Study of Automated Social Engineering, its Vulnerabilities, Threats and Suggested Countermeasures

Priya Kaul
Department of Computer Engineering
K.J. Somaiya College of Engineering
University of Mumbai, India

Deepak Sharma
Department of Computer Engineering
K.J. Somaiya College of Engineering
University of Mumbai, India

ABSTRACT

Automated Social Engineering (ASE) is how social networking sites (SNSs) are exploited for Social Engineering by automated bots. Classical social engineering is an attack on the security of systems, based on exploiting human factors. ASE is an automated form of traditional social engineering which makes use of bots to attack SNS. One such bot is KOOBFACE [1] that infected Facebook for a long time until it was detected in mid of 2011 by Sophos lab. ASE bots can be developed easily using open source web automation and web scrapping tools. These tools combined with appropriate chat logic with enhanced intelligence pose a great threat to the security of SNSs. Countermeasures like Captchas have proved ineffective in preventing bots from infiltrating SNS's. New techniques like Multi Modal Captchas (MMC), and Fast Flux Network (FFN) detection are the future of the ASE prevention. In this paper we present a survey of vulnerabilities, threats and propose some countermeasures for Automated Social Engineering.

General Terms

Social Engineering, System Security, privacy issues.

Keywords

Social Networking Sites(SNSs), Fast-Flux Networks(FFNs), Multi-Modal Captcha(MMC), bot, Automated Social Engineering(ASE), botnet

1. INTRODUCTION

Social engineering is an attack on the security of systems, based on exploiting human factors. Automated Social Engineering illustrates how social networking sites can be used for social engineering. Classical social engineering is taken one step further by automating tasks which formerly were very time-intensive. ASE's goal is to automate an attack in order to reach a large number of victims, and it should be human-like so that more victims fall for it. SNSs facilitate the automation of attacks by providing data in machine readable form. SNSs serve as a communication platform by offering services such as private messaging and chats which can be used by automated social engineering bots. A bot (short for "robot") is a program that operates as an agent for a user or another program or simulates a human activity. A bot has ability to establish a Command and Control (C&C) channel that allows an attacker to remotely control or update a compromised machine. A number of bot-infected machines that are combined under the control of a single, malicious entity are referred to as a botnet. Such botnets are often abused as platforms to launch denial of service to send spam or to host scam pages. This paper discusses three different bots in detail- two experimental bots viz. ASE bot, Honeybot, and one which actually infiltrated Facebook from 2008 till mid 2011. Section 2 discusses ASE bot, how SNSs make themselves resistant against such attacks and one weakest link that still makes some SNSs vulnerable to ASE bots. We then discuss a bot which is most difficult to detect- Honeybot based upon traditional man-in-the-middle attack. In the same section Koobface bot is discussed and the reason why it haunted some SNSs for so long. Section 3 discusses results of experiments conducted by some researchers. Section 4 discusses Analysis of bots based on the results of experiments. Section 5 discusses several vulnerabilities and some Countermeasures on the part of users as well as SNSs which can curb attack of ASE to much greater extent.

2. REVIEW OF LITERATURE

ASE Bot [2] works on the basis of an ASE attack cycle. This ASE attack cycle is derived from a holistic model for S.E. attacks: 'The Cycle of Deception- A Model of Social Engineering Attacks, Defences and Victims' [3]. Bot is implemented that chats with users on FB to recruit them to fill a malicious online survey. ASE bot works in two phases: first finding victims i.e. Data Mining and then chatting with victims. While chatting with them they are recruited to fill a malicious online survey. Artificial replies are generated using ALICE chat logic. Steps of cycle are- Plan: The attacker sets up the ASE bot to attack the "Royal Institute of Awareness" to steal credentials of the institute. Map and bond : The ASE bot searches for the private network of the "Royal Institute of Awareness" in Facebook. Information about users within the private network is gathered in order to get a list of possible future targets. The bot sends its targets of the "Royal Institute of Awareness" initial messages to get into rapport with. *Execute*: If victims replied to the messages sent before, the ASE bot assumes that the bonding was successful and executes the actual attack. They are asked to fill an online survey (malicious one). Recruit and Cloak: In case cloak has been enabled, the ASE bot deletes the account used to carry out the attack. If recruit was selected, the ASE bot tries to recruit the attacked user and her/his circle of friends for future attacks. Evolve/Regress: The link, the users receive, points to a malicious survey to gather information ("survey on password security" etc.). Proof of concept is explained in detail for ASE bot by Mr. Marks Huber in his theses work [4]. In Honeybot attack [5] every instance of attack involves two users and a bot in the middle. After initiating a conversation with a user, whatever replies bot receives they are simply forwarded to a second user chosen at random from entire chat channel population (conversation bootstrapping). Bot has ability to replace some specific words with corresponding words of opposite sex using a translation dictionary. After building a good rapport with users, attack is executed by sending a link or a question to one of the two users. Links can be Keyword links- automatically replying to keywords in messages, Random links- randomly inserting a link into conversation. To make this look more natural, Honeybot requires both users to have exchanged a minimum number of real messages before inserting artificial messages, Replacement link- If one of the users sends a message containing a link, Honeybot can replace that link with its own one. This method looks the most natural, because the message has been written by a human for the current context, and the recipient may be expecting a link. Koobface bot [1] is a revolutionary malware, being the first to have a successful and continuous run propagating through social networks. KOOBFACE is composed of various components, each with specific functionalities. While most malware cram their functionalities into one file, KOOBFACE divides each capability into different files that work together to form the KOOBFACE botnet. A typical 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." Clicking the link will redirect the user to a website designed to mimic YouTube (but is actually named YouTube), which asks the user to install an executable (.EXE) file to be able to watch the video. The .EXE file is, however, not the actual KOOBFACE malware but a downloader of KOOBFACE components. 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. The KOOBFACE downloader is also known as the fake "Adobe Flash component" or video codec the fake *YouTube* site claims you need to view a video that turns out to be nonexistent. The downloader's actual purpose includes the following: determine what social networks the affected user is a member of, connect to the KOOBFACE Command & Control (C&C), download the KOOBFACE components the C&C instructs it to download. In order to determine what social networks the affected user is a member of, the KOOBFACE downloader checks the Internet cookies in the user's machine. KOOBFACE downloader checks the cookies for the social networking sites like Facebook, MySpace, Hi5, Friendster, myYearbook, Tagged, Bebo, Netlog, fubar, Twitter.

Bots with different features are effective tools for executing spam campaigns and spreading malware on SNSs. Recently emerged Bot is with fast flux feature, in which hosts associated with a domain name are constantly changed to make it harder to block the delivery of the malicious web pages and effectively hide the address of the actual web server, often referred to as the "mothership" [6]. In this case, the proxying Bots are usually organized as a FFSN. Technique for detecting such bots contains nine steps: Dragging data- Social Networking data between April and June of 2009 in form of URLs is dragged. Their anonymzed userID, friend list, default privacy setting and interaction records associated with the timestamp are recorded. Validation steps are followed**:** deobfuscation of URLs is done, wall messages having well-known keywords that are indicative of malicious nature, such as "love" "free money" and "free gift" are detected. Filter User's Wall Posts- derive each user's wall posts as a <description, URL> pair. URL is the destination the attacker wants the target to visit. Based on the similarity between two wallposts , a similarity graph is made. Next malicious clusters are identified in the graph. In the end Fast Flux Based Bot is detected using TTL Value. Now if TTL value of any user is low (less than 6) [6] then it is FFSN based Bot because, FFSN Based Bot live for limited and short period of time and where higher TTL (greater than 6) value shows that valid, normal and authenticate user. Hence finally this work detect a fast flux based Social Bot.

CAPTCHA is an automated test that humans can pass, but current computer programs can't. The most widely used CAPTCHAs are rarely based on the distortion of text images making them unrecognizable to the state of the art of pattern recognition techniques, and these text-based schemes have found widespread applications in commercial websites. The increase in bots breaking CAPTCHAs shows the ineffectiveness of the text-based CAPTCHAs. Bots can easily read the distorted letters and words using optical character recognition (OCR). A new technique to build a CAPTCHA which is multi-modal (Picture and Text based) is discussed in this paper. An image is being rendered on the screen and many text labels are drawn over it. A user has to identify the correct name of the underlying image among the set of text labels that are scattered over it, in order to pass a human verification test. Cursive text will be used instead of plain text labels. To implement Multi Modal CAPTCHA [7] thousands of images (animals, fruits, furniture etc) are collected from the popular search engines like Google, Bing etc. The collected data is publicly available to all users through these search engines to maintain the 'Public' feature of the CAPTCHAs. A large set of images and text labels are stored in the database. Whenever a user tries to access the service, an image is fetched along with four text labels for verification. Cursive text labels are used instead of normal text.

3. RESULTS

ASE experiments have been conducted by many researchers to execute attack on an organizational level without informing the test subjects beforehand but rather debriefing them on the experiment. As ethical approval for study could not be achieved, two different ASE experiments were conducted. First was conducted to find out the success rate of data mining with ASE bot by taking large user base of five Sweden based MNC's in consideration. Second was conducted to test the chat logic of bot. Both were a clear success.

In case of Honeybot two Dating channels, one in English and one in French, and an Italian Chat channel were selected. Honeybot sends three different types of links. The IP address and TinyURL links point to a web server (of research team) that counts the click and subsequently forwards the browser to an external, popular website. The MySpace link points to a profile that has been created by research team for the purpose of this study. Evaluation results showed TinyURLs were the most likely to be clicked, followed by MySpace profile links and IP addresses.

4. ANALYSIS OF BOTS

When the studies conducted on ASE bot were published, in no time within the same year several SNSs made several changes in its features like removing "geographical networks" option. Reason being some of these networks had millions of members and it was very easy to join such networks. Because of the default privacy settings most of the profiles within a network are fully accessible. These settings were especially problematic with regional networks which were open to everyone. If an SNS user for example joined the "Sweden" network, she/he will be able to see the full profile information of all other members of this network who did not change their default privacy settings. Facebook even automatically modified the privacy settings to the less restrictive default settings once changes in the network settings have been made. Even if facebook has removed such option of “geographical network”, “joining a group” (especially open groups) is another option that can act as a strong platform for initiating ASE bot attacks. One of the pre-requisites of ASE bot is huge victim base that can be easily obtained from the groups on FB. Honeybot attack is one of its kinds which are most difficult to detect. It doesn’t make use of any chat logic but forwards human conversations to-and-fro between two human beings. It is this fact that makes it different from other bots say spam bots which are easy to detect as their nature of action is bursty- bulk of messages are sent at a time. More human-like an ASE attack is, more difficult is to detect it. Koobface bot was based on fast flux networks. It took facebook 3 years to crack Koobface botnet [8].

5. VULNERABILITIES AND SUGGESTED COUNTERMEASURES

ASE bot’s experimental implementation was successful and even after measures adopted by SNSs, it still is an active potential threat to the security of SNS’s. Default Privacy Settings of SNSs is the one and only main reason that allowed ASE attack to happen. These settings make a user’s profile information visible to every other user on SNS. By default a SNS profile can always be searched from outside using search engines. Text based Captchas proved ineffective when ASE bot experiment was conducted. Multi-modal captcha scheme is answer to the ineffective captcha problem. Still most of the websites and SNS’s are dependent on text based captchas. Honeybot is one of the most effective and difficult bots to detect. One of the solutions for such attacks is keeping a keen eye on the activities happening on SNSs. Suspicious looking activities conversations should be parsed thoroughly to check presence of malicious links. Moreover a warning should be displayed always before a link warning user of malicious nature of links so that they can do a background check before falling prey to such attacks. Koobface bot is based on FFNs. Even if gets detected, it becomes very difficult to find out the actual people behind such attacks because hosts associated with a domain name are constantly changed to make it harder to block the delivery of the malicious web pages and effectively hide the address of the actual web server. Some techniques like “Detection of fast flux network based social bot using analysis based techniques” [6] can prove useful in detecting botnets. Some other vulnerabilities of SNS’s which can be exploited by ASE bots are: Privacy issues which include Leakage of information to 3rd party application, Leakage of information through poor privacy settings, Identity Theft issues which include Profile Cloning and Social Phishing, Malware issues such as Drive-by Download Attack (as in case of KOOBFACE attack), Fake Profile (as in case of ASE attack), Cross-Site Scripting Attack (as in case of KOOBFACE attack), Shortened and Hidden Links. In order to deal with privacy issues users should access only trustworthy 3rd party applications on SNSs. Before accessing a little background check should be done so as to ensure security. Also one should keep privacy settings of their accounts very restrictive, making personal information available to only those whom they can trust. This will reduce the chances of profile cloning as well as phishing. In order to avoid Drive-by Download attacks and cross-scripting attacks attention on users part is required- they should be very cautious towards clicking any catchy URL links from anonymous sources, and should never disclose any personal credentials to any anonymous website. Short URLs are often used by malicious websites to hide their real identity real meaning,e.g.“nafignasdo.ru/w.php?f=cf234&e=2”,“pervonah.pl/w.php?f=c2567&e=2”,“sjkpxpimy.lflinkup.com/PJeHubmUDaovPDRCJxGMEzlYXdvvppcg” etc. Before downloading any anonymous software, extension of executable file should be keenly observed by the user, and once user has full faith that extension doesn’t look like a potential threat, then only he should continue. Example- incase of KOOBFACE bot, user were directed to YUOTUBE link and were convinced to download a file with a suspicious extension. Smart users can always avoid such kind of traps.

6. CONCLUSION

SNSs have brought world closer, and as people say now geography has become history with physical distance being no barrier because of SNSs. Blind meetings and coincidents have become real now as every person can be found sharing his life, events, personal choices with the whole world via SNSs. But lack of awareness and education regarding the privacy concerns of individuals has become a big concern now-a-days. No SNS has strict or highly restrictive default-privacy-settings facility because of vested economical interests. More visibility of data along with more revelation of personal choices means more opportunity of advertising for SNS owners. No doubt vulnerabilities are being discussed a lot and almost every day a new vulnerability is being discovered by researchers. But not much has been done by scientists so as to ensure privacy of users. After going through a very large literature survey of ASE, the hazards of using SNSs have become very clear. By simply avoiding some basic activities like clicking on the Catchy URL’s from anonymous sources, not accepting friend requests from strangers, or participating in any suspicious online surveys and by making use of highly restrictive privacy settings - users can themselves act as defenders of their Privacy.

7. FUTURE RESEARCH

Social networks can be described as web applications that allow users to create their semi-public profile. Most social network users share a large amount of their private information in their social network space. This information ranges from demographic information, contact information, comments, images, videos, etc. Many users publish their information publicly without careful consideration. Hence, social networks have become a large pool of sensitive data. With these social network characteristics and the more aggressiveness of attacker’s methods, privacy and security issues in social networks has become a critical issue in the cyber world. Attacks like Koobface are only the beginning. Seeing the trend and the rate at which user base of SNS’s has increased in the recent years, very little work has been done in the area of techniques to overcome related security issues. Thus need is to implement bots in real life on SNSs, of course, after satisfying all ethical concerns of cyber world so as to find out the closeness or difference between simulations and real world scenarios/demos. More research needs to be done in the field of countermeasures against bots.

8. REFERENCES

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

[2] 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.

[3] M. Nohlberg and S. Kowalski, “The Cycle of Deception- A Model of Social Engineering Attacks, Defences and Victims,” in Proceedings of the Second International Symposium on Human Aspects of Information Security & Assurance (HAISA 2008), Jul. 2008.

[4] M. Huber, “Towards automating social engineering using social networking sites” theses work 2009.

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

[6] Amit Kumar Tyagi, G.Aghila, “Detection of fast flux network based social bot using analysis based techniques”, IEEE, 2012.

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

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

[9] 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.

[10] Catherine Dwyer, Starr Roxanne Hiltz, “Proceedings of the Thirteenth Americas Conference on Information Systems, Keystone, Colorado August 09 - 12 2007”.