iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 7 **Issue:** IV **Month of publication:** April 2019

DOI: https://doi.org/10.22214/ijraset.2019.4390

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 7 Issue IV, Apr 2019- Available at www.ijraset.com

Detecting Mobile Malicious Pages in Real Time

Shivani A. Nevgi[1], Sitesh M. Sawant[2], Pratiksha A. Sharma[3], Prof. Priyanka Bandagale[4]
[1, 2, 3, 4]*Finloex Acadmey of Management & Technology, Ratnagiri, Maharashtra, India.*

Abstract: ***The Mobile webpages are generally different from desktop webpages. The attacker can easily deploy different types of malwares on mobile devices, by using feature like drive-by-download. To detect this type of webpages we are purposing intelligent and feasible solution based on classification and association data mining algorithm. This algorithm is used to classify malicious pages and alert user. The classification is done on the basis of the URL of webpage and the content of webpage like number of iframes. By using classification & association technique the accuracy of the system is increases. Then we also create browser extension for the same to detect malicious webpage in real time.***
Keywords: Malicious; URL; Detection System, iframes, webpage.

I. INTRODUCTION

Malicious means having mal (having bad intension) intension to harm or to steal any information. Malicious website is a site it attempt to install malware on to your Mobile devices. Malware is a software that will disturb your computer, steal your personal information or in worst scenario you will gain total control of your system. Now a day number of malicious websites are used to host exploit kits. Exploit kits force visitor browser to identify security vulnerabilities that can be exploited without user interaction. Malicious URL's are created with malicious purpose which can be content in spam or phishing massages, or even improve its ranking in search engines like google, yahoo by using black-hat SEO techniques.

With the increasing population, the number of mobile devices used by peoples is also increasing. As the shape and size of mobile devices reduced, the shape and size of webpages is also reduce. Along with this the number of attacks through the mobile webpages is also increased. This is due the compactness of mobile webpages and features like easy access to users contact and location. The attackers are taking the advantage of this feature by installing malware, spyware, m-ad-ware and grayware on user devices through webpages.

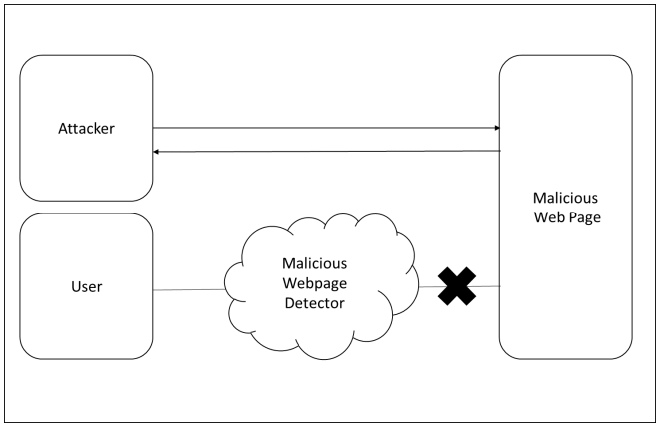


Fig.1 Mobile Malicious Page Detection System

The desktop malicious webpages can be detected easily as compare to mobile malicious pages. As it is difficult to detect them in mobile in mobile devices so they can be dangerous for user's devices. The existing systems and techniques also not accurately detects this type of malicious webpages due to the attackers are using newer techniques to create this type of mobile malicious webpages. Majority of the system based on desktop webpages and also they detects and block malicious pages manually.

In this paper, we purpose a system named as Detecting mobile malicious pages in real time. This system uses hybrid analysis to detect mobile malicious pages more accurately. This system first target the URL of webpages performs all the security checks achieved by static analysis. For this we collect 10000 malicious URL'S from the well-known services like Google safe browsing and phishtank.com, then we apply data mining techniques to develop the system. Also system has some dynamic part like no of iframes etc. When user access any webpage, system fetch that webpage URL and detects malicious webpages dynamically if they malicious then system gives alert message in real time to the user.

II. LITERATURE SURVEY

CHAITRALI AMRUTKAR, YOUNG SEUK KIM, and PATRICK TRATNOR [1] has proposed a mechanism called KAYO, which classifies a webpage presence of fraudulent phone number and malware. KAYO uses static features of mobile webpages derived from their HTML and JavaScript content, URL and Advance mobile specific capabilities. They also created the extension using KAYO to protect user from malicious webpages. KAYO is applied over huge data set of known original and malicious webpages.

G. ASHOK KUMAR, A. VENU GOPAL, I. ABHILASH BALU and M. M. V. VAMSI [2] have implemented Knock Cold, which distinguishes between malicious and benign mobile webpages and alert the user about it. Knock cold makes these detections by 44 mobile relevant options from webpages. Also knock cold gives feedback in time period. This system primarily apply static approach to detect malicious webpages.

M. ANANTHA RAMAN, R. ANIL KUMAR, S. GOWRI SHANKAR, P. DEVENDRAM [3] proposed a system called Malicious Webpage Tracker (MWPT) which depends on who is visiting the site and also the mechanism is built which detects cloaking. Where cloaking is the technique to view content according to condition – who is visiting the site. This system uses binomial classification technique to detect Mobile malicious webpages.

ABDULGANI ALI AHMED and NIK QUOSTHONI SUNAIDI [4] have reviewed all the existing systems and found following techniques which can be used for detection of malicious pages. They also found some unlawful purposes of attackers like spam advertising, propagating malware, financial frauds and malvertising. They proposed following techniques to detect malicious websites.

1) *Blacklist Approach:* A Blacklist is a list containing IP address information, website name or URL of known malicious website.
2) *Honey Clients:* It detects malicious website in two modes - low interaction and high interaction mode.
3) *Machine Learning:* Uses existing information from the URL and develops a learning model to classify malicious webpages.
4) *Page Content Analysis:* Inspect the page content according to set of specified base rules.

DR. JITENDRA AGARWAL , DR. SHIKHA AGARWAL, ANURAG AWATHE, DR. SANJEEV SHARMA [5] have used different features of extraction techniques such as information gain , N- gram, Score Gram and Confidence weighted scheme to study nature of malicious website and avoid security threats like phishing, drive-by-download and spamming. They used some web based features to detect malicious website like URL lexical features, domain host based features, webpage content based feature, HTTP response graph feature. This detection is based on machine learning using support vector.

HEMALI SAMPAT, MANISHA SAHARKAR, AJAY PANDEY and HERAL LOPES [6] implemented classification and association algorithm with WHOIS protocol. They also developed series of steps to check characteristics of websites which are different from other websites. This system finds relations of malicious websites with each other and performance.

G. VASANTH KUMAR, U. SESHADRI [7] have proposed a system with many anti phishing solution like content analysis and HTML code analysis to detect phishing webpages. They also used techniques based on URL like domain similarity, IP matching and Image matching. This system detects the websites in three layers.

a) Similarity with URL's in database.
b) IP matching.
c) Number of key point matched.

III.PROPOSED SYSTEM

This section describes the proposed model of Mobile Malicious Webpage Detection in real time. This model focuses on classifying malicious webpages based on checking features of webpages, Blacklist. Selected features of website or webpage can be used to classify genuine and malicious webpage. These selected features include URL's, Domain Identity, page style, Number of iFrames etc. This system focuses on only URL's and No of iFrames. Features of URL are checked by different criteria's like Keywords present in URL, adding a prefix or suffix, redirecting using symbol "//", Special symbols present in URL etc. These features are checked using set of rules in order to classify the Malicious Webpages and alert the user in real time.

A. URL Based

Following Features are checked in this approach,

1) URL containing IP address.
2) Long URL to hide the Suspicious Part.
3) URL containing Prefix or Suffix Separated by '-'
4) Submitting Information to Email using 'mailto:' function.
5) Using Pop-up's

B. Content Based

The malicious webpages mainly contain madwares as well as malwares. Mainly this wares are hidden in iframes. Hence in this approach this system will count number of iFrames present to classify the webpage.

C. Blacklist Based

A Blacklist is created in the proposed model in which the website detected as malicious is saved for the future use and to keep record of malicious webpages. This can be useful in analysing the malicious webpages to increase the efficiency of the system.

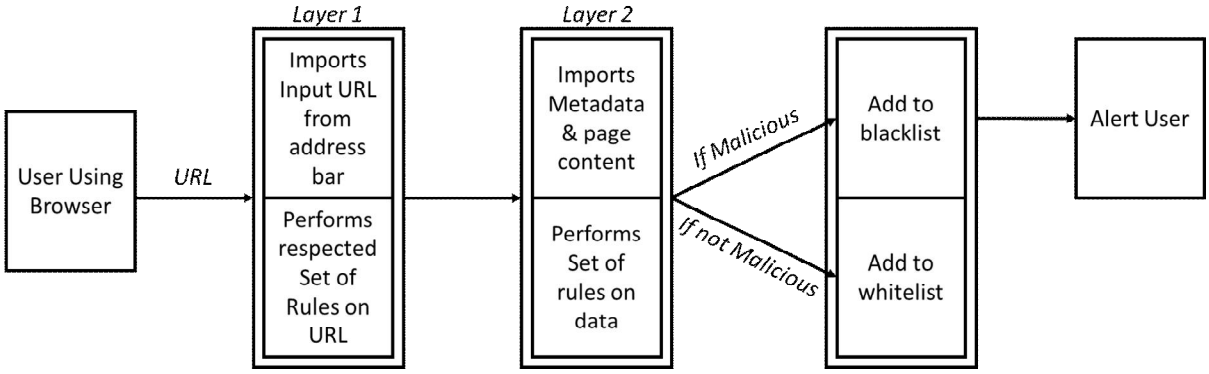


Fig.2 Working of System

IV. FUTURE WORK

After studying all the technique related to detection of mobile malicious webpages, we conclude that using only static or dynamic analysis technique is useful but not able to detect malicious pages accurately. So we will use hybrid approach to detect mobile malicious webpages by checking its URL as well as some of the page content, which will more accurately detect mobile webpages in real times.

This system can further developed to detect phishing attacks in the presence of embedded objects like flash. Also various strategies for discovering malicious pages should be design further to improve performance. The accuracy of the system can also be increased using new techniques.

REFERENCES

[1] CHAITRALI AMRUTKAR, YOUNG SEUK KIM, PATRICK TRATNOR, "Detecting Mobile Malicious Webpages in Real Time," IEEE Transaction on Mobile Computing,2016.Science and Software Engineering, Volume 3, Issue 7, July 2013

[2] G. ASHOK KUMAR, A. VENU GOPAL, I. ABHILASH BALU, M. M. V. VAMSI, "Detecting Mobile Malicious Webpages in Real Time," International Journal of Engineering Research in Computer Science and Engineering (IJERCSE) Vol 5,Issue 4, April 2018.

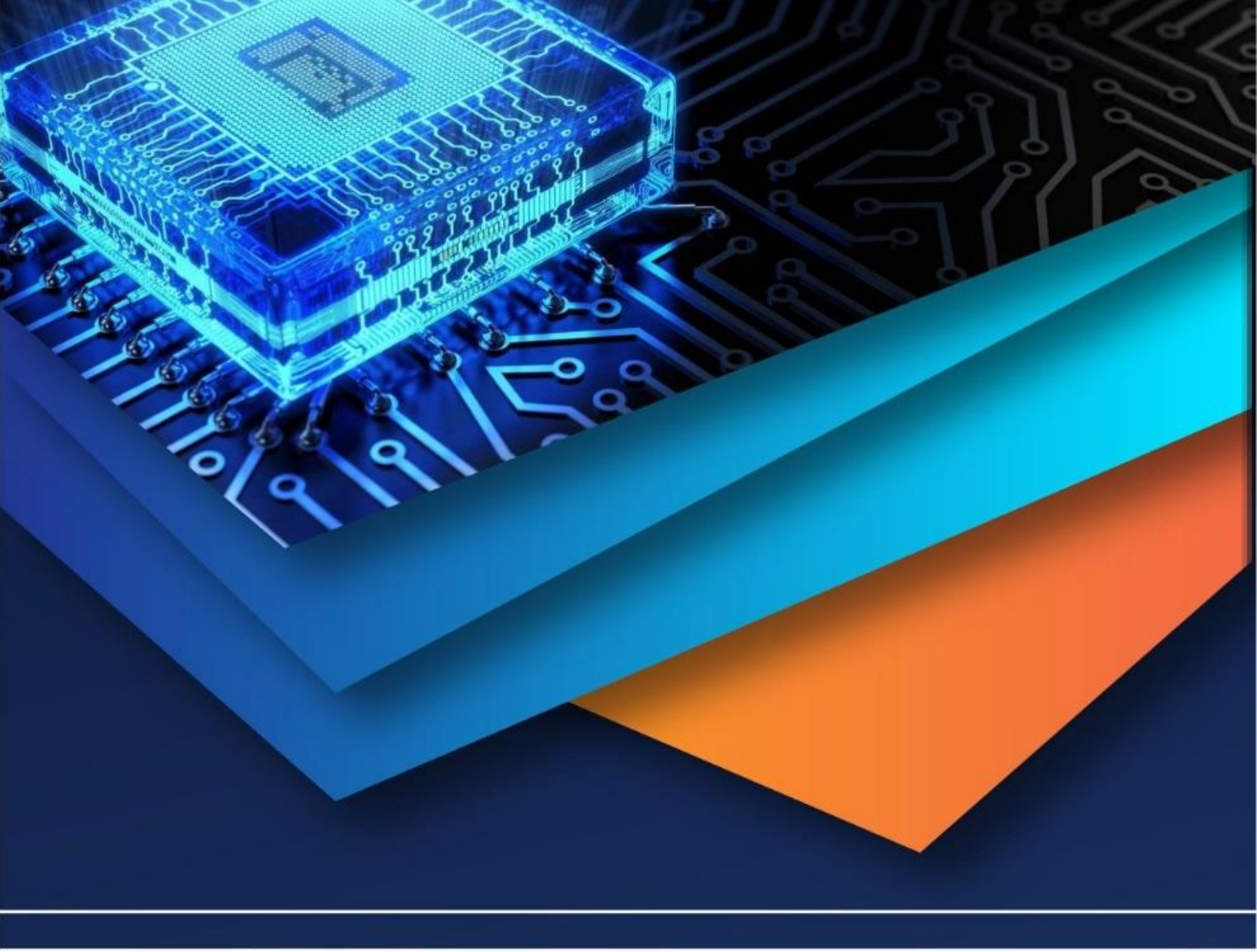
[3] M. ANANTHA RAMAN, R. ANIL KUMAR, S. GOWRI SHANKAR, P. DEVENDRAM, "Detecting Malicious Web Pages in Real Time," International Journal of Innovative Research in Science, Engineering And Technology, vol. 7, Special Issue 2, March 2018.

[4] ABDULGANI ALI AHMED and NIK QUOSTHONI SUNAIDI, "Malicious Website Detection: A Review," International of Forensic Science And Criminal Investigation ISSN: 2476-1311, volume- 7 Issue 3 February 2018.

[5] DR. JITENDRA AGARWAL, DR. SHIKHA AGARWAL, ANURAG AWATHE, DR. SANJEEV SHARMA, "Malicious Web Page Detection through Classification Technique: A Survey", ILCST, Vol.8, ISSUE 1, JAN-MARCH 2017.

[6] HEMALI SAMPAT, MANISHA SAHARKAR, AJAY PANDEY and HERAL LOPES, "Detection Of Phishing Website Using Machine Learning," International Research Journal of Engineering and Technology (IRJET), Volume: 05 Issue: 03| Mar-2018.

[7] G. VASANTH KUMAR, U. SESHADRI, "Detection of Phished Websites," International Advanced Research Journal in Science, Engineering and Technology. Vol. 1, Issue 2, October 2014.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY