On Effectiveness of Various Browsers in Phishing Detection: An analysis

Madhuresh Mishra, Gaurav, Anurag Jain

Abstract -Phishing is a method of obtaining confidential information of victim using fraudulent websites that appear to be legitimate. It is affecting all the major sectors of industry day by day with a lot of misuse of user credentials. Seeing a lot of ill effects of phishing attacks various browsers has started using different anti-phishing strategies as one of their security shield. In this paper we have analyzed comparative effectiveness of various browsers like Google chrome, Mozilla Firefox, internet explorer and opera, in detection of phishing attacks**.**

Index term-phishing, anti-phishing

1. INTRODUCTION

The primary purpose of phishing is to illegally carry out fraudulent financial transactions on behalf of users using a forged email that contains a URL pointing to a fake web site masquerading as an online bank or a government entity. A phisher may lure a victim into giving his/her Social Security Number, full name, & address, which can then be used to apply for a credit card on the victim's behalf [1].

Attacker uses replica of original website as a bait that is send to the user. When user grabs the bait by filling and submitting his useful information attacker pulls the bait means saves the data for its own use illegally.

In general, phishing attacks are performed with the

following four steps[2]:

1) A fake web site which looks exactly like the legitimate Web site is set up by phished

2) Phisher then send link to the fake web site in large amount of spoofed e-mails to target users in the name of legitimate companies and organizations,

3) Trying to convince the potential victims to visit their web sites.

4) Victims visit the fake web site by clicking on the link and input its useful information there.

5) Phishers then steal the personal information and perform their fraud such as transferring money from the victims' account.

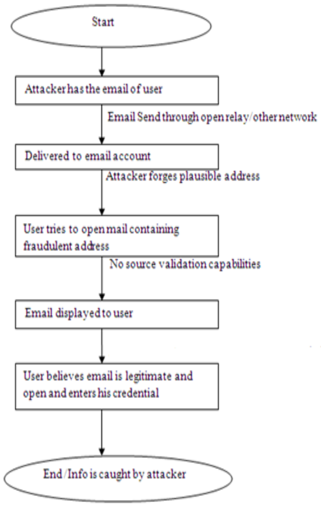

Start
Attacker has the email of user
Email Send through open relay/other network
Delivered to email account
Attacker forges plausible address
User tries to open mail containing fraudulent address
No source validation capabilities
Email displayed to user
User believes email is legitimate and open and enters his credential
End/Info is caught by attacker

Fig.1: flow chart of phishing attack.

There are a lot of fake phishing websites created and uploaded online every day, luring a number of customers. According to a phishing activity trend report published by Anti-phishing working group on 23 Dec 2011, a lot of phishing attacks were done in first half of year 2011 as can be seen from fig 2. The number of unique phishing reports submitted to APWG in H1, 2011 reached a high of 26,402 in March, dropping to the half year low of 20,908 in April[3].

Madhuresh mishra belongs to university school of information technology,GGSIPU Delhi,lordmacrolle@gmail.com
Gaurav belongs to university school of information technology,GGSIPU Delhi,gaurav.baksas@gmail.com
Anurag jain belongs to university school of information technology,GGSIPU Delhi,lordmacrolle@gmail.com

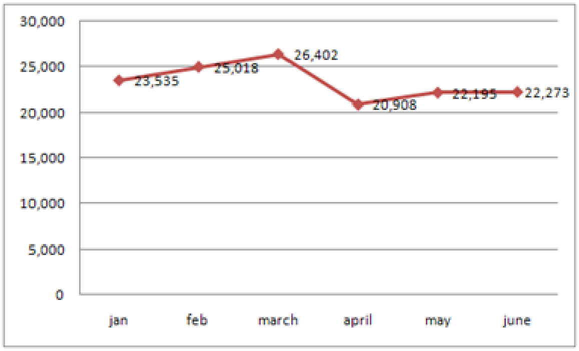


Fig 2: phishing attacks done in first half of year 2011.

The report also stated that Financial Services continued to be the most targeted industry sector in the first half of 2011[3] as can be seen from figure 3.

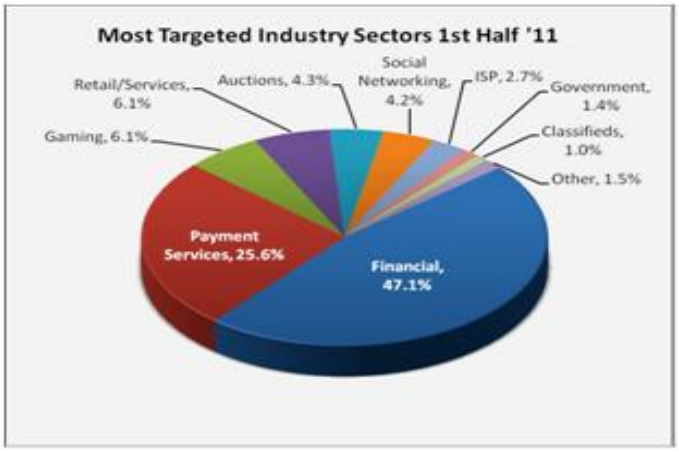


Fig 3: Industry sector area wise affect of Phishing [3]

As it can been from the above figure that financial service sector and payment service sector is targeted most and financial service sector and payment service sectors deals with money transactions ,so it can be concluded that main objective of phishes is to steal financial details of victims and misuse that for their own gain. Retail sector appears to be third most vulnerable and classified as the least vulnerable to phishing attacks.

So phishing attacks are emerging as one of the major area where immediate concern is needed as it is affecting all the major sectors of industry creating a lot of loss.

2. LITERATURE SURVEY

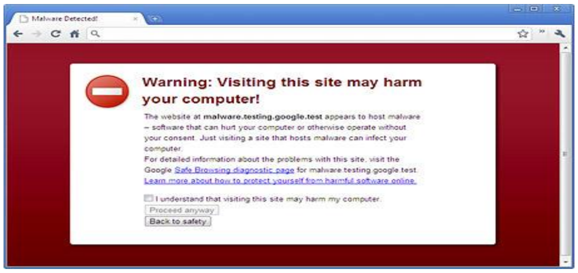
Today there are many browsers available in market with great functionalities. Each browser has its own unique services and qualities. In regard to ability in detection of phishing attacks each browser follows its own strategies and policies. The details of technique/procedure used in phishing detection by different browsers are given below:

1. Chrome

Google Chrome uses technologies such as Safe Browsing, sandboxing, and auto-updates against phishing and malware attacks [4].

1. a.Safe Browsing

Chrome shows a warning message before a site that is suspected of containing malware or phishing is visited. With Safe Browsing technology enabled in Chrome, if a website suspected of containing phishing or malware is suspected as we browse the web, a warning page like the one below is shown.



Warning: Visiting this site may harm your computer!

The website at **malware.testing.google.test** appears to host malware – software that can hurt your computer or otherwise operate without your consent. Just visiting a site that hosts malware can infect your computer.

For detailed information about the problems with this site, visit the Google Safe Browsing diagnostic page for malware.testing.google.test.

Learn more about how to protect yourself from harmful software online.

☐ I understand that visiting this site may harm my computer.

Proceed anyway

Back to safety

Fig 4:warning message shown by google chrome

According to http://support.google.com/chrome Safe Browsing works in two ways. First, the link of visited page is matched with the downloaded list of phished pages maintained by Google and if the match is found the page is considered is phished else browser contacts Google server to provide more information by analyzing contents of the webpage.

1.b.Sandboxing

Sandboxing helps prevent malware from installing itself on computer or using what happens in one browser tab to affect what happens in another. The sandbox adds an additional layer of protection to browser by protecting against malicious web pages that try to leave programs on computer, monitor web activities, or steal private information from hard drives [4].

1. c.Auto-updates

Chrome checks for updates regularly to make sure that it's always kept up-to-date. The update check ensures that user's version of Chrome is automatically updated with the latest security features and fixes without any action required on user part [4].

Following message are shown when chrome found something suspicious on site

Message: Something's Not Right Here!

Appears when Google Chrome detects that the site you're trying to visit may have malware.

Message: Suspected phishing site!

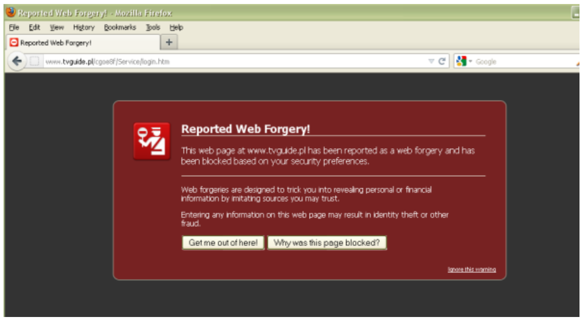
Appears when Google Chrome detects that the site you’re trying to visit is suspected of being a phishing site.

2. MOZILLA

Firefox 3 or later contains built-in Phishing and Malware Protection. These features generates warning when user visits a page that has been reported as a Web Forgery of a legitimate site [5]

Phishing and Malware Protection works by checking the sites visited against lists of reported phishing and malware sites. These lists are automatically downloaded and updated every 30 minutes or so when the Phishing and Malware Protection features are enabled [5].

Google provides data for the anti-phishing feature implemented in Firefox. These clients get their blacklist and whitelist data using an "update protocol".


Reported Web Forgery! - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Reported Web Forgery!
www.tvguide.pl/cgoe8f/Service/login.htm
Google
Get me out of here!
Why was this page blocked?
Ignore this warning

Reported Web Forgery!

This web page at www.tvguide.pl has been reported as a web forgery and has been blocked based on your security preferences.

Web forgeries are designed to trick you into revealing personal or financial information by imitating sources you may trust.

Entering any information on this web page may result in identity theft or other fraud.

Fig 5: warning message shown by Mozilla

3. OPERA

Opera also checks the visited sited against the list of suspected sites that has been previously created.

The server used for Opera’s Fraud and Malware Protection does not save IP address or any other information related to user identity[6]. There are no cookies related to the use of this feature. By default, Opera Fraud and Malware Protection is enabled. With Opera Fraud and Malware Protection enabled, the domain name of websites visited is sent to Opera’s Fraud and Malware Protection server together with a hash of the domain name. HTTPS sites are checked via an encrypted channel, while IP addresses on the local intranet will never be checked [6].

URLs containing characters that are not allowed in the server name, such as exclamation marks, parentheses, and so on, are blocked for security reasons[6]. Opera's list of illegal characters is slightly longer than the official IDNA list An internationalized domain name (IDN) is an Internet domain name that contains at least one label that is displayed in software applications, in whole or in part, in a language-specific script or alphabet[6]

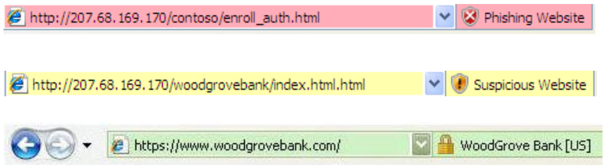
4. INTERNET EXPLORER

Previous version of internet explorer that is IE 6 was launched with the lack of capability of detecting phishing attacks.

When IE 7 was launched, it was an upgrade to IE 6 with addition of phishing filter. When you visit a Web site, IE7 first checks the local 'safe list'. The locally stored data is a list of 'safe sites' that is downloaded and installed by Internet Explorer 7. If the URL is there or it appears in the local cache, it represent something suspicious is there [7].

If, on the other hand, the site is not in those lists then the users must opt in to use the Phishing Filter. If the user decides to enable the Phishing Filter, IE will then transmit details of the URL being visited for checking. Also, from that time on, IE7 will maintain a dynamic cache of sites that have already been checking by the Phishing Filter for a certain period of time [7].

Internet Explorer 7 introduces a new notification area called the Security Status Bar. If a web site is a known phishing site the Address Bar turns red. If a web site is a suspected phishing site, the Address Bar turns yellow. High trust, legitimate sites will display a green Address Bar [7].


http://207.68.169.170/contoso/enroll_auth.html
Phishing Website
http://207.68.169.170/woodgrovebank/index.html.html
Suspicious Website
https://www.woodgrovebank.com/
WoodGrove Bank [US]

Internet Explorer 8, display the entire URL in grey, with just the domain name itself in black, as a means of assisting users in identifying fraudulent URLs. Screenfilter[8] is used in IE 8 to detect phishing sites.

SmartScreen operates in the background as user browse the web, analyzing webpages and determining if they have any characteristics that might be suspicious. If it finds suspicious webpages, SmartScreen will display a message giving an opportunity to provide feedback and advising user to proceed with caution[8].

SmartScreen Filter checks the sites visited against a dynamic list of reported phishing sites and malicious software sites governed by Microsoft service agreement. If it finds a match, SmartScreen Filter will show a red warning notifying that the site has been blocked for safety[8].

3. REPORTS AND ANALYSIS

We collected 60 links that were reported as phished link at www.millersmiles.co.uk.The links were collected for 8 days from 29th feb 2012 to 7th mar 2012. We executed these links on various browsers to check their capability in detection of phishing attack. on the basis of result obtained we performed individual and comparative analysis as follows.

A. INDIVIDUAL ANALISYS

1. Chrome 17.0.963.78 m

Total Links	Detected as phished	Not detected as phished	Page not found
60	37	10	13

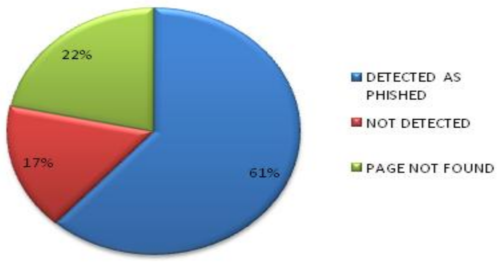


Fig 6: pie chart for Google chrome 17.0.963.78 m

from the above figure we can see 61.66 % of checked links were detected as phished by Google chrome and 16.66% links were not detected by Google chrome that were reported as phished one by www.millersmile.co.uk 21.66% links were not found on server.

2. Mozilla 10.0.2

Total Links	Detected as phished	Not detected as phished	Page not found	Access denied
60	26	8	21	5

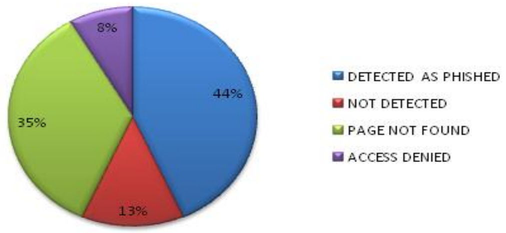


Fig 7: pie chart for Mozilla 10.0.2

As can be seen from above figure 44 % of checked links were detected as phished by Mozilla Firefox v10.0.2 and 13% links were not detected by Mozilla Firefox v10.0.2 that were reported as phished one by www.millersmiles.co.uk, 35% links were not found on server and access was denied on 8% of total checked links.

3.Internet Explorer 6

Total Links	Detected as phished	Not detected as phished	Page not found	Access denied
60	0	13	40	7

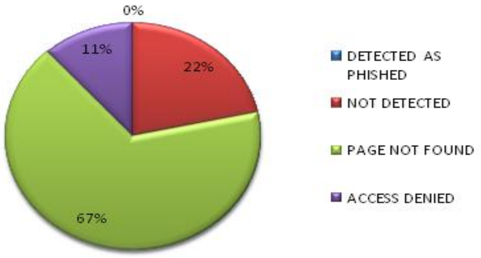


Fig 8:pie chart for internet explorer 6

from the above figure we can see 67 % of checked links were detected as phished by IE 6 and 22 % links were not detected by IE 6 that were reported as phished one by www.millersmiles.co.uk 67 % links were not found on server

4.Internet Explorer 7

Total Links	Detected as phished	Not detected as phished	Page not found	Access denied
60	25	13	17	5

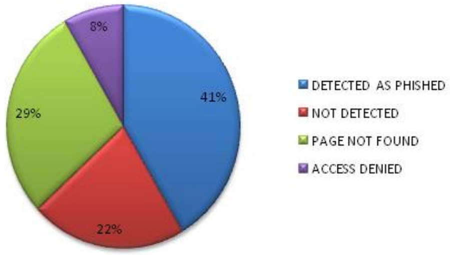


Fig 9: pie chart for internet explorer 7

As can be seen from above figure 41 % of checked links were detected as phished by IE 7 and 22 % links were not detected by IE 7 that were reported as phished one by www.millersmiles.co.uk, 29 % links were not found on server and access was denied on 8% of total checked links.

5.Opera 11.61

Total Links	Detected as phished	Not detected as phished	Page not found	Access denied
60	13	18	25	4

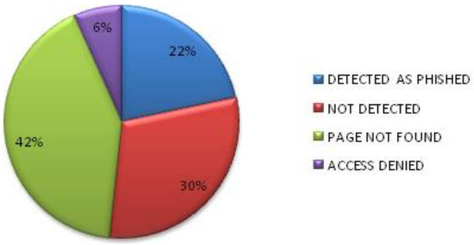


Fig 10: pie chart for opera 11.61.

As can be seen from above figure 22 % of checked links were detected as phished by opera 11.61 and 30 % links were not detected by opera 10.61 that were reported as phished one by www.millersmiles.co.uk,42 % links were not found on server and access was denied on 6% of total checked links.

B.COMPARATIVE ANALYSIS OF ALL

total links	detected by chrome	detected by Mozilla 10.0.2	detected by ie 6	detected by ie 7	detected by opera 11.61
60	37	26	0	25	13

Maximum no. of links that is 61% were detected by Google chrome and minimum no. of links that is 0% were detected by IE 6. IE 7 was capable of detecting 41% of the phished linked and 43%,21%,detection was reported by Mozilla 10.0.2 and opera 11.61 respectively.

4. CONCLUSION AND FUTURE WORK

From the above study we can see that various browsers following different approach for phishing detection differs in their capabilities in phishing detection. Some follows blacklist and whitelist maintained at servers and some follows checking of content of web page visited in phishing detection. The one following blacklists appears to be good in phishing detection. From the above result analysis we can conclude that goggle chrome appears to have maximum detection capability rate and IE 6 appears to be worst in detection of phishing attacks.

As a future work we can focus on improvement of techniques used in phishing detection to increase detection rate. Preventive measures are also effective in curbing phishing attacks.

5.REFERENCES.

1. 1. Hicham Tout, William Hafner "Phishpin: An identity-based anti-phishing approach" in proceedings of international conference on computational science and engineering, Vancouver, BC, pages 347-352, 2009 .
2. Gaurav, Madhuresh Mishra, Anurag Jain "Anti-Phishing Techniques: A Review" in/ International Journal of Engineering Research and Applications (IJERA) Vol. 2, Issue 2,Mar-Apr 2012, pp.342-347
3. Phishing activity trend report 1st half /2011,http://www.antiphishing.org.
4. http://support.google.com/chrome
5. http://www.mozilla.org/en-US/firefox/phishing-protection/
6. http://windows.microsoft.com/en-IN/windows-vista/Phishing-Filter-frequently-asked-questions
7. http://windows.microsoft.com/en-US/windows7/SmartScreen-Filter-frequently-asked-questions
8. www.millersmiles.co.uk.