International Journal of Engineering & Technology, 7 (4.6) (2018) 363-367

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Checksec Email Phishi Trasher Tool

Manoj B[1]*, Fancy c[2]

SRM Institute Of Science And Technology
SRM University
Chennai, India (TN)
SRM Institute Of Science And Technology
SRM University
Chennai, India (TN)
Corresponding author E-mail: manoj_b@srmuniv.edu.in[1]

Abstract

In this faster networking world, Phishing has become the most popular practice among the criminals of the web. Various phishing types are deceptive, spear phishing, Email phishing, malware-based phishing, key loggers, session hijacking, man in middle, Trojan, DNS poisoning, cross-site scripting attacks. There is a need for automated tools to solve the problem by the victim side. Existing methods are regularly too tedious to be utilized in reality as far as recognition and relief session. Hence it is decided to propose a model which focuses on detecting and preventing the email phishing attack. In this paper, we present PhishiTrasher, another discovery and relief approach, where we initially propose another system for Deep Packet Inspection afterward use in phishing exercises through email and electronic correspondence. The proposed packet inspection approach comprises parts, vulnerable mark arrangement then continuous DPI. With the help of the phishing assault marks, outline the continuous DPI with the goal that PhishiTrasher can adapt to address the elements of phishing assaults in reality. PhishiTrasher gives better system movement administration to containing phishing assaults since it has the worldwide perspective of a system. Moreover, we assess PhishiTrasher utilizing a true test bed condition and databases comprising of genuine email with installed joins. Our broad test contemplate demonstrates that PhishiTrasher gives a powerful and effective answer for prevent phishing attacks through email. Results demonstrate that profiling should be possible with very high genuine.

Keywords: *Phishing; Email Attack; Email Phishing; Social Engineering; DNS Fraud;*

1. Introduction

Phishing is a criminal plan to take the client's close to home information and other accreditation data. It is a misrepresentation that obtains casualty's private data, for example, secret key, ledger detail, charge card number, monetary username and secret word and so on and later it very well may be abuse by aggressor. There is a need for automated tools to solve the problem by the victim side. Hence it is decided to propose a model which focuses on preventing the email phishing attack. Among an overwhelming heap of new email inbox messages lies an unstable hyper connect to a pernicious site, sitting tight for a client's snap. This inbox message sent by a risk on-screen character is generally known as phishing, where the danger performing artist sits tight for the end client to tap on such a connection to conceivably trade off an association or figuring framework. Numerous associations receive Security Education Training Awareness projects to advise end clients will aware of mistrustful inbox messages, however various end clients neglect to stick to such strategies that prompt potential information misfortune. Phishing has turned out to be a standout amongst the most fatal assaults. There have been various methodologies to obstructing phishing assaults from a foundation perspective yet the two frameworks require email activity rerouting to every security apparatus. In spite of the fact that seller arrangements may distinguish phishing inbox messages, they don't keep an end client from tapping on a pernicious connection inside a hailed email that may prompt trading off a registering framework. To deflect such concerns, ones propose an assortment of Intrusion Detection Systems (IDS) to deal with distinguishing and dissuading phishing inbox messages, however they need practicality or can't be utilized when email correspondence moves toward becoming encoded, which is commonly done these days. Also, when cautions are raise to run of the mill in the utilization of an intermediary benefit or arrangements and to address such test, discovery session decrease is required where identification session is characterized as an opportunity to assess a link by PhishiTrasher through earliest starting point by moment that started. A basic angle to SF is the putting away element of a system bundle. A system stream comprises of a wide range of bundle composes and estimate. One worry to SF is the cradle to hold every bundle while movement review is anticipated. Customary security arrangements give different details.

2. Requirement Analysis

In this paper, we utilize information mining to help profile phishing inbox messages. Typically a phisher contacts a casualty through inbox messages; thus we take the most huge piece of the email - the hyperlink data as highlights. For our investigations, we create three distinctive databases from hyperlink data for producing profiles. We utilize attributes like the structure of the inbox messages sent by the phishers to their potential casualties (which

we call basic data) and metadata on the hyperlinks - the whois data. We consider these qualities as classes that will compare to marks in a multi-name grouping issue. Using an information characterization procedure will give the connections between the hyperlinks in the phishing inbox messages and their pre-indicated classifications/classes. Advance we can utilize the multi-name classifier to dole out obscure inbox messages to their classifications or classes and accordingly to specific attributes in their profiles. Recognition with the information gives confirmation that most precedents would give various marks that would be useful as far as profiling. The methodology proposed considers: Accessing highlights from the inbox messages that are basic and successful. The specific qualities of the inbox messages that can be considered as characteristics in profiles. Our view is that profiles ought to have the capacity to recognize distinctive gatherings. For instance, an email may have the accompanying attributes, it has, a table, a picture et cetera. Another gathering may have distinctive subsets of these attributes. Phishers have distinctive business as usual or methods for working. In one case, phishers have diverse methods for dealing with phishing action. Some phishers may install contents and pictures in the shape which can securely pass finders and when clicked by the client takes them to a site that isn't the first one. In different examples, another gathering may embed a phony connection in the shape and when clicked will take the client to a phishing site. Subsequently the business as usual is distinctive for various gatherings. In light of this reality, we would need to distinguish bunches utilizing the distinctive types of structures implanted inside inbox messages. On the off chance that we characterize the list of capabilities as comprising of these qualities then information bunching would give distinctive gatherings having comparative profiles. This issue has been considered. Primer examination demonstrates that there are numerous troublesome issues in bunching. Diverse calculations give distinctive group results. In this paper we take after an alternate methodology. We pick these qualities as classes and attempt to anticipate an arrangement of classes or marks of new inbox messages. The list of capabilities utilized for this situation, is basically the hyperlink data from inbox messages. In this area, we initially portray investigate foundation and afterward distinguish look into challenges. Vulnerable assaults has variation, for example, stick phishing and whaling are normal dangers to an endeavor association. Tragically, numerous individuals don't understand how complex phishing assaults. Other than the application layer, the recognition and moderation of such assaults are exceptionally troublesome difficulties may have just traded off a figuring gadget before discovery cautions are raised and alleviation is finished. Conventional through vulnerable assaults are utilized through email. It will be recognized utilizing methods, for example, intermediary administrations, firewall applications, and IDS/IPS arrangements. Scrambled correspondence, for example, SMTPS and HTTPS makes a test for activity recognizable proof because of the absence may suitable private key to unscramble inbox content. Regular systems will tackle issues are using an association accreditation expert and blend of the affirmation specialist with an intermediary benefit. Also, IDS/IPS arrangements generally use static string coordinating systems as the heuristic way to deal with decide exercises, however they need in distinguishing obscure or new dangers. It can't represent the elements of vulnerable assaults. Ultimately, traded off gadget through phishing assaults can be calamitous for an association because of secret information misfortune. Different strategies to anticipate in danger by employments of loss of data administrations, however it vigorously depend in client side assets for relieve vulnerable endeavors and it is a rising systems administration structure that means to defeat constraints of heritage systems. The brought together administration of SDN ensures steady strategy authorization, better adaptability, all encompassing perceivability and flex programmable system work. PhishiTrasher use the programmability and worldwide perspective of a system to protection phishing assaults. Although recognition and procedures are conventional ways to deal with discourage such danger, there are two noteworthy difficulties as takes after. Timing is a key worry in foiling danger on-screen characters/aggressors. The session in which a data security arrangement avoids, prevents, or mitigates a phishing assault is basic to ensuring an end-client. Differing from client to client, a warning of another email inbox message may trigger a quick reaction from the end client with the end goal that they may open the inbox message and tap on the different connections and connections. This planning is basic for an arrangement as the reaction session might be past the point of no return for the rising risk and the focused on registering framework might be imperiled. Network Performance: Using an intermediary benefit in conventional examination gives the capacity to email and web activity correspondence to be precisely reviewed and sent in a convenient way. One worry of the intermediary benefit approach is the assessment session/defer that is characterized as an opportunity to review, PhishiTrasher in earliest starting point till final need desperation in inbox methodology. For more readily reduce criticalness, investigation session should be limited to deal with any movement compose for arrange correspondence enhancement. Moderation session is basic in the responsive planning to rising phishing assaults.

3. Proposed Methodology

Before you Using PhishiTrasher for the identification and moderation of a phishing assault is a basic resource in an IDPS arrangement with the end goal to anchor an association. Additionally, session in PhishiTrasher utilizing measure the execution of distinguishing dangers. Our assessment looks at the choice explanations and think about them against three databases, investigation session shifts relying upon the many-sided quality of every URL. In PhishiTrasher, the investigation session is an overhead where a bundle can't be sent before the assessment is finished and limited with the end goal that PhishiTrasher can be utilized in reality. Spam Filtering is to discover whether or not the emails are spam or no longer. In our test, the elegance of personal letter was the handiest magnificence that changed into described as ham. But for a selected user, the recruitment massages could also be crucial and beneficial, therefore, the emails within the class of recruitment ought to be identified as ham for this user. So with the a couple of category the personalised unsolicited mail filtering system was a whole lot extra less complicated to broaden. In the Proposed System we've got carried out the LDA and SVM Algorithm. If the Email is having following attributes way, that email is a junk mail Attributes are, Invoicing, schooling, recruiting, eroticism, internet site, promoting, letter, defrauding, Etc. We have created the web application as like gmail. By the usage of the LDA and SVM Algorithm, unsolicited mail mails are filtered primarily based at the category. Accuracy for both the algorithms is calculated. And subsequently it proved that LDA has better accuracy than the SVM Algorithm. Generally, a disparaged email is sent to a considerable social event of people from a convey that appears, apparently, to be from their bank or some other bona fide foundation. The email is ordinarily worded to instill a sensation of distress and to motivate a brisk response from the recipient.

Existing System:
Because junk mail emails could be exposed in every a part of the email delivering technique, there are many methods frequently utilized in unsolicited mail filtering and usually labored in conjunction, such as whitelists/blacklists, mission-response, rule-based filtering, keyword-based filtering, content material-primarily based filtering, etc. Spam filtering can be seemed as a unique binary classification assignment of textual content to decide whether or not an electronic mail is unsolicited mail or not. The maximum familiar manner to symbolize a fixed of texts is transform each text right into a vector based totally on the phrases of it, then a vector space version of all texts within the set is fashioned. With such kind of vector area model, the text class will be executed by means of clustering approach or system studying algorithms effortlessly. Machine studying algorithms are widely

implemented in text class and generally perform properly, among which Support Vector Machines [7][8][9] and naive Bayes classifier [10][11] are the most famous junk mail filters supplied within the literature. However, picking words as capabilities to create textual content vector always lead to massive quantity of computation in the technique of classification, due to the excessive measurement of vector area model built up, specifically while massive extent of texts are worried that is familiar in unsolicited mail filtering nowadays. Although masses of function choice strategies were proposed within the literature [12][13], the vast feature phrases nevertheless are the major problem in text type and unsolicited mail filtering thus far. This is any other weak spot of unsolicited mail filters requiring development.

For instance, 'check your record subtle elements or your record will be shut'. The lie email likewise contains a connection to an online shape that is marked to look precisely like the association's site. The shape must be filled in utilizing touchy data like passwords, client account subtle elements, Mastercard points of interest. Up to this point most phishers used the names of money related foundations to swindle individuals into giving ceaselessly their record data. They currently utilize the names of different associations like eBay and Apple. There have been numerous ways to deal with distinguish and counteract phishing assaults like enemy of phishing toolbars, and trick site blockers. Additionally machine learning approaches have likewise been concocted for this reason. Additionally another way to deal with build up an engineering for recognizing phishing. In addition, recognition instrument will decide unfriendly practices. One worry of such reaction session is the point at which a client taps on a hyperlink prompting trading off a framework before an alarm can be brought up notwithstanding alleviation endeavors utilizing an IPS. To battle such difficulties, we present PhishiTrasher, another location phishing assaults are recognized utilizing an assortment of existing discovery procedures, however strategies has restricted ability in adjusting dangers, then need regulatory arrangement control. 'Phishing' can be characterized as a trick by which an email client is hoodwinked into surrendering private data that will be utilized for wholesale fraud. Phishing assaults utilize both social designing and specialized subterfuge to take individual character information and money related record accreditations.

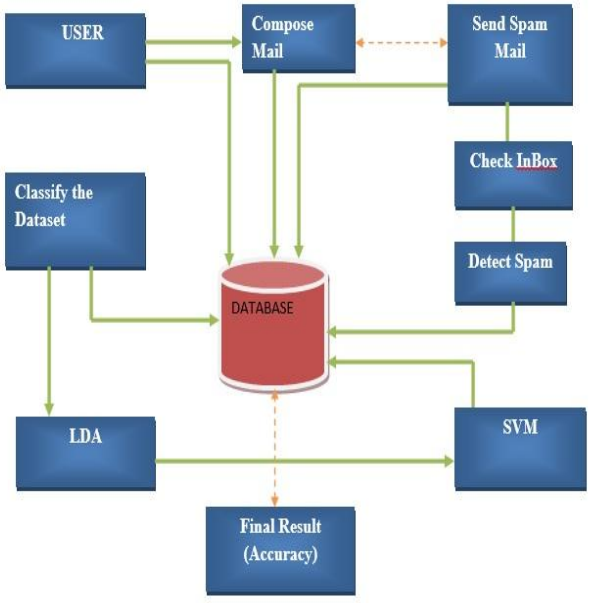

Fig. 3.1: System Architecture

It is one of the quickest developing tricks on the Internet. The selective inspiration of phishers is monetary benefit. Phishers utilize a wide range of procedures from satirize connects to malware (keyloggers) to DNS Cache Poisoning (which is additionally known as 'Pharming') to bait the unsuspected client into disclosing their own data. They additionally misuse diverse vulnerabilities in the program like concealing the location of the real site in the status bar. Likewise pernicious programming diverts clients to parodied destinations. The toolbar has a component called 'Record Guard' that screens the area names that clients visit and give cautioning as a shaded tab on the toolbar. The tab is normally dark yet it turns green if the client is on eBay or a PayPal site. It turns red if the client is on a site that is distinguished as parodied by eBay. Additionally spoofguard is an Internet Explorer program module that cautions clients when website pages have a high likelihood of being ridiculed. The phishing issue has been and still is imperative, and the location and cautioning approach taken to the issue isn't sufficient. The current writing primarily manages phishing discovery issues. The primary issue tended to in the writing is the recognition of phishing inbox messages in light of some huge highlights that they have. In this work an alternate perspective of phishing is examined, in particular the profiling of phishing inbox messages. Phishers generally take after an assortment of procedures, so a profile can be required to demonstrate a mixture of various exercises. Profiles can be comprehended as metadata on phishers, specifically, data on exercises of a related individual or a gathering engaged with the action. For this reason, we additionally assess the review session of PhishiTrasher utilizing an alternate number of layers.

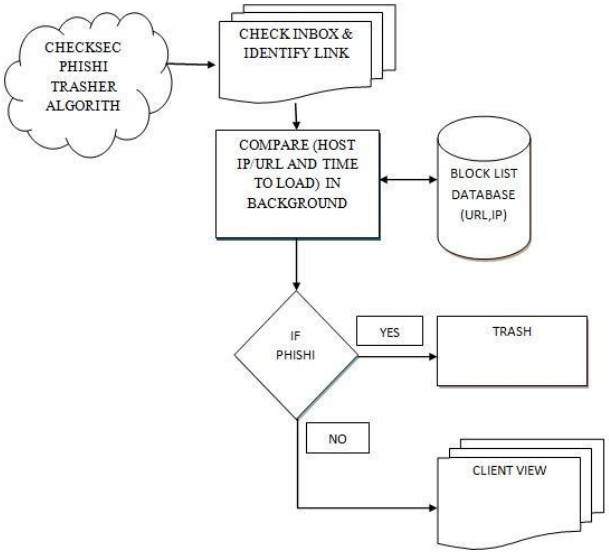

Fig. 3.1: Proposed Methodology

User Registration:
As like Gmail, we've created the utility for sending and receiving mail. By using this application, junk mail mails are filtered. In this module, User needs to register first by giving all of the info. Then the given info are get stored within the database. So, all of the customers have to sign up before login.
User Login:
After Registration process completed, User can login with username and password. If both get fits, then the consumer might be considered as a legitimate person in any other case invalid user. Valid consumer can send mail to different customers.
Compose Mail:
In this module, consumer can compose mail after login. The User can enter the message what he desires to send to different consumer. After composing the message, person enters the To mail and send the mail to the alternative user. User can compose each the spam and ham mails.
Inbox:
In this module, Inbox which includes all the acquired mails despatched by the person. It accepts best the ham mails and it will not permit the spam mail in inbox. All the obtained mails can be read through the users.
Spam:

If any consumer sends spam mail manner, robotically it's going to involves Spam module. It will now not display in Inbox. So that the person can get to realize about the unsolicited mail mails. It avoids the user to click on at the spam mails.
Sent Mail:
In this module, User can able to see the despatched messages. All the sent mails are display right here.
Classification:
We have collected the dataset which incorporates both unsolicited mail and ham mails. By using the LDA and SVM set of rules, we've labeled the Spam and Ham mails. The Result indicates that LDA has the higher accuracy than the SVM.
As a rule, expanding the quantity of from 2 to 3 builds the investigation session.For PhishTrasher, we saw that the review session expanded, individually, yet it diminished for Others. We have seen that Ham database is not the same as other two databases in light of the fact that gives a warmth delineate all experiments of all databases. We watch the comparative. Utilizing PhishiTrasher, we can ruin a danger differing on both assessment methods of moderate and quick. The session expected to moderate a danger, known as relief session, is basic to a security contraption, present the alleviation session of PhishiTrasher acquired from our broad analyses on each database. The alleviation session was about 1.1 seconds or less. In spite of the fact that risk alleviation is vital to ruining danger performing artists. As observed the review every URL in encoded movement. The overhead adds to investigations the URL utilizing the host IP address and URL coordinating procedures. We assessed PhishiTrasher utilizing to distinguish URLs inside the payload of a parcel and check the square recorded IP in past destroyed sends and spam box at that point assess. Our assessment has demonstrated that identification played out the best and proficient in contrast with the insignificant review session required per URL. To be compact, the execution of every location technique has demonstrated the intricacy of databases where others recognize every URL at a normal assessment session which is the general arrived at the midpoint of relief session once there was a caution. False positives are pervasive in any discovery framework including PhishiTrasher. At the point when a inbox message crosses, a false positive can be negative to an end client because of the possibly profitable misfortune (drop) of an email. The neural system utilized by PhishiTrasher has been deliberately tweaked and assessed for precision, yet can be heedless to false positives, and therefore– an isolate organize is vital for PhishiTrasher drops inbox messages that are related to a probability of maximum likelihood, and can be altered by the chairman. Inbox messages that have a minimum likelihood esteem can be assessed in the accompanying methods.

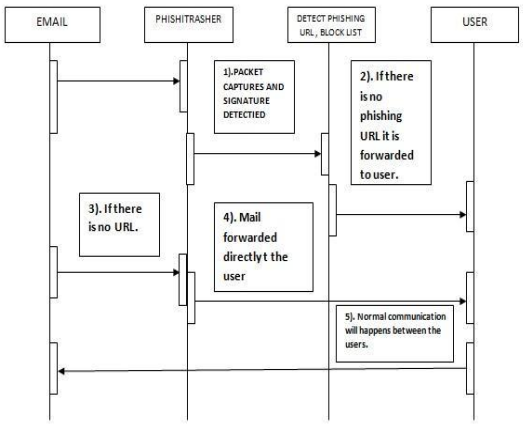

Fig 1.2: Sequence Diagram For Phishitrasher

Denoting: The email can be manIPulated by PhishiTrasher with the end goal that proper header data in the inbox message demonstrates a sign that the framework has recognized a possibly unsafe email. This sign ought to be generally clear and obtrusive to an end client with the end goal that there are no perplexity or visual weaknesses to such cautioning. Inbox message Rerouting: The inbox message can be diverted to a freely detached post box with the end goal that it requires an end client to recover the inbox message safely. A notice inbox message can be sent to an end client demonstrating that a inbox message was diverted. One basic piece to the utilization of the Inbox message Rerouting system is that a more profound review can be executed on connection records to recognize various malevolent substance, for example, malware.

3.1. Mathematical Calculation

I). U=Universal set collection of all vulnerable web pages url
II). X=subset of U collection of url from inbox inbox messages
III). R=Relation/matching subset in universal set

$R^*(X)=UX \in U^*R(X)$

IV). R*(X)=Collection of url matched
V). UX=Collection of both url that are matched and new vulnerable websites
VI). R(X)=Set of vulnerable url that are matched with universal set in relation.
VII). ϕ=Database with collection of vulnerable url by netsearch.

If
(RNR(X)=ϕ=>vulnerable url
RNR(X)$\neq \phi$=>non vulnerable url

$R^*(X)=UX \in U \{R(X):R(X)nX \neq \phi\}$

3.2. Algorithm

It has four test cases

I) True True

II) False False

III) True False

IV) False True

pl:plaintext
ul:url database
murl:url
mhtml:html
mdns:domain name server
mphp:php
fr:final report

for each murl in ul
fr=url

if murl in ul
then
return
mhtml<-url. response html()
mdns<-url. response dns()
mphp<-url. response php()
endif

fr[url]=url
fr[dns]=mdns
fr[html]=mhtml

4. Result

This segment gives our test assessment of Phish-Limiter and portrays different territories of execution investigation and our danger marks for phishing assaults. We leave each system connect flawless with no impacts. Ultimately, Floodlight uses various ways to deal with taking care of connections propose and create parallel/multi-string projects to think about the execution of PhishiTrasher on 1, 2, and 3 centers, informational collections comprising of phishing sites. This database contains various phishing dangers phishing assaults, we use three openly accessible databases comprising of information from this present reality. To be brief, the three databases we use are as portrayed as pursues. For our first database, we use the SpamAssassin venture as our benchmark assessment. In addition, this database is made out of 4,150 real email correspondence and 1897 spambased inbox messages. Because of this thought, we regard this database as typical email correspondence. In addition, this database gives broad the unpredictability of URLs from normal phishing strategies laid out in our past arrangement recorded. Because of the aggregation of phishing email information, we regard this database to analyze an online substance to decide if this data has a vindictive goal. We regard this database as another debilitating arrangement of data in our assessment to look at the methodologies of electronic correspondence. This database is made blend every one of the three databases through PhishiTrasher various emphasess with the end goal to decide the execution and adequacy the execution of distinguishing dangers. Our assessment looks at the chose three regex articulations and think about them against three databases. We exhibit such outcomes and express a more careful measurable investigation. As appeared, examination session changes relying upon the many-sided quality of every URL.

5. Conclusion

A phishing assault is an exceptionally regular social designing way to deal with focusing on an association and end clients. It has happened to the most destructive assaults these days. There have been various investigations on recognizing and alleviating phishing assaults. Conventional arrangements center on the utilization of inline assessment methods, for example, an IPS or intermediary benefit in light of static string coordinating in customary IDS. In this paper, we have proposed PhishiTrasher as another answer for upset phishing assaults. PhishiTrasher can deal with system movement elements for containing phishing attacks and can give a superior activity administration since it has a worldwide perspective of systems because of SDN. In particular, we have first arranged by phishing marks by building up an ANN show utilizing a PLS framework. In this paper, we have displayed a novel strategy for acquiring profiles from phishing inbox messages utilizing hyperlink data as highlights and auxiliary and whois data as classes. We have changed the issue of profiling into a multi label characterization issue in which profiles are created in view of the expectations of the classifier. We have utilized a well known grouping calculation for our trials. Further, we make three distinctive databases from the hyperlink data in inbox messages and utilize fourcrease cross-approval to produce our forecasts. The outcomes gave high grouping precision, consequently more exact profiling was acquired. We have likewise given expectation weights produced by the classifier that demonstrate the relative significance of the classes utilized in profile age. In future, we would upgrade this strategy to get more noticeable highlights and grow more agent classes for profiling. Likewise we might want to explore different avenues regarding distinctive classifiers and look at the profiles created all the while. Further, we intend to accomplish a legitimate standard for estimating the significance of the classes present in profiling.

References

[1] S. Merchel, J. Franc¸ois, T. Engeletal., "Proactive discovery of phishing related domain names," from International Workshop on Recent Advances in Intrusion Detection. Springer, 2012, pp. 190 – 209.

[2] Barracda, "Barracda email security gateway," 2017 . https://www.barracuda.com/products/email security gateway

[3] Symantec, "Symantec messaging gateway," 2017. https://www.symantec.com/products/threat-protection/

[4] messaging-gateway

[5] Phaul L. Karstein, ―How can we stop Phishing PharmingScams http://web.archive.org/web/20080324080028/http://www.csoonline.com/talkback/071905.html

[6] Phishing techniques

[7] http://www.phishing.org/phishing-technique

[8] M. Tsikerdekis, "Identity deception prevention the use of common contribution

[9] community facts," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 188–199, 2017.

[10] T. Anwar and M. Abulaish, "Ranking notably influential net forum customers," IEEE Transactions on Information Forensics and Security, vol. 10, no. 6, pp. 1289–1298, 2015.

[11] Y. Boshmaf, I. Muslukhov, K. Beznosov, and M. Ripeanu, "Design and analysis of social botnet," Computer Networks, vol. 57, no. 2, pp. 556– 578, 2013.

[12] D. Fletcher, "A quick records of unsolicited mail," TIME, Tech. Rep., 2009.

[13] Y. Boshmaf, M. Ripeanu, K. Beznosov, and E. Santos-Neto, "Thwarting fake osn debts by means of predicting their sufferers," in Proc. AISec., Denver, 2015, pp. 81-89.

[14] N. R. Amit A Amleshwaram, S. Yadav, G. Gu, and C. Yang, "Cats: Characterizing automation of twitter spammers," in Proc. COMSNETS, Banglore, 2013, pp. 1–10.

[15] K. Lee, J. Caverlee, and S. Webb, "Uncovering social spammers: Social honeypots + machine getting to know," in Proc. SIGIR, Geneva, 2010, pp. 435– forty two.

[16] G. Stringhini, C. Kruegel, and G. Vigna, "Detecting spammers on social networks," in Proc. ACSAC, Austin, Texas, 2010, pp. 1–9.

[17] H. Yu, M. Kaminsky, P. B. Gibbons, and A. Flaxman, "Sybilguard: Defending against sybil assaults via social networks," IEEE/ACM Transactions on Networking, vol. Sixteen, no. 3, pp. 576–589, 2008.

[18] H. Gao, J. Hu, C. Wilson, Z. Li, Y. Chen, and B. Y. Zhao, "Detecting and characterizing social unsolicited mail campaigns," in Proc. IMC, Melbourne, 2001, pp. 35–forty seven.

[19] W. Wei, F. Xu, and C. C. Tan, "Sybildefender: Defend in opposition to Sybil attacks in massive social networks," in Proc. INFOCOM, Orlando, 2012, pp. 1951–1959.

[20] C. Yang, R. C. Harkreader, and G. Gu, "Die free or live tough? Empirical assessment and new design for combating evolving twitter spammers," in Proc. RAID, Menlo Park, California, 2011, pp. 318–337.

[21] S. Lee and J. Kim, "Warningbird: A near real-time detection device for suspicious urls in twitter stream," IEEE Transaction on Dependable and Secure Computing, vol. 10, no. 3, pp. 183–195, 2013.

[22] M. Sahami, S. Dumais, D. Heckerman, and E. Horvitz, "A Bayesian approach to filtering junk e mail," in Proc. Of Workshop on Learning for Text Categorization, Madison, Wisconsin, 1998, pp. Ninety eight–one hundred and five.

[23] C. Schafer, "Detection of compromised electronic mail accounts used by a unsolicited mail botnet with country counting and theoretical geographical traveling speed extracted from metadata," in Proc. ISSRE, Naples, 2014, pp. 329–334.