IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 18, Issue 3, Ver. VI (May-Jun. 2016), PP 11-15
www.iosrjournals.org

Dark Secret of SNS's Popularity

Sanjiv Kumar
Master of Information Technology (Professional)
Deakin University
Melbourne, Australia

Abstract
Facebook pages promising possibility to reach mass audience simply by using Facebook advertising platforms. Lately, the number of likes in Facebook play it role as an analysis to check its demand and advantage, this conduces boosting page likes; such as farm comes into the surface. Based on what has been suggested by some reports, like Farm which using network profile that likes other many pages to stay away from spam detection system, although based on our awareness Facebook promotions of pages uses systematic analysis also. This paper compares the different measurement of the study of the page, Facebook by likes cumulate and by like bots. We create a page which is a honeypot page, analyse using Facebook and bot method and analyse gathered "likes" based on profiles background. We came across few interesting things, including that some of the Farms do not feel the urge to hide the nature of their operation and seem to be operated by bots, while others trying to follow the stealthier path, resemble regular users' behaviour.

Introduction

Social Networking Sites (SNSs) such as Facebook plays a n important role as a primary channel for business and enterprises to advertise and contacting the customers. In 2015 Facebook's net ad earnings reached $8.2billion , ie ., 7.64% of the global market [12]. Facebook offer pages business pages, e.g., for products or events. The user can be notified and can directly be connected to the company by *liking* the page. The amount of interactions and "likes" a page holds is often seen as a calculation of genuinity and popularity: It is predicted that the expected revenue from each like to be $11.17, while others predict diverse between $5.04 , $189.86 and $299.89 [6].

To obtain maximum possible audience, a business can publicise their Facebook profile and pages using targeting strategies, through *ads.* Apparently, ads can be targeted to specific audience; young, old, location, group or user who has a special interest, according to the preferences. According to the guidelines, the only legitimate way to collect likes for the pages is this [13]. However, the new type of underground industry has appeared which provide commercial service, aka *marketplaces* to increase the number of likes on Social Networking sites. Some current press article [3, 7, 14, 18] has begun to investigate Facebook methods of page promotion and contemplate like *Farms* using fake profile try to mimic the behavior of the real audience. As the likes coming from the fraud medium does not really contribute to the business in the term of genuine interest, they are less beneficial for the business promising customer engagement and revenue. On the other hand, another report [19 ,20 ,22] suggested that it does not close the possibility of fake likes by using Facebook's legitimate ad campaign. One possible scenario of this case is, fake profiles tend to diverse it likes in order to avoid Facebook anti-fraud algorithm. By doing that, it is necessary for them to like other pages besides what they are paid for. However, based on our knowledge, Facebook's pages promotion methods has not equipped with systematic analysis, even though it is crucial to understand fake likes to improve algorithms for detection of fraud in the social platform.

In this paper, we compare and contrast the likes and services gathered from legitimate sources and some underground like services. We created one Facebook *test* page and promoted it through both methods. We observed the likes garnered by the page and collected information about the profiles who like the page and carry out a comparative analysis of the likers based on different criteria.

Our experiment made some interesting discoveries. When we targeted Facebook worldwide, we only obtain like from several countries, which likers tend to be a male profile. We have come to a conclusive decision that many like bots, garner likes from the same source. We also saw two main *modes of operations* of the bots. The first set does not really cover the tracks and uses bots, not in an array manner, delivering likes at once and many at times which is easily detectable. On the other side, they use a different approach in which they try to deliver a very small set of likes from same users and occasionally thus bypassing the fraud detection system. The first method is a dirty approach, as the likes are given in a burst and the other method is stealthier and uses a systematic approach.

We did not get any more information on how the likes are generated from a bot. We did, however, notice that the profile handled by the bot had liked many such pages from their profile.

Related Work

Community structures have played important role on studied and expose sybil and/or fake SNS accounts [5, 10, 28, 29, 30]. We also discover the typical of imitation profile activity which tends to link nature or rushing activity. Not only the nature of fake profile that was used by algorithm analysis highlighted by our analysis but also the new pattern that might accompaniment them. Many passive studies of measurement have additionally centred around portraying fake client accounts and their action. Nazir[21] concentrated on apparition profiles in Facebook gaming applications, while Thomas[25] showed the number of fake Twitter account suspensions which was over 1.1 million. Gao[15] understands the Facebook battle of spam as there were over 57,000 affected client accounts. Yang[27] observed the connection of social accounts on Twitter Site, and Dave[11] proposed a new method of spam fingerprint system. Our work is different from all of these as our work is to setup a fan page on Facebook as to see how many profiles which are fake gets attracted to it.

Stringhini[23] and Lee[17] made honeypot master documents in Facebook, Twitter and Myspace to distinguish fraud. Their paper contrasts from our own. Our honeypot pages effectively pulled in fake profiles by a method for paid methods, rather than uninvolved profiles. Furthermore, Stringhini[24] examined the business sector of Twitter followers (which is same as the marketplace for the facebook likes), which, to note is different from Facebook as twitter has *followe d and following back* system is not present in Facebook and likewise, there is no Facebook page liking ecosystem on Twitter.

Beutel[4] tried to analyse and find the fake profiles by going through the users who would like a set of similar pages. However, this is not provi ng to be an efficient method as it follows a pattern and cannot really tell if the likes are fake. By complexity, we are taking the first step to better fake like detection system by creating pages which are empty and attracting likes by the method of payment also taking some inspiration from [4].Many Reports have been published on the same matter [3, 7, 14, 20] but without any proper analysis or solution.

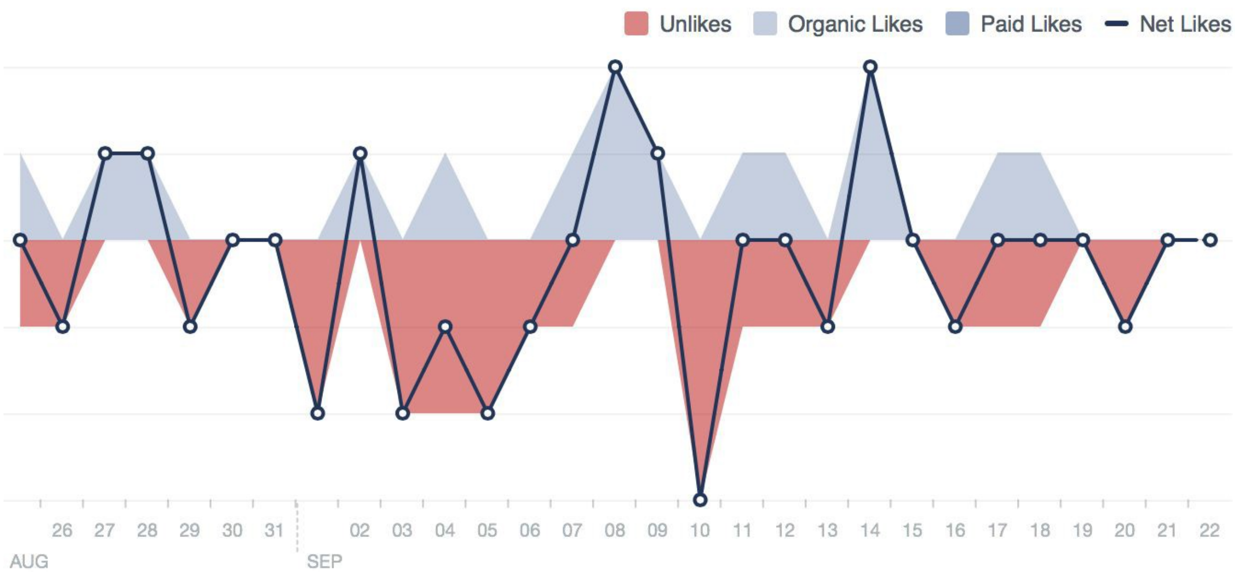
Methodology

This part of the paper will explain the steps we are taking to setup the honeypot page and get likes from both the Facebook advertisement and Like marketplace. We made a page on Facebook called “Sanjiv Kumar". For the page, we used real Facebook Promote (FB-ADS) feature and also marketplaces such as BoostLikes and Social-Formula on worldwide users. In *Table 1*, we highlight the data we collected and the likes we got compared to the cost and duration. Each FB-ADS was planned at a most extreme of
$6/day to a sum of $90 for 15 days. The cost for purchasing preferences fluctuated crosswise over preferred like marketplace: Boost Likes charged the most elevated cost for "100% genuine preferences" ($71 and funnily enough with 35% discount). Other like places additionally asserted to convey likes from "active", "genuine", and "real" user profiles, yet guaranteed to deliver them in less time. By and large, the cost of 1000 likes changed between $29.99–$71.

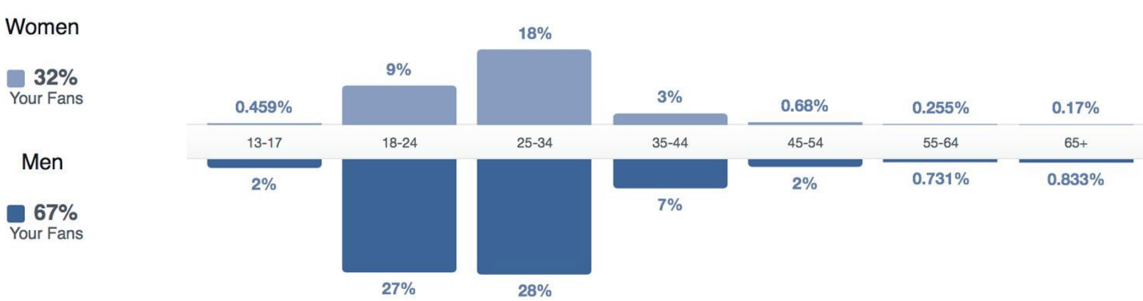
ID	Provider	Budget	Likes	Received	Terminated
BL-SK	BoostLikes	$71	1000	621	1
SF-SK	Social-Formula	$29.99	1000	738	11

Using the software Selenium web driver [2], we try to monitor the activity on the pages every 2hours for the number of likes increase. By the almost completion of the campaign we bring it down to a lower frequency and we stopped when there was no further activity going on on the page.

We also used Facebook's build in data collection tools such insight to aggregate the likes and more information like location and demography, as many people don't tend to hide their age and location on Facebook[8], we also used this information to aggregate the data gender wise and age wise, later, we use this data to measure the similarities and differences between the number of our setup-page liking profile to that of Facebook Pages as whole. Also, we went forward and collected the data suggesting that the profiles liking our page has more than a million friends and has liked over 7 million pages in total.



We accept the fact the lack of budget on this campaign we were only able to setup and monitor one Facebook Page. However, our method filters out many techniques that could broaden the spectrum of research in this field and in turn helping develop a better and robust fraud detection system. According to Table 1. We discussed and maintained a proper monitoring system for the page and reported the provider and the number of likes received and terminated in a period of time. [1], Facebook uses a different algorithm to aggregate these data such it uses IP address to determine the origin of likes. For the likes that we didn't receive and/or terminated, we tried to reach the administrator, however, we didn't receive any response.



Analysis

We compare and contrast the number of likes accumulated from FB-ADS, BL-SK and SF-SK.

Age, Sex and Location Analysis

For the campaign, we set up we mostly received likes from India, USA and Bangladesh. Philippines and Germany were the countries with less like numbers.

In Figure, age and sex of the profiles that liked our page are shown and as seen on the page most of the profiles are of male users and is biassed towards 25-34 age category. FB-ADS, BL-SK and SF-SK all present the similar data.
Pattern Analysis

We try to understand the pattern at which we received like on the page of ours. Like marketplaces, such SocialFormula gives out a burst of likes in few hours and stops. On the other hand, sites such as Boostlikes is more socially and strategically placed. Appears as if the fake profiles are operated by humans and not bot like the usual case with likes marketplaces. We will discuss the two strategies further in coming pages.

Social Connections Analysis

In this section, we analyse the social connection of the user's profile which liked our page. We look at the number of friends and if they are interconnected. We came to know that many of the profiles keep the data in 'private' mode and we were not able to retrieve any more data from those profiles. However, we did come to know that most of the profiles of either BL-SK and SF-SK have a huge friends list.

Analysis of the likes

We have also analysed and observed the other pages liked by the users who liked our page. There is a huge variation in the numbers of pages that have been liked by the profiles, ranging from 1- to 20000. The profiles from bought likes have 600 to up to 1000 pages liked from the profile.

In a nutshell, the profile which liked our page was also liking other pages without any pattern or categories.

Conclusion

In this paper, we discussed a measurement and observed the Facebook promo methods of the pages and we looked at the marketplaces which sell like and followers, etc.

In this paper we have observed and found out that there essentially two modes the like marketplaces profiles work in, first method is when a bot like method is utilized and the likes are given at one burst and the other where the marketplace bots use a bit of strategically timed likes and it is more silent method and mimics a real user on such sites.

After the experiment, we looked at the accounts again and saw that about 1 account of BoostLikes and about 11 accounts of Social-Formulae. In our finding, we found that spending on Facebook ads is not effective at all. The profiles that are liking the Facebook page from the ads have a characteristic which is different from that of a real Facebook profiles. Also, we found that there is a certain pattern between the likes that we received. we can implement all this information into the fraud system, for the identification of fake profiles.

References

[1] R. Olbrich and C. Holsing, 'Facebook Ads', WIST, vol. 43, no. 10, pp. 557-560, 2014.
[2] Docs.seleniumhq.org, 'Selenium WebDriver'. [Online]. Available: https://seleniumhq.github.io/selenium/docs/api/java/org/openqa/selenium/safari/SafariDriver.html. [Accessed: 04- Sep- 2015].
[3] YouTube, 'Facebook Fraud', 2014. [Online]. Available: https://www.youtube.com/watch?t=19&v=oVfHeWTKjag. [Accessed: 13- Sep- 2015].
[4] Alex Beutel, 'Stopping Group Attacks by Spotting Lockstep Behavior in Social Networks', 2013. [Online]. Available: http://alexbeutel.com/papers/www2013_copycatch.pdf. [Accessed: 07- Sep- 2015].
[5] V. Baker, 'Battle of the bots: Fake social media accounts on the attack', Index on Censorship, vol. 44, no. 2, pp. 127-129, 2015.
[6] L. Bullock and O. Agbaimoni, 'Social Media Marketing - why businesses need to use it and how (includes a study of Facebook)', Transactions of the Institute of Aviation, vol. 227, no. 6, pp. 109-119, 2012.
[7] bbc.co.uk, 'Rory Cellan-Jones on his bagel experiment', 2012. [Online]. Available: http://emp.bbci.co.uk/emp/SMPf/1.13.13/StandardMediaPlayerChromelessFlash.swf. [Accessed: 09- Sep- 2015].
[8] J. Egebark and M. Ekström, 'Like What You Like or Like What Others Like? Conformity and Peer Effects on Facebook', SSRN Electronic Journal.
[9] FreeHaven, 'How Much is too Much? Leveraging Ads Audience Estimation to Evaluate Public Profile Uniqueness', 2013. [Online]. Available: http://freehaven.net/anonbib/papers/pets2013/paper_19.pdf. [Accessed: 15- Sep- 2015]. [10] W. Zang, P. Zhang, X. Wang, J. Shi and L. Guo, 'Detecting Sybil Nodes in Anonymous Communication Systems', Procedia Computer Science, vol. 17, pp. 861-869, 2013.
[11] V. Dave, S. Guha and Y. Zhang, 'Measuring and fingerprinting click-spam in ad networks', ACM SIGCOMM Computer Communication Review, vol. 42, no. 4, p. 175, 2012.
[12] Emarketer.com, 'Mobile Growth Pushes Facebook to Become No. 2 US Digital Ad Seller - eMarketer', 2013. [Online]. Available: http://www.emarketer.com/Article/Mobile-Growth-Pushes-Facebook-Become-No-2-US-Digital-A d-Seller/1010469. [Accessed: 08- Sep- 2015].
[13] Facebook.com, 'Why shouldn't I buy fake Page likes? | Facebook Help Center | Facebook', 2014. [Online]. Available: https://www.facebook.com/help/241847306001585?sr=1&query=buy%20likes&sid=2b4oXQ2j1A Mpk9r0T. [Accessed: 13- Sep- 2015].
[14] Search Engine Journal, 'Is Paying for Likes on Facebook Worth it? [RESEARCH] - Search Engine Journal', 2014. [Online]. Available: http://www.searchenginejournal.com/paying-likes-facebook-worth-case-study-search-engine-jou rnal-exclusive/88111/. [Accessed: 05- Sep- 2015].
[15] K. Lee, S. Webb and H. Ge, 'Characterizing and automatically detecting crowdturfing in Fiverr and Twitter', Soc. Netw. Anal. Min., vol. 5, no. 1, 2015.
[17] D. Dittrich, 'The ethics of social honeypots', Research Ethics, 2015.
[18] Mercurynews.com, 'Selling social media clicks becomes big business', 2014. [Online]. Available: http://www.mercurynews.com/california/ci_24849539/celebs-others-buy-clicks-social-media-boo st. [Accessed: 18- Sep- 2015].
[19] Facebook.com, 'I Want My Friends Back', 2012. [Online]. Available: https://www.facebook.com/iwantmyfriendsback. [Accessed: 17- Sep- 2015]. [20] YouTube, 'The Problem With Facebook', 2014. [Online]. Available: https://www.youtube.com/watch?v=l9ZqXlHl65g. [Accessed: 19- Sep- 2015].
[21] RubiNet, 'Ghostbusting Facebook: Detecting and Characterizing Phantom Profiles in Online Social Gaming Applications', 2010. [Online]. Available: http://rubinet.ece.ucdavis.edu/paper/2010/wosn10-fakeprofile.pdf. [Accessed: 15- Sep- 2015].
[22] M. Sweney, 'Facebook quarterly report reveals 83m profiles are fake', the Guardian, 2012. [Online]. Available: http://www.theguardian.com/technology/2012/aug/02/facebook-83m-profiles-bogus-fake. [Accessed: 19- Sep- 2015].
[23] M. Fazeen, R. Dantu and P. Guturu, 'Identification of leaders, lurkers, associates and spammers in a social network: context-dependent and context-independent approaches', Soc. Netw. Anal. Min., vol. 1, no. 3, pp. 241-254, 2011.
[24] A. Bruns, D. Woodford and T. Sadkowsky, 'Towards a methodology for examining Twitter follower accession', First Monday, vol. 19, no. 4, 2014.
[25] H. Al-Khalifa, 'On the Analysis of Twitter Spam Accounts in Saudi Arabia', International Journal of Technology Diffusion, vol. 6, no. 1, pp. 46-60, 2015.