ISSN:0975-9646

PhishIdentifier: A Mozilla Firefox plugin to protect user against Phishing attacks

Pooja V. Kalola[#1], Sachin Patel[*2], Rakesh Pandit[#3]

[#]*Master of Information and Technology,Patel College of Science and Technology, Ralamandal Indore,Madhya Pradesh, India*

[*]*Department of Information and Technology,Patel college of science and Technology, Ralamandal, Madhya Pradesh,Indore*

***Abstract*--Web Spoofing is an activity that attackers use to hack the personal information of a victim; it directs a web site visitor to a web site that looks similar to the one that they believe they are visiting. In this paper we present a technique which compares domain information of a false page with a legitimate page and also compares the html form tag's action attribute of two web pages. Here we provide a browser based plug-in that examines the web page and warn a user if web site is untrusted.**

Keywords— **phishing, plugin, Firefox, vital information, User protection**

I. INTRODUCTION

Web Spoofing is an activity of online identity theft that aims to steal the user's personal information like userid, password, credit card number etc. According to a study by Gartner, 57 million US Internet users have identified the receipt of e-mail linked to phishing scams and about 2 million of them are estimated to have been tricked into giving away sensitive information [1].The phishing problem has become so serious that the German Minister of Internal Affairs recently drew attention to the urgency of the problem and called upon researchers and industry to find solutions [3].As per APWG reports The United States continued to be the top country hosting phishing sites during the fourth quarter of 2013[9].In this the victims often receives an email that convince the user to visit the link of a web page that is spoofed. The site is prepared such that it looks similar to the original site. The phishers typically imitate the visual corporate identity of the target organization by using similar colors, icons, logos and textual descriptions. In order to update his/her personal information the user is asked to enter his/her personal information like login id, password, and credit card number etc. into the site. When user enters his valid data onto the phishes site the attacker captures the data and transfers this information on his site. To prevent our data to be stolen from attacker we propose a Mozilla Firefox plug-in based approach. This plug-in will capture and stores the personal credentials of a user and keeps track of these data and prevent these data to be passed to the untrusted web site.

II. FUNCTIONALITY OF A PHISHIDENTIFIER.

The PhishIdentifier is an application which integrates with Mozilla Firefox web browser. The plug-in keeps track of the user's sensitive information and prevents this information from being passed to the untrusted web sites.

The concept of PhishIdentifier is taken from the browsers functionality that automatically fills the form data if user wants. The content of the form data is protected by a master password. Once the master password has been entered the previously stored login form will be automatically filled by the browser. We take this functionality one step further and checks that where these data is sent. After installing PhishIdentifier user can store the private information by using PhishIdentifier menu. User can also view and delete the previously stored information. Currently user interaction is needed to capture information by clicking the menu 'store sensitive information on this page'

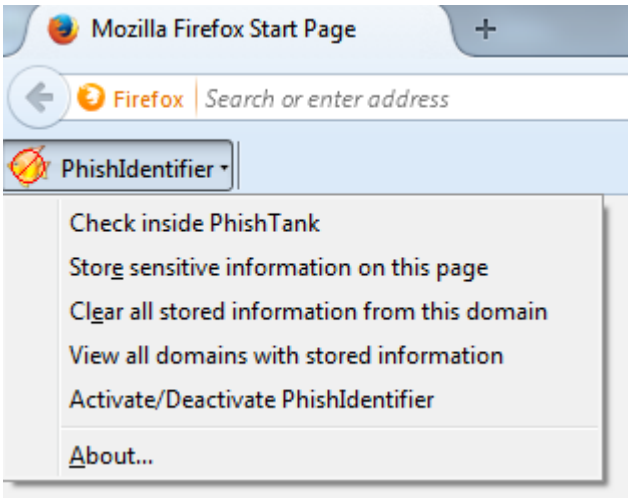

Fig.1 PhishIdentifier with all options

It also stores the domain information along with data where the originally information was entered. PhishIdentifier stores the domain information instead of web site addresses because it may happen that same domain may be accessed

from multiple web servers. Hence if web server addresses are used instead of domains false results may be generated.

If user wants to use same information on more than one web site than this information has to be captured by PhishIdentifier for all web sites. This can be done by first deactivating the PhishIdentifier and then activate it when user needs to capture the information from different web sites.

A. *Working of PhishIdentifier*

Every page that contains HTML form element is might be a phished page. Attackers use HTML elements like text, password and text area to phish information. Attacker generates phished page having same layout of the original page. Fig 2 and Fig 3 displays the original page and phished page respectively.

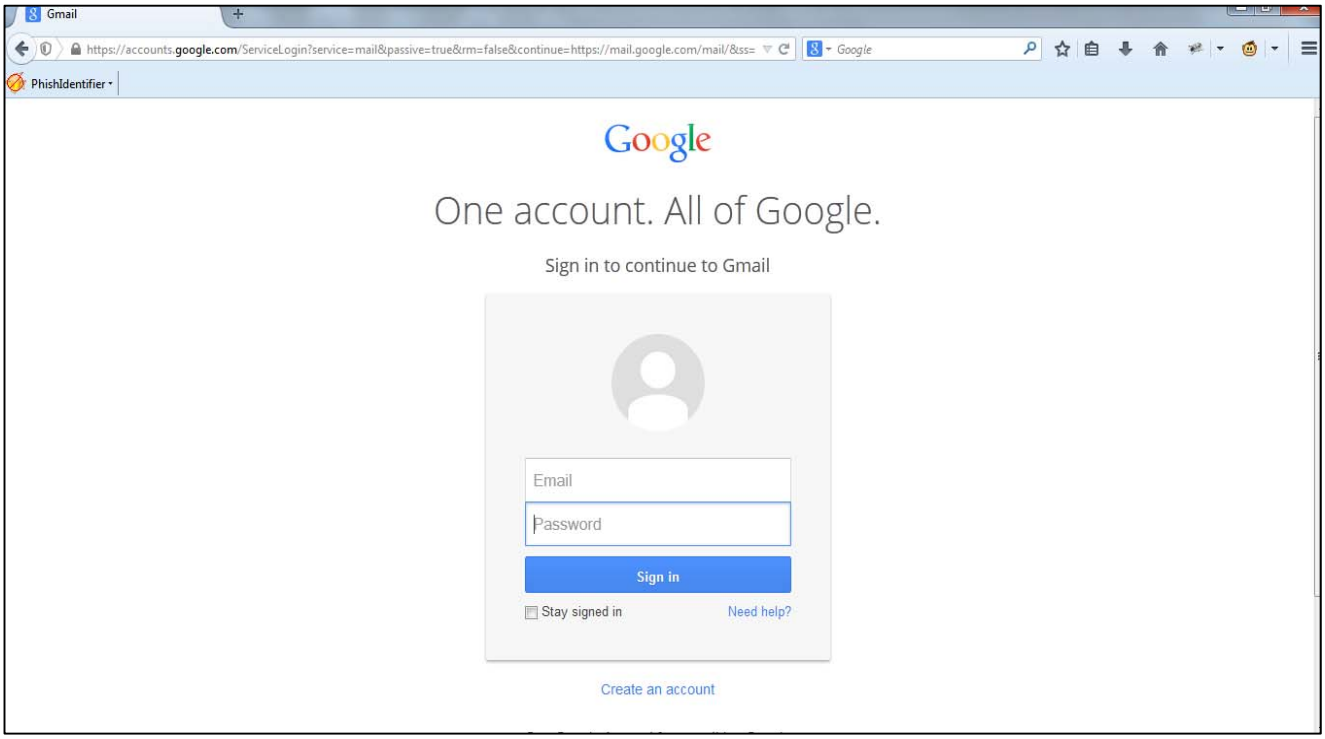

Fig.2 Original Gmail Page.

Now attacker will use the phished page to fool the user and captures user's stored information on phished page and transfers this information on his/her domain. To transfer the information of user on to the attacker's domain he/she makes change in HTML's form element's action attribute. Attacker will change the value of action attribute to his/her URL and save the passed data to his/her domain. Table 1 shows the difference between action attribute of phished page and original page.

PhishIdentifier also compares this action attribute by using java's JSOUP library. By using Jsoup library we can get all the information of HTML tags, its attributes and values of the attributes. Here we have used AJAX to call JSP page which uses Jsoup library functions to compare action attribute and other HTML tags with previously stored web page and current web page which might be phishing attack.

Here we have created the fake page of Gmail and uploaded it into our domain server named truelineinfotech for only testing purpose. Users are requested not to try this URL.

TABLE I
ORIGINAL PAGE V/S PHISHED PAGE

Original page	**Phished Page**
<form novalidatemethod="post" action="https://accounts.google.com/ServiceLoginAuth"id="gaia_loginform">	<form novalidate method="get" action="login.php" id="gaia_loginform">

B. *Ways of bypassing PhishIdentifier with Java Script*

If the web page the user is viewing is only HTML then PhishIdentifier can easily detect the phished page because the attacker can only steal the sensitive information if user press the submit button but before this can happen PhishIdentifier

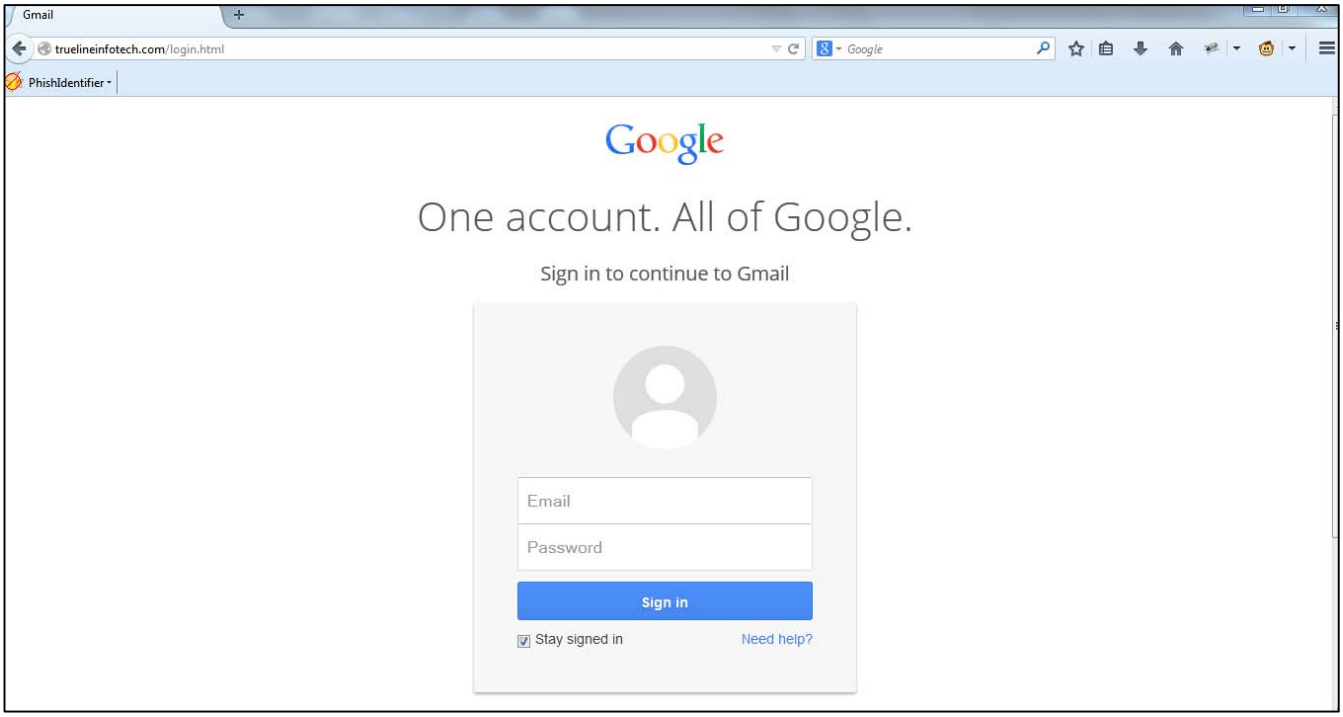

Fig.3 Fake page of Gmail

detects that sensitive information has been typed into form and it will cancel the operation.

JAVASCRIPT is a very powerful scripting language which is used for web application for performing different tasks. It can also used by attacker to create hooks for intercepting user generated events like key strokes. Instead of waiting for user to submit forms attacker will capture the information by creating such hooks. The easiest solution for this problem is to disable the JavaScript on a web page but this is not a feasible solution, as JavaScript is widely used for client side validations and submission purposes.

To resolve this problem, PhishIdentifier deactivates the JavaScript every time the focus is on HTML text element and again reactivate it when focus is lost. This way we can sure that attacker is not able to create hooks. At the same time PhishIdentifier has already determined if the information typed is sensitive or not and if web page is untrusted the operation will be canceled. One drawback of our approach is that the valid user input validation based on key presses event will not function.

C. *Details of implementation*

PhishIdentifier is implemented as a Mozilla Firefox browser extension written using Mozilla XML user interface language (XUL)[6] and JavaScript. We used Paul Tero'sJavascript DES implementation for safely storing the sensitive information [7]. We have also used JAVA's JSOUP library to compare HTML's element in JSP file by calling it using AJAX [4].

D. *Example*

Suppose a non technical user regularly uses a bank's web site for its transactions. The online banking password is a target of the attacker.

When the first time the user visits the web site after installing PhishIdentifier, the user's password is stored using Phish Identifier's menu. Now if attacker has developed a phished page for this bank's web site at the IP address 192.168.1.101. Now attacker will send thousands of emails to the user containing the link of phished page and force his/her to visit the site. The attacker will only need to save the web site's login page and copy the HTML source so that it looks same as the legitimate page.

The user or victim believes that the email is from valid server and click on the given link which has been masked. When victim visits the page he/she will not find anything wrong. When he/she starts typing the user id in text field it will prompt for the master password which is used to decrypt the stored sensitive information and compare it with user input.

After entering user id when user types the password in a text field the alert message will prompt when user types the last character of the password. Figure 4 shows the phished web page with alert message.

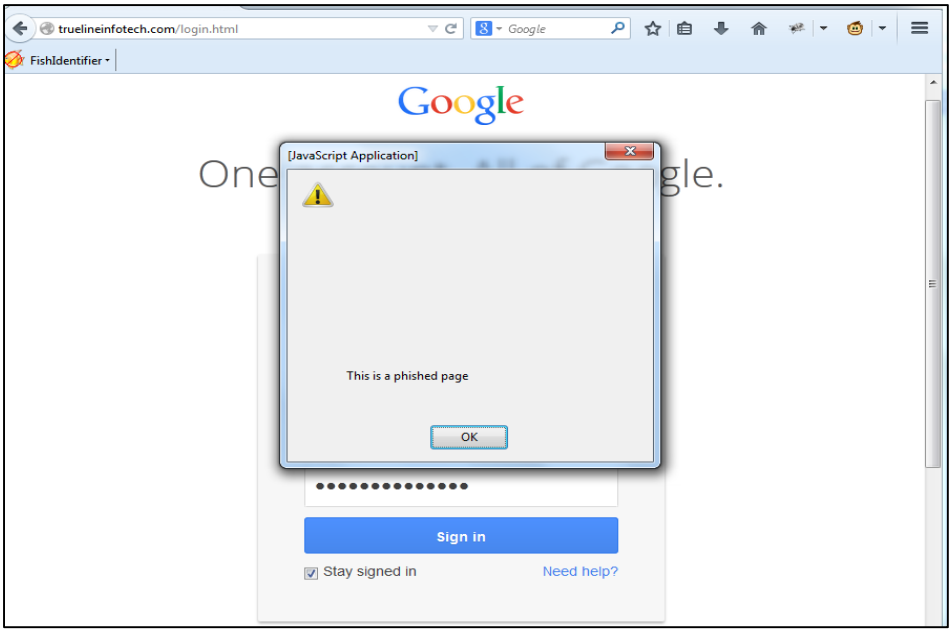

Fig 4. The alert message box

The detail alert message box is given in figure 5 below. This message box gives the detail of domain information also.

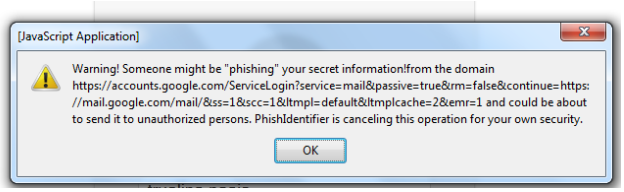

Fig 5.Alert box with Detail message.

III. RELATED WORK

There are two browser based plug-in solutions available both are from Stanford University. PwdHash [2] is an Internet Explorer plug-in that transparently converts a user's password into a domain-specific password so that the user can safely use the same password on multiple web sites. SpoofGuard [8] is a plug-in solution specifically developed to mitigate phishing attacks. The main difference between Spoof Guard and AntiPhish is that Spoof Guard is symptom-based. That is, the plug-in looks for "phishing symptoms" such as similar sounding domain names and masked links in the web sites that are visited. Alerts are generated based on the number of symptoms that are detected. Fished Identifier is based on user input and guarantees that the sensitive information will not transferred to the untrusted website.

VeriSign has recently started to provide an antiphishing service [10]. The company is crawling millions of web pages to identify "clones" in order to detect phishing web sites. Furthermore, blacklists of phishing web sites are maintained. AOL has also recently announced that it is planning to integrate black list-based antiphishing support into the Netscape browser [5].

IV. CONCLUSION

Web spoofing is an activity of online identity theft that steals the user's sensitive information like banking password, credit card numbers etc. The effective solution for this is to train the users not to follow the link blindly but this is not the realistic solution. In this paper we have proposed the browser's based solution to protect users against web site based phishing attacks. Phish Identifier will track the sensitive information of the user and generates the warning whenever this data transmits to the untrusted web site.

REFERENCES:

[1] Phishing Susceptibility and Anti-Phishing Security Strategies-Literature Review , International Journal of Scientific & Engineering Research, Volume 4, Issue 12, December-2013
[2] Blake Ross, Collin Jackson, Nick Miyake, DanBoneh and John C.Mitchell. A Browser PlugIn Solution to the Unique Password Problem.http://crypto.stanford.edu/PwdHash/, 2005.
[3] Heise Security. German Interior Minister Schilyrequests protection against online scams.http://www.heise.de/security/, 2005.
[4] JSOUP book : http://jsoup.org/cookbook/
[5] News.Com.Netscape readies antiphishing browser.http://news.com.com/2100-73553-5558006.html, 2005.
[6] Nick Dikean. XULTU Tutorial. http://www.xulplanet.com/, 2005.
[7] Paul Tero. Javascript DES. http://www.shopable.co.uk/des.html, 2001.
[8] SpoofGuard. Client-side defense against webbased identity theft.http://crypto.stanford.edu/SpoofGuard/, 2005.
[9] The Antiphishing Working Group. Phishing Activity Trends Report. Apwg_trends_report_q4_2013.pdf
[10] Verisign. Anti-Phishing Solution.http://www.verisign.com/verisign-businesssolutions/anti-phishing-solutions/, 2005.