ANALYSIS OF MALWARE PROPAGATION IN SOCIAL NETWORK – FACEBOOK

[1]GOPAL SHIVHARE, [2]VARTIKA GUPTA, [3]ABHISHEK VAISH

Student IIIT-A, Student IIIT-A, Associate Professor IIIT-A
Email: shivhare.gopal@gmail.com, vartika929@gmail.com, abhishek@iiita.ac.in

Abstract— Social Network the Facebook is an online community of people formed on the basis of real social connections. Facebook is commonly used by millions of people around the globe. The fact of real social connections is utilised by many malware writers to propagate the malicious code into the Facebook. It is a potential risk which results in breach of confidential and personal identifiable data of users whose accounts has been compromised by these malicious codes commonly known as malware. In past recent years, Facebook was under the attack by a Trojan type of malware known as koobface. In this paper we have discussed about different types of malware propagation in Facebook. We also identify the parameters related to malware attacks on Facebook and verifying these parameters on a simulator. Simulator used is NetLogobased simulator. Further, we investigate the attacking vectors of clickjacking and Trojan type of malware in Facebook. Our analysis concludes that spreading of malware is widely affected by use of social engineering technique by exploiting the trust relationship formed by the fact of real social relations and this raises the importance of user awareness to prevent exponential propagation of malware. Infection of many user profiles is also done by exploiting the structure of Facebook while considering the probability of clicking the links.

Index Terms— Facebook, Trojan, Click Jacking, XSS

I. INTRODUCTION

Malware and its impact are always been a topic of concern and complex to solve. Also the propagation of malware is difficult to understand and to solve the problem of malware propagation. Before the advent of social network like Facebook, attackers used to spread via newsgroups & emails. The recent example of the rise of malicious software such as Pay-Per-Install (PPI) which is commonly used for financial gain. Other forms of attacks may be like mounting denial of service attacks, identity theft, confidential information theft and forming a botnet.

Social network the Facebook had already flashed its vulnerability when attacked by clickjacking malware and by koobface. Twitter was also targeted by overloading its servers. The reason of these attacks is the facts that users are not aware of the risks and also because of technological loopholes. The main motive behind exploiting these risks is financial gain and this social network acts as a resource which gives platform to launch these attacks with the aid of technologies like short-URL and specified advertisement.
Social network like Facebook and Twitter are built on real social relationships in which a profile represents a user whose social network connections are established through virtual friendship. This implies that you may add them as a friend, if you have an acquaintance with them in the real world. On getting connected the two parties can communicate each other and see their profiles and like their posts. There is a possibility that a user can restrict their access by applying privacy setting but in this paper we have assumed that messages are readable on the other side.
Due to trust relationship it is easy for most of the malware to spread via social network. For example if one of the connection in a friend list shares a message containing malicious link then the reaction of different connected people will not be the same as it depends on the user awareness also. Some may click the link and spread the malware further; others, who are aware of it, mark it as a spam. Malware like Cross Site Scripting (XSS), which requires no user intervention, infects the user due to flaw in the web application.

The first malware which hit the social network was in MySpace known as Sammy worm, which exploited the security flaw present in the web application. Starting from a single user, it exceeded its infection in more than one million users profile after 20 hours. As a result within two days they were bound to completely shut down to resolve the issue. Since in this there was no user intervention required, so it was easy for malware writers to propagate active worm without using social engineering technique which deceives users to click on a special malicious crafted link. In the year 2008, Facebook users were hit by new type of malware known as koobface. In this the infected users were directed to a third party website and were prompted to download an executable file, which was pretending to be a new version up gradation of the flash player. On execution, the computer gets infected with koobface.

In this paper we are going to identify the parameters related to malware attacks on Facebook and verifying

these parameters on a simulator. Simulator used is NetLogobased simulator. Further, we investigate the attacking vectors of clickjacking and Trojan type of malware in Facebook.

Our analysis concludes that spreading of malware is widely affected by use of social engineering technique by exploiting the trust relationship formed by the fact of real social relations and this raises the importance of user awareness to prevent exponential propagation of malware.

Infection of many user profiles is also done by exploiting the structure of Facebook while considering the probability of clicking the links. The effect of intervention of user is analysed through simulation, which shows how a social engineering technique increases the speed of malware propagation exponentially. Finally based on simulation we have suggested few constant factors which can affect the malware propagation and are included in the analytical malware propagation model.

The rest of the paper is categorized as follows: Section II gives background of Facebook Structure and preliminaries. In section III we have discussed about the different types of malwares and their propagation in social network. Section IV, discusses about simulation experiment and suggestion of new model on the basis of simulation results. Section V finally concludes this paper.

II. BACKGROUND

Facebook structure can be divided into 2 distinct entities: a User → Wall-Post model and a trending hash '#' – model. The flow of information in Wall-Post model occurs through 'Like', in which when a user likes a post; he becomes its follower automatically.

Here we have assumed that users are directly connected with each other profiles without any privacy restrictions and locks and can post and like every wall post or shared post on their friends profile or groups.

Another way can be using string syntax @user_name, which directly tags a user and used for direct messages and gaining specific attention.

In the Wall-Post model it is important to notice that friends are able to see Wall-post and is not visible to non-connected users.

However if the post is made publically then it will be visible to all users. And for non-connected users it is possible to see and follow post if the friend of the originator profile shares the Wall-Post.

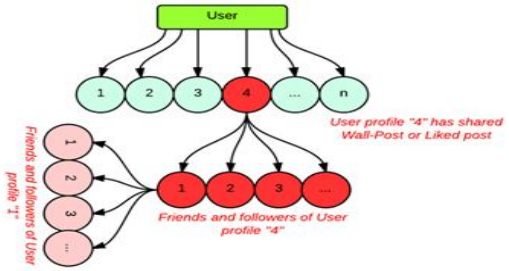


Figure 1: Facebook structure

Facebook Structure presented in Figure 1 shows the process of Wall-Post model that is how a user shares Wall-Post and his friends becomes the followers and how Wall-Post are only visible to his friends only. In the given figure it can be seen that the user "4" shares a Wall-Post or Likes a post, which then becomes visible to all the people connected to his profile and further the user "1" likes or shares that Wall-Post and it becomes visible to his connections. It is important to note that those who are not directly connected to the original user also gain access and are able to see that Wall-Post. You can also see that Facebook has a tree structure and follows preferential attachment model of free scale social network and the flow of information occurs down the tree.

The second model is "trending hash'#'- model", when used it broadcast the information by appending the topic to the hash '#'. This is similar to Twitter and when the topic is searched then all the tagged post with this tag appended comes as trending news in the search result. This is the concept of trending topic list which is heavily used be researchers and users for fetching current news and trending Wall-Posts.

Many Facebook profile users has started using this trending hash'#'- model even for their general communication in their Wall-Post. It is crucial to note that it includes all the users who are not following any one or any trending topic. The User → Wall-Post model and trending hash'#' tag model makes a unique structure of Facebook security/Privacy, as it provides to easiest way to propagate any malicious link.
Attack using social engineering is one of the biggest threats for unaware Facebook users.

This technique misuses the trust relationship concept of social network and combines it with present vulnerabilities. Now a day's short URL (Universal Resource Locators) are used in place of long URLs.

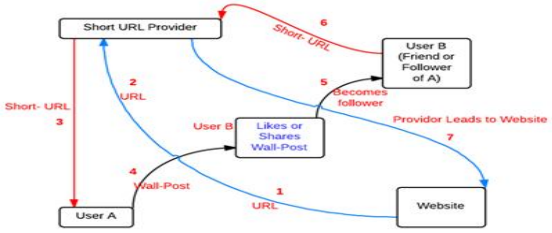


Figure 2: How short-URL works in Facebook

Normal URLS are encoded in short URL using fewer characters (bit.ly or tiny URL are example of short URL providers). The decoding is required, which is depicted in figure 2.

Figure 2 shows how a short URL is used in Wall-Post. Red flow lines depict the use of short URL and blue flow lines depict use of normal URL. It clearly shows how short URL restricts the actual visibility of target website. It can be easily used for malicious activities. In the following coming section we will discuss about propagation of different types of malware.

III. MALWARE PROPAGATION IN FACEBOOK

On the basis of literature survey we came out with three major types of malwares for social network Facebook. ClickJacking (requires user intervention) types, Trojan (requires user intervention) Types and Cross Site Scripting (XSS) (no user intervention is required) types. The first malware which hit the social network was in MySpace (year 2005) known as Sammy worm, which exploited the security flaw present in the web application. Starting from a single user, it exceeded its infection in more than one million users profile after 20 hours. As a result within two days they were bound to completely shut down to resolve the issue.

An XSS type of malware also categorized as XSS virus is a major type of malware attack on Facebook which is basically a malicious code that propagates automatically among users visiting the infected profile. This is because of the presence of flaw in web applications. The propagation of XSS worn is a two-step process. In first step the malware worm writer appends a malicious payload to his own profile. And subsequently any user who is visiting this infected profile will also get payload appended to his profile due to XSS flaw and the aid of exploiting the AJAX. Thus this visitor becomes infected and propagates it further and acts as a new source of propagation.

Another category of malware on Facebook is Trojan types. It is very important to note that this type of malware requires user intervention, unlike XSS which propagates automatically. Facebook has already been targeted with this type of malware in 2008, which is Koobface. It uses social engineering technique which deceives unaware users using interesting topics. Notice that his type can be used with both types of model Wall-Post as well as "Hash'#'" trending model. On clicking the message, users were redirected to a third party website and were prompted to download an executable file, which was pretending to be a new version up gradation of the flash player. On execution, the computer gets infected with koobface. Not only Facebook, MySpace was also targeted by this malware. The infected user machine also becomes zombie. Besides infection of profile, it also sends this malicious message to all the people on the infected user list. This type of malware activity is also very common in chat client and video conferencing client like Skype.

The third major category of malware in Facebook is ClickJacking. This technique is one of the most useful for normal unaware users which deceived using counterfeit posts. In ClickJacking technique the malicious code writer create a fake graphical message or uses trending YouTube video to hide malicious link which is also used to hide "Like" button of Facebook. This hiding method is known as UI redressing. And it opens a straight pathway for malware propagation. When user clicks on the link or image, it actually Likes that post and becomes follower and also gets visible in his Wall-Post and further propagated by his connections. This can be combined with other types of malwares and will generate a new hybrid type of malware attack. ClickJacking and Trojan types requires user intervention hence their propagation is also similar.

IV. SIMULATION EXPERIMENT

Simulator used is Netlogo Based Simulator. The first experiment shows the spread of malware through a social network. The effect of clustering coefficient is already been studies for the speed of propagation of malware. The effect of user behaviour in malware propagation is studied through simulated model. In this simulation first interpretation is that every user is represented through a node and we are trying to model the propagation of malware through this simulated social network.

Every user (node) may be in 1 out of the 3 defined states: susceptible state of user, infected state of user and resistant state of user.

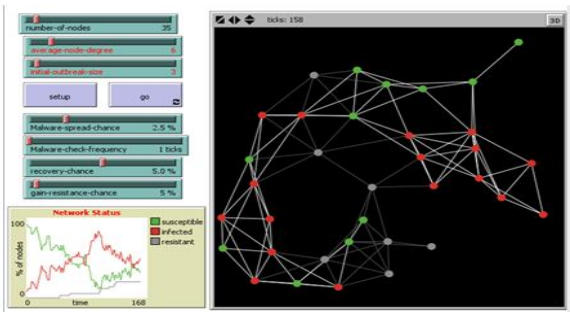


Figure 3: Screenshot of Malware simulator for illustration purposes only

With each tick (time step), every infected node (Red colour) tries to infects all its surrounding nodes.

Susceptible nodes (Green Colour) will get into infected state with a probability given by the slider which is termed MALWARE-SPREAD-CHANCE slider. This slider represents the probability that some Facebook profile user will click on the malicious shared Wall-Post or any malicious post using trending Hash'#' model and it will get infected. Resistant nodes (Grey colour) cannot be infected. This is the scenario when a user gets security awareness or their profile as already been patched and used to of social engineering techniques used to deceive Facebook users. MALWARE-CHECK-FREQUENCY slider check whether nodes are infected by malware or not. When the malware is identified then there is a new probability that the malware will be truncated and is given by a probability slider which RECOVERY-CHANCE slider. After recovering there is a probability that it will become resistant from further infection from malware. And this is determined by GAIN-Resistance-Chance Slider. This corresponds to user awareness and once become aware the link between its connection and neighbours nodes are darkened, since they are now having a nil probability of getting infected.

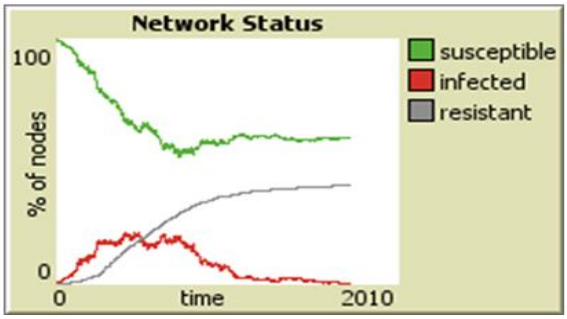


Figure 4: Propagation of Malware and Different states of Nodes

Number of Nodes	1000
Average number of degree	6
Initial-Outbreak-size	3
Malware Spread Frequency	2.5%
Malware Check Frequency	1 tick
Recovery Chance	5.0%
Gain Resistance Chance	5%

Table 1: showing Number of node and Probabilities Defined

Figure 4 clearly shows that higher the malware spread frequency, higher the rate of propagation and which corresponds to unaware users. In ClickJacking and Trojan type of malware when user is not aware and click on the link containing malicious code increases the probability of spreading of malware.

The Figure 4 also shows that increasing the recovery chance increases the power of gaining resistant and hence reducing the rate of propagation of malware in social network.

In future work, we will suggest adjustment to the present exiting analytical model of malware propagation which is known as Susceptible-Infection (SI) model [9]. It will include constant factors of intervention of user like Malware spread chance probability, Malware check frequency probability and Recovery chance probability.

CONCLUSIONS

In this paper effect of social engineering technique and user awareness is studied through simulations. In this simulation we have performed using different sets of values and got the same result. Degree of distribution is same for all experiments and it clearly shows that higher the malware spread frequency, higher the rate of propagation and which corresponds to unaware users. In ClickJacking and Trojan type of malware when user is not aware and click on the link containing malicious code increases the probability of spreading of malware. And also shows that increasing the recovery chance increases the power of gaining resistant and hence reducing the rate of propagation of malware in social network. Imparting awareness to user will prevent the malware propagation at a higher rate and will show down the crime conducted using social network Facebook.

REFERENCES

[1] M. Mannan and P.C. van Oorschot, "On Instant Messaging Worms, Analysis and Countermeasures," in Proc. of the 2005 ACM Workshop on Rapid Malcode-WORM'05. New York, NY, USA: ACM, 2005, pp.2-11.

[2] C. Shin-Ming, A. Weng Chon, C. Pin-Yu, and C. Kwang-Cheng, "On Modeling Malware Propagation in Generalized Social Network," Communications Letters, IEEE, vol. 15, no. 1, pp. 25–27, 2011

[3] Gary Wassermann, Zhendong Su, "Static detection of cross-site scripting vulnerabilities", Proceedings of the 30th international conference on Software engineering, ICSE '08, Leipzig, Germany. 2008

[4] McAfee Avert® Labs Threat Library, Available from: http://vil.nai.com/

[5] "Bitly— Do More With Your Links." [Online]. Available: https://bitly.com/

[6] "TinyURL.com - Shorten That Long URL in a Tiny URL." [Online]. Available: http://tinyurl.com/

[7] Stonedahl, F. and Wilensky, U. (2008). NetLogo Virus on a Network model. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL

[8] Wilensky, U. (1999). NetLogo. Center for Connected Learning and Computer-Based Modeling, Northwestern University, Evanston, IL.

[9] M. R. Faghani, H. Saidi, "Social networks' XSS worms", In Proc CSE09, 2009, pp. 1137 – 1141.

[10] Analysis of Malware Propagation in Twitter, 2013 IEEE 32nd International Symposium on Reliable Distributed Systems

[11] Faghani, Mohammad R., Ashraf Matrawy, and Chung-Horng Lung. "A Study of Trojan Propagation in Online Social Networks", 2012 5th International Conference on New Technologies Mobility and Security (NTMS), 2012.

[12] http://electronics.wesrch.com/paper_details/pdftext/EL11TZJMKSBUP/malware_propagation_in_online_social_networks,April, 2010

[13] http://faghani.info/A-Study-of-Trojan-Propagation-in-Online-Social-Networks, 2012

[14] http://modelingcommons.org/browse/one_model/1604

★★★