Social Networking - Another Breach In The Wall

Gajendra Bamnote*, Gajendra Patil **, Amol Shejole*

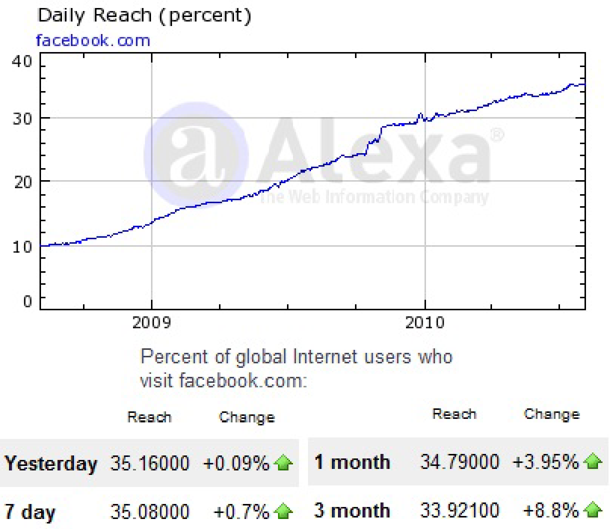
*Head, Department Of Computer Science, PRMITR, Badnera, Amravati, India
** Head, Department Of Computer Science, MCOET, Shegaon, Amravati, India
*Software Engineer, Infosys Technologies Ltd., Bangalore, India

Abstract — With the increasing popularity of social networks like Facebook and MySpace, such sites have lately become the favourite destinations for spammers and attackers. Social networks have experienced complex social engineering attacks, massive spam and aggressive malware distribution in the recent past. This paper presents a practical case study of social engineering, malware distribution and phishing attacks against social networking sites that are identified over last few months. It is explained how private data of the users are exposed to attackers and how easily their privacy is compromised as a result of these attacks and their own careless behaviour.

Keywords— Spam, Social Engineering, Threats, Malware distribution, Social networks, Phishing

I. INTRODUCTION

According to recent statistics, the number of people using social networks like facebook is increasing exponentially. A big percentage of internet users visit these social networks on a daily basis. Facebook currently has more than 500 million active users, from which 50% logon to the site in any given day. According to alexa.com statistics, facebook reaches more than 35% of the internet users. An average facebook user has 130 friends and people spend over 400 billion minutes per month on facebook per month. Also around 100000 businesses from all over the world have their page on facebook. The above statistics clearly show that a social network like facebook is an ideal place for an attacker to plan a social engineering attack.



Percent of global Internet users who visit facebook.com:

	Reach	Change		Reach	Change
Yesterday	35.16000	+0.09% ↑	1 month	34.79000	+3.95% ↑
7 day	35.08000	+0.7% ↑	3 month	33.92100	+8.8% ↑

Figure 1. Facebook stats from alexa.com

The main reason behind the popularity of facebook is its innovative application platform which allows anybody with the knowledge of software development to develop and distribute applications freely. The facebook statistics page shows that over 70% of the users engage in the platform applications every month. Due to the same reason it has become easier for attackers to develop and distribute malware. In the last part of this paper we will see a practical case study to analyze the user acceptance of such social engineering schemes.

II. SOCIAL APPLICATIONS, A BOON FOR ATTACKERS

Facebook first introduced the concept of social applications in early 2009, followed by which a huge number of applications where developed for the users. Other sites followed facebook in order to keep in pace with facebook. Many of these applications access user's private data. Soon attackers started fabricating applications to deceive the potential victims into thinking that they are installing legitimate applications which in fact were fake.

A big number of these applications include social games like Farmville, Mafia Wars, etc. which require more number of friends to achieve better scores. In order to achieve good scores at these games people started adding more and more friends to their lists without even bothering about the authenticity of the profile which is being added. All this things made spamming a cakewalk for the attackers. Once a spambot is added to your account, it doesn't constitute an abuse as you are the one who added it and not the other way around. Soon the bot will send some informal messages followed by some link which can lead you to anything from a Trojan to a phishing page.

III. CHARITY SCAMS AND HOAXES

Social networks provide a platform for the users to interact. Some people use this platform constructively while other don't. In past it has been proved that social networks can act

CP1324, International Conference on Methods and Models in Science and Technology (ICM2ST-10)
edited by R. B. Patel and B. P. Singh
© 2010 American Institute of Physics 978-0-7354-0879-1/10/$30.00

as a very good medium to collect charities for various natural disasters like Tsunami, Haiti quake, etc. Soon spammers started making fake groups and pages on various social networks which titled "HELP HAITI REBUILD" followed by a link which take you to the payment page where you will be asked to enter your credit-card information to send your charity amount to those affected in the Haiti quake. In fact the amount you pay will be credited to the attacker's bank account. Such scams are common on all the social networking sites these days.

On the other hand hoaxes tend to be rather funny than dangerous. Still the fact is there is a huge community of internet users who take such claims seriously. A lot of groups exist on facebook which have some false Hoaxes as the title and still manage to gain quick popularity. One such group was "NO I WILL NOT PAY $3.98 A MONTH TO USE FACEBOOK AS OF JULY 10TH 2010!" which managed to accumulate close to 1 million members within a week's time. The scale of this hoax was so large that facebook had to come up with a press conference to announce that it has no such plans in the near future.

IV. Phishing Attacks on Social Accounts

Phishing is a way of stealing usernames and passwords of social accounts of users by presenting a fake login page in front of them. As soon as the user enters his information into such a page it is directly conveyed to the attacker. Such hacked accounts are then used to post spam links and malware to friends' accounts. The harmful effects of phishing include:

- Identity theft and users' personal details.
- It can result in financial or in some cases it prevents users from accessing their own accounts.
- Excessive consumption of resources at corporate level (bandwidth, saturated mail boxes, etc).

Phishing has reached to the next level, recently it has been discovered that attackers not only hack the user accounts but after logging into the fake site they ask the user to download some plug-in which is nothing but a malware which infects their computer and turns it into a 'zombie" machine which does the work of spreading the malware to other machines.

One very dangerous form of phishing is known as pharming. It includes modifying the domain name resolution system to redirect users to false web pages. When a user enters a website address into the address-bar of the browser, the browser first contacts the domain name servers to find the IP-address of that domain. But before that it first checks for the IP-address in a locally located file called 'HOSTS'. Some types of malware modify this file and force the browser to redirect to a fake IP-address even if a valid domain is entered. Pharming is a continuous process in which the attacker waits for the user to visit the target site instead of tricking him into visiting the fake page which makes this method very effective.

Below are some tricks to avoid falling victim to phishing attacks:

- Always check the source of an email that you received before entering any personal information to any of the links that it contains.
- To open links in a suspected email type the link into a new browser window instead of clicking on it.
- Check that the webpage you visit is a secure site whenever possible. It can be identified by checking for "https://" in the URL and a little closed lock displayed on the status bar of the browser.

V. Social Malware

A considerable amount of spam was massively distributed through social networks over the last year. The method used by the attackers to do this was simple but effective. They used some phished social accounts to post messages containing link to the malware. These messages were posted to the victim's friends' accounts and it was observed that the confidence one has in clicking the links sent by friends is way more than the links which are posted by spam bots.

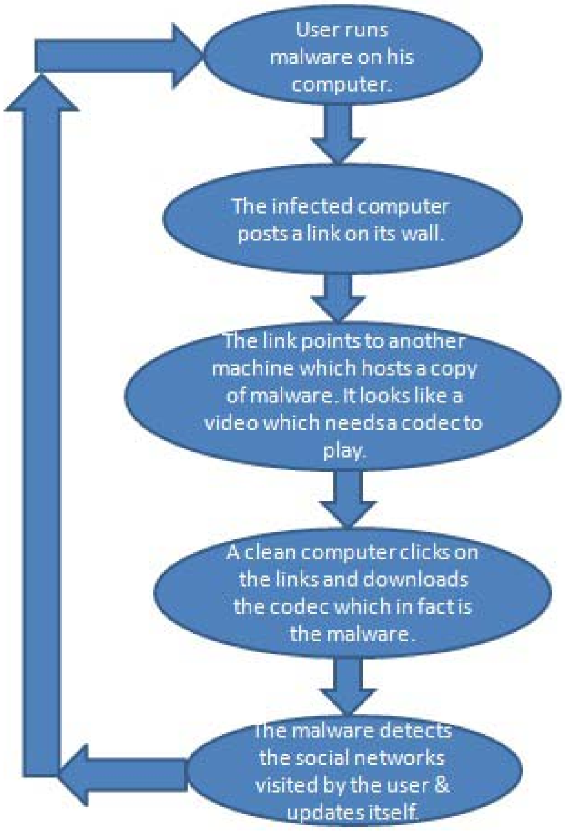

User runs malware on his computer.
The infected computer posts a link on its wall.
The link points to another machine which hosts a copy of malware. It looks like a video which needs a codec to play.
A clean computer clicks on the links and downloads the codec which in fact is the malware.
The malware detects the social networks visited by the user & updates itself.

Figure 2. Lifecycle of Koobface

"Koobface" was one of the most massively distributed malware which used facebook as a medium to spread. The key to the wide spread of "Koobface" was reputation stealing as it used the users account to send the malware link to his friends who blindly opened it thinking that it has been sent by an authentic user. As soon as a user opens the link, it points him to a page which looks like a YouTube video asking him to download some plug-in. The user thinks that the plug-in is required by the video to play and he clicks the download button. In fact it is nothing but a copy of the malware which is being downloaded by the user from some already infected machine. This newly infected machine will in turn act as a host to store a copy of the malware. A diagram with the steps that are followed by "Koobface" in its entire lifecycle is shown in Figure 1.

VI. User Acceptance Case Study

One of the main reasons why social engineering schemes prove to be so successful in social networks is that it is very easy to enter into the circle of trusted friends of a user. To observe and analyze how easily social network users can be tricked into adding unknown people to their friends list we conducted an experiment which is explained in the next section.

We created the following three types of facebook accounts which will act as honey-pots in our experiment:

- Account1: A profile with a no picture and as few details as possible.
- Account2: Another profile with more details and a picture.
- Account3: Yet another facebook profile with a hot girl picture and a lot of details.

After that we joined a few social groups like "We are from Mumbai", "I love chocolate" etc. and added 100 random friends in each of the profiles. After two days we checked the status of the profiles and two our surprise, our first socializing effort proved to be effortless. We managed to add 29 friends in Profile1, 44 friends in Profile2 and 58 in Profile3.

In the second step we installed some social applications on all the three profiles and tried to add friends in social games groups. The friends count increased to 111, 163 and 203 for profile1, profile2 and profile3 respectively.

The third step consisted of adding mutual friends of all the friends in every profile. And the figures we got were quite unexpected. More than 60% of the mutual friends accepted the requests. The final counts of the in the three profiles were –

- Profile1: 233
- Profile2:367
- Profile3:499

The fourth and last part of the study consisted of posting a link which was cloaked using a free URL cloaking service. 28% of the users followed the link posted by an unknown person who is on their list without even knowing where it points to.

VII. Conclusions

We concluded from our studies that the complexity of attacks on social networks is increasing day by day. The attacks which are being carried out in 2010 are way more complex than those experienced in 2009.

It was proved from the case study that people tend to accept unknown people in their friends list thereby creating a conducive environment for spammers and attackers in the form of social networks.

To conclude, we can say that being the most popular concept of the modern age, social networking is also the most vulnerable

References

[1] Wikipedia http://www.wikipedia.org

[2] Facebook Statistics page: http://www.facebook.com/press/info.php?statistics

[3] BBC Portal: http://www.bbc.co.uk

[4] Alexa: http://www.alexa.com

[5] Unofficial guide to Ethical Hacking by Ankit Fadia

[6] Fighting Malacious Code by Ed Skoudis and Lenny Zeltser

[7] Stop Being a victim by Dave Gray

[8] The truth about avoiding scams by Steve Weisman (FT Press)