International Journal of Computer Networks and Applications (IJCNA)
Volume 3, Issue 3, May – June (2016)

RESEARCH ARTICLE

TabSecure: An Anti-Phishing Solution with Protection against Tabnabbing

Priyanka Joshi
Computer Engg., PIIT, New Panvel, Mumbai University, India.
pjoshi02@student.mes.ac.in

Madhumita Chatterjee
Computer Engg., PIIT, New Panvel, Mumbai University, India.
mchatterjeee@mes.ac.in

Abstract – With an upsurge in the use of internet, there are various attacks being launched every day. These attacks target the vulnerabilities of various computer resources, such as, the operating system, web browsers, toolbars, etc. along with the susceptibility of the users due to lack of awareness about the possible scams. The existing solutions suffer various drawbacks. The website phishing solutions fail when JavaScript is used in the webpage. The email phishing solution propose use of a special web browser instead of the existing popular ones, in order to secure the user from phishing emails. The tabnabbing solutions follow visual cues which are prone to false negatives. The proposed approach aims to resolve these issues and provides a solution to phishing through websites, email phishing and tabnabbing using web browser monitor and an email phishing detection module that uses Bayesian classifier, but in a way different from the way it was used in a solution proposed earlier. The system keeps sending popups to the user until the user closes the phishing page detected by the system, hence reducing the chance of the user getting masqueraded.

Index Terms – Phishing, Tabnabbing, Browser monitor, Deceptive phishing.

1. INTRODUCTION

Phishing is a form of social engineering in which an attacker attempts to deceptively retrieve genuine users' sensitive identifications by imitating electronic communications from a reliable organization in an automated fashion. Baking sites and social networking sites are major targets of the attackers. Since it is easy to acquire sensitive information from both the kinds of sites, that financial and personal. These attacks are launched through emails or links to fake websites. [1] According to APWG Trends Report Q2 2013, the number of brands targets by phishers reached an unparalleled high of 441 in April, breaking the old monthly record of 430 that was noted in November 2012. [2] According to Ihab Shraim, the canvas continues to develop as fraudsters find new victims in untapped markets by targeting more brands. During the second quarter of 2013, a total 639 unique brands were targeted by phishing attacks. This number topped the previous high of 614 seen in Q4 2012 [3]. According to APWG report, they identified 27,253 (28.6%) domains that were registered maliciously, by phishers.

1.1. Purpose Of Phishing Attacks

The impetuses and financial rewards for phishing have changed and will continue to evolve in the future. The most common purpose of phishing attacks include: [4]

a. Stealing login credentials: This is majorly targeted on e-commerce sites such as Amazon or ebay.

b. Stealing banking credentials: The purpose behind such attack is obvious financial gains. This also includes sneaking into credit card details such as CVV no., card expiry date, card no. etc.

c. Capturing personal details: This includes stealing the address and other personal contact details and selling to some marketing companies at an exorbitant cost.

d. Theft of a firm's confidential data: This is majorly done to steal trade secrets and proprietary information of a firm to cause financial or good-will losses.

e. Installing botnets and DDoS agents on unsuspicious systems. These agents in combination with spear phishing can prove to be an entry point for the attacker into a private network.

1.2. Motivation

Attack vectors used to launch phishing attacks: [5]

a. Man-in-the-middle attack

b. Cross-site scripting (XSS)

c. Session hijacking

d. URL Obfuscation

e. (Consumer) Data theft

f. Attack through security loopholes on the client-side.

g. DNS poisoning

h. Hidden frames

Study showed that the attackers these days make use of user trust and fear to make their phishing attacks a success. The tabnabbing attack makes use of the same principle. The attacker keeps a watch on user's browser and see whether the pages has lost focus for more than some interval of time and then replaces that tab with malicious webpage to gain credentials of the user. For email phishing also, the naïve user never checks for the sender's address. The links that are sent through the emails are also misleading and the user does not check the address to which it has been redirected and falls prey to the attack. [6] Traditional spam filters are insufficient in detecting uninvited emails, and this causes consumers and businesses wishing to do business online to be reluctant and insecure. [7] With an upsurge in the use of internet, there are various attacks being launched every day. These attacks target the vulnerabilities of various computer resources, such as, the operating system, web browsers, toolbars, etc. along with the susceptibility of the users due to lack of awareness about the possible scams. [8]

The main motive behind implementing our proposed system is to notify the user against the potential phishing attempt. The browser monitor module of the system helps in doing this.

2. LITERATURE SURVEY

Engin Kirda et.al, [1] in their paper present a browser extension called AntiPhish that aims to protect users against impersonated web site-based phishing attacks. The system tracks the sensitive information of a user through an automated form filler and also keeps track of the domain to which that information is being sent. It generates warnings whenever the user attempts to transmit this information to a web site that is considered untrusted. The trust of the website is determined by the database of previous forms filled by the form filler. This may cause high amount of false-positives.

Sophie Gastellier-Prevost et.al, [10] propose a dual approach to provide an anti-pharming protection integrated into the client's browser. This approach performs an IP address check as well as a webpage content analysis, using the information provided by multiple DNS servers. In this approach, the source codes of the web pages obtained from the default DNS and the third party DNS respectively are compared word by word to check the amount of similarity between the two pages. Higher the amount of similarity, more the page is legitimate, else it is considered suspicious.

Aanchal Jain et.al, [11] propose a web browser which can be used as an agent to process each arriving email for phishing attacks. The browser scans the email before it is opened by the user. The email is checked for visible links, invisible links and mismatching links, and a count of each of these is maintained. If the count of invisible and mismatched links is greater than 0, then the user is intimated that the email is suspicious.

Aza Raskin [12] proposed the firefox manager similar to an automated form filler application that provides login details after once recorded. When users' login information doesn't appear; they may notice it as a suspicious page. It can be combined with the password manager.

Rableen Kaur Suri et.al [13], in their paper proposes the signature based detection mechanism to handle tabnabbing attack. The signatures are based on Javascript events such as onmouseover, onmouseout, onblur, onfocus, which are used along with iframes.

Philippe De Ryck et.al, [14] proposed a system that captures the appearance of each tab at regular intervals. It compares both the appearances and highlights the parts that were changed, allowing the user to distinguish between legitimate changes and malicious ones.

3. PROPOSED MODELLING

Our solution handles phishing attack launched through fake websites and deceptive emails. It is also be capable of handling the latest launched phishing attack, called tabnabbing.

3.1. Proposed System Architecture

The idea is to create a complete anti-phishing solution, which protects the user against phishing websites, phishing e-mails and tabnabbing. Our proposed system architecture consists of three modules viz. Phishing website detection, Tabnabbing detection and Email phishing detection module, as depicted in the figure below. Figure 1. Shows the system architecture of the proposed system.

3.1.1. Module 1: Phishing Website Detection

This module communicates with the Browser monitor engine. Figure 2. Shows flowchart of phishing website detection module. Each module of this architecture works independently. The interaction of each module is with the databases or source codes of the web pages. The database used for the system is a downloaded version of phishtank database openly available. [15]

3.1.2. Browser monitor engine:

This module watches the activities of the browser. It uses a dual approach. IP address check as well as web page content analysis. Each time the user enters a URL in the address bar; the URL is checked with a database of phishing sites. If a matching entry is not found in the database, then the source code of the page is checked for non-matching URLs, IP-based URLs, etc.

When a URL is entered in the address bar, the browser monitor is invoked. The browser monitor then queries the phishing database to check whether or not a match is found. If a match is not found then the browser monitor invokes the feature detection engine.

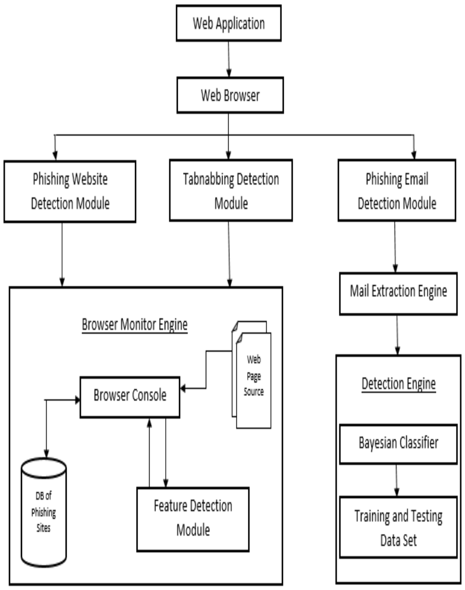


Figure 1. Proposed System Architecture

3.1.3. Feature Detection Engine:

This module traverses the source code of the page, which is checked for the following properties:

- Mismatching href tag and link text

3.2. Module 2: Phishing E-mail Detection:

It is very easy to obtain email address of targeted victims through social media since they are kept publicly available. So, with these, the attacker sends phishing emails to the attacker. [1] There are numerous features are used by major spam filters to detect unwanted emails. Some of these features are already used in spam filters.

- IP-based URLs
- Long URLs
- Number of dots

Figure 3 shows the flowchart of phishing email detection module.

3.2.1. Mail Extraction Engine:

Phishing mail detection module requires the mails to be extracted and zipped. Mail extraction engine does this work. Emails are extracted from the mail box and are then converted to a .txt file. Once the mails are extracted, they are sent to the Detection engine.

3.2.2. Detection Engine:

This module uses Bayesian Classifier to separate the mails as phishing and non-phishing. Detection engine relies on training set for detection of phishing emails.

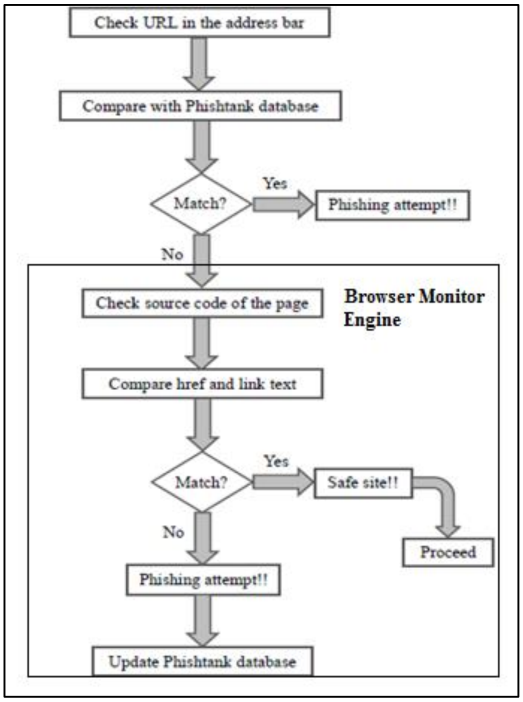

Check URL in the address bar
Compare with Phishtank database
Match?
Yes
Phishing attempt!!
No
Browser Monitor Engine
Check source code of the page
Compare href and link text
Match?
Yes
Safe site!!
Proceed
No
Phishing attempt!!
Update Phishtank database

Figure 2. Flowchart for phishing website detection

The emails to be segregated as phishing or legitimate are placed in testing set. Bayesian Classifier has been used earlier with a different approach, to the best of my knowledge. The corpus of mails is available on the internet. The system is trained on the basis of following properties:

-Requires urgent actions
-Generic greetings
-Links to fake website
-Poor grammar
-Request for personal credentials
-Unbelievable offers

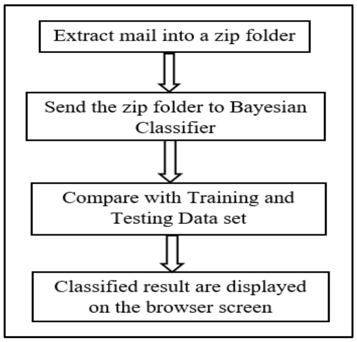
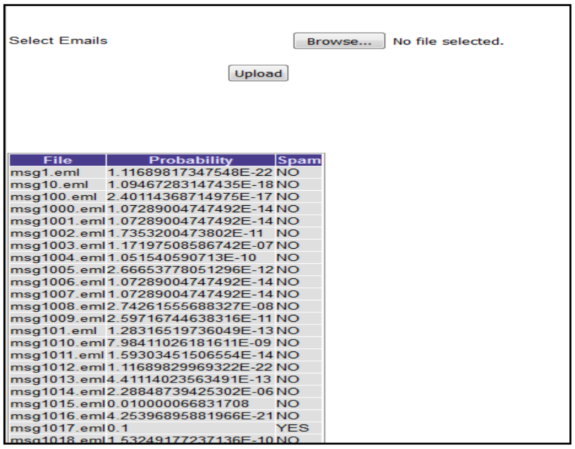

Extract mail into a zip folder
Send the zip folder to Bayesian Classifier
Compare with Training and Testing Data set
Classified result are displayed on the browser screen

Figure 3. Flowchart for detecting E-mail phishing

The zipped mails are sent to the testing set. They are placed into two folders, "phishing" and "nonphishing", temporarily. Once the classification results are displayed, both the folders are emptied to free the space temporarily consumed. Figure 4. Shows the results of phishing emails displayed on the browser window.



File	Probability	Spam
msg1.eml	1.11689817347548E-22	NO
msg10.eml	1.09467283147435E-18	NO
msg100.eml	2.40114368714975E-17	NO
msg1000.eml	1.07289004747492E-14	NO
msg1001.eml	1.07289004747492E-14	NO
msg1002.eml	1.7353200473802E-11	NO
msg1003.eml	1.17197508586742E-07	NO
msg1004.eml	1.051540590713E-10	NO
msg1005.eml	2.66653778051296E-12	NO
msg1006.eml	1.07289004747492E-14	NO
msg1007.eml	1.07289004747492E-14	NO
msg1008.eml	2.74261555688327E-08	NO
msg1009.eml	2.59716744638316E-11	NO
msg101.eml	1.28316519736049E-13	NO
msg1010.eml	7.98411026181611E-09	NO
msg1011.eml	1.59303451506554E-14	NO
msg1012.eml	1.11689829969322E-22	NO
msg1013.eml	4.41114023563491E-13	NO
msg1014.eml	2.28848739425302E-06	NO
msg1015.eml	0.010000066831708	NO
msg1016.eml	4.25396895881966E-21	NO
msg1017.eml	0.1	YES
msg1018.eml	1.53249177237136E-10	NO

Figure 4. Classification of mails as phishing and non-phishing

3.3. Module 3: Tabnabbing Protection:

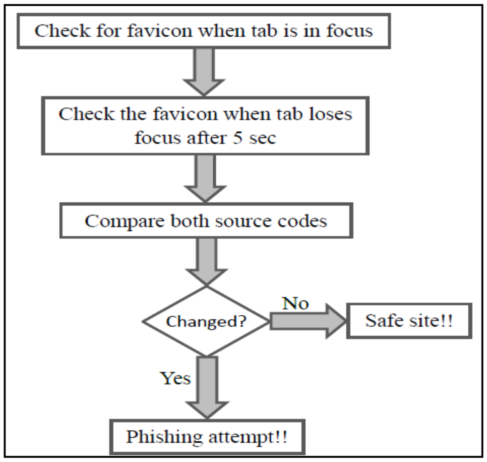
Tabnabbing is a deceptive phishing attack that fools a user into believing a fake website as a legitimate website. A user navigates to a normal looking site. The attacker detects when the page has lost its focus and hasn't been interacted with for a certain time interval. The favicon of the originally opened site is replaced with a favicon of a cloned website. The title is kept absolutely similar to the legitimate page that is cloned, and the page is replaced by the cloned page. [17] This can all be easily done with a little bit of JavaScript. As the user scans their many open tabs, the favicon and title act as a strong visual cue and the user will, many a times, simply think they left a legitimate tab open. Figure 6. shows flowchart of tabnabbing protection module. Table 1 shows comparison of methods used by existing solutions for tabnabbing protection.

Figure 5. A seemingly innocuous page on the left performs a tabnabbing attack once the user switches focus, resulting in the page on the right [16]

Table 1. Comparison of methods used by existing solutions for tabnabbing protection

Title	Method
NoTabNab	Mozilla password manager.
Approach to perceive Tabnabbing	Signature based approach to detect tabnabbing.
TabShots	Compares appearance of each tab and highlights the parts that were changed.
Proposed Approach	Browser monitor

When they click back to the tab with fake contents, they will see the standard page of the original page, assume they have been logged out, and provide their details to log in. The attack succeeds on the perceived inalterability of tabs.



Check for favicon when tab is in focus
Check the favicon when tab loses focus after 5 sec
Compare both source codes
Changed?
No
Safe site!!
Yes
Phishing attempt!!

Figure 6. Flowchart for Tabnabbing

Unlike earlier methods that use browser account management and visual cues, this method relies on browser monitor that keeps a watch on each tab and notifies when there is a change in the content of the tab. If there is a change noticed then it is reported as a phishing attempt. Figure 7 shows a tabnabbing attack detected by our system.

Figure 7. Tabnabbing detection using browser monitor

4. RESULTS AND DISCUSSIONS

The implementation is in ASP.NET and SQL Server database.

Module 1: Phishing website detection:

The system is designed to detect phishing websites that are already listed in the phishing database as well as the ones that are not, but are potentially phishing websites.

A.1. Detection through database:

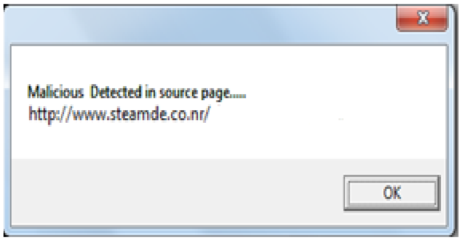
When the user enters the URL in the address bar, the system captures it and compares with the phishing database. If a match is found, then an alert is displayed in the message box. The message box keeps appearing till the user closes the tab.

A.2. Detection through source page:

The parameters that are used for the detection of phishing websites are as follows:

- Long URLs in the anchor tag
- Encrypted URLs
- External non-matching links
- URL based image source

Figure 8 shows a popup displayed by the system on detection of attack.



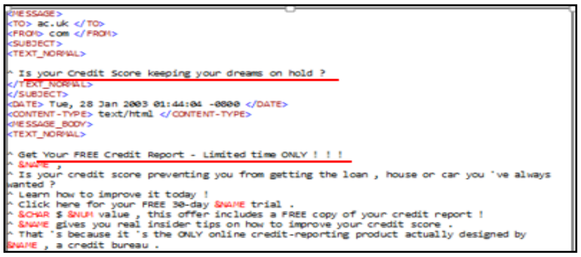
Malicious Detected in source page.....
http://www.steamde.co.nr/

Figure 8. Phishing site detection through phishing database

For testing purpose, a known malicious site was taken, and the entry from the database was erased. The system detected the site as malicious and displayed the alert.

Module 2: Email Phishing Detection:

The system is designed to learn from the training sets provided to the system.



```
<MESSAGE>
<TO> ac.uk </TO>
<FROM> com </FROM>
<SUBJECT>
<TEXT_NORMAL>

^ Is your Credit Score keeping your dreams on hold ?
</TEXT_NORMAL>
</SUBJECT>
<DATE> Tue, 28 Jan 2003 01:44:04 -0800 </DATE>
<CONTENT-TYPE> text/html </CONTENT-TYPE>
<MESSAGE_BODY>
<TEXT_NORMAL>

^ Get Your FREE Credit Report - Limited time ONLY ! ! !
^ &NAME ,
^ Is your credit score preventing you from getting the loan , house or car you 've always
wanted ?
^ Learn how to improve it today !
^ Click here for your FREE 30-day &NAME trial .
^ &CHAR $ &NUM value , this offer includes a FREE copy of your credit report !
^ &NAME gives you real insider tips on how to improve your credit score .
^ That 's because it 's the ONLY online credit-reporting product actually designed by
&NAME , a credit bureau .
```

Figure 9. Example of potential phishing attempts

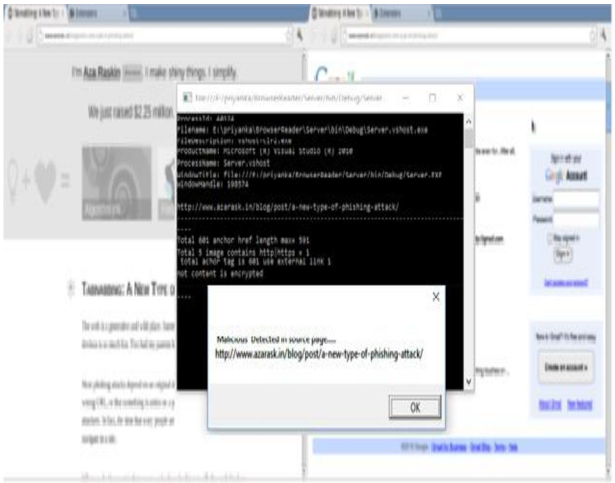
The above given Figure 9 shows a training example of a mail which is a potential phishing attempt. The system is trained using a large corpus which is freely available on the internet.

Module3: Tabnabbing Protection:

In this module, the expected functionality of the system is to generate a popup and warn the user of a phishing attempt if the content of the page change after the page has lost its focus. Table 2 shows a comparison of previously implemented approaches with proposed approach.

Table 2. Comparison of Existing Solutions to our proposed solution

Title	Email Phishing	Website Phishing	Tabnabbing
Protecting users against phishing: AntiPhish	×	✓	×
Dual approach to detect pharming attack	×	✓	×
Web Browser with phishing detection capabilities	✓	×	×
NoTabNab	×	×	✓
Approach to perceive Tabnabbing	×	×	✓
TabShots	×	×	✓
Proposed Approach: TabSecure	✓	✓	✓



```
ProcessId: 40174
Filename: E:\priyanka\BrowserReader\Server\bin\Debug\Server.vshost.exe
FileDescription: vshost-clr2.exe
ProductName: Microsoft (R) Visual Studio (R) 2010
ProcessName: Server.vshost
WindowTitle: file:///F:/priyanka/BrowserReader/Server/bin/Debug/Server.EXE
WindowHandle: 198374

http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/
---------------------------------------------------------------------------
----
Total 601 anchor href length max 591
Total 5 image contains http|https = 1
 total achor tag is 601 use external link 1
not content is encrypted
----
----
```

Malicious Detected in source page.....
http://www.azarask.in/blog/post/a-new-type-of-phishing-attack/

Figure 10. Detection due to content change in the tab

So, for this, the system checks the "onblur" events of JavaScript. The system gives desired results by generating a message box saying, "Malicious page detected in the source page…."

Each module of this architecture works independently. The interaction of each module is with the databases or source codes of the web pages. The implementation is in ASP.NET and SQL Server.

The literature survey and the discussion of the proposed system give us a complete idea, that there does not exist a complete solution that protects the user from website phishing, email phishing as well as tabnabbing. The survey is detailed and complete to the best of my knowledge.

The approach used for email phishing detection has been partially used earlier, but with a machine learning approach. On the other hand, our proposed system uses the Bayesian Classifier in conjunction with the Browser Monitor.

Also, the approach of Browser monitor has not been used so far for website phishing detection as well as tabnabbing protection. The system is evaluated to check whether the site detected as phishing is correct or not.

Mostly anti-phishing solution either provides relevant answer for the user query or it simply decides the site to be safe. It is more like a Hit or Miss System i.e. either we will get answer for a question or we won't get answer.

In Figure 12 the additional reading section depicts the phishing sites detected by the system correctly. These are the sites that were originally not mentioned in the database of phishing sites. These sites have been detected by the system due to various parameters such as URL based image sources, extremely long URLs, number of dots in the URL and unusual popups.

Site with illicit content detected:

In Figure 13 additional reading section show sites that are rated to contain illicit content. Without the proposed system in place, the sites were not flagged. But the system detected the site based on the no. of external links and URL based image sources.

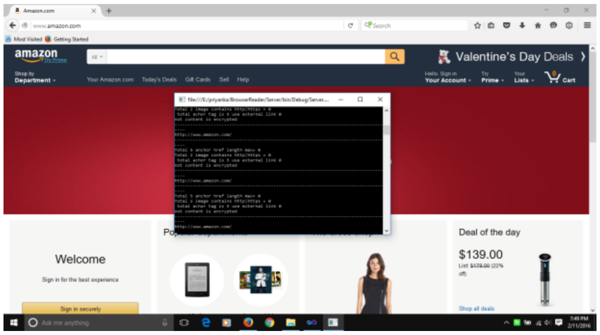
Site flagged to be a hacking site:

In Figure 12 addition reading section shows hacking sites. It was checked by the system and was found to contain all the features of potential phishing site. For this, the entries of these sites were removed from the database of phishing sites. The system could detect the site correctly as a phishing site.

In Figure 15 addition reading section show sites that look absolutely innocent, but actually is a phishing site. This site was found when searching on the internet. Without the system in place, the site was opened on the browser. But with the system in place, the site was detected to be a potential phishing site.

Testing a legitimate site:

For this, we took a few known legitimate sites and checked if the system could detect it correctly. We tested the system for Amazon.com and were found to be legitimate by the system. Figure 10 shows a legitimate site.


file:///E:/priyanka/BrowserReader/Server/bin/Debug/Server....

```
otal 1 image contains http|https = 0
 total achor tag is 5 use external link 0
not content is encrypted
-----------------------------------------------------------------------
----
http://www.amazon.com/
-----------------------------------------------------------------------
----
otal 5 anchor href length max= 0
otal 1 image contains http|https = 0
 total achor tag is 5 use external link 0
not content is encrypted
-----------------------------------------------------------------------
----
http://www.amazon.com/
-----------------------------------------------------------------------
----
otal 5 anchor href length max= 0
otal 1 image contains http|https = 0
 total achor tag is 5 use external link 0
not content is encrypted
-----------------------------------------------------------------------
----
http://www.amazon.com/
```

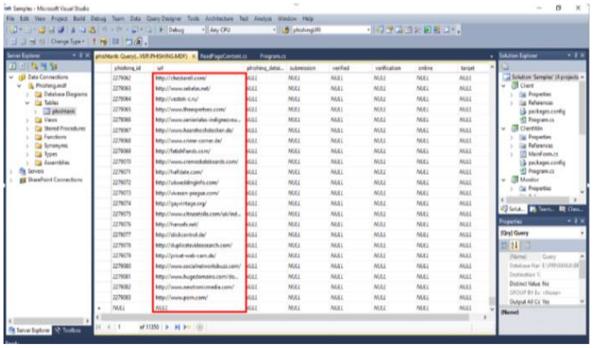
Figure 11. Amazon.com was checked and found legitimate

5. CONCLUSION

From all the discussion in the report, it can be clearly seen that protection against phishing is very important. The proposed solution TabSecure is a complete anti-phishing solution for a naïve user in order to detect phishing through fake websites, tabnabbing attack and email phishing. The browser monitor module makes it a strong solution to phishing since each activity of the browser is watched and any unusual event is reported to the user. The system was checked for over 500 sites. And the accuracy of the system was found to be 93%. The system can be implemented for android and other mobile OSs. The system can also be made as an entirely new framework that will support all the existing web browsers. This is not possible at the current point of time since the implementation requirements of each browser and the required framework for the same also differ.

ADDITIONAL READING

Sites detected by proposed system:


phishtank Query(...VER\PHISHING.MDF)

phishing_id	url	phishing_deta...	submission	verified	verification	online	target
2279062	http://checkerell.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279063	http://www.sebelas.net/	NULL	NULL	NULL	NULL	NULL	NULL
2279064	http://vostok-c.ru/	NULL	NULL	NULL	NULL	NULL	NULL
2279065	http://www.theexpertseo.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279066	http://www.senioriales-indignezvou...	NULL	NULL	NULL	NULL	NULL	NULL
2279067	http://www.haarehochstecken.de/	NULL	NULL	NULL	NULL	NULL	NULL
2279068	http://www.crime-corner.de/	NULL	NULL	NULL	NULL	NULL	NULL
2279069	http://fetishfiends.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279070	http://www.cremeskateboards.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279071	http://halfdate.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279072	http://ukweddinginfo.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279073	http://viveam-prague.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279074	http://gayvintage.org/	NULL	NULL	NULL	NULL	NULL	NULL
2279075	http://www.citrusetoile.com/uk/ind...	NULL	NULL	NULL	NULL	NULL	NULL
2279076	http://hansofx.net/	NULL	NULL	NULL	NULL	NULL	NULL
2279077	http://slickcontrol.de/	NULL	NULL	NULL	NULL	NULL	NULL
2279078	http://duplicatevideosearch.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279079	http://privat-web-cam.de/	NULL	NULL	NULL	NULL	NULL	NULL
2279080	http://www.socialnetworkbuzz.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279081	http://www.hugedomains.com/do...	NULL	NULL	NULL	NULL	NULL	NULL
2279082	http://www.newtonicmedia.com/	NULL	NULL	NULL	NULL	NULL	NULL
2279083	http://www.porn.com/	NULL	NULL	NULL	NULL	NULL	NULL
NULL	NULL	NULL	NULL	NULL	NULL	NULL	NULL

1 of 11350

Figure 12. The sites detected by the system

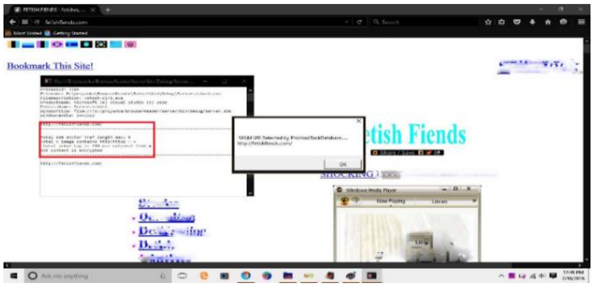


Figure 13. The sites containing illicit content

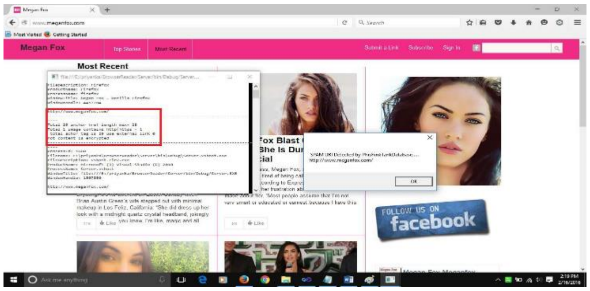


Figure 14. The site with long href tags and URL based Image sources

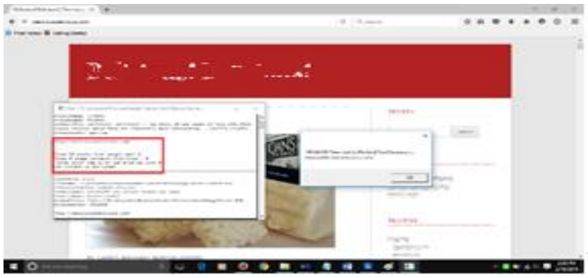


Figure 15. The site with long href tags and URL based Image sources

REFERENCES

[1] Joe, M. Milton, B. Ramakrishnan ,"A Survey of Various Security Issues in Online Social Networks", International Journal of Computer Networks and Applications Volume 1, Issue 1, November – December (2014).

[2] 2 Greg Aaron, Rod Rasmussen, "Phishing Activity Trends Report", Anti-Phishing Work Group (APWG), November 2013.

[3] Phishing Activity Trends Report, 2nd Quarter 2013.

[4] Christine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz, "Anatomy of a Phishing Email", MailFrontier, Inc., 2005.

[5] Gunter Ollmann, "The Phishing Guide Understanding & Preventing Phishing Attacks", IBM Internet Security Systems, 2007.

[6] Christian Ludl, Sean McAllister, Engin Kirda, Christopher Kruegel, "On the Effectiveness of Techniques to Detect Phishing Sites", 2008.

[7] Gunter Ollmann, "The Phishing Guide Understanding & Preventing Phishing Attacks", IBM Internet Security Systems, 2007.

[8] Phishing Activity Trends Report, 2nd Quarter 2013.

[9] Engin Kirda, Christopher Kruegel, "Protecting Users Against Phishing Attacks with AntiPhish", The Computer Journal, 2005.

[10] Sophie Gastellier-Prevost, Gustavo Gonzalez Granadillo, and Maryline Laurent, "A dual approach to detect pharming attacks at the client-side", IEEE 2011.

[11] Aanchal Jain, Prof. Vineet Richariya, "Implementing a Web Browser with Phishing Detection Techniques", World of Computer Science and Information Technology Journal (WCSIT), 2011.

[12] Aza Raskin Tabnabbing: A New Type of Phishing Attack [ONLINE]. Available: http://www.azarask.in/blog/post/a-new-type-of-phishing-attack, accessed on: 12/02/2014

[13] Rableen Kaur Suri, Deepak Singh Tomar, Divya Rishi Sahu, "An Approach To Perceive Tabnabbing Attack", International Journal Of Scientific & Technology Research Volume 1, Issue 6, July 2012.

[14] Philippe De Ryck, Nick Nikiforakis, Lieven Desmet, Wouter Joosen, "TabShots: Client-Side Detection of Tabnabbing Attacks", ASIA CCS'13, May 8–10, 2013

[15] Phishtank database [ONLINE]. Available: http://www.phishtank.com, accessed on: 20/01/2014.

[16] Aza Raskin Tabnabbing: A New Type of Phishing Attack [ONLINE]. Available: http://www.azarask.in/blog/post/a-new-type-of-phishing-attack, accessed on: 12/02/2014

[17] Christine E. Drake, Jonathan J. Oliver, and Eugene J. Koontz, "Anatomy of a Phishing Email", MailFrontier, Inc., 2005.

Authors

Priyanka Joshi received the B.E. degree in Computer engineering from Mumbai University, Maharashtra, India, in 2012, and is pursuing ME in computer engineering from Mumbai University. She works as a lecturer at VPM's Polytechnic, Thane, Maharashtra, India. Her study interests include Networks, Information security, Cloud computing.

Madhumita Chatterjee received M.Tech. in Computer Engineering from IIT Mumbai and Ph.D. in Security in Distributed Computing from IIT Mumbai. She has a teaching experience of 24 years. Her research interest include Network and Information Security, Network Protocols, Mobile Security.