LOW USER AWARENESS AGAINST SOCIAL MALWARE: AN EMPIRICAL STUDY AND DESIGN OF A SECURITY AWARENESS APPLICATION

Eleftherios Karavaras, Department of Informatics, Ionian University, Greece
p12kara@ionio.gr

Emmanouil Magkos, Department of Informatics, Ionian University, Greece
emagos@ionio.gr

Aggeliki Tsohou, Department of Informatics, Ionian University, Greece
atsohou@ionio.gr

Abstract

During the past few years, in harmony with the fast growing rate of user population in Online Social Networks (OSNs), a trend for malware writers has been to take advantage of the social relationships of OSN users, in order to lure them into following malicious URLs that lead to malware infection. One reason for the success of such Social Engineering (SE)-based malware has been the low security awareness of OSN users. Indeed, it can be shown that, on the average, OSN users do not have sufficient knowledge of the malicious link threats they may come up against, and thus are easy victims of SE attacks. In this paper we conduct an empirical investigation which, on the one hand, demonstrates Facebook users' low awareness of malicious link threats, and on the other hand explores the views of OSN users on the desirable properties of a security application that protects them against social malware. Furthermore, we design and describe the architecture of a security application which intends to raise Facebook users' security awareness by informing them about (possibly) malicious posts on their walls before or after they get infected. Our application acts proactively by helping users to not get infected by malicious posts, and reactively by helping the users who got infected to gain an understanding of the threat and become more alerted towards identifying malware links.

Keywords: Social Engineering, OSN users' security awareness, Social malware

INTRODUCTION

During the recent years, the number of Online Social Network (OSN) users has grown in an enormous rate. By October 2015 there were 1.01 billion daily active users and 1.55 billion monthly active users, 14% more than October 2014 (Facebook Reports Third Quarter Results, 2015). On the other hand, there has been a fast growing rate of malware spreading through users following malicious URLs, e.g., clicking on a malware download link. Indeed, 75.76% of all web malware attacks were malicious URLs in 2015 (Kaspersky Security Bulletin, 2015a). Also in 2015, almost every third computer of a company (29%) was subjected to web-based malware attacks, 57% of which were conducted through malicious URLs (Kaspersky Security Bulletin, 2015b). A natural trend for malware writers has been to try taking advantage of the social relationships of OSN users, in order to lure users into following malicious URLs (FBI Internet Crime Report, 2014). As a result, a significant fraction of Facebook posts can be characterized as spam and a non-negligible portion may lead to phishing or malware infection (Chen & Alzubi, 2011). Malware of this kind has been referred to as social engineering malware or simply as social malware (Abraham & Chengalur-Smith, 2010), which may propagate through emails, websites, social networks or portable storage media.

A motivating example. Alice, a Facebook user, signs to her account and receives one unread notification. On the top of the list of notifications, Alice reads the following message: “User Bob mentioned you in a post”. By clicking on this notification Alice is redirected to a post where she is tagged by her friend,
Bob. Alice clicks on the URL contained in the post, which redirects to a website that prompts her to download and install a specific program. Unfortunately, Alice gets infected and, after a while, she unknowingly tags (some or all of) her friends in a post containing that (or a similarly) malicious URL.

The issue of user security awareness evidently becomes crucial for addressing the social malware problem and Internet security threats in general. As Kritzinger and von Solms (2010) state the most important factor for home users being vulnerable to security threats is their lack of awareness about risks of using the Internet. Researchers in previous years have mentioned that the weakest link in information security is computer users (Arachchilage, 2013; Purkait, 2012). The most frequent type of attack that takes place in OSN is social engineering because as Irani (2011) mentioned “it is easy to propagate, difficult to trace back to the attacker and usually involves a low cost per targeted user”. To this end, for example, the European Commission has been supporting numerous national campaigns and initiatives in most European member states, under the name ‘Safer Internet’, in an effort to address the low user awareness on Internet security threats.

**Our contribution.** In this paper we focus on exploring how aware OSN users are regarding malicious URLs in social media as well as on designing a security application to address social malware. Specifically, we conducted an empirical investigation to explore the awareness of Facebook users regarding malicious link threats. Our findings demonstrate Facebook users’ low awareness with respect to such threats. As a remedy to the low awareness of OSN users for malicious links, and also by taking into account the results of the empirical investigation, we sketch the architecture of Soc-Aware, a security application which intends to raise Facebook users' security awareness by informing them about (possibly) malicious posts on their walls before or/and after they get infected by them and, at the same time, informing them about the number of times they tagged (or were tagged by) someone in a malicious post. After a threshold of incidents, users are redirected to relevant awareness material, in order to increasingly stimulate their understanding of social malware threats. Unlike previous works, our application also aims on helping users who got infected (reactive) and not only prevent users from getting infected (proactive). Soc-Aware has been designed by taking into account the fact that a few OSN users prefer an application that only alerts for possible malware link threat, instead of an application that automatically deletes a possibly malicious post.

This paper is organized as followed. In Section 2, we review related work in the area of raising OSN users' security awareness against SE-based attacks that may lead to malware infection. In Section 3, we present the results of an empirical investigation regarding Facebook users' awareness of social malware attacks. Section 4 gives a sketch of the architecture of a Facebook application that aims to raise Facebook users’ security awareness. Sections 5 concludes the paper.

**RELATED WORK**

In order to examine existing work associated with our research objective we identified literature sources that fall under any of the following areas: a) social engineering threats against OSN users, b) software tools protecting users from social engineering attacks in OSNs and c) software tools protecting users specifically from malicious URL in social networks. For our examination we used Google Scholar, Elsevier/ScienceDirect and ACM digital library information systems and computer science databases.

Several researchers examine Security Engineering (SE) in OSNs (Hobgen, 2007; Chitrey et al., 2012; Algarni & Xu, 2013; Heartfield & Loukas, 2015). SE attacks in OSNs that had been studied include spam threats, phishing, cross-site scripting, viruses, spoofing, and identity theft (Minchev, 2012; Kumar et al., 2013), as well as automatic ways of social-engineering attacks such as ASE bots (Lauinger et al., 2010; Huber et al., 2009; Boshmaf et al., 2012; Boshmaf et al., 2013). However, there is limited research on SE attacks to OSN users through malicious links that may lead to malware infection, as well as regarding the user awareness level regarding to such threats. Dowland and Furnell (2008) discuss that home users can become an easy target for malware threats, scamming and identity theft, especially if they lack awareness. Their empirical investigation reveals that home users in general lack information security awareness concerning malware. Based on these insights we were interested, in particular, to investigate how aware social network users are concerning malware threats.
Some researchers have developed countermeasures to prevent malicious link threats in general. For example, Thomas et al (2011) created Monarch, a crawler for detecting URLs that redirect to spam content, while Lee et al (2012) developed Warningbird, a real-time classifier that detects suspicious URLs in Twitter streams. In another work, Rahman et al (2012) developed an application which crawls the walls of Facebook users and searches for malicious URLs and if it finds any it notifies the owner of the post and the users in whose wall that post appears. Our envisaged application, described in Section 4, specifically focuses on malicious link threats that specifically lead to malware infection: Taking into account that security awareness aims at stimulating security protective behaviors, motivating users to recognize security concerns and respond to them (Katsikas, 2000), our proposed application not only informs users about possible malicious links, in order to prevent their infection, but also provides them with personalized information about the times they were victims of social malware and redirects them to relevant awareness material to stimulate their understanding of social malware threats.

To the best of our knowledge, there has been limited work in the area of developing real security systems that detect malicious links, posted in OSN profiles that can possibly lead to malware, and notify users about the associated risks (e.g., Lee et al, 2012; Rahman et al, 2012). Defensio\(^1\), in another example, is a Facebook application that monitors all posts in a profile and determines, among others, whether they may lead to malware. Most such works, by using Machine Learning to detect malware, cannot avoid a non-negligible amount of false negatives/positives. Our envisaged application, described in Section 4, differentiates from such works in the way it detects malware. Specifically, our application acts as a normal user, it follows every URL and downloads any additional software it is asked to and, if any of the above actions lead to (potentially) malicious the user is notified and redirected to relevant awareness material. Moreover, and unlike previously described works, our application also aims at helping users who got infected and not only prevent users from getting infected.

AN EMPIRICAL STUDY OF USER AWARENESS REGARDING SOCIAL MALWARE

**Methodology.** In order to study the level of OSN users’ security awareness regarding social malware threats, we conducted a survey using a questionnaire. The purpose of the survey was to investigate how aware Facebook users are regarding the threat of malicious URLs that spread through Facebook posts, to explore if they had been affected by such malware and how they would wish to be protected from this threat. After developing the survey instrument, we shared it with three Facebook users, whose profession or studies are irrelevant to information security, in order to ensure face validity. These participants assessed each question in terms of the clarity of the wording, whether the target audience would be able to understand and answer the questions and the layout and style. After receiving feedback, we revised the questionnaire accordingly. In order to design and distribute the final questionnaire (please see Appendix) we used Google Forms due to its popularity and characteristics, such as provision of real-time statistical results, and the security and anonymity protection that it offers. The questionnaire was distributed online via Facebook to the authors’ known contacts and was then diffused by those contacts to other Facebook users. The survey was running for 13 days and we received 190 answers in total. We consider that this number of responses is sufficient to reach our goal of getting a realistic perception of users’ level of awareness, understanding their experiences related to social malware, and verifying our original assumption that although users are conscious about general malware threats they haven’t catch up with this evolved malware threat. The 190 participants were equally distributed in terms of gender (87 Males and 103 Females), mainly aged between 13 and 35 with different range of educational background. The results of the questionnaire are analysed below.

**Results.** Our results reveal the social network users’ low level of awareness regarding malware threats that can be propagated through social networks. Compared to the conclusions of the empirical investigation of Furnell and Katsabas (2006) that home users appear aware of malware threats, our investigation demonstrates that, while malware attacks evolved into more sophisticated and social networking-specific forms, the users haven’t followed this evolution. In particular, of all 190 respondents, 20\% did not know that Facebook applications can post on behalf of them on their wall (Fig.

\(^1\)http://www.websense.com/content/facebook.aspx
1) and another 9% did not know that they can get infected by malware just by clicking on a URL. At this point it is important to notice that although there is such a small amount of people unaware of this danger, there is a 34% of people who actually got infected by clicking on a URL on a Facebook post. That means that at least 25% of those aware about the danger, actually got infected. Moreover, 55% of all respondents have clicked on a URL in a friend's post and have been redirected to a page asking them to download some kind of software (Fig. 2). 65% of the respondents said they had been tagged in a friend's post which appeared to be a suspicious URL redirecting to a malicious page (e.g. Spam).

Within our empirical investigation we explored the type of application that users would prefer considering malware protection: an application that only alerts for possible malware link threat or an application that takes preventive action, e.g., automatically deleting a post containing a suspicious URL. Our findings indicate that there is no clear preference in this aspect, as 56% prefers the first category
and 44% the second. As an answer to this preference, in the next section we sketch the architecture of Soc-Aware, a security application which warns Facebook users about possibly malicious posts, and gives them the capability to decide whether a (potentially) malicious link will be followed or not.

**SOC-AWARE, AN APPLICATION FOR RAISING FACEBOOK USERS' SECURITY AWARENESS**

In this section we sketch the architecture of Soc-Aware, an application for raising the awareness of Facebook users regarding malware infection. Soc-Aware has been designed in a way that takes into account the results of our empirical investigation. In particular, although OSN users’ preferences seem to be balanced between an application that only alerts for possible malware link threat compared to one application that automatically deletes a possibly malicious post, there is a small inclination towards the first option. That is why Soc-Aware has been designed accordingly to these empirical finding. As an answer to that, and by informing users about (potentially) malicious posts on their Facebook wall, Soc-Aware will allow users to become more aware of malicious threats. In addition, by providing personalized awareness messages after the user had been infected by malicious links, Soc-Aware will allow users to increasingly become more alerted about the threat.

Soc-Aware is consisted of five logical modules, which cooperate as follows (Fig.3):

**Setup.** When a user installs the Soc-Aware client a unique Access Token (AT) is created by Facebook Graph API allowing Soc-Aware to have access on posts that are published in the user’s Facebook wall.

**Module 1.** This module runs a modified version of open source web crawler Norconex which will receive the AT and parse every post from user’s wall.
Module 2. This module is responsible for separating the posts containing URLs from those who do not and making a list of the URLs found in the parsed posts.

Module 3. This module receives this list of URLs and filters them based on the domain name. For example, any URL which is under the domain name of youtube.com or google.com typically has no reason to be checked. Any URLs not filtered are passed to Module 4.

Module 4. This module receives each non-filtered URL and visits the website that URL is pointing to. As a next step, it searches for any buttons and clicks on them too, in order to ensure that there is not any logic prompting the user to download some software. If any such logic is detected, Module 5 will be notified. Note that Module 4 will be run within a security sandbox so that any malware will not affect the hosting system.

Module 5. Module 5 makes a user aware about a potentially malicious post. Module 5 will include a counter per user which will increase every time the user gets tagged in a post which was characterized by Module 4 as malicious, or when the user tags his friends in a malicious post. After a threshold of $x$ posts (where $x$ is a security parameter, e.g., 5) that tag the user or his/her friends, a new notification will appear making the user aware about the number of times he/she was part of a malicious action and will redirect him/her to a Facebook page that contains malware-related awareness raising content. Furthermore, Module 5 will check whether user was the one who actually tagged his/her friends on a post which was diagnosed as malicious. In this case user will also get informed about the action he can take in order to minimize the effects of this infection.

Typically, after a malicious URL is clicked, the post that contained the URL spreads itself to the victim’s friends. In order to prevent such behavior, Module 4 will be linked to a “dummy” Facebook account, let say $A$. In this way, all suspicious URLs will be first clicked on behalf of the “dummy” user $A$ in order to study the full behavior of the malware. Furthermore, Module 5 will also be linked to a second “dummy” account, let say $B$. If any of the URLs clicked has as a goal to spread itself to the victim’s friends, this will lead to a malicious post on B’s wall. When this kind of action is detected, Module 5 is responsible to inform the user about the malicious post on his/her wall.

Soc-Aware will take into account requirements that derive from Furnell (2005). Furnell had investigated the reasons why security is not “usable” by home users and cannot enable awareness. As a remedy he recommends that security solutions should not be fractured across different menus and sub-options, should not place security settings or functions under ‘advanced’ menus and should provide visible indication of security status to the home user. Soc-Aware will be running on the background – therefore the two first requirements are indirectly satisfied – and through the counter Soc-Aware will offer to the user a visible indication of the times that she endangered and potentially infected her computer.

Currently, Soc-Aware is under development and its basic functionality being tested. In a future work, we intent to systematically evaluate the effectiveness of Soc-Aware with respect to state-of-the-art factors that affect the effectiveness of a security awareness system. Such factors could include properties such as (Ikhalia and Serrano, 2015):

- **Time efficiency.** That is, to deliver multi-media contextual security awareness to end-users as briefly as possible.
- **End-user engagement.** That is to deliver messages that are appealing to the consciousness of the intended users and enjoyable to engage with.
- **Integration.** That means to provide awareness software that is integrated with the online social networking platform.
- **Activity specific property.** The awareness actions need to be specific to the users’ particular social networking activities.

---

2 For this reason, a database with such unsuspicious domains will be created so as to make Soc-Aware more time-efficient.
•  Knowledge testing. The awareness software should allow assessing the impact and learnability of the awareness program to the user and this knowledge testing should be integrated with the security awareness program deployed to the user.

CONCLUSIONS

The focus of this paper was on investigating the awareness level of Facebook users regarding malicious URL threats which can lure them into getting infected by malicious software. Our survey that run with 190 Facebook users, verified our initial intuition about the low level of awareness regarding malware threats that can be propagated through social networks. Indeed, a few users were not aware that a Facebook application can post on behalf of them on their wall, while more than one third of participants had experienced infection by clicking on a URL in Facebook. Our results emphasize the need to raise security awareness of OSN users as a way to reduce the risks associated with social malware threats, and in general with social-engineering based threats in OSNs.

In addition, we gave a sketch of the architecture of Soc-Aware, a security application which intends to raise Facebook users' security awareness by informing them about (possibly) malicious posts on their walls and, at the same time, redirecting them to relevant awareness material, in order to stimulate their understanding of social malware threats. Our application will have both proactive and reactive security features, in that it also aims on helping users who got infected but also protect users from getting infected. Soc-Aware is under development: A systematic evaluation of its security, awareness and performance characteristics will be provided in a future work.

References

Boshmaf, Y., Muslukhov, I., Beznosov, K., &Ripeanu, M. (2012). Key challenges in defending against malicious socialbots. 5th USENIX Workshop on Large-Scale Exploits and Emergent Threats, 12-16.


---

**APPENDIX**

**User Security Awareness on Social Networks**

The following questionnaire is part of an academic research which studies the level of user security awareness on social networks. We kindly ask you to take part in this research as a
Facebook user, in order to provide us with your personal opinion and experience. Your participation is voluntary and you will need about 5 minutes to complete the questionnaire. We affirm that the data will only be used for academic purposes, ensuring participants' anonymity.

What is your gender?
- Male
- Female

What is your age?
- Under 25
- 26-35
- 36-45
- 46-55
- 56 or over

What is your education level?
- No education
- Elementary School Graduate
- Secondare School Graduate
- High School Graduate
- Bachelor’s Degree
- Master’s Degree
- Doctoral Degree

Do you have a Facebook account?
- Yes
- No

How often do you sign in to your account on Facebook?
- Less than once a day
- Once a day
- More than once a day

How much do you trust Facebook in protecting Facebook users against malware that spreads through the social network?
- Not at all
- A bit
- A lot
- Very much
- Absolutely

How much do you trust that your Facebook friends post/share content which is not related to malware infection?
- Not at all
- A bit
- A lot
- Very much
- Absolutely

How much do you trust Facebook Applications with regards to possible malware propagation?
- Not at all
- A bit
- A lot
- Very much
- Absolutely

Did you know that Facebook applications can post on your wall on behalf of you?
- Yes
- No
Did you know that Facebook applications usually have access to your friend list and to your friends' information details?

- Yes
- No

Have you ever rejected installing a Facebook application because it was requesting excessive access permissions?

- Yes
- No

Did you know that your personal computer could get infected by malware just by clicking on a URL?

- Yes
- No

Have you ever experienced malware infection by clicking on a URL posted by a friend?

- Yes
- No

Have you ever clicked on a URL, posted by a friend, which redirected you to a page asking you to download software?

- Yes
- No

Have you ever been tagged in a Friend's post which appears to be a suspicious link (e.g., spam, a Web site that urges visitors to download/install a program etc)?

- Yes
- No

Considering malware protection, you would prefer an application that:

- Protects you from possible malware on Facebook by automatically deleting a (possibly) infected URL
- Warns you about a (possibly) infected URL on Facebook, and letting you decide if you click on the URL