Impact Factor (SJIF): 5.301

International Journal of Advance Research in Engineering, Science & Technology

e-ISSN: 2393-9877, p-ISSN: 2394-2444

Volume 5, Issue 3, March-2018

DETECTING PROFILE CLONING AND ELEMINATING IMAGE INFLUENCING

M.Dhivya [*1], VS.Padminikumari [*2],S.Keshni [*3], R.Jothipraveena [*4]

Department of computer science, Panimalar Institute of technology

Abstract - Social Networks have permitted people have their own virtual identities which they use to interact with other online users. It is also completely possible and not uncommon for a user to have more than one online profile or even a completely different anonymous online identity. Sometimes it is needed to unmask the anonymity of certain profiles, or to identify two difference profiles as belonging to the same user. Entity Resolution (ER) is the task of matching two different online profiles potentially from social networks. Solving ER has a identification of fake profiles. This solution compares profiles based similar attributes. The system is tasked with matching two profiles that were in a pool of extremely similar profiles.

I. INTRODUCTION

On-line Social Networks (OSNs) are increasingly influencing the way people communicate with each other and share personal, professional and political information. Well known sites such as Facebook, LinkedIn, Twitter, and Google+ have millions of users across the globe. With the wide popularity there are lot of security and privacy threats to the users of Online Social Networks (OSN) such as breach of privacy, viral marketing, structural attacks, malware attacks and Profile Cloning.

Nowadays usage of social networking is increased and people. Online social networks, such as Facebook and Twitter, have become one of the main media to stay in touch with the rest of the world.Over time, social network users build trust relationships with the accounts they follow. This trust can develop for a variety of reasons. For example, the user might know the owner of the trusted account in person or the account might be operated by an entity commonly considered as trustworthy, however, demonstrate that attackers can cause havoc and interference even by compromising individual, but high-profile accounts. Recent attacks show that compromising these high profile accounts can be leveraged to disseminate fake news alerts, or messagesTo elimate this we have proposed a project using data mining.

II. LITERATURE SURVEY

A. Title: Design and evaluation of a real-time url spam filtering service

Authors: Kurt Thomas[1], Chris Griery[1], Justin Ma[1], Vern Paxsony[1], Dawn Song[1]

Abstract : On the heels of the widespread adoption of web services such as social networks and URL shorteners, scams, phishing, and malware have become regular threats. Despite extensive research, email-based spam filtering techniques generally fall short for protecting other web services. a real-time system that crawls URLs as they are submitted to web services and determines whether the URLs direct to spam. We evaluate the viability of Monarch and the fundamental challenges that arise due to the diversity of web service spam. The Internet has seen a massive proliferation of web services, including social networks, video sharing sites, blogs,and consumer review pages that draw in hundreds of millions of viewers. On the heels of the widespread adoption of these services, phishing, malware, and scams have become a regular threat. While email spam has been extensively researched,many of the solutions fail to apply to web services. In particular, recent work has shown that domain and IP blacklists currently in use by social network operators and by URL shortening services perform too slowly (high latency for listing) and In accurately for use in web services. By restricting our analysis to URLs, Monarch can provide spam protection regardless of the context in which a URL appears, or the account from which it originates. This gives rise to the notion of spam URL filtering as a service. Email spam provides little insight into the properties of Twitter spammers, while the reverse is also true. We explored the

distinctions between email and Twitter spam, including the overlap of spam features, the persistence of features over time, and the abuse of generic redirectors and public web hosting.[1]

B. Title: Toward Worm Detection In Online Social Networks

Authors: Wei Xu[2], Fangfang Zhang[2], Sencun Zhu[2]

Abstract: Worms propagating in online social networking (OSN) web-sites have become a major security threat to both the web-sites and their users in recent years. Since these worms exhibit unique propagation vectors, existing Internet worm detection mechanisms cannot be applied to them. In this work, we propose an early warning OSN worms detection system, which leverages both the propagation characteristics of these worms and the topological properties of online social networks. OSN websites have become an attractive target for these worms (hereinafter referred to as OSN worms) because of the following properties of the online social networks.First, online social networks are small-world networks, which mean they have the properties of small average shortest path length and high clustering. . Meanwhile, the high clustering property suggests that users are tightly connected together, which facilitates the explosion of OSN worms. Second, online social networks are also scale-free networks, which are a class of power-law networks where high-degree nodes tend to connect with other high-degree nodes. An algorithm based on the heuristic derived from the topological properties of social graphs to keep the OSN web-sites under surveillance by monitoring only a few hundreds of users.[2]

C.Title: Spam: The Undergrund On 140 Characters Or Less

Authors: Chris Grier,Kurt Thomas[3], Vern Paxson[3], Michael Zhang[3]

Abstract: In this work we present a characterization of spam on Twitter. We find that 8% of 25 million URLs posted to the site point to phishing, malware, and scams listed on popular blacklists. We analyze the accounts that send spam and find evidence that it originates from previously legitimate accounts that have been compromised and are now being puppeteered by spammers. spam URLs into campaigns and identify trends that uniquely distinguish phishing, malware, and spam, to gain an insight into the underlying techniques used to attract users. the use of URL blacklists would help to significantly stem the spread of Twitter spam. Despite an increase in volume of unsolicited messages, Twitter currently lacks a filtering mechanism to prevent spam, with the exception of malware, blocked using Google's Safebrowsing API .Instead, Twitter has developed a loose set of heuristics to quantify spamming activity, such as excessive account creation or requests to befriend other users. Using over 400 million messages and 25 million URLs from public Twitter data, we find that 8% of distinct Twitter links point to spam. Of these links, 5% direct to malware and phishing, while the remaining 95% target scams. Analyzing the account behavior of spammers, we find that only 16% of spam accounts are clearly automated bots, while the remaining 84% appear to be compromised accounts being puppeteered by spammers. Even with a partial view of tweets sent each day, we identify coordination between thousands of accounts posting different obfuscated URLs that all redirect to the same spam landing page. By measuring the click through of these campaigns, we find that Twitter spam is far more successful at coercing users into clicking on spam URLs\ than email, with an overall click through rate of 0.13%.[3].

D.Title: Detecting Spammers On Twitter

Authors: Fabr´ıcio Benevenuto[4], Gabriel Magno[4], Tiago Rodrigues[4], and Virg´ılio Almeida[4].

Abstract: With millions of users tweeting around the world, real time search systems and different types of mining tools are emerging to allow people tracking the repercussion of events and news on Twitter. However, although appealing as mechanisms to ease the spread of news and allow users to discuss events and post their status, these services open opportunities for new forms of spam. Spammers post tweets containing typical words of a trending topic and URLs, usually obfuscated by URL shorteners, that lead users to completely unrelated websites. We first collected a large dataset of Twitter that includes more than 54 million users, 1.9 billion links, and almost 1.8 billion tweets. Using tweets related to three famous trending topics from 2009, we construct a large labeled collection of users, manually classified into spammers and non-spammers. Approximately 70% of spammers and 96% of non-spammers were correctly classified. Our results also highlight the most important attributes for spam detection on Twitter has recently emerged as a popular social system where users share and discuss about everything, including news, jokes, their take about events, and even their mood. With a simple interface where only 140 character messages can be posted, Twitter is increasingly becoming a system for obtaining real time information.. Tweet spammers are driven by several goals, such as to spread advertise to generate sales, disseminate pornography, viruses, phishing, or simple just to compromise system reputation. They not

only pollute real time search, but they can also interfere on statistics presented by tweet mining tools and consume extra resources from users and systems. All spam wastes human attention, maybe the most valuable resource in the information age.[4].

E.Title: Detecting Spammers On Social Networks

Authors: Gianluca Stringhini[5], Christopher Kruegel[5], Giovanni Vigna[5]

Abstract: Social networking has become a popular way for users to meet and interact online. Users spend a significant amount of time on popular social network platforms (such as Face- book, MySpace, or Twitter), storing and sharing a wealth of personal information. we analyze how spammers who target social networking sites operate. To collect the data about spamming activity, we created a large and diverse set of "honey-profiles" on three large social network- ing sites, and logged the kind of contacts and messages that they received. We then analyzed the collected data and identified anomalous behavior of users who contacted our profiles. Based on the analysis of this behavior, we developed techniques to detect spammers in social networks, and we aggregated their messages in large spam campaigns. Over the last few years, social networking sites have become one of the main ways for users to keep track and communicate with their friends online. Sites such as Facebook, MySpace, and Twitter are consistently among the top 20most- viewed web sites of the Internet. Another important characteristic of social networks is the different levels of user awareness with respect to threats. We believe that these techniques can help social networks to improve their security and detect malicious users. In fact, we develop a tool to detect spammers on Twitter.[5]

F.Title: Social Phishing

Authors: Tom Jagatic[6], Nathaniel Johnson[6], Markus Jakobsson[6], and Filippo Menczer[6]

Abstract: Phishing is a form of social engineering in which an attacker attempts to fraudulently acquire sensitive information from a victim by impersonating a trustworthy third party. Phishing attacks today typically employ generalized "lures." a phisher misrepresenting himself as a large banking corporation or popular on-line auction site will have a reasonable yield, despite knowing little to nothing about the recipient. For instance, suppose a phisher were able to induce an interruption of service to a frequently used resource, e.g., to cause a victim's password to be locked by generating excessive authentication failures. The phisher could then notify the victim of a "security threat." Such a message may be welcome or expected by the victim, who would then be easily induced into disclosing personal information. Support from the IT Policy and Security Offices was also critical to the success of this study. The UITS Support Center should be credited for their service during the peak periods of user inquiry.[6]

G.Title:Uncovering Social Spammers: Social Honeypots + Machine Learning

Authours: Kyumin Lee[7], James Caverlee[7], Steve Webb[7]

Abstract: The opportunities for participants to engage, share, and interact. This community value and related services like search and advertising are threatened by spammers, content polluters, and malware disseminators. The conceptual framework and design considerations of the proposed approach, and we present concrete observations from the deployment of social honeypots in MySpace and Twitter. One of the key features of these systems is their reliance on users as primary contributors of content and as annotators and raters of other's content. This reliance on users can lead to many positive effects, including large-scale growth in the size and content in the community, bottom-up discovery of "citizen- experts", serendipitous discovery of new resources beyond the scope of the system designers, and new social-based information search and retrieval algorithms. The relative openness and reliance on users coupled with the widespread interest and growth of these social systems has also made them prime targets of social spammers. It develop effective tools for automatically detecting and filtering spammers who target social systems. By focusing on two different communities, we have seen how the general principles of (i) social honeypot deployment, (ii) robust spam profile generation, and (iii) adaptive and ongoing spam detection can effectively harvest spam profiles and support the automatic generation of spam signatures for detecting new and unknown spam.[7]

H.Title:Towards Online Spam Filtering In Social Networks

Authors: Hongyu Gao[8], Yan Chen[8], Kathy Lee[8], Diana Palsetia[8], Alok Choudhary[8]

Abstract:Online social networks (OSNs) are extremely popular among Internet users. Unfortunately, in the wrong hands, they are also effective tools for executing spam campaigns. Accordingly, our system adopts a set of novel features that effectively distinguish spam campaigns. It drops messages classified as "spam" before they reach the intended recipients, thus protecting them from various kinds of fraud. We evaluate the system using 187 million wall posts collected from Facebook and 17 million tweets collected from Twitter. Online social networks (OSNs) are extremely popular collaboration and communication tools that have attracted millions of Internet users. Unfortunately, recent evidence shows that they can also be effective mechanisms for spreading attacks. Popular OSNs are increasingly becoming the target of phishing attacks launched from large botnets.URL comparison to incrementally reconstruct spam messages into campaigns, which are then identified by a trained classifier. We evaluate the system on two large datasets composed of over 187 million Facebook wall messages and 17 million tweets, respectively. The experimental results demonstrate that the system achieves high accuracy, low latency and high throughput, which are the crucial properties required for an online system.[8].

I.Title: Warning Tweet: A Detection System For Suspicious URLS In Twitter Stream

Authors: Manjeet Chaudhary[9], A Hingoliwala[9]

Abstract: Twitter is a social networking site where users can exchange messages to other users particularly their followers. Usually the messages sent over twitter are known as tweets. Users can sent messages or tweets to users who do not follow thesender . This system find the correlations of URL redirect chains extracted from several tweets. It uses the fact that the malicious users or attackers have limited resources and thus they need to reuse them. URL redirect chains frequently share the same URLs for the attackers or malicious users. Twitter is a social networking Site used to share information between users. Users can send tweets to its followers, to a particular user and also to users who are not the followers of the sender. Twitter tweets can contain only a restricted number of characters thus twitter uses URL shortening services to reduce URL length. Conventional suspicious URL detection systems are ineffective in their protection against conditional redirection servers that distinguish investigators from normal browsers and redirect them to benign pages to cloak malicious landing pages. A new suspicious URL detection system for Twitter that is based on the correlations of URL redirect chains, which are difficult to fabricate. The system can find correlated URL redirect chains using the frequently shared URLs and determine their suspiciousness inalmost real time.[9]

J.Title : Compa: Detecting Compromised Accounts On Social Networks

Authors: Manuel Egele[10[, Gianluca Stringhini[10], Christopher Kruege[10], and Giovanni Vigna[10]

Abstact: As social networking sites have risen in popularity, cyber-criminals started to exploit these sites to spread malware and to carry out scams. Previous work has extensively studied the use of fake (Sybil) accounts that attackers set up to distribute spam messages (mostly messages that contain links to scam pages or drive-by download sites). Fake accounts typically exhibit highly anomalous behavior, and hence, are relatively easy to detect. Compromising legitimate accounts is very effective, as attackers can leverage the trust relationships that the account owners have established in the past. Online social networks, such as Facebook and Twitter, have become increasingly popular over the last few years. People use social networks to stay in touch with family, chat with friends, and share news. The users of a social network build, over time, connections with their friends, colleagues, and, in general, people they consider interesting or trustworthy. We presented a novel approach to detect compromised accounts in social networks. More precisely, we developed statistical models to characterize the behavior of social network users, and we used anomaly detection techniques to identify sudden changes in their behavior.[10]

III. PROPOSED WORK

In the proposed system w have e designed mechanisms to detect the same site profile cloning. This mechanism also detects the Fake profile if it is present in the site. We propose a technique using steganography in which we add an id to the profile and posted pictures which the id will be an email id of the user which is added to the image while uploading. The images downloaded from fake profile users and uploaded it when the notification alert sends to the original users. If the original profile user gives the permission when the picture was uploaded otherwise it was blocked.

Advantages of this system are immediate alert to the victim. Can eliminate (delete) or block the attacker from using the victim's information of photographs. Fake profiles can be checked and eliminated within less time. Alerts the victim and will gain permission of the victim as soon as his/her photo is being downloaded. Data mining concepts is being used along with stenography to detect fake profiles and secure from attackers.

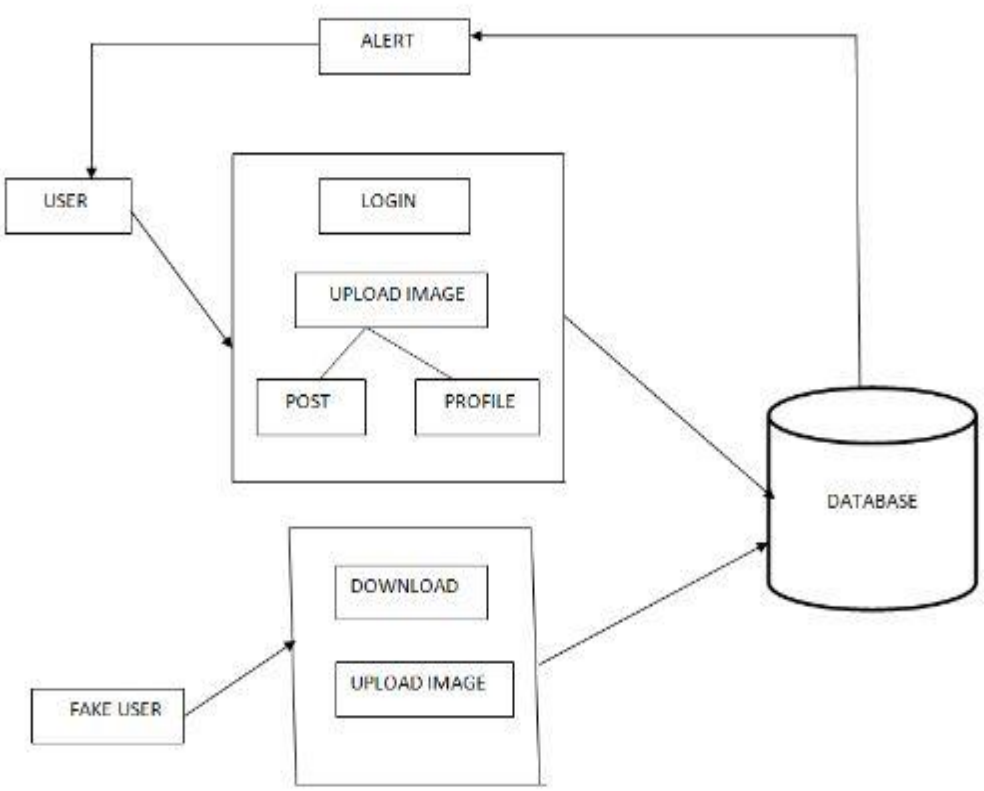

Figure 1.Block diagram

IV. CONCLUSION

Thus this is a system to detect com-promised accounts on social networks. The results show that our approach can reliably detect compromises affecting high- profile social network accounts, and can detect compromises of regular Accounts by data mining.

V. REFERENCES

[1] T. Jagatic, N. Johnson, M. Jakobsson, and T. Jagatif, "Social Phishing," Comm. ACM, vol. 50, no. 10, pp. 94–100, 2007.

[2] C. Grier, K. Thomas, V. Paxson, and M. Zhang, "@spam: the underground on 140 characters or less," in ACM Conference on Computer and Communications Security (CCS), 2010.

[3] "Fox news's hacked twitter feed declares obama dead," http://www.guardian.co.uk/news/blog/2011/jul/04/ fox-news-hacked-twitter-obama-dead, 2011.

[4] "U.s. stocks tank briefly in wake of associated press twitter account hack," http://allthingsd.com/20130423/ u-s-stocks-tank-briefly-in-wake-of-associated-press-twitter-account-hack/.

[5] http://theonion.github.io/blog/2013/05/08/