ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Mobile Malicious WebPages Detection in Real-Time

Kuttakula Farhana
Department of Computer Science &Amp; Engineering,
Akshaya Bharathi Institute of Technology,
Kadapa, AP, India.

P.Gangadhar
Department of Electronics and Communications Engineering,
Akshaya Bharathi Institute of Technology,
Kadapa, AP, India.

Abstract:
Mobile specific WebPages disagree considerably from their desktop counterparts in content, layout and practicality. Consequently, existing techniques to notice malicious websites area unit unlikely to figure for such WebPages. During this paper, we have a tendency to style and implement knock cold, a mechanism that distinguishes between malicious and benign mobile WebPages. Knock cold makes this determination supported static options of a webpage starting from the amount of frames to the presence of identified dishonorable phone numbers.

First, we have a tendency to by experimentation demonstrate the requirement for mobile specific techniques so establish a spread of recent static options that extremely correlate with mobile malicious WebPages. We then apply knock cold to a dataset of over 350,000 identified benign and malicious mobile WebPages and demonstrate ninetieth accuracy in classification. Moreover, we have a tendency to discover, characterize and report variety of WebPages lost by Google Safe Browsing and Virus Total, however detected by knock cold. Finally, we have a tendency to build a browser extension exploitation knock cold to guard users from malicious mobile websites in time period. In doing thus, we offer the primary static analysis technique to notice malicious mobile WebPages.

Index Terms:
Mobile security, WebPages, internet browsers, machine learning.

INTRODUCTION:

Mobile devices area unit progressively being employed to access the net. However, in spite of great advances in processor power and information measure, the browsing expertise on mobile devices is significantly completely different. These variations will for the most part be attributed to the dramatic reduction of screen size, that impacts the content, practicality and layout of mobile webpages. Content, practicality and layout have frequently been wont to perform static analysis to see spitefulness within the desktop area [1]. Options appreciate the frequency of iframes and therefore the variety of redirections have historically served as sturdy indicators of malicious intent. Because of the numerous changes created to accommodate mobile devices, such assertions could not be true.

For instance, whereas such behavior would be flagged as suspicious within the desktop setting, several standard benign mobile webpages need multiple redirections before users gain access to content. Previous techniques conjointly fail to think about mobile specific webpage parts appreciate calls to mobile arthropod genus [2]. to Illustrate, links that spawn the phone's dialer (and the name of the amount itself) will offer sturdy proof of the intent of the page. New tools area unit so necessary to spot malicious pages within the mobile internet. During this paper, we have a tendency to gift kAYO1, a quick and reliable static analysis technique to notice malicious mobile web- pages.

Cite this article as: Kuttakula Farhana & P.Gangadhar, "Mobile Malicious WebPages Detection in Real-Time", International Journal & Magazine of Engineering, Technology, Management and Research, Volume 5, Issue 10, 2018, Page 8-12.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

derived from their hypertext markup language and JavaScript content, computer address and advanced mobile specific capabilities [3]. We initial by experimentation demonstrate that the distributions of identical static options once extracted from desktop and mobile webpages vary dramatically. We then collect over 350,000 mobile benign and malicious webpages over a amount of 3 months. We have a tendency to then use a binomial classification technique to develop a model for knock cold to produce ninetieth accuracy and eighty nine true positive rate. kAYO's performance matches or exceeds that of existing static techniques employed in the desktop area. knock cold conjointly detects variety of malicious mobile webpages not exactly detected by existing techniques appreciate Virus Total and Google Safe Browsing [4]. Finally, we have a tendency to discuss the restrictions of existing tools to notice mobile malicious webpages and build a browser extension supported knock cold that gives real time feedback to mobile browser users.

we have a tendency to create the subsequent contributions: Experimentally demonstrate the variations within the "security features" of desktop and mobile webpages: We by experimentation demonstrate that the distributions of static options employed in existing techniques (e.g., the amount of redirections) area unit completely different once measured on mobile and desktop webpages [5]. Moreover, we have a tendency to illustrate that sure options area unit reciprocally related or unrelated to or non indicative to a webpage being malicious once extracted from every area. The results of our experiments demonstrate the requirement for mobile specific techniques for police work malicious webpages. style and implement a classifier for malicious and benign mobile webpages: we have a tendency to collect over 350,000 benign and malicious mobile webpages. We have a tendency to then establish new static options from these webpages that distinguish between mobile benign and malicious webpages.

Knock cold provides ninetieth accuracy in classification and shows improvement of 2 orders of magnitude within the speed of feature extraction over similar existing techniques. We have a tendency to more by trial and error demonstrate the importance of kAYO's options [6]. Finally, we have a tendency to conjointly establish 173 mobile webpages implementing cross-channel attacks, that conceive to induce mobile users to decision numbers related to identified fraud campaigns. Implement a browser extension supported kAYO: To the simplest of our data knock cold is that the initial technique that detects mobile specific malicious webpages by static analysis. Existing tools appreciate Google Safe Browsing don't seem to be enabled on the mobile versions of browsers, thereby precluding mobile users. Moreover, the mobile specific style of knock cold permits detection of malicious mobile web pages missed by existing techniques.

Finally, our survey of existing extensions on Firefox desktop browser suggests that there's a scarceness of tools that facilitate users establish mobile malicious webpages. To fill this void, we have a tendency to build a Firefox mobile browser extension exploitation knock cold, that informs users concerning the spitefulness of the webpages they shall visit in time period [7]. We have a tendency to conceive to create the extension publically on the market post publication. we have a tendency to note that we have a tendency to outline spitefulness broadly speaking, as is completed within the previous literature on the static detection within the desktop area. However, as a result of driveby- downloads don't seem to be the least bit common within the mobile area at the time of writing, the overwhelming majority of detected pages area unit regarding phishing. kAYO Feature Set A webpage has many parts together with hypertext markup language and JavaScript code, images, the URL, and therefore the header. Mobile specific internet pages conjointly access applications running on a user's device exploitation web arthropod genus (e.g., the dialer).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We have a tendency to extract structural, lexical and quantitative properties of such parts to get kAYO's feature set. We have a tendency to specialize in extracting mobile relevant options that take stripped extraction time [8]. Our hypothesis is that such options area unit sturdy indicators of whether or not a internet page has been designed for helping a user in their web browsing expertise or for malicious functions. Our feature set consists of forty four options, eleven of that area unit new and not antecedently known or used. We have a tendency to describe these new options well. A set of options in knock cold are utilized by alternative authors in static review of desktop webpages within the past.5 However, it's necessary to notice that these options in mobile webpages and desktop webpages disagree in magnitude (e.g., variety of iframes) and show varied correlation with the character of the webpage (i.e., malicious/benign) [10].

we have a tendency to divide kAYO's forty four options into four classes: mobile specific-, JavaScript, hypertext markup language and computer address options. To the simplest of our data, we have a tendency to area unit the primary to use these mobile specific options, and don't claim novelty on exploitation subsets of alternative antecedently known options. Table one summarizes the eight mobile, ten JavaScript, fourteen hypertext markup language and twelve computer address options. We have a tendency to by trial and error illustrate the effectiveness of every of the options in Section five.2 [9].

IMPLEMENTATION AND ANALYSIS

We describe the machine learning techniques we have a tendency to thought-about to tackle the matter of classifying mobile specific webpages as malicious or benign. we have a tendency to then discuss the strengths and weaknesses of every classification technique, and therefore the method for choosing the simplest model for knock cold. we have a tendency to build and judge our chosen model for accuracy, false positive rate and true positive rate.

Finally, we have a tendency to compare knock cold to existing techniques and by trial and error demonstrate the importance of kAYO's options [12]. we have a tendency to note that wherever automatic analysis is feasible, we have a tendency to use our full datasets; but, as is often worn out the analysis community, we have a tendency to use at random hand-picked subsets of our information once intensive manual analysis and verification is needed.

ARCHITECTRURE

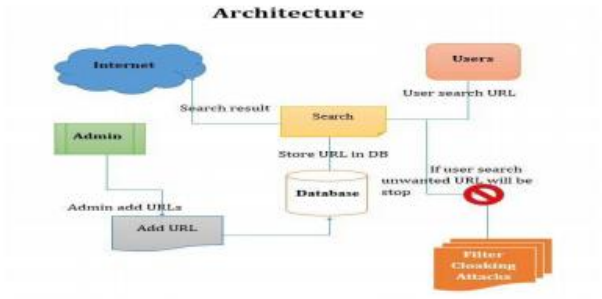
Building a browser extension based on MWPT adds value for two reasons. First, the mobile specific design of MWPT enables detection of new threats previously unseen by existing services (e.g., pages including spam phone numbers). Second, building an extension allows immediate use of our technique. We discuss other potential avenues of adopting MWPT. We developed a browser extension using MWPT for Firefox mobile, which informs users about the maliciousness of the webpages they intend to visit. Our goal was to build an extension that runs in real-time. Therefore, instead of running the feature extraction process in a mobile browser, we outsourced the processing intensive functions to a backend server. Figure shows the architecture of the extension.

User enters the URL he wants to visit in the extension toolbar. The extension then opens a socket and sends the URL and user agent information to MWPT's backend server over HTTPS. The server crawls the mobile URL and extracts static features from the webpage. This feature set is input to MWPT's trained model, which classifies the webpage as malicious or benign. The output is then sent back to the user's browser in real-time. If the URL is benign according to MWPT, the extension renders the intended webpage in the browser automatically. Otherwise, a warning message is shown to the user recommending them not to visit the URL [11]. Users of the extension will browse both mobile specific and desktop webpages since not all websites offer a mobile specific version.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Recall that being a mobile specific technique, MWPT does not perform well on desktop webpages. Consequently, processing all pages of interest through MWPT might output incorrect results for Desktop web pages. To address this problem, the backend server first detects whether the intended webpage is mobile specific using the same method explained in Section 4.2. The webpage is processed by MWPT only if it is mobile. The desktop web pages are analyzed using Google Safe Browsing. Note that any other existing technique for detecting desktop malicious webpages can be used instead of Google Safe Browsing. We performed manual analysis of 100 randomly selected URLs (90 benign and 10 malicious) from our test dataset and measured the performance of MWPT in real time.

On an average, an output was rendered in 829 ms on average from the time the user entered a URL in MWPT's toolbar. We argue that the good performance is due to careful selection of quickly extractable features and lower complexity of mobile webpages as compared to desktop webpages. The maximum delay in result generation was seen in scraping the input webpage from its respective server. Caching already scraped webpages can reduce this delay, as we demonstrated experimentally, by an average of 85%. Figure 7 shows a screen shot of our browser extension at work. We plan to make the extension available publicly post publication.



ALGORITHMS USED

We describe the machine learning techniques we Considered to tackle the problem of classifying Mobile specific Web pages as malicious or We then discuss the strengths and Weaknesses of each classification technique, And the process for selecting the best model For MWPT. We build and evaluate our chosen Model for accuracy, false positive rate and true Positive rate. Finally, we compare MWPT to Existing techniques and empirically demonstrate The significance of MWPT features. We note That where automated analysis is possible.

CONCLUSION

Mobile webpages area unit considerably completely different than their desktop counterparts in content, practicality and layout. Therefore, existing techniques exploitation static options of desktop webpages to notice malicious behavior don't work well for mobile specific pages. We have a tendency to designed and developed a quick and reliable static analysis technique referred to as knock cold that detects mobile malicious webpages. Knock cold makes these detections by activity forty four mobile relevant options from webpages, out of that eleven area unit recently known mobile specific options.

Knock cold provides ninetieth accuracy in classification, and detects variety of malicious mobile webpages within the wild that don't seem to be detected by existing techniques appreciate Google Safe Browsing and Virus Total. Finally, we have a tendency to build a browser extension exploitation knock cold that gives time period feedback to users. we have a tendency to conclude that knock cold detects new mobile specific threats appreciate internet sites hosting identified fraud numbers and takes the primary step towards distinguishing new security challenges within the trendy mobile web.

REFERENCES

[1] Chaitrali Amrutkar, Young Seuk Kim and Patrick Traynor, "Detecting Mobile Malicious Webpages in Real Time," IEEE Trans. Services Computing, IEEE, 2017.

[2] Shuang Liang, Yong Ma and Yong Ma, "The Scheme of Detecting Encoded Malicious WebPages Based on Information Entropy", IEEE, 2016.

[3] Xi Xiao Ruibo Yan, and H. Yan Runguo Ye, "Detection and Prevention of Code Injection Attacks on HTML5-based Apps," IEEE,2016.

[4] Lookout. https://play.google.com/store/apps/details?hl=en&id=com.lookout.

[5] Malware Domains List. http://mirror1.malwaredomains.com/files/domains.txt.

[6] Phish tank. http://www.phishtank.com/.

[7] Pin drop phone reputation service. http://pindropsecurity.com/phone-fraud-solutions/phone reputation service prs/.

[8] Scrapy — an open source web scraping framework for python. http://scrapy.org/.

[9] Virus Total. https://www.virustotal.com/en/.

[10] Google developers: Safe Browsing API. https://developers.google.com/Safe browsing/, 2012.

[11] Alexa, the web information company. http://www.alexa.com/topsites,2013.

[12] Dot mobi. Internet made mobile. Anywhere, any device. http://dotmobi.com/, 2013.