DETECTING MOBILE MALICIOUS WEBPAGE IN REAL-TIME

Saifulla Shariff
PG, Student
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
saifullashariff2000@gmail.com

Dharamvir
Associate Professor
Dept. of MCA
The Oxford College of Engineering,
Bommanahalli, Bengaluru- 560068
dhiruniit@gmail.com

ABSTRACT

In contrast to desktop sites, m-specific sites are less user-friendly and accessible. Why? Why? Therefore, the existing techniques for discovering m websites .' The work employs this method to examine static information from iframes and kAYO, which is helpful in differentiating malicious and harmless mobile webpage types. This is are the grounds for applying this method. The initial step is to set the significance of mobile-friendly approaches through evaluation, and then finding the static elements usually associated with malicious sites. We will be displaying more than 350,000 innocuous web pages utilizing kAYO. In addition, we identified and classified different websites that Google Safe Browsing and even again 'failed' to access (and then were marked as possibly unsafe by kAYO. Our kAYO-based browser add-on offers real-time defense against malicious device websites for users. Detection of maliciousmobile sites at the same time is our first static analysis task. We have applied this method.

Keyword: Mobile web page security, malicious site detection, static analysis, phishing prevention, real time browser protection, kAYO, google safe browsing, virus total.

INTRODUCTION

The use of mobile phones for information transfer, online trading, and communication has grown significantly. However, with these advancements, mobile security threats have emerged even more in the form of malicious websites, which harness the existing vulnerabilities in the mobile phones to breach privacy of users and instigate security threats. As a response to these emanations there should be a real-time mobile malicious webpage detecting system developed that will be able to learn emerging threats and develop accordingly.

The project involves ideas about the creation of an evolving software able to look and categorize malicious Webpages on mobile device in real-time so as recursively avoid any form of potential plagiarism threat. The normal types of antivirus software and protective measures cannot keep pace with the ever-growing number of practices that the hackers

devise with the view of infiltrating into the systems . The project will be concentrated in the design of high system that will enable display of malicious websites that will be targeted to mobile devices. The other approaches that will also be implemented in the project are additional will be run as sandboxes to look at how things behave while they are running, which is how they can be tagged. As machine learning and deep learning become more common, It was also argued that they should make new, better approaches i.e., machine learning, data analysis and pattern recognition with regard to the determination of potential threats in terms of web contents, behaviour or any other comparable factor. This futuristic approach will ensure the process of browsing the internet is safe and would reduce the chances of threats such as downloading of malware and phishing

LITERATURE SURVEY

The threats of the proliferation of smart phones and the prevalence of mobile internet has been the availability of malicious web sites or rather phishing along with other categories of cyber attacks to which the affected user has been subjected Desktop detection systems don't always beneficial in a mobile environment due to hardware and operating system differences as suitable, and network differences. Thus, the attention of the researchers has been turned at the real- time aspect of detecting the malicious webpages targeting the mobile users. We have talked about the ways that Machine Learning has helped us find bad URLs. In the first-mover case, models. Recent reports also investigated the coordination between ensemble models, hybrids and detection systems which help combine both the static and the dynamic modes of analysis. But these methods make it harder to figure out how much it will cost to get the results, can't be used in real-time systems, and aren't flexible enough to keep up with attackers who change the system are the different part as they check for the update to be used as they are perform the things were be done the task as they are doing blacklists were used to match against known malicious domainsto the suspect factors. The downside of this method is that it is easy to use, so it doesn't work well for large groups of people and can't stop zero-day attacks. The methods look at HTML, JavaScript, and web redirects on webpages to figure out if someone is trying to hurt you. They will be designed for dynamic analysis,

EXISTING WORK

protection of the internet.

All these uses heuristics and signature-based rules combined with threat intelligence to intercept detain malicious.

web sites before they can reach mobile users.

Mobile devices. MDM solutions can provide security to the users in the occurrence of an attack as they are able to identify the threats, offer web filters. They can also keep track of web usage, block access to dangerous sites and alert the user about potentially incorrect sites. The leading mobile web browsers, such as chrome, and Safari, as well as firefox also

provide security features that are in-built to give protection to web users against dangerous sites. These features include the capability to be real-time against phishes and malware and this is founded on reputation and threat information systems to warn a person on a potential threat or block the visit to a malichrous site. Due to the fact that the security can be installed on the cloud, it will provide a security in real time to mobiles users against harmful web pages. These services have been given the responsibility to use the infrastructure for the control and monitoring of web traffic along with the identification of the security threats. The operations can be carried out through different mechanisms for example the usage of machine learning algorithms and the behaviour pattern analysis for identification of a malicious web page or even using reputation systems.

PROPOSED SYSTEM

Just come with a plan for the monitoring network module that would enable the gathering of data about the network usage made by mobile devices. In fact, such a module can be built using network sensors, proxy servers, or simply through the integration with MDM (mobile device management) solutions. Employ a real-time traffic analyzer tool for examining the network data traffic statistics..This is advantageous. It should extract the necessary information from requests to and from responses to web pages (i.e, URLs, headers and payload data).". Utilize behavioral analysis methods to identify suspicious or malicious behaviors on web pages. The scope of this may involve examining the execution of JavaScript, manipulating the DOM, fulfilling network requests, and other runtime behaviors. Utilize reputation databases and blacklists that contain data on malicious websites, URLs, and IP addresses.By cross-examining the extracted domains and URLs, this database can be used to identify malicious web pages. Ensure that external threat intelligence sources are aware of new threats by integrating their current information into the system.This integration allows the system to extract threat feeds that are based on real-time threats and add fresh data to enrich analysis. Develop a system that can rate websites on their level of risk or danger by identifying if these sites are harmful in any way. Such a process is scored through decision making and risk assignment. Partially relegate the classification outputs of various machine learning models, behavioral analytics, reputation scoring and heuristics to an intermediate threat estimation stage to 'weigh' the attraction of threats.

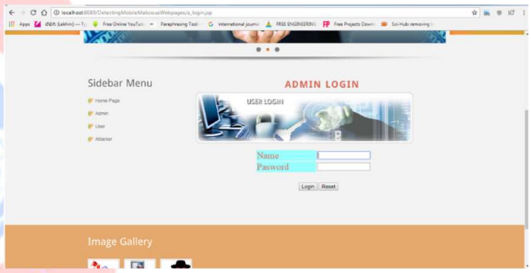
SYSTEM DESIGN

Generally, data gathering initiates with mobile devices or local people. That is data in the form of HTTP requests and responses over mobile phones, which are made when accessing a web page. This can be a result of local visitor tracking or an integration with cell browsers or security programs. Some initial data are filtered to extract the relevant data. This may involve examining HTTP headers, retrieving URLs and

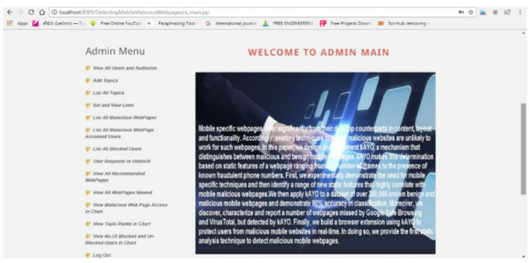
differentiating web page content from other community data. The extraction of relevant capabilities from the content and metadata of an internet web page is done through feature extraction. Among the capabilities available are various ones that cover URL properties (length, area recognition), HTML structure (tags and scripts), JavaScript behavior, malware detection, and information. Extracting the capabilities is then fed into a real-time evaluation factor that employs a variety of detecting techniques to identify malicious web pages. It usually involves models that understand the system, computational methods (heuristics), and rule-based structures designed to quickly assess capabilities and arrive at a decision .The structure integrates with danger intelligence reassets, including recognition databases, blacklists and recognised malware signatures. The reassets present more details and particulars about identified harmful websites, URLs, or IP addresses. Through real-time evaluation, the extracted capabilities can be contrasted with this danger intelligence information to enhance the detection accuracy. By analyzing the evaluation results and potential danger, the system decides whether an internet page is malicious, suspicious, or secure by making a selection about its character. The selection may be binary (malicious vs. non-mallicious) or comprise only a few categories that are predominantly determined by the severity of the threats.

IMPLEMENTATION

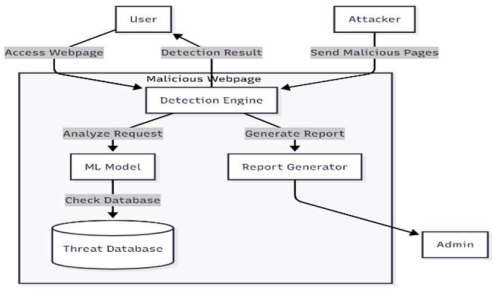
HOME PAGE



ADMIN MAIN PAGE



ADMIN RELATED PAGES WELCOME



Future Enhancements

Identify and apply The most effective and machine learning-based methods, such as The most efficient and ensemble solutions/anomaly detection, to enhance The precision and effectiveness are malicious internet site detection machine. Utilizing enhanced behavioral measurement approaches, behavioral analysis can create diffused styles and identify irregularities in web page behavior cells. The interpersonal action of reading and consultational acts can be compared to individual sports and run-time actions.' Improves the machine' s ability to detect zero-day threats, which are unclassified or unknown malicious websites. Created systems to screen and promptly detect problem websites that are tagged as new or emerging threats.Based on the beauty of the detection machine, Group Intelligence feedback, as well as collective intelligence is an assemblage of structures, which allow person feedback and collective intelligence. Users will possess the ability to keep track of potentially dangerous websites and your comments on the false positives/false negatives, which can result in a continuous increase in the device's performance.It is also instructive to examine how this opportunity such as ability and level is to be determined, differing between debate of the organization and Web site on the one side and debate of the location, the individual profile and settings of the community on the other side. Connect the computer with external safety data (feed and stores) and threat intelligence to receive a new information about harmful sites.

CONCLUSION

The mobile web pages widely vary in structure, functionality and their content compared to their desktops counterparts only rendering conventional methods of detection that were based on generic desktop features ineffective in the mobile platform. To fill this gap we developed and enforced a stable static analysis tool, kAYO, that was able to identify malicious webpages in the mobile domain with high effectiveness. To enhance accuracy of detection, the system examines 44 mobile-specific features, 11 of them are new parameters, identified by the system. In accordance with the findings of the trials, they manage to run kAYO with an accuracy of nearly 90% in identifying a threat, which existing tools does not effectively do. kAYO was also incorporated into a lightweight browser extension such that end-users received real-time protection and notification of attacks in real-time. The specified strategy demonstrates that it is possible to implement a form of machine learning working

in conjunction with mobile-specific features to provide beneficial security strategies. Besides fraud number detection, and malicious hosting, the framework will offer the possibility to detect phishing attacks, malicious ads as well as social engineering condemners.Overall, this paper can be considered a substantial contribution to the improvement of mobile web security and the need to carry continuation research to counteract the ever-delopmental ways of attackers. The model can also be employed in the future to expand the scope to the cross platform browsers and dynamically analyse and respond to the behaviour. It is also possible to adjust the model to be used to identify zero-day mobile threats.

REFERENCES

[1] hphosts, a community managed hosts file. http://hphosts.gt500.org/hosts.txt.

[2] Joewein.de LLC blacklist. http://www.joewein.net/dl/bl/dom-bl-base.txt.

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

[4]MalwareDomainsList.http://mirror1.malwaredomains.com/files/domains.txt.

[5] Phishtank. http://www.phishtank.com/.

[6] Pindrop phone are reputation service. http://pindropsecurity.com/phone-fraud-solutions/phone are reputation service prs/.

[7] Scrapy is an open-source Python web scraping platform. http://scrapy.org/.

[8] VirusTotal. https://www.virustotal.com/en/.

[9] Developers at Google: Safe Browsing API. https://developers.google.com/safe-browsing/,2012.

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

[11] dotmobi. internet made mobile. anywhere, any device. http://dotmobi.com/, 2013.

[12] C. Amrutkar, K. Singh, A. Verma, and P. Traynor. VulnerableMe: Measuring systemic weaknesses in mobile browser security. In Proceedings of the.