ISSN:0975-9646

Study of Automated Social Engineering bots

Chintan Shah, Aruna Gawde

Department of Computer Engineering
D.J Sanghvi College Of Engineering
University of Mumbai, India

Abstract- Social Networking is a way of socializing on web where users interact in variety of ways such as e-mail, instant messages, form communities etc. It is a stage of building a social relationship among people. Automated social engineering is an automated form of revealing confidential information by exploiting human factors. ASE uses bots to attack on Social Networking Sites (SNS). One such bot is Koobface that caused enough disturbances to social networking site. With an increase in Koobface activity, On July 9, 2009, Twitter decided to temporarily suspend infected accounts in order to limit the infection [7]. Honeybot is an attack that instruments human conversations for social engineering. At the end of this paper, we present a solution to overcome problem associated with honeybot and koobface.

Keywords - Automated Social Engineering (ASE), Social Networking Site (SNS), Fast-Flux Networks (FFNs), Multi-Modal Captcha(MMC), bot, botnet

1. INTRODUCTION

Social networks connect people at low cost. These networks often act as a customer relationship management tool for companies selling products and services. Companies can also use social networks for advertising in the form of banners and text ads. Since businesses operate globally, social networks can make it easier to keep in touch with contacts around the world.

Social networks at beginning were adopted by healthcare professionals as a means to manage institutional knowledge, disseminate peer to peer knowledge and to highlight individual physicians and institutions but now it has become an integral part of every human life and as a means to maintain relationship and share information among each other and thus resulting in creation of accounts with social networking site (SNS). Therefore SNS have become a popular medium to launch attack. However social engineering requires a lot of time in maintaining relationship, gaining trust and confidence and then exploiting user in revealing secret information. Automated social engineering (ASE) is an automated way of social engineering which can save lot of time by performing all the activities of social engineering in an automated way.

In the rest of the paper, we first review related research work in Section 2. Then we describe our proposed solution (Section 3). Finally, draw conclusions in section 4.

2. REVIEW OF LITERATURE:

In Honeybot attack [3] every occurence of attack involves two users with a bot in the middle. It is a new attack that instruments human conversations for social engineering. The approach is similar to a traditional man-in-the-middle attack. The honeybot can make participant to click on the link which might point to a fake website. Link can be a keyword link which may automatically reply to keywords found in the messages, or can be a replacement link that replaces the link with its own one. The link can also be a random link where bot itself inserts a link in an ongoing conversation.

KOOBFACE [2] is a malware, being the first to have a successful and continuous flow through social networks. KOOBFACE is a collection of various components. A typical KOOBFACE infection starts with a spam sent through Facebook, Twitter, MySpace, or other social networking sites containing a popular message with a link to a “video.” As soon as user clicks on the link, the link will redirect user to some other website designed to mimic Youtube(but actually it is named YuoTube), where it asks the user to install an executable(.EXE) file to watch video. The .EXE file that user downloads is actually a downloader of KOOBFACE components. It took 3 years for facebook to crack koobface bot [5].The components are subdivided as: KOOBFACE downloader, Social network propagation components, Web server component, Ads pusher and rogue antivirus (AV) installer, CAPTCHA breaker, Data stealer, Web search hijackers, Rogue Domain Name System (DNS) changer. Once KOOBFACE components are downloaded, checks for internet cookies on client’s machine to get information about the social networking sites like Myspace, Facebook, Orkut, Twitter,Friendster,Linkedin where client has an account.

CAPTCHA is an automated test to find out whether the user is human or not. It is a test that humans can pass, but computer program can't. The most widely used CAPTCHAs consist of distorted text images. However with increase in bots breaking CAPTCHAs it is difficult to find out the difference between a human and an automated computer program. Bots can easily read letters and words that are distorted using optical character recognition (OCR). To overcome the problem associated with CAPTCHA, a multi modal captcha(MMC)is proposed in this paper[4]. In MMC, An image is provided on screen with many text labels on it. A user has to find out the correct name of the given image among the set of text labels that are scattered over an images in order to go by a human verification test.

3. PROPOSED SOLUTION:

It is usually found that koobface and honeybot attack occurs due to lack of awareness among the user communicating with each other. Honeybot attack influences the topic of the ongoing conversation, making the participants click on links that researchers inserted into

the conversation thereby diverting the user to some other website which user has never expected. Similarly KOOBFACE infection starts with a spam sent through Facebook, Twitter, MySpace, or other social networking sites containing a catchy message with a link to a "video." Whenever a user clicks on the link, the user is redirected to a website designed to mimic YouTube (but is actually named YuoTube), which asks the user to install an executable (.EXE) file to be able to watch the video.

Fig.I shows the proposed solution in the form of flowchart diagram to overcome the drawback associated with koobface and honeybot attack. The flowchart steps are discussed which will explain the proposed solution in detail.

The proposed flowchart steps are as follows:

1. Whenever a link is shared among user, the user is asked to solve captcha that is displayed. To make it stronger a MMC is proposed.
2. An image is provided with four text label on it, the user has to enter a correct label in the text box provided.
3. If sender succeeds in entering correct text with predefined attempts then the sender is allowed to share a link with the receiver.
4. If sender fails in recognizing image and text over it within number of attempts, the system denies sharing link and treats as a bot.

3.1 PROPOSED FLOWCHART DIAGRAM

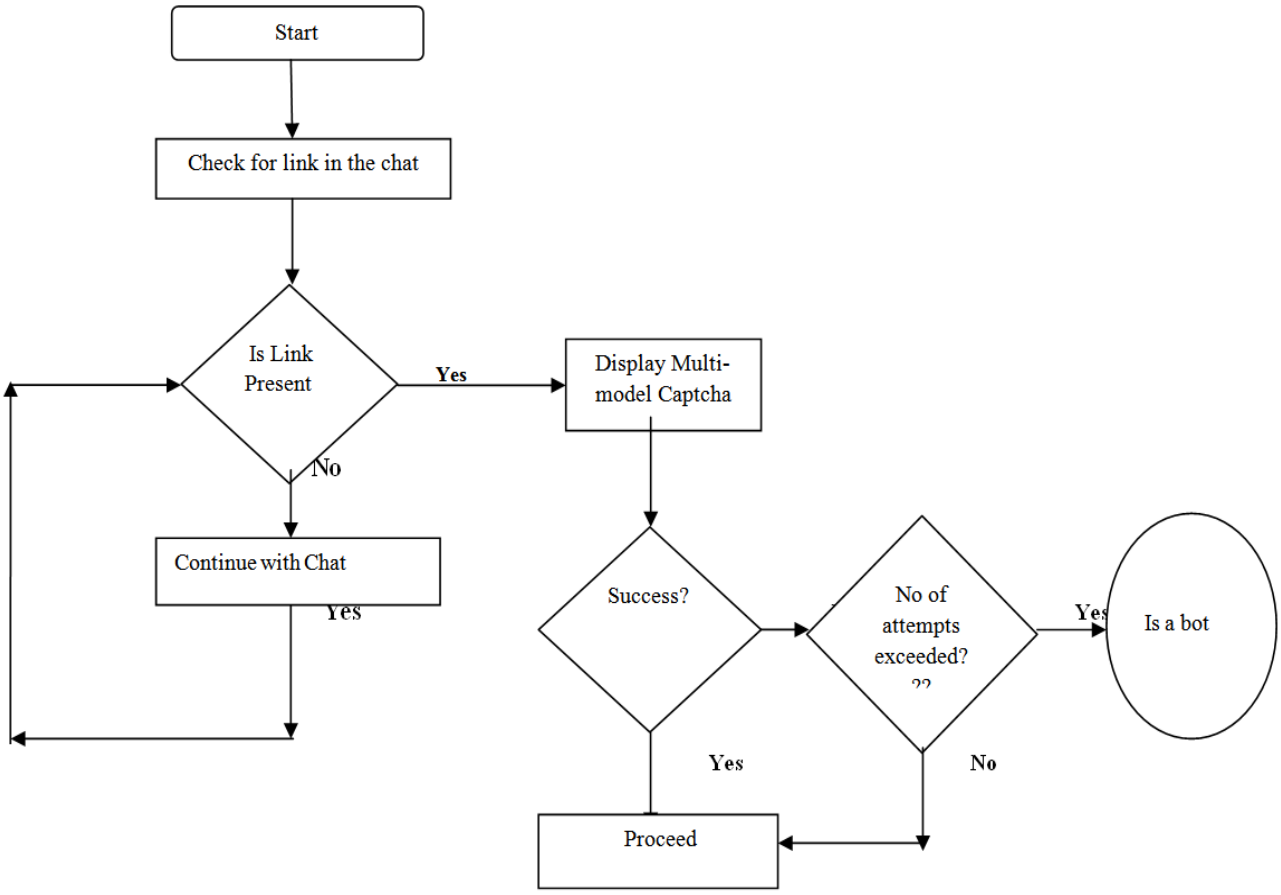

Figure 1: Flowchart of Proposed System

4. CONCLUSION

SNS have brought the world closer. However with increase in use of social networking among users, the new techniques to reveal the information has also increased. Social engineering has been used in an automated way to reveal confidential information in quick time. It is usually found that it is due to lack of awareness among users which is the main concern in revealing the confidential information. Therefore we have proposed solution which will avoid attacks like honeybot and koobface and thereby preventing user to reveal confidential information.

REFERENCES

[1] M. Huber, S. Kowalski, M. Nohlberg, and S. Tjoa, "Towards automating social engineering using social networking sites", In CSE (3), p. 117–124. IEEE Comp. Soc., 2009.

[2] M. Huber, "Towards automating social engineering using social networking sites" theses work 2009.

[3] Tobias Lauinger, Veikko Pankakoski, Davide Balzarotti, Engin Kirda, "Honeybot, Your Man in the Middle for Automated Social Engineering", IEEE, 2008.

[4] Abdulaziz S Almazyad, Yasir Ahmad, Shouket Ahmad Kouchay, "Multi-Modal CAPTCHA: A User Verification Scheme", IEEE, 2011.

[5] The Koobface malware gang - exposed! , An investigation by Jan Drömer, independent researcher, and Dirk Kollberg, SophosLabs, http://nakedsecurity.sophos.com/koobface/.

[6] Hongyu Gao, Jun Hu, Christo Wilson, Zhichun Li, Yan Chen, Ben Y. Zhao, "Detecting and Characterizing Social Spam Campaigns", IMC'10, November 1–3, 2010, Melbourne, Australia. Copyright 2010 ACM 978-1-4503-0057-5/10/11.

[7] Jonell Baltazar, Joey Costoya, and Ryan Flores, "The real face of KOOBFACE: The largest Web 2.0 botnet explained", Trend Micro Threat Research, unpublished.