ISSN (Online): 2455-7838
SJIF Impact Factor (2017): 5.705

EPRA International Journal of

Research & Development

(IJRD)

Monthly Peer Reviewed & Indexed International Online Journal

Volume: 3, Issue:11,November 2018

Published By :
EPRA Journals

SJIF Impact Factor: 5.705 Volume: 3 | Issue: 11 | November | 2018 ISSN: 2455-7838(Online)
EPRA International Journal of Research and Development (IJRD)

DETECT MOVABLE MALICIOUS WEBPAGE IN ACTUAL TIME

R. Bhuvaneswari[1]
[1]Research Scholar, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India,

S.Jayabharathi[2]
[2]Assistant Professor of Computer Science, Vivekanandha College for Women, Tiruchengode,India,

P.Saranya[3]
[3]Research Scholar, Department of Computer Science, Vivekanandha College for Women, Tiruchengode, India,

ABSTRACT

Mobile specific web pages differ significantly from their desktop counterparts in content, layout, and functionality. Accordingly, existing techniques to detect malicious websites are unlikely to work for such web pages. In this paper, we design and implement KAYO, a mechanism that distinguishes between malicious and benign mobile web pages. KAYO makes this determination based on static features of a webpage ranging from the number of frames to the presence of known fraudulent phone numbers. First, we experimentally express the need for mobile specific techniques and then identify a range of new static features that highly correlate with mobile malicious web pages. We then apply KAYO to a dataset of over 350,000 known benign and malicious mobile web pages and express 90 percent accuracy in classification. Moreover, we discover, characterize, and report a number of web pages missed by Google Safe Browsing and Virus Total, but detected by KAYO. Lastly, we make a browser increase using KAYO to protect users from malicious mobile websites in real-time. In doing so, we provide the first static analysis technique to detect malicious mobile web pages.

KEYWORDS: *KAYO mechanism, static analysis algorithm, Web Browsing, Mobile Security.*

I. INTRODUCTION

Malicious Web pages are more and more increase while we accessing the web. Though, in spite of significant advances I processor power and bandwidth, the browsing incident on mobile devices is considerably different. These differences can largely be credited to the dramatic cut of screen size, which impacts the content, functionality and layout of mobile web pages. Content, functionality and layout have commonly been used to perform static analysis to determine malicious in the desktop space. Features such as the frequency of I frames and then redirections have traditionally served as strong indicators of malicious intent. Due to the significant change made to

contain mobile devices, such assertion may no longer be true. For example, whereas such behavior would be flagged as chary in the desktop setting, many popular benign mobile web pages require multiple re directions before users gain access to content.

2. RELATED WORK

Content-based and in power experiment techniques to notice malicious websites: Dynamic approach mistreatment virtual machines and honey client systems give deeper visibility into the behavior of hinders measure ability of dynamic approaches.

This performance penalty may be avoided by break static approach. Static approach trusts on the structural and lexical properties of a webpage and do not execute the content of the webpage. One such technique of sleuthing malicious URLs is spite applied math ways for URL classification support a URL's lexical and host-based properties.

But, URL-based techniques usually suffer from high false positive rates. Using HTML and JavaScript options extracted from a webpage in adding to URL classification helps address this downside and provides higher results. Static approaches avoid performance price of dynamic approaches. In addition, mistreatment quick and reliable static approaches to notice benign web pages will avoid high-ticket in-depth analysis of all web pages.

3. MOTIVATION

Static analysis techniques to find malicious websites usually use options of a webpage such as HTML, JavaScript and character of the URL. Commonly, these options are fed to machine learning techniques to classify kind and malicious web pages. These techniques are predicated on the idea that the options are dispersed otherwise across caring and malicious web pages. Therefore, any changes within the division of static options in benign and/or malicious web pages impacts classification results of static analysis techniques. Whereas productive, these static analysis techniques have been used solely for desktop web pages. Mobile websites are considerably totally different from their desktop counter parts in content, practicality and layout. Consequently, existing tools utilize static options provide malicious desktop web pages which are unlikely to figure for mobile web pages. We tend to make a case for four factors that encourage building separate static analysis techniques to observe malicious mobile web pages.

4. METHODOLOGIES

Our object is to design and develop a method to identify mobile specific malicious web pages in real-time. We extract static features from a webpage and make did not think phone number strings simply listed on web pages without an API prefix. We row that due to the reputation of application markets such as Google play and iTunes, a website hosting its own mobile application binary possibly suggest bad behavior. If we found more than an entry of file son the same webpage, we implicit that the webpage was a third-party app store was unlikely to be malicious.

4.1 KAYO Feature Set

A web page has some mechanism counting HTML and JavaScript code, images, the URL, and the header. Mobile specific web pages also contact applications running on a user's device using web APIs. We extract structural, lexical and quantitative property of such mechanism to make KAYO's feature set. We focus on extracting mobile relevant features that take minimal removal time. Our hypothesis is that such features are strong indicator of whether a webpage has been built for support a user in their web browsing knowledge or for malicious purposes.

4.2 Data Collection

Our data meeting process included accumulate labeled benign and malicious mobile specific web pages. First, we explain an experiment that identify and defines 'mobile specific web pages'. We then perform the data collection process over three months in 2013.We use these crawl specifically because they are close to the publication of the connected work, making them as Close to equal as possible.

5. PROBLEM OF ANALYSIS

Presented static analysis techniques and tools for detecting malicious web pages are alert on desktop web pages. Therefore, they are unable to detect mobile specific pressure with high accuracy. Several web pages built expressly for mobile, return empty pages when render in a desktop browser. Thus, even existing dynamic analysis techniques that execute websites in desktop browsers on virtual machines, are useless on such mobile websites. At last, signature based tools such as Google Safe Browsing at present only work with desktop browsers. Open application KAYO is similar to those of existing malicious website detection tools using static analysis. Many complete set of features makes it harder to evade KAYO, as seen from estimate over a large data set. Presented application statically crawl the top million websites of Alex. But it did not collect web pages that use JavaScript to detect and forward to the mobile webpage. It also missed the mobile web pages represent by ways other than the ones used by the top 1,000 websites. It doesn't meeting all mobile web pages from Alex top one million.

6. PROPOSED WORK

Proposed work includes the following:

- The future method focus on mobile specific threats. Future method work on the mobile specific web pages. Presented techniques to detect malicious websites are unable to work on mobile. Now determination is based on the static as well as dynamic features.

- Our purpose is use to check the malicious function and phishing site. At this point SLD (second level domain) and OCR (optical character recognition) technique are also introduced. OCR is technique that change image into text to detect valuable phishing attack.
- Currently user first enters the URL he wants to visit then the system will match the URL with existing malicious URL. If URL matches then it will show advice message otherwise go to the next step.
- Next it motivation study the HTML tags. If it found any frame tags then it shows the see point that the URL contain malicious function and add the URL in database else go to next step.
- Next our request will read for cross site scripting. If any unnecessary script found then it will show a message that URL conation malicious function and add the URL in the database. If not go to the next step.
- As a final point of check for the phishing attack. Now SLD is use with the help of OCR technique to find the phishing site. Now if the SLD matches with the text extract by the OCR then the site are safe if not a warning message will pop.

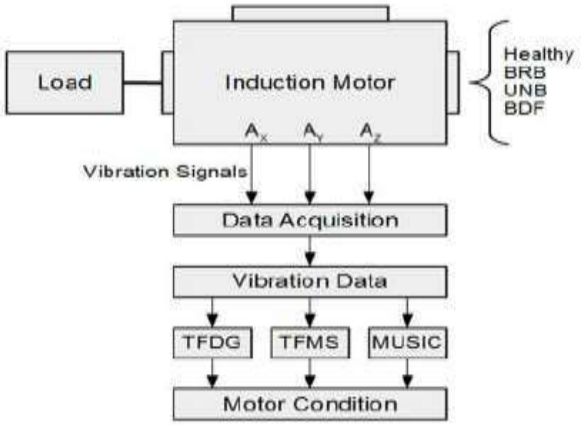

Figure.6 proposed methodology

7. ALGORITHMS USED

We explain the machine learning techniques we consider to tackle the problem of classifying Mobile specific Web pages as malicious. We then discuss the strength and Weaknesses of each organization technique, and the process for selecting the best model for static analysis algorithm. We build and evaluate our chosen Model for correctness, false positive rate and true Positive rate. Lastly, we compare to the static analysis algorithm presented technique and empirically display. The importance of the static analysis algorithm features. We note that where automated analysis is possible.

8. CONCLUSION

We study the framework for detect movable malicious webpage in actual time. Then existing the techniques using static features of desktop web pages to detect malicious performance for mobile specific pages. We designed and developed a fast and reliable static analysis technique that detect movable malicious web pages and also detect phishing sites. Our application provides greater correctness in classification, and detects a number of malicious web pages in the wild that are not detected by accessible techniques such as Cantina. To finish, we make a browser expansion that provide actual-time feedback to users. We planned an request for mobile platforms. We identified the weakness of the heuristics-based anti-phishing schemes that highly rely on the HTML source code of web pages. We end that our application detects new movable specific threats such as websites hosting and takes the first step towards identifying new security challenges in the modern web.

9. REFERENCES

1. *Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor, Senior Member, IEEE "Detecting Mobile Malicious Webpages in Real Time" Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor, Senior Member, IEEE*
2. *Charles Arthur, "Mobile internet devices 'will outnumber humans this year'." http://www.theguardian. com/ technology/ 2013/feb/07/ mobile-internet-outnumber-people.*
3. *Chakradeo, S., Reaves, B., Traynor, P., and Enck, W., "MAST: Triage for Market-scale Mobile Malware Analysis," Tech. Rep. GT-CS-12-01, College of Computing, Georgia Institute of Technology, 2012.*
4. *N. Provos, P. Mavrommatis, M. A. Rajab and F. Monrose, "All Your iFRAMEs Point to Us", Proceedings of the 17th Conference on Security Symposium, SS, USENIX Association Berkeley, (2008); CA,USA.*

5. *D. Canali, M. Cova, G. Vigna, and C. Kruegel. Prophiler: a fast filter for the large-scale detection of malicious webpages. In Proceedings of the 20th International Conference on World Wide Web (WWW), 2011.*
6. *L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi. EXPOSURE: Finding malicious domains using passive DNS analysis. In Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS), 2011.*
7. *A. P. Felt and D. Wagner. Phishing on mobile devices. In Web 2.0 Security and Privacy (W2SP), 2011.*
8. *"Cross-site Scripting (XSS) Attacks and Defense Mechanisms: classification and state-of-art" by Shashank Gupta and B.B Gupta ,14 September,2015, Springer.*
9. *Dr. Jitendra Agrawal, Dr. Shikha Agrawal, Anurag Awathe, Dr. Sanjeev Sharma. "Malicious Web Page Detection through Classification Technique: A Survey". In Proceeding of the IJCST March 2017.*