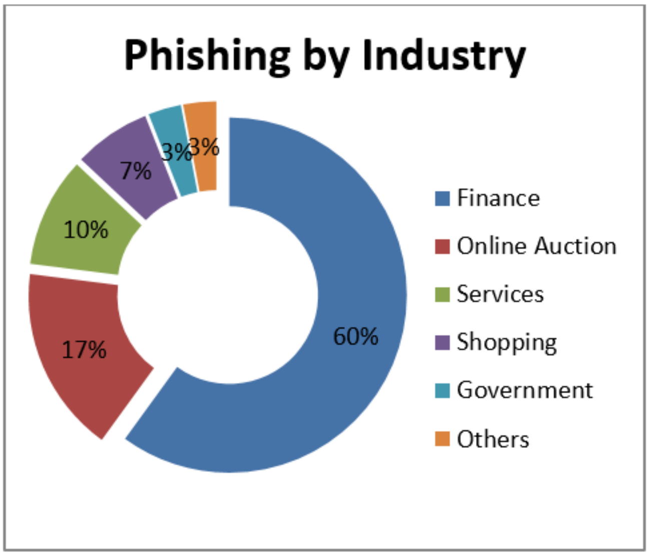
```
  nano 2.6.3       File: harvester_2017-05-26 22:29:30.469024.txt

Array
(
    [lsd] => AVpR02OC
    [display] =>
    [enable_profile_selector] =>
    [isprivate] =>
    [legacy_return] => 0
    [profile_selector_ids] =>
    [return_session] =>
    [skip_api_login] =>
    [signed_next] =>
    [trynum] => 1
    [timezone] => -345
    [lgndim] => eyJ3IjoxMjgwLCJoIjo4MDAsImF3IjoxMjgwLCJhaCI6NzYwLCJjIjoyNH0=
    [lgnrnd] => 225033_JYol
    [lgnjs] => 1495951896
    [email] => iamthevictim@gmail.com
    [pass] => iamthevictim
)
                        [ Read 19 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos
^X Exit       ^R Read File  ^\ Replace    ^U Uncut Text^T To Spell    ^  Go To Line
```

V. PHISHING ATTACKS FACTS AND STATISTICS

As per the data procured by Barkly

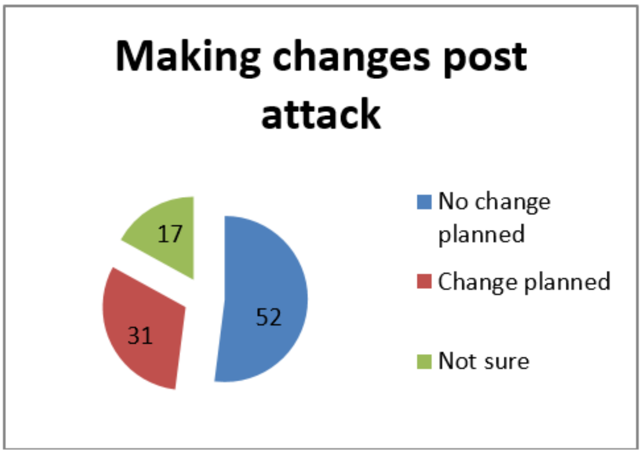
- New malware bred in 2016 was on average of 200,000 per day.
- 4000+ attacks of ransomware transpired everyday in the same year and these figures were 300% more than the previous year’s figures.
- Ransomware together with phishing jumped to 97.25% in the third quadrant of 2016 from 92% in the first quadrant of the same year.

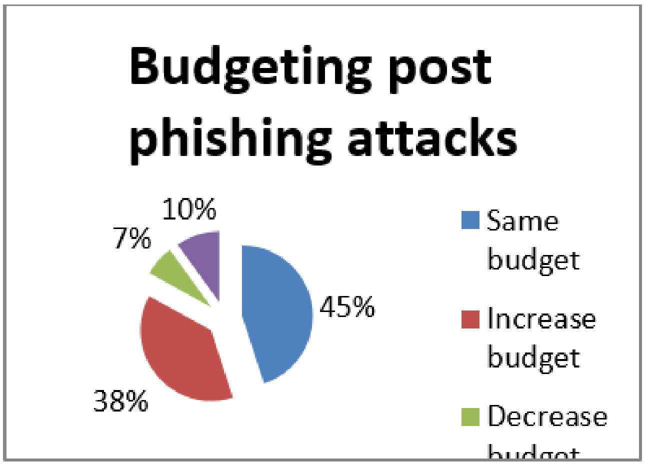
The companies being targeted by the phishers are shown in the circular chart.



Changes are being brought to curb these cyber security attacks by most of the companies

About 52% companies who were the victims of phishing attacks during 2016 are still not ready to mend their security systems. While 17% are in dilemma of what actions to take, the remaining 31% firms are making the changes effective immediately. Also these victim companies are bringing about changes in the budget for cyber security as shown in the second pie chart





VI. CONCLUSIONS

Phishing attack is one of the largest and fastest growing cyber crime and one must be aware of the the types of attack can be conducted on him and how to protect self from these threats. Although many laws have been given by the government and educating people is the best defence against phishing attacks. Being a bit suspicious of all electronic communications and websites is recommended. Also, one must pet the habit of comparing the provided URL with the an independent search for the company's website ie. Compare the provided mail with the companies' original URL.

VII. ACKNOWLEDGMENTS

I would like to take this opportunity to express my profound gratitude and deep regard to my Mr. Deo Prakash, for his exemplary guidance, valuable feedback and constant encouragement throughout the duration of the project. His valuable suggestions were of immense help the roughout my project work. His perceptive criticism kept me working to make this project in a much better way. Working under him was an extremely knowledgeable experience for me.

VIII.REFERENCES

[1] Junaid Ahsenali Chaudhry, Shafique Ahmad Chaudhry, Robert G. Rittenhouse,2016, Phishing

attacks and defences, International Journal of Security and Its Applications V ol. 10, No. 1 (2016), pp.247-256

[2] Mohd. Mahmood Ali, Owais A.W. Siddiqui, Mohd. Nayeemuddin and Lakhsmi Rajamani, 2015, An approach for Deceptive Phishing Detection and Prevention in Social Networking Sites Using Data Mining and WordNet Ontology.

[3] “what are the various types of phishing?”; google help; http://www.phishing.org/phishing-techniques

[4] “keylogger” http://www.webopedia.com/TERM/K/keylogger.html

[5] Mahmoud Khonji, Youssef Iraqi, Senior Member, IEEE, and Andrew Jones,2013, Phishing Detection: A Literature Survey

[6] Arpan chandel.et.al. Phishing attacks and its countermeasures, 2017, IJARC.