# Facebook – Another breach in the wall

George Lucian Petre

*Threat Intelligence Team Leader*
*BitDefender, Bucharest, Romania 062204*
glpetre@bitdefender.com

***Abstract*— As the most popular Social Network of the moment, with an impressive growth in the last year, Facebook has become lately the scene of complex social engineering attacks, aggressive spam and massive malware distribution. This paper presents an overview of phishing, spam and other social engineering attacks against Facebook identified over the last year. In addition, it is explained how the users' private data are exposed as a result of social gaming. In the last part of the paper, we conduct an experiment which illustrates how carelessly users rush to add unknown friends to their profiles, join unknown groups or become fans of hazardous pages.**

***Keywords*— Facebook, Phishing, Spam, Social engineering, Malware,Tthreats**

## I. INTRODUCTION

According to statistics presented on their site[1], Facebook have more then 350 millions worldwide active users on January 2010, exceeding United States population and representing 5.14 % of the worldwide population and 20.18 % of the worldwide internet users[2]. Also, more than 700000 businesses have a page on Facebook. With such a large number of users representing both segments: private users and businesses, we can certainly say Facebook is the ideal location for an attacker to plan a social engineering scheme.

Our 2008 workshop on spam at Spam Conference [2] focused on analysing threats associated with social networks at the time when it was difficult to identify dangerous attacks within the Facebook network and even find samples of simple attacks. Today we can easily identify spam campaigns, malware with multiple variants targeting Facebook users(KoobFace), phishing campaigns for collecting Facebook accounts or fake donations for disasters like Haiti earthquake.

## II. SOCIAL GAMES, A GATE TO THE USER

A considerable amount of new social games like Farmville, Mafia Wars, Castel Age and others appeared in the second part of 2009. To achieve a better score at these games, you need as many friends as possible. This is why, as shown in the Fig nr. 1 we found a lot of groups designed to obtain instant a huge number of friends to the favorite social games.

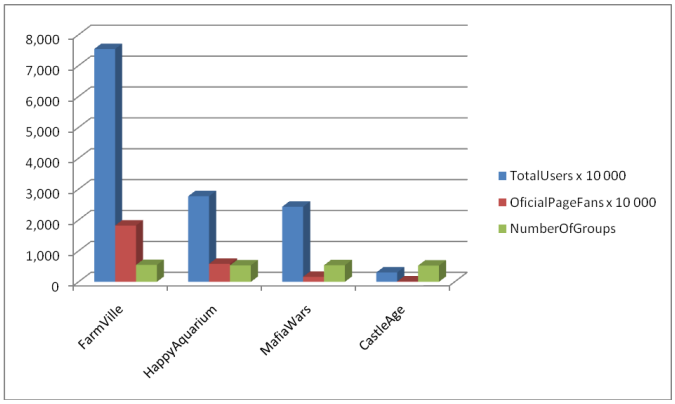


Fig. 1 – A comparative graph showing some of the most popular games on Facebook, including number of users, number of fans on the main page and groups dedicated to them

These groups are the best place for spambots to enter legitimate users friends lists. To understand better how these bots work, we joined some of these groups using a honeypot Facebook profile. We chose Farmville because this is the most popular game on Facebook. We joined several groups and added to our friends list the profiles with a "hot picture" that posted on the wall of the group messages like "add me as your neighbour". Following the addition of our profile, we received a "Hi" introduction message to which we replied. Subsequently, we received a link to a video chat website. Even if this scenario is a familiar one for e-mail spam campaigns, this particular situation presents some distinctive features:

- The user added the spammer to his profile, and not the other way around, when the spammer ads the user. This is why the spammer's action doesn't constitute an abuse, therefore his account can't be suspended
- Spambot first sends a "Hello" message. This is a strategy to win the user's trust
- Finally, after user response, the link to the video chat website is sent through a shortening url service, which doesn't allow the user to see the final destination of the page until he clicks
- Photos and details from the profile make spambot look more "human".

## III. HOAXES AND CHARITY SCAMS

The old messenger hoaxes such as "If you don't give this messages forward Yahoo will delete your account" have now a friendlier approach. "NO, I WILL NOT PAY £3.99 A MONTH TO USE FACE BOOK FROM JULY 9TH 2010!" is a group that has over 888 594 members. More than 500 groups are cloning the idea and discuss about different fees and dates when Facebook account will be charged. Because of the large scale of this phenomenon, Facebook was forced to deny these rumours in an important newspaper[4].

If the hoaxes tend to be rather funny than dangerous, on the other hand there are a lot of potentially dangerous scams based on charity appeals. The earthquake in Haiti triggered a global outpouring of sympathy which resulted in considerable donations through various channels worldwide. As a result of this, a lot of phishing schemes were developed, and a considerable amount of Facebook applications or pages started to promote themselves using the "donation to Heiti" idea.

One of the most interesting cases is about a Facebook group that pretended it will donate 00.01$ for each Facebook user who becomes fan of that page. In just 5 days the page reached to a staggering 2 000 000 fans. A lot of spammy links were distributed to users through this page. After reaching about 2 million fans, the page was shut down for abuse.

## IV. PHISHING OF FACEBOOK ACCOUNTS

At the end of October 2009, our e-mail honeypots were the target of a massive phishing attack designed to collect credentials of Facebook users. The attack was even more vicious as, together with the phishing, it delivered also a version of Zbot[5] . There are two delivery methods:

- as an attachment of e-mail
- as an utility delivered after the user logged into the fake Facebook site. This kind of phishing attacks are conceived as a double strike: one is the spambot that distributes malware and phishing via e-mail and the other is the theft of Facebook account credentials that, as it results from our experiment, start posting malware and spam links on user profiles.

## V. FACEBOOK MALWARE

A considerable amount of worms was massively distributed through Facebook wall. The method was simple but effective. Using some Facebook phished accounts, attackers posted a malware link associated with a provocative picture and a catchy message. Exemples are: "Wanna C Somthin' HOT!??" or "My Ex-Girlfriend Cheated on me. Here is my revenge!". While some of these worms were just posting embarrassing entries in every Facebook logged-in user using the Share feature, some of them distributed malware through this method.

It may sound quite unsophisticated, but the confidence one has when clicking links from friends is considerably higher than clicking spam e-mail.

## VI. KOOBFACE – A REVOLUTIONARY MALWARE

Koobface was the first massivly distributed malware especially designed for social networks. Koobface has many modules, one of them being dedicated to social network spreading. The success key of Koobface is reputation stealing. An infected user starts posting links to a fake youtube link. The link points to another koobface infected machine, that runs another component of Koobface malware, called the downloader. A chart with the scheme of Koobface infection can be seen in the Fig. 2

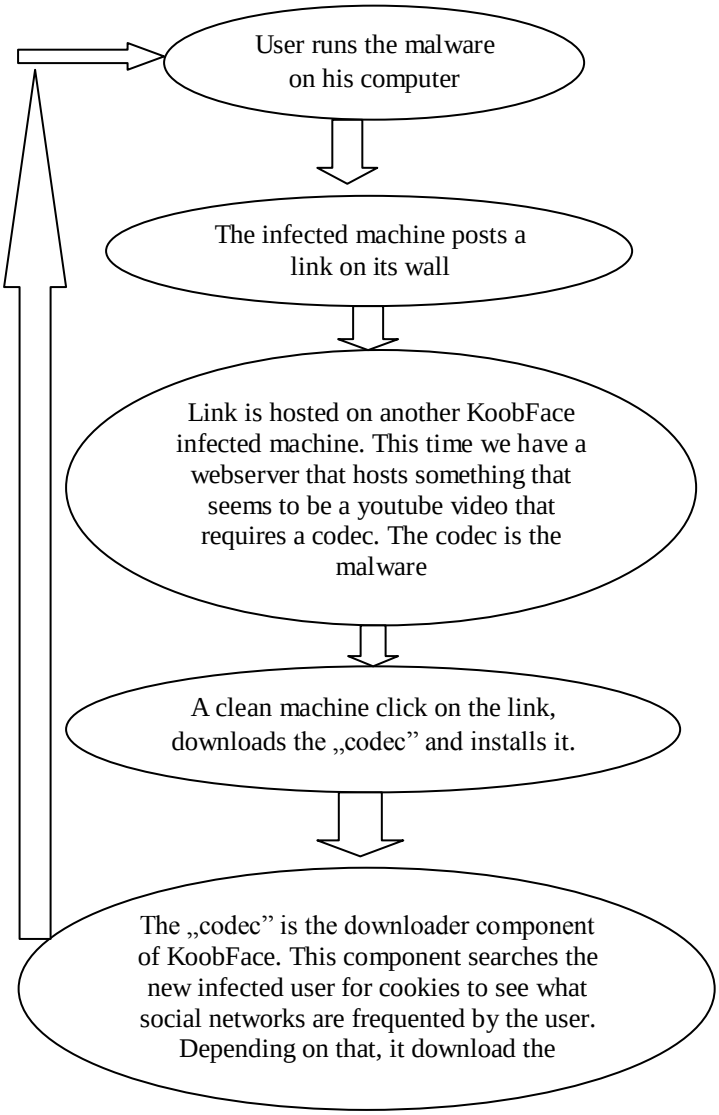


Fig. 2 – How KoobFace is spreading on social networks

## VII. USER ACCEPTANCE EXPERIMENT

One of the main reasons why social engineering schemes are so successful in social networks is that attackers can easily enter the circle of trusted friends. We conducted an experiment to observe and analyse how easily Facebook users can be tricked to add unknown persons as friends.

We created the following type of accounts: one profile without picture and containing as few details as possible(1st profile), another profile with a picture and a few details(2nd profile) and yet another profile with a large amount of details and pictures(3rd profile). With each profile we joined some groups of general interest to make a few friends: "Bitch Please. I'm from New York", "BMW", "ADDICTED TO FAMILY GUY", "Chocolate = Love ♥ !!!".

Our first socializing attempt was rather effortless. Just one hour after starting to add people to each profile, we managed 23 connections with the 1st profile, 47 with the 2nd profile and 53 with the 3rd profile.

Subsequently, we joined social games groups, and started to add friends there. At this point, we were even more successful in adding people. As a result, after 24 hours of monitoring all 3 profiles, the statistics showed: 85 for 1st profile, 108 for 2nd profile and 111 for 3rd profile.

The 3rd step consisted in giving add to "mutual friends". The success was again on our part because more then 50% of mutual friends accepted a connection with our profile.

The last part of the experiment focused on posting a bit.ly url without text on each of the 3 profiles and observing how many people follow it. The experiment showed that about 24% of the total number of friends of the profiles followed the link, even if they didn't know where the link goes or from where/whom it comes.

## VIII. CONCLUSIONS

This overview of the threats faced by Facebook and Facebook users revealed that starting with 2008 attacks are far more complex than before.

As it is shown in the acceptance experiment, users are more likely to accept spammers in their friends list when they are in a social network than in any other online communication environment. This fact brings spam and social engineering schemes closer and more effectively to the user than any email spam or scam.

Moreover, we have seen that in social networks, users can easily be tricked to add spammers to their profile.

To conclude, we can say that being the most popular social network at this moment Facebook is also the most exposed social network to these kinds of attacks.

## REFERENCES


[1] *Facebook Statistics Page* http://www.facebook.com/press/info.php?statistics

[2] Internet World Stats http://www.internetworldstats.com/stats.htm

[3] Cosoi C. , Petre G. – Spam 2.0 (Workshop) – MIT Spam Conference 2008,Cambridge, MA, USA

[4] Telegraph http://www.telegraph.co.uk/technology/facebook/6973757/Facebook-dismisses-rumours-of-charging-plans.html

[5] *ZBot Trojan Explained* http://www.bitdefender.com/VIRUS-1000561-en--Trojan.Spy.ZBot.EHE.html

[6] *The real face of Koobface* – J. Baltazar, J. Costoya, R. Flores, Trend Micro Threat Research

[7] *Is Britney Spears Spam?* - A. Zinman, J. Donath - CEAS 2007 – Fourth Conference on Email and Anti-Spam, August 2-3, 2007, Mountain View, California USA

[8] *Brazen Black Hats: How we fight online fraud in a socially networked world* – V. Sharma- VB 2009, Geneva, Switzerland

[9] *Socialnetworkeering*: or, the friend of my friend is my enemy – *A. Lee* - VB 2009, Geneva, Switzerland

[10] http://fitzgerald.blog.avg.com/2009/11/new-facebook-worm-dont-click-da-button-baby.html

[11] http://mashable.com/2010/01/29/facebook-revenge-worm/