World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:3, 2015

Analysis of Spamming Threats and Some Possible Solutions for Online Social Networking Sites (OSNS)

Dilip Singh Sisodia, Shrish Verma

***Abstract*—**In this paper we are presenting some spamming techniques their behaviour and possible solutions. We have analyzed how Spammers enters into online social networking sites (OSNSs) to target them and diverse techniques used by them for this purpose.

Spamming is very common issue in present era of Internet especially through Online Social Networking Sites (like Facebook, Twitter, and Google+ etc.). Spam messages keep wasting Internet bandwidth and the storage space of servers. On social networking sites; spammers often disguise themselves by creating fake accounts and hijacking user's accounts for personal gains. They behave like normal user and they continue to change their spamming strategy.

Following spamming techniques are discussed in this paper like clickjacking, social engineered attacks, cross site scripting, URL shortening, and drive by download. We have used elgg framework for demonstration of some of spamming threats and respective implementation of solutions.

***Keywords*—**Online social networking sites, spam attacks, Internet, clickjacking/likejacking, drive-by-download, URL shortening, cross site scripting, socially engineered attacks, elgg framework.

I. Introduction

COMPUTER and social networking sites are now parts of our life. Social networking has been very popular in day to day life as people work on internet, interact with people and search whatever they want to social networking sites collects information from end users. This information which is collected by the sites may contain user's interest, likes, private profile or other sensitive information. Friends on the network and cyber criminals/spammers take equal interest in this information.

The use of social networking comes with the vulnerability of web. This gives the spammers an edge to do spam or fulfill their need. The word spam means flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. The unsolicited emails that are received by any person in his / her mailbox are called spam.

These junk mails are usually sent in bulk for advertising and marketing some products. Spam's spread in the network very fast as the people see that the content is shared and liked by their trusted friend. Spammers use various techniques to go through the security restrictions and uncover the sensitive information and steal the people's data. To achieve this goal spammers can create a fake profile and pose as friend, sends friend request to people and makes large number of friends. Once they get the confidence of people and when his friend request is accepted by the user, they r steal the information of the users. A spammer can post malicious link on the victim's timeline and if he/she clicks on this link, the link routes to different target where they wanted to. Sometimes this may causes dangerous consequences.

Similarly the spammers can post a malicious video on user's timeline, when the user downloads the video it requires extension. When he/she downloads the extension for watching this video he/she actually downloads the browser extension which injects malicious JavaScript and this controls victim's profile. Spammers can also use URL Shorteners to do spam attacks on social networking sites [1], [2].

There are several solutions do overcome these spam attacks. Still there are some attacks which are unresolved. So this paper is all about the techniques of spamming, problems raised by the spam attacks and their solutions. In this paper we are covering click jacking [3], social engineered attack [4], cross site scripting [5], URL shortening attacks [6] and drive by downloads [7] with possible solutions of all the spam attacks.

The rest of paper is organized as follows. In Section II we describe the background and related work. In Section III we give description of experimental setup with some proposed solutions and in Section IV we concluded the paper with future work.

II. Background and Related Work

In this section some popular spamming techniques used for spam attacks on online social networking sites (OSNS) are discussed.

A. Clickjacking or Likejacking

It is a technique that gives an attacker the ability to trick a user into clicking on something only barely or momentarily noticeable. The term "click jacking" was coined because the attack aims to "hijack" the number of clicks meant for a particular page. It then routes to the clicks to another page. Cybercriminals hide malicious content under the veil of legitimate pages and may use IFRAME and malicious JavaScript to load this content from a third-party site.

Dilip Singh Sisodia is with the Department of Computer Science and Engineering of National Institute of Technology Raipur, G.E. Road, Raipur (C.G.)-492010, India (e-mail: Sisodia_dilip@rediffmail.com).

Dr. Shrish Verma is with the Department of Electronics and Tele Communication Engineering of National Institute of Technology Raipur, G.E. Road, Raipur (C.G.)-492010, India.

Therefore, if a user clicks on a Web page, they may actually be clicking on content from another page [8]. The IFRAME objects are usually hidden using Cascading Style Sheet (CSS) and JavaScript. Clickjack takes the form of embedded code or a script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function [9].

B. Social Engineered Attacks

Social engineering [4] is the art of manipulating people so they give up confidential information. The types of information these criminals are seeking can vary, but when individuals are targeted, the criminals are usually trying to trick you into giving them your passwords or bank information, or access your computer to secretly install malicious software, that will give them access to your passwords and bank information as well as giving them control over your computer. Criminals use social engineering tactics because it is usually easier to exploit your natural inclination to trust than it is to discover ways to hack your software. For example, it is much easier to fool someone into giving you their password than it is for you to try hacking their password. Some very popular socially engineered spamming techniques are as follows [10]:

Phishing

Phishing [11] is the act of attempting to acquire information such as usernames, passwords, and credit card details by masquerading as a trustworthy entity in an electronic communication. Phishing is typically carried out by email spoofing or instant messaging and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Some popular phishing techniques are as follows;

Shot Gun (Spray and Spray) Phishing

Attackers try to gather as many emails as they can and hope that someone will open it and click on a malicious link or attachment.

Spear Phishing

Phishing attempts directed at specific individuals or companies have been termed spear-phishing. Attackers may gather personal information about their target to increase their probability of success.

Whaling

Several recent phishing attacks have been directed specifically at senior executives and other high profile targets within businesses, and the term whaling has been coined for these kinds of attacks. LinkedIn has been a target of this type of phishing method in recent years.

Pretexting

It is a practice of presenting oneself as someone else in order to obtain private information [12].

Baiting

In this attack, the attacker leaves a malware infected floppy disk, CD-ROM, or USB flash drive in a location sure to be found, gives it a legitimate looking and curiosity-piquing label, and simply waits for the victim to use the device.

Quid Pro Quo

The attacker will "help" solve the problem and, in the process, have the user type commands that give the attacker access or launch malware [13].

C. Cross-Site Scripting (XSS)

Cross-site scripting (XSS) is a type of computer security vulnerability typically found in Web applications. XSS enables attackers to inject client-side script into Web pages viewed by other users. The expression "cross-site scripting" originally referred to the act of loading the attacked, third-party web application from an unrelated attack site, in a manner that executes a fragment of JavaScript prepared by the attacker in the security context of the targeted domain (a reflected or non-persistent XSS vulnerability). The definition gradually expanded to encompass other modes of code injection, including persistent and non-JavaScript vectors (including ActiveX, Java, VBScript, Flash, or even HTML scripts) [14]. There are three types of Cross-site Scripting attacks Persistent, Non-persistent and DOM-based.

Persistent attacks occur when the malicious code is submitted to a web site where it's stored for a period of time.

Persistent Attack Example

Many web sites host bulletin boards where registered users may post messages which are stored in a database of some kind. A registered user is commonly tracked using a session ID cookie authorizing them to post. If an attacker were to post a message containing a specially crafted JavaScript, a user reading this message could have their cookies and their account compromised.

Cookie Stealing Code Snippet

```
<SCRIPT>document.location='http://attackerhost.example/cgi-bin/cookiesteal.cgi?'+document.cookie </SCRIPT>
```

Due to the fact that the attack payload is stored on the server side, this form of XSS attack is persistent.

Non-persistent attacks require a user to either visit a specially crafted link laced with malicious code, or visit a malicious web page containing a web form, which when posted to the vulnerable site, will mount the attack.

Non-Persistent Attack Example

Many web portals offer a personalized view of a web site and may greet a logged in user with "Welcome, <your username>". Sometimes the data referencing a logged in user is stored within the query string of a URL and echoed to the screen

Portal URL Example:

```
http://portal.example/index.php?sessionid=12312312&username=Joe
```

DOM-based Attacks: This type of attacks does not require the web server to receive the malicious XSS payload. Instead, in a DOM-based XSS, the attacker abuses runtime embedding of attacker data in the client side, from within a page served from the web server.

D. URL Shortening

URL shortening is a technique on the World Wide Web in which a Uniform Resource Locator (URL) may be made substantially shorter in length and still direct to the required page. This is achieved by using an HTTP Redirect on a domain name that is short, which links to the web page that has a long URL [15]. For example, the URL "http://en.wikipedia.org/wiki/URL_shortening" can be shortened to http://bit.ly/urlwiki. This is especially convenient for messaging technologies such as Twitter, which severely limit the number of characters that may be used in messages. Short URLs allow otherwise long web addresses to be referred to in a tweet. In November 2009, the shortened links of the URL shortening service Bitly were accessed 2.1 billion times. [16], other uses of URL shortening are to "beautify" a link, track clicks, or disguise the underlying address.

Problem

Users may be unduly impacted with privacy or security problems due to URL shortening. The URL shortener service may open the ability for their user behaviors to be tracked over the Internet. The shorter URL serves as a targeting address and could be used to redirect users elsewhere online. This could be redirection to affiliate websites, scam pages, malware WebPages, spyware distributors, bypass URLs or shock websites. Some URL shortening WebPages like Tiny URL attempt to disable spam links and their redirection capabilities, but this is not always successful. Some URL shorteners also have internal filtering of their created links through services like Google or other safe browsing applications online. Many websites simply do not accept URL shortening; such redirected URLs are blocked automatically. Some websites additionally blacklist URLs that are identified as having redirected website addresses. This is true of many major website including Twitter, Yahoo and Wikipedia, at least for certain URL shortener WebPages.

E. Drive by Download

Drive-by download means two things, each concerning the unintended download of computer software from the Internet. Downloads which a person authorized but without understanding the consequences (e.g. downloads which install an unknown plugging, counterfeit executable program, ActiveX component, or Java applet. Any download that happens without a person's knowledge, often a computer virus, spyware, malware, or crime-ware results in Drive-by-download. Drive-by downloads may occur during visiting a website, viewing an e-mail message or by clicking on a deceptive pop-up window by clicking on the window in the mistaken belief. Hackers use different techniques to obfuscate the malicious code, so that antivirus software is unable to recognize it. The code is executed in hidden iframes, and can go undetected [17].

III. Experimental Setup

It is illegal to perform experiments on real Online Social Networking Sites (OSNS) for offensive security testing. So we have used an open source social networking engine, Elgg on our servers. Elgg platform has most of the features of a matured platform like Face book [18]. This test bed helped us to imitate as well as understand the details of these spamming threats and also test our proposed solutions. We have created few genuine accounts and a bogus account. This bogus account is act as spammer and used to spread the malicious code in test bed environment.

Solutions Clickjacking or Likejacking:

A clickjacked page tricks a user into performing undesired actions by clicking on a concealed link. On a clickjacked page, the attackers load another page over it in a transparent layer. The users think that they are clicking visible buttons, while they are actually performing actions on the hidden page. The hidden page may be an authentic page; therefore, the attackers can trick users into performing actions which the users never intended. There is no way of tracing such actions to the attackers later, as the users would have been genuinely authenticated on the hidden page [8].

Clear Click

The most specific and ambitious is called ClearClick. Whenever you click or otherwise interact, through your mouse or your keyboard, with an embedded element which is partially obstructed, transparent or otherwise disguised, No Script prevents the interaction from completing and reveals you the real thing in "clear". At that point you can evaluate if the click target was actually the intended one, and decide if keeping it locked or unlock it for free interaction. This comes quite handy now that more dangerous usages of click jacking are being disclosed, such as enabling your microphone or your webcam behind your back to spy you through the inter webs. No Script allows executable web content such as JavaScript, Flash and other plug-ins only if the site hosting it is considered trusted by its user and has been previously added to a white list [19].

Frame Busting

Frame Busting checks if the web page is the topmost window or embedded in frame. If embedded it will burst out of the frame and make itself as the topmost frame. It is achieved by DOM property called top [20].

```
If (window.top! =window.self)
{
 Window.top.location=window.self.location;
}
```

With html5

The sandbox attribute which enables a set of instructions on content loaded into iframe. Similarly we have security

attribute which when set to "restricted" ensures that JavaScript and redirects to other sites do not work.

<iframesrc="target site" security="restricted">

X-Frame-Options: All modern browsers support the X-Frame-Options header. The header allows or disallows rendering of the document when inside an iframe. It may have two possible values [21].

Same origin: The document will be rendered in a frame only if the frame and its parent have the same origin.

Deny*:* The document may not be rendered inside a frame. Browsers ignore the header if specified in the META tag. So the following META will be ignored:

<Meta http-equiv="X-Frame-Options" content="deny">

Allow: From URI the page can only be displayed in a frame on the specified origin.

Solution for Social Engineered Attacks

Solutions offered by different vendors in form of software, hardware, firmware or combination of them works to protect your business from the earliest stages of a phishing attacks, including pharming and malware, to the takedown and removal of phishing websites. These turnkey solutions cover the entire phishing life cycle [2].

For example Cyveillance [22] can detect attacks involving malware, cross-site scripting (XSS), dynamic code obfuscation, URL obfuscation, and client-side redirects.

Solutions for Drive-by Download

1. *Encourage users to keep their software up to date :* Single most important measure can take to protect users from drive-by downloads is to encourage them to keep all of their software up to date, especially their antivirus software, their browsers and all of their add-ons, including Java, Flash and Adobe Acrobat. Ensuring that users are using the latest versions of their browsers and extensions is critical because so many users run a few versions behind the latest releases and because most drive-by downloads exploit known vulnerabilities inside older versions of browsers and plug-ins.
2. *Install web-filtering software:* Web-filtering products can potentially prevent people from going to sites compromised by drive-by downloads, says Peck. They may have mechanisms built in to them that allow them to detect if a site is unsafe, and if so, to prevent users from going there, he says. Some look for known exploits and known indicators of drive-by downloads. Others have heuristics built into them that help determine if a site is safe.
3. *Install No Script on your Firefox browser:* No Script is free, open source add-ons that allow only trusted websites that you choose to run JavaScript, Java and Flash.
4. *Disable Java:* Disable JavaScript within PDF documents in their PDF reader's preferences. Uninstall Java from any system they control, at least until a patch is released to particular address (i.e. CVE-2011-3544), a malicious Java applet stored within a Java Archive file that allows an unsigned applet to potentially have unrestricted access to run arbitrary Java code.
5. *Keep tabs on BLADE:* BLADE, which stands for Block All Drive-By Download Exploits, is an emerging Windows immunization system that prevents drive-by download exploits from infecting vulnerable Windows machines.
6. *Don't give users admin access to their computers:* Limiting end users' administrative access to the computer mitigates the damage malware can do [23], [24].

IV. Conclusion and Future Work

Online social networking sites have millions of users from all over the worlds. The ease of reaching these users, as well as the possibility to take advantage of the information stored, attracts spammers and other malicious users. In this paper we have analyzed various modern techniques which are used by spammers on social networking sites. The five modern techniques discussed are clickjacking, social engineered attack, cross site scripting, URL shortening and drive-by-download attacks. We have given some possible solutions to prevent from these attacks. To understand these techniques we have implemented a platform using elgg framework [18], in which gave us a way to test each of the technique. But to avoid these attacks certain rules and parameter have been discussed in the paper. In future we can understand modes operandi of ever increasing spamming techniques using open source platform. We can also suggest for some solutions to mitigate the effect of more and more spamming techniques.

Disclaimer

Software names used in this paper are owned by their respective owners and we have no intention to use it in our profitable use.

Acknowledgment

Authors hereby acknowledge the valuable contribution made by various bloggers and online communities.

References

[1] Detecting Spammers on Social Networks by Gianluca Stringhini, Christopher Kruegel and Giovanni Vigna, http://www.cse.fau.edu/~xqzhu/courses/Resources/GSC.acsac10-socialnets.pdf
[2] OSWAP, https://www.owasp.org/index.php/
[3] Huang, Lin-Shung, et al. "Click jacking: Attacks and Defences." USENIX Security Symposium. 2012.
[4] Jagatic, Tom N., et al. "Social phishing." Communications of the ACM 50.10 (2007): 94-100.
[5] Al Hasib, Abdullah. "Threats of online social networks." IJCSNS International Journal of Computer Science and Network Security 9.11 (2009): 288-93.
[6] Lee, Kyumin, James Caverlee, and Steve Webb. "Uncovering social spammers: social honeypots+ machine learning." Proceedings of the 33rd international ACM SIGIR conference on Research and development in information retrieval. ACM, 2010.
[7] Lu, Long, et al. "Blade: an attack-agnostic approach for preventing drive-by malware infections." *Proceedings of the 17th ACM conference on Computer and communications security*. ACM, 2010.

[8] L.-S. Huang, A. Moshchuk, H. J. Wang, S. Schechter, and C. Jackson, "Clickjacking: Attacks and defences," in USENIX Security Symposium. USENIX Association, 2012.
[9] The Click jacking attack by Ilya Kantor http://javascript.info/tutorial/clickjacking
[10] Linda Criddle, http://www.webroot.com/in/en/home/resources/tips/online-shopping-banking/secure-what-is-social-engineering
[11] Phish tank, https://www.phishtank.com/what_is_phishing.php
[12] Blog,http://www.symantec.com/connect/blogs/web-application-penetration-te
[13] Weboedia, http://www.webopedia.com/TERM/S/social_engineering.html
[14] XSS examples by Lakhmanan Ganapathy, http://www.thegeekstuff.com/2012/02/xss-attack-examples/
[15] M. Vilas, "Having fun with url shorteners," Blog, Jan2010, http://breakingcode.wordpress.com/2010/01/11/having-fun-with-url-shorteners/.
[16] URL shortening site, https://bitly.com/
[17] Security news, http://www.pctools.com/security-news/drive-by-downloads/
[18] E. Foundation, "Elgg- an award-winning social networking engine," Website, http://www.elgg.org/.
[19] G. Maone, "Hello clearclick, goodbye clickjacking!" Blog, October 2008.
[20] G. Rydstedt, E. Bursztein, D. Boneh, and C. Jackson, "Busting frame busting: a study of click jacking vulnerabilities at popular sites," in in IEEE Oakland Web 2.0 Security and Privacy (W2SP 2010), 2010.
[21] M. IE Team, "Combating click jacking with x-frame-options," Blog, March 2010.
[22] http://www.dhs.gov/sites/default/files/publications/privacy/PIAs/dhsprivacy_pia_usss_cyveillance_12272012.pdf
[23] K. Rieck, T. Krueger, and A. Dewald, "Cujo: Efficient detection and prevention of drive-by-download attacks," in Proceedings of the 26th Annual Computer Security Applications Conference, ser. ACSAC '10. New York, NY, USA: ACM, 2010, pp. 31–39.
[24] Mineola Community Bank, https://www.mineolacb.com/avoiding-attacks.htm