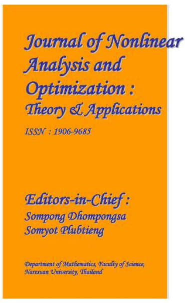
Journal of **N**onlinear **A**nalysis and **O**ptimization
Vol. 15, Issue. 1, No.15 : 2024
ISSN : **1906-9685**



Journal of Nonlinear Analysis and Optimization : Theory & Applications
ISSN : 1906-9685
Editors-in-Chief :
Sompong Dhompongsa
Somyot Plubtieng
Department of Mathematics, Faculty of Science, Naresuan University, Thailand

DECIPHERING IN-APP ADVERTISING: UNVEILING HIDDEN THREATS ACROSS MOBILE APP-WEB INTERFACES

D.Shiva kumar, B.Tech Student, CSD, Vaagdevi College of Engineering (Autonomous), India
M. Akhil, B.Tech Student, CSD, Vaagdevi College of Engineering (Autonomous), India
K.Lokesh Reddy , B.Tech Student, CSD, Vaagdevi College of Engineering (Autonomous), India
G. Kranthi Kumar, B.Tech Student, CSD, Vaagdevi College of Engineering (Autonomous), India

Mrs.G. Pallavi**,** Assistant Professor, Department of CSE (Data Science), Vaagdevi College of Engineering (Autonomous), India

ABSTRACT

Mobile users are increasingly becoming targets of malware infections and scams. In order to curb such attacks, it is important to know how these attacks originate. We take a previously unexplored step in this direction. Numerous in-app advertisements work at this interface when the user taps on the advertisement, she is led to a web page which may further redirect until the user reaches the final destination. Even though the original applications are not malicious, the Web destinations that the user visits could play an important role in propagating attacks. We develop a systematic static analysis methodology to find ad libraries embed in applications and dynamic analysis methodology consisting of three components related to triggering web links, detecting malware and scam campaigns, and determining the provenance of such campaigns reaching the user. Our static analysis system identified 242 different ad libraries and dynamic analysis system was deployed for a two month period and analyzed over 600,000 applications while triggering a total of about 1.5 million links in applications to the Web. We gain a general understanding of attacks through the app-web interface and make several interesting findings including a rogue antivirus scam, free iPad scams, and advertisements propagating SMS trojans.

1. INTRODUCTION

Android is the predominant mobile operating system with about 80% worldwide market share [1]. At the same time, Android also tops among mobile operating system in terms of malware infections [2]. Part of the reason for this is the open nature of the Android ecosystem, which permits users to install applications for unverified sources. This means that users can install applications from third-party app stores that go through no manual review or integrity violation. This leads to easy propagation of malware. In addition, industry researchers are reporting [3] that some scams which traditionally target desktop users, such as ransomware and phishing, are also gaining ground on mobile devices. In order to curb Android malware and scams, it is important to understand how attackers reach users. While a significant amount of research effort has been spent anaa lyzing the malicious applications themselves, an important, yet unexplored vector of malware propagation is benign, legitimate applications that lead users to websites hosting malicious applications. We call this the app-web interface. In some cases this occurs through web links embedded directly in applications, but in other cases the malicious links are visited via the landing pages of advertisements coming from ad networks.

A solution directed towards analyzing and understanding this malware propagation vector will have three components: triggering (or exploring) the application UI and following any reachable web links; detection of malicious content; and collecting provenance information, i.e., how malicious content was reached. There has been some related research in the context of Web to study so-called malvertising or malicious advertising [4], [5]. The context of the problem here is broader and the problem itself requires different solutions to triggering and detection to deal with aspects specific to mobile platforms (such as complicated UI and trojans being the primary kinds of malware).

2. LITERATURE SURVEY

Android is the predominant mobile operating system with about 80% worldwide market share [6]. At the same time, Android also tops among mobile operating systems in terms of malware infections [7]. Part of the reason for this is the open nature of the Android ecosystem, which permits users to install applications for unverified sources. This means that users can install applications from third-party app stores that go through no manual review or integrity violation. This leads to easy propagation of malware. In addition, industry researchers are reporting [8] that some scams which traditionally target desktop users, such as ransomware and phishing, are also gaining ground on mobile devices. To curb Android malware and scams, it is important to understand how attackers reach users. While a significant amount of research effort has been spent analyzing the malicious applications themselves, an important, yet unexplored vector of malware propagation is benign, legitimate applications that lead users to websites hosting malicious applications. We call this the app-web interface. In some cases, this occurs through web links embedded directly

in applications, but in other cases the malicious links are visited via the landing pages of advertisements coming from ad networks. A solution directed towards analyzing and understanding this malware propagation vector will have three components: triggering (or exploring) the application UI and following any reachable web links; detection of malicious content; and collecting provenance information, i.e., how malicious content was reached. There has been some related research in the context of the Web to study so-called advertising or malicious advertising [9]. The context of the problem here is broader and the problem itself requires different solutions to triggering and detection to deal with aspects specific to mobile platforms (such as complicated UI and trojans being the primary kinds of malware).

Targeted advertising has transformed the marketing landscape for a wide variety of businesses, by creating new opportunities for advertisers to reach prospective customers by delivering personalized ads, using an infrastructure of a number of intermediary entities and technologies. The advertising and analytics companies collect, aggregate, process, and trade a vast amount of users' personal data, which has prompted serious privacy concerns among both individuals and organizations. This article presents a comprehensive survey of the privacy risks and proposed solutions for targeted advertising in a mobile environment. We outline details of the information flow between the advertising platform and ad/analytics networks, the profiling process, the measurement analysis of targeted advertising based on user's interests and profiling context, and the ads delivery process, for both in-app and in browser targeted ads; we also include an overview of data sharing and tracking technologies. We discuss challenges in preserving the mobile user's privacy that include threats related to private information extraction and exchange among various advertising entities, privacy threats from third-party tracking [10], re-identification of private information and associated privacy risks. Subsequently, we present various techniques for preserving user privacy and a comprehensive analysis of the proposals based on such techniques; we compare the proposals based on the underlying architectures, privacy mechanisms, and deployment scenarios. Finally, we discuss the potential research challenges and open research issues [12].

Online advertising has become a prevalent marketing tool [13], commanding most of the spending and taking over from the traditional broadcast advertising in newspapers, television, and radio. According to StatistaFootnote1, in 2022, 62% of global ad spending is forecast to be on internet ads, while television will have around 23%. This is primarily due to the ability of online ad platforms to tailor or personalize ads, and thereby target specific customer segments [14]. Targeted advertising is based on big data analytics, where user's personal information is collected and processed to enable segmenting users into groups based on interests, location, or personal attributes like age, gender, etc., with a varying size of the selected customer segment, down to the level of an individual [15**].**

3. PROBLEM STATEMENT

In the existing system, several researchers have also studied privacy leakages through ad libraries. Taint Droid [16] and some follow-up works all present results in which a large majority of privacy leakages happen through ad libraries included in the applications. While the previous list of works uses dynamic analysis, researchers have also used static analysis to identify privacy leaks in applications, and through ad libraries in particular [17]. Privacy leakages in ad libraries are not in the scope of this paper. However, we do study scams that extract personal information of the users, even with their consent. Grace et al. [18] perform static analysis of ad libraries to discover a number of implications such as private data leakage and execution of untrusted advertisement code in applications. Industry researchers also detected vulnerabilities in ad libraries that can provide escalated privileges to the advertisement code that these libraries execute [19]. Ad Split [20] discusses that ad libraries should be separated from the main application, running in a different sandbox, so that they can have different permissions from the applications, and vulnerabilities and privacy leakages in them do not affect the main application. Quire [21] also proposed techniques that can achieve a similar effect. The goal of this paper is not to identify vulnerabilities due to the inclusion of ad libraries or to fix such problems. The web links or advertisements embedded in applications may themselves not be malicious, but their end result is.

DISADVANTAGES

- There are no Methods to find more advertised products on published data sets.

- There is no Data Disclosure Model to find the attackers.

4. PROPOSED SYSTEM

The proposed system has developed a framework for analyzing the app-web interfaces in Android applications. We identify three features for a successful methodology: triggering of the app-web interfaces, detection of malicious content, and provenance to identify the responsible parties. We incorporate appropriate solutions for the above features and have implemented a robust system to automatically analyze app

web interfaces. The system is capable of continuous operation with little human intervention.

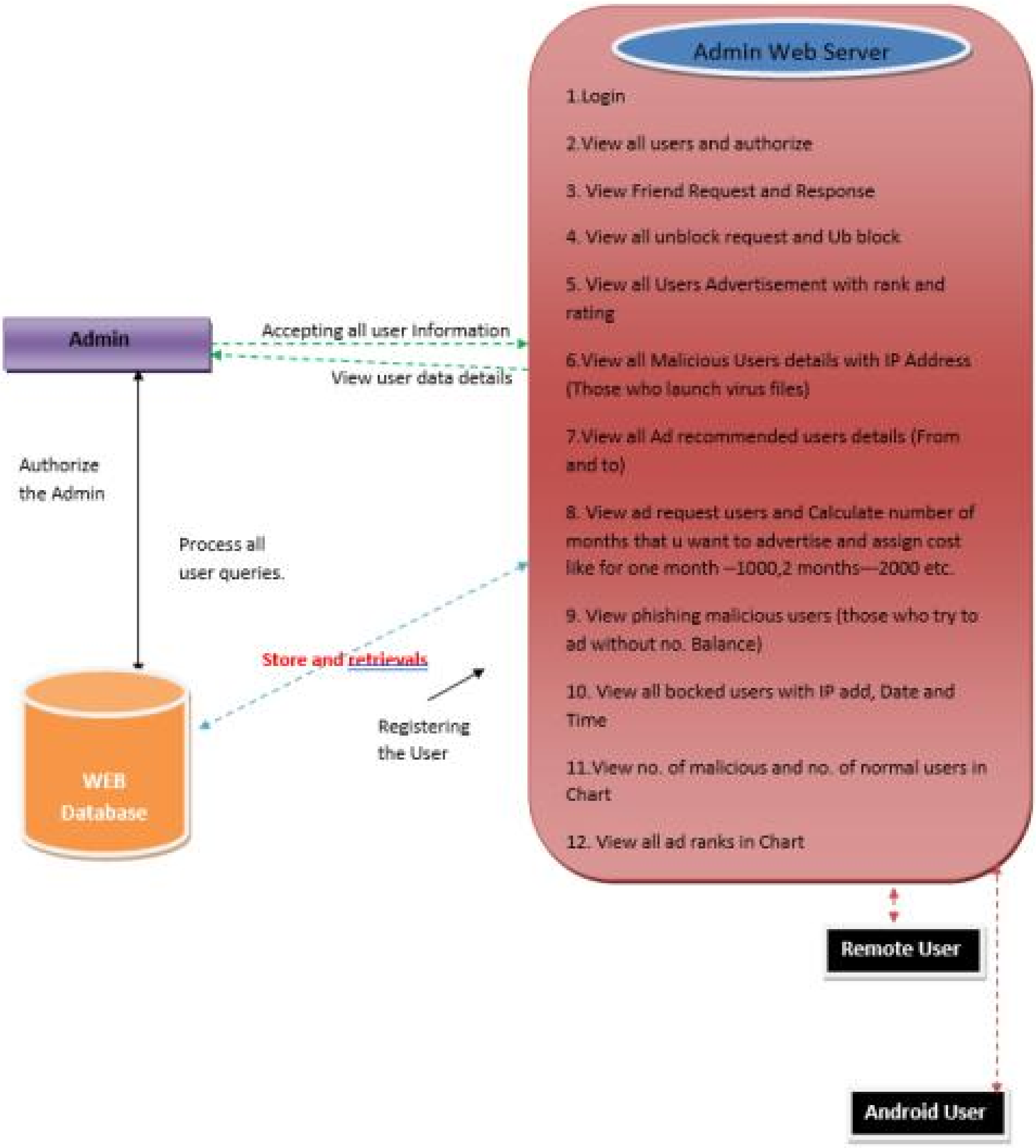
As part of our triggering app-web interfaces, we developed a novel technique to interact with UI widgets whose internals do not appear in the GUI hierarchy. We develop a computer graphics-based algorithm to find clickable elements inside such widgets.

The system deployed our system for a period of two months in two locations, one in North America and another in China. We studied over 600,000 applications from Google Play and four Chinese stores for a period of two months and identified hundreds of maliciousfiles and other scam campaigns [22]. We present a number of interesting findings and case studies in an attempt to characterize the malware and scam landscape that can be found at the app-web interface. As some examples, we have found rogue ad networks propagating rogue applications; scams enticing users by claiming to give away free products propagating through both in-app advertisements and links embedded in applications; and dangerous SMS trojans propagating through well-known ad networks.

ADVANTAGES

- The proposed technique easily supports incremental analysis to identify new ad libraries in newly published applications.
- The proposed system can easily support real phones for analyzing apps although we do not choose it. Therefore, each application is run in a virtual machine based on the Android emulator.

5. SYSTEM ARCHITECTURE


Admin Web Server
1.Login
2.View all users and authorize
3. View Friend Request and Response
4. View all unblock request and Ub block
5. View all Users Advertisement with rank and rating
6.View all Malicious Users details with IP Address (Those who launch virus files)
7.View all Ad recommended users details (From and to)
8. View ad request users and Calculate number of months that u want to advertise and assign cost like for one month –1000,2 months—2000 etc.
9. View phishing malicious users (those who try to ad without no. Balance)
10. View all bocked users with IP add, Date and Time
11.View no. of malicious and no. of normal users in Chart
12. View all ad ranks in Chart
Admin
Accepting all user Information
View user data details
Authorize the Admin
Process all user queries.
Store and retrievals
Registering the User
WEB Database
Remote User
Android User

6. IMPLEMENTATION

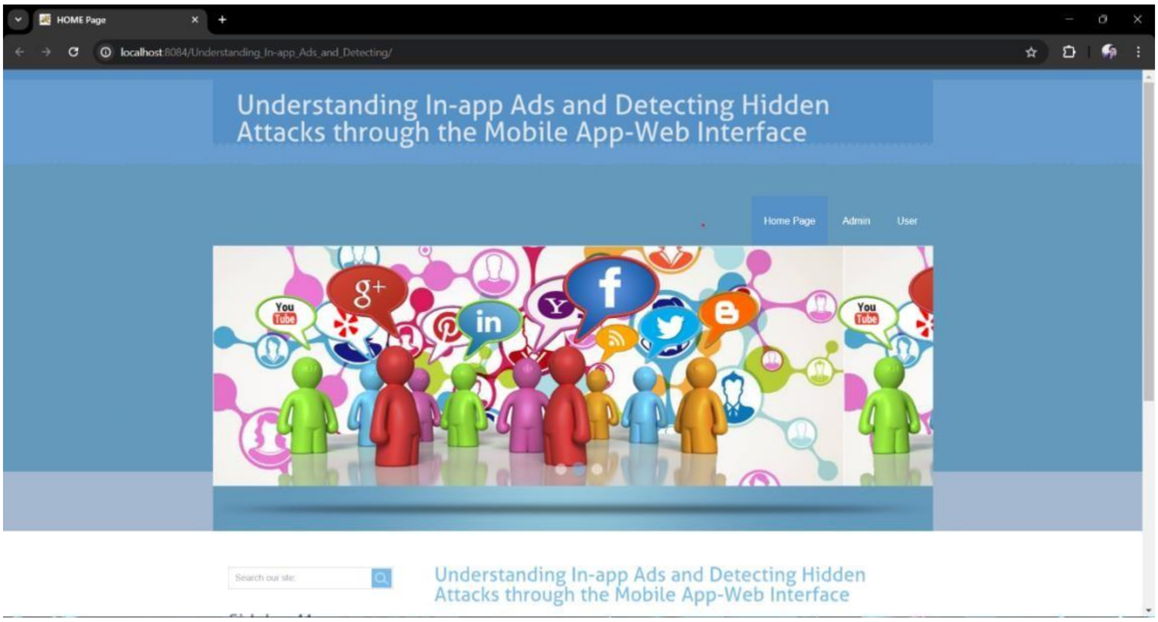
6.1. ADMIN

In this module, admin has to login with valid username and password. After login successful he can do some operations such View all users and authorize, View Friend Request and Response, View all un block request and Ub block, View all Users Advertisement with rank and rating, View all Malicious Users details with IP Address(Those who launch virus files),View all Ad recommended users details(From and To),View ad request users and Calculate number of months that u want to advertise and assign cost like for one month -- 1000,2 months---2000 etc., View phishing malicious users(those who try to ad without no. Balance), View all blocked users with IP add, Date and Time, View no.of malicious and no.of normal users in Chart, View all ad ranks in Chart

6.2. USER

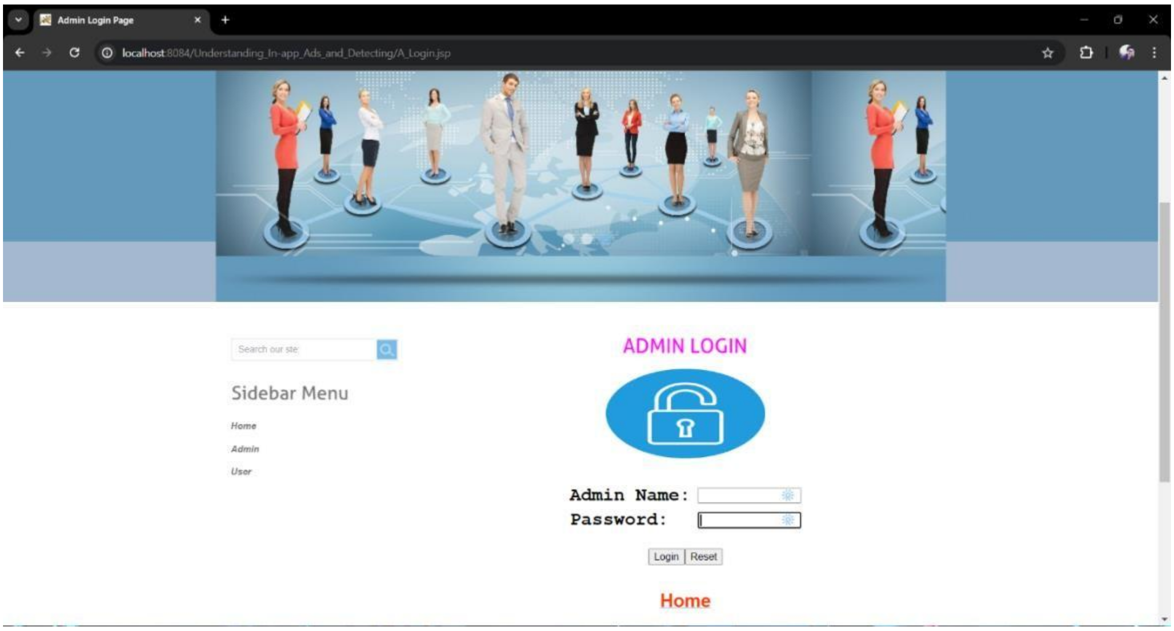
In this module, there are no numbers of users present. Users should register before doing some. After registration successfully he can login by using valid user name and password. After Login successful, he will do some operations like Register with Location and Login and Request to un block if u blocked, View your profiles with Account Type(Malicious or Normal),Search Friend and Find Friend Request, View all Your Friends, Create Bank Account, View Account Details, View Mini Statement, Enter your from to Date and send request to admin to launch Advertisement, Add Advertisement Details(Advertisement category, Ad name, Ad desc(attach file),Ad Date and Time, Company name, company est. Year),View all your ad details with rank and rating, View all your friends ad details and recommend to other friends.

7. RESULTS / EXPECTED OUTPUT



Understanding In-app Ads and Detecting Hidden Attacks through the Mobile App-Web Interface

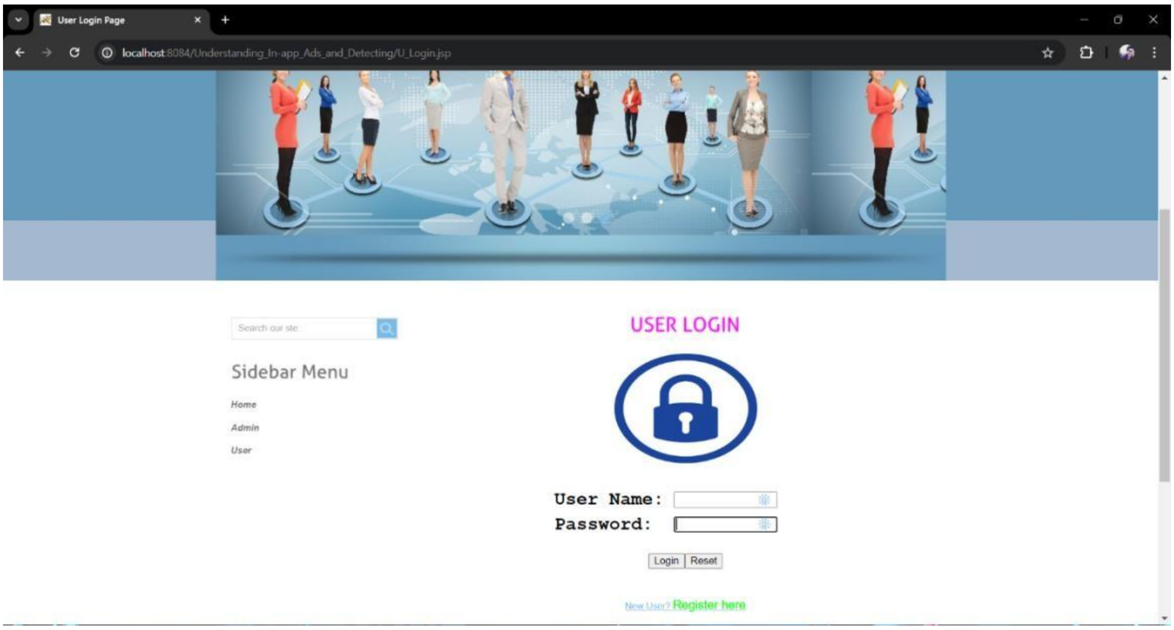
Understanding In-app Ads and Detecting Hidden Attacks through the Mobile App-Web Interface



ADMIN LOGIN

Admin Name:

Password:

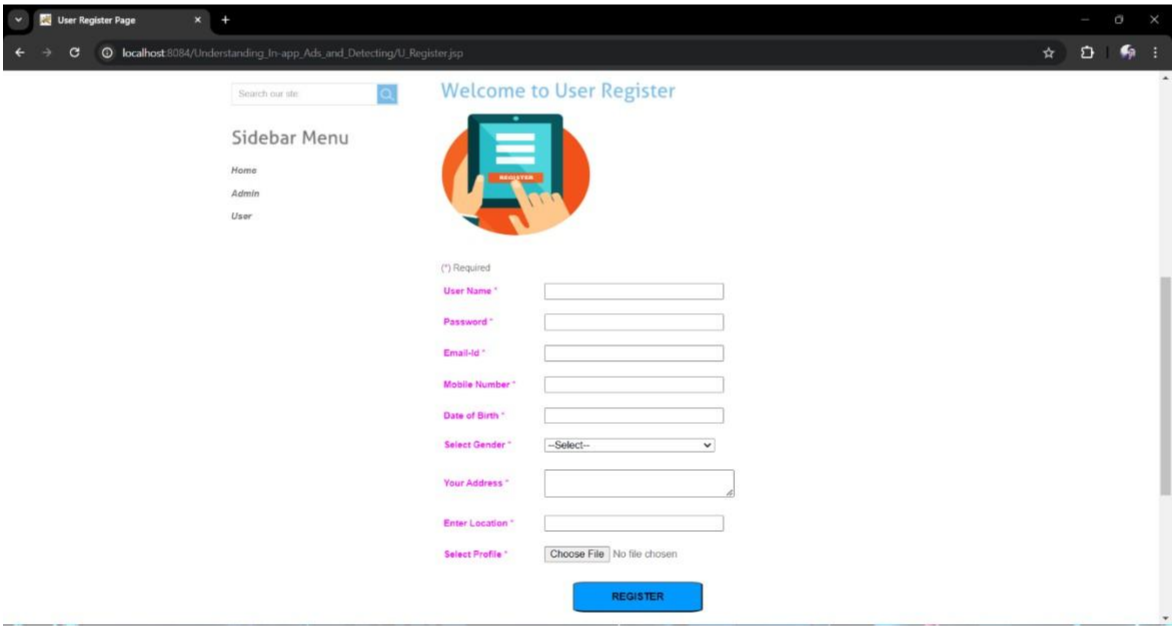

User Login Page
localhost:8084/Understanding_In-app_Ads_and_Detecting/U_Login.jsp
Search our site
Sidebar Menu
Home
Admin
User
Login
Reset

USER LOGIN

User Name:

Password:

New User? Register here



Welcome to User Register

(*) Required

User Name *

Password *

Email-Id *

Mobile Number *

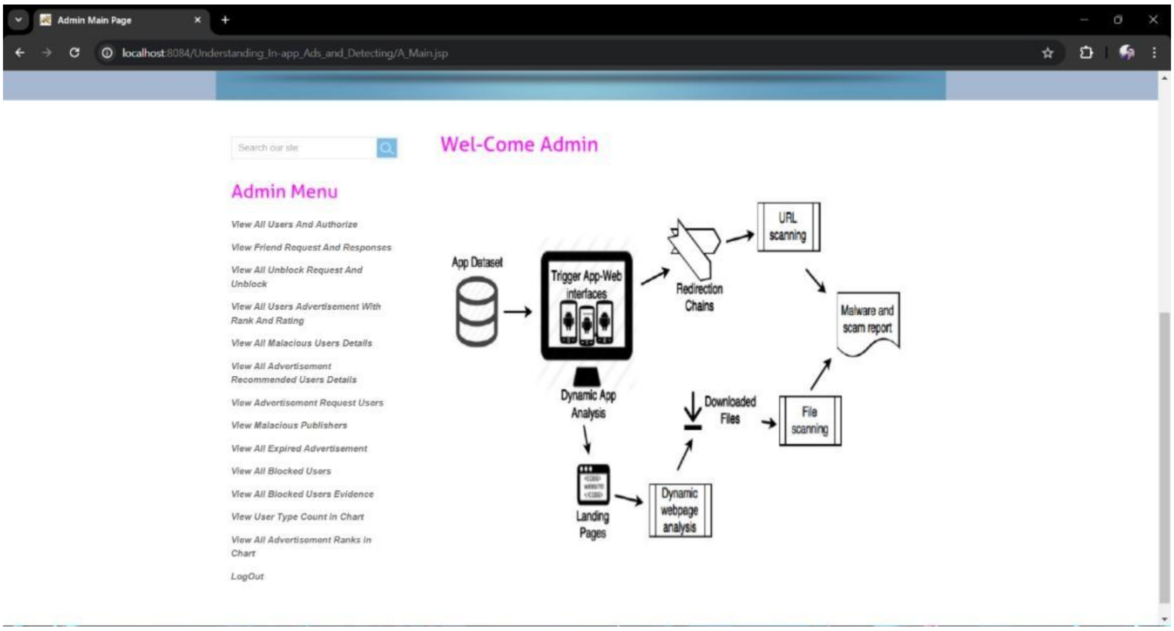
Date of Birth *

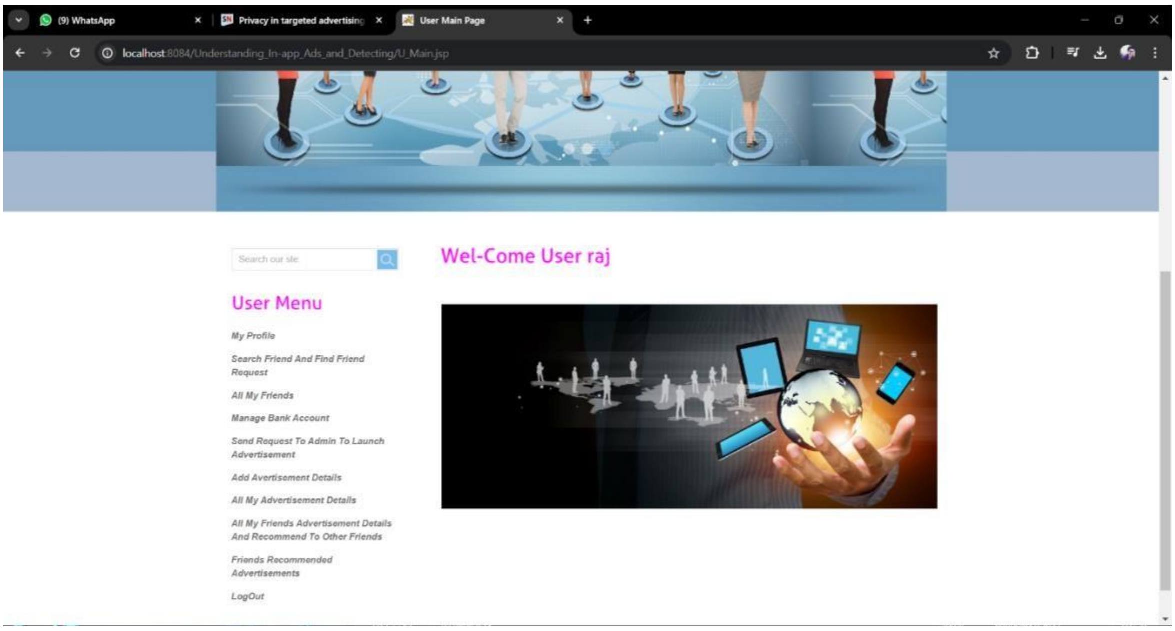
Select Gender * --Select--

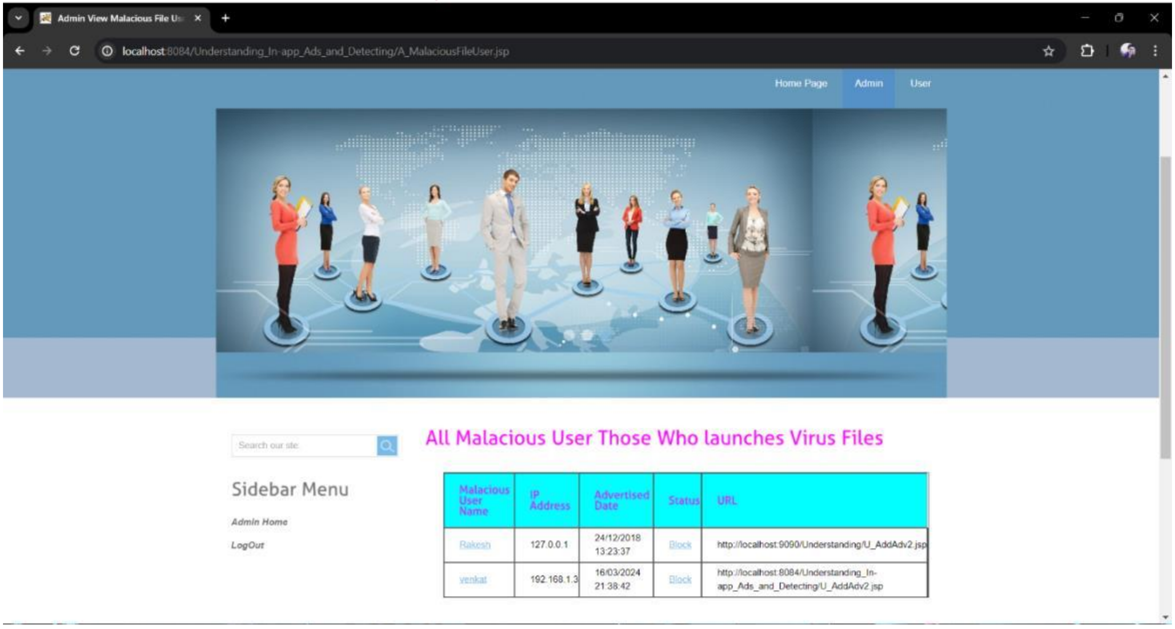
Your Address *

Enter Location *

Select Profile * No file chosen

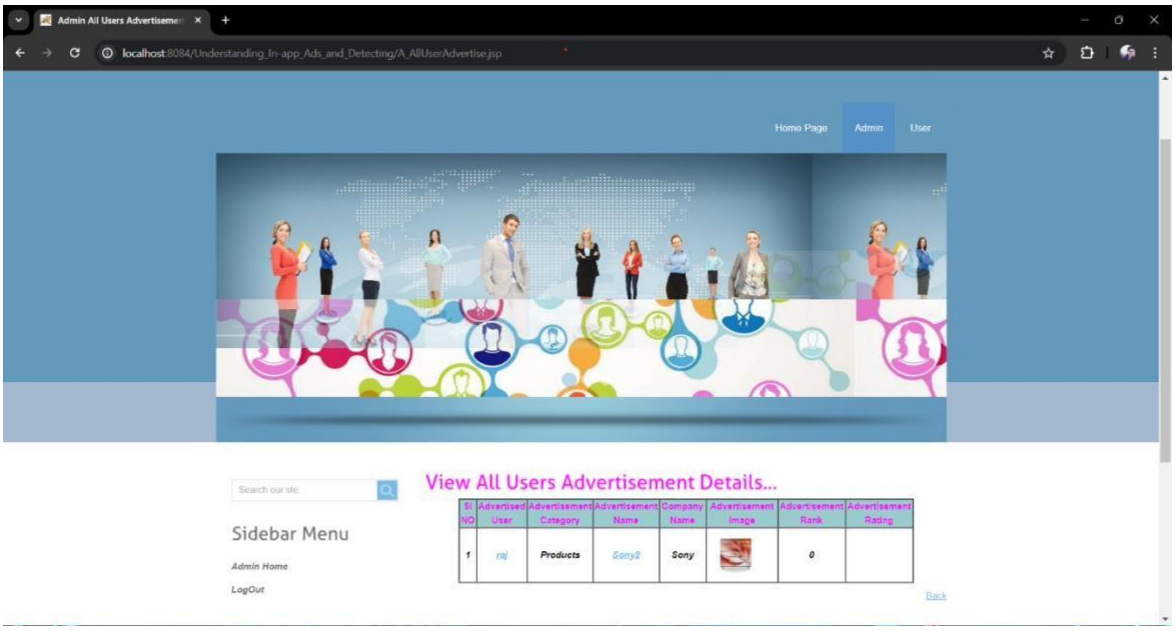

Admin Main Page
localhost:8084/Understanding_In-app_Ads_and_Detecting/A_Main.jsp
Search our site
Wel-Come Admin
Admin Menu
View All Users And Authorize
View Friend Request And Responses
View All Unblock Request And Unblock
View All Users Advertisement With Rank And Rating
View All Malacious Users Details
View All Advertisement Recommended Users Details
View Advertisement Request Users
View Malacious Publishers
View All Expired Advertisement
View All Blocked Users
View All Blocked Users Evidence
View User Type Count In Chart
View All Advertisement Ranks In Chart
LogOut
App Dataset
Trigger App-Web interfaces
Dynamic App Analysis
Redirection Chains
URL scanning
Malware and scam report
Downloaded Files
File scanning
Landing Pages
Dynamic webpage analysis


(9) WhatsApp
Privacy in targeted advertising
User Main Page
localhost:8084/Understanding_In-app_Ads_and_Detecting/U_Main.jsp
Search our site
Wel-Come User raj
User Menu
My Profile
Search Friend And Find Friend Request
All My Friends
Manage Bank Account
Send Request To Admin To Launch Advertisement
Add Avertisement Details
All My Advertisement Details
All My Friends Advertisement Details And Recommend To Other Friends
Friends Recommended Advertisements
LogOut


Admin View Malacious File Us
localhost:8084/Understanding_In-app_Ads_and_Detecting/A_MalaciousFileUser.jsp
Home Page
Admin
User
Search our site
Sidebar Menu
Admin Home
LogOut

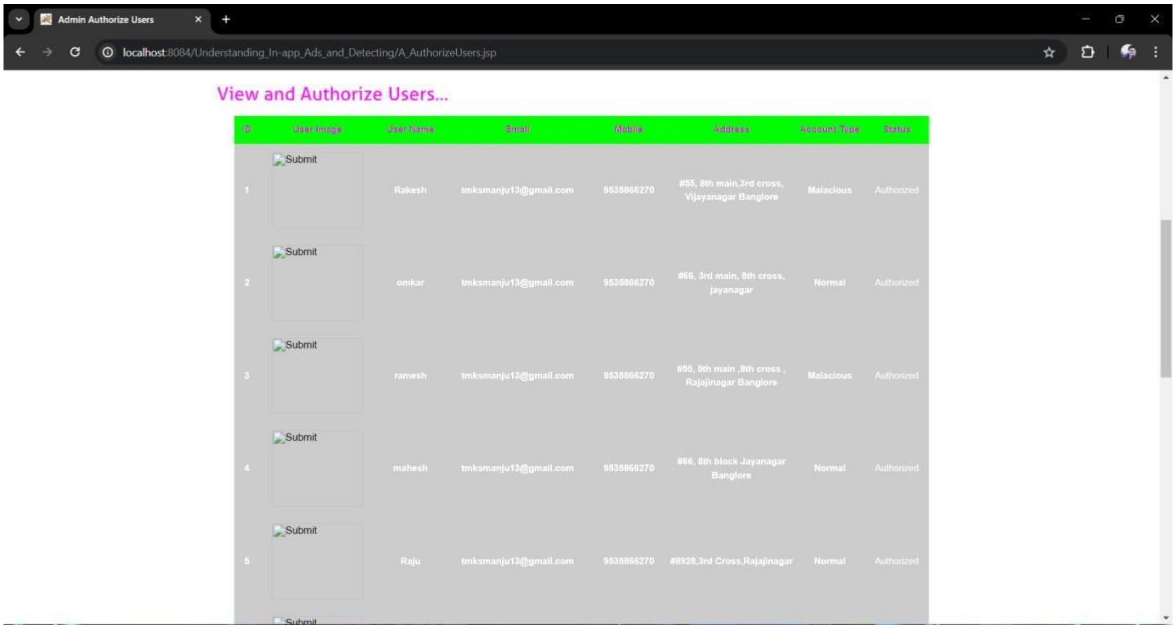
All Malacious User Those Who launches Virus Files

Malacious User Name	IP Address	Advertised Date	Status	URL
Rakesh	127.0.0.1	24/12/2018 13:23:37	Block	http://localhost:9090/Understanding/U_AddAdv2.jsp
venkat	192.168.1.3	16/03/2024 21:38:42	Block	http://localhost:8084/Understanding_In-app_Ads_and_Detecting/U_AddAdv2.jsp


Admin All Users Advertisemen
localhost:8084/Understanding_In-app_Ads_and_Detecting/A_AllUserAdvertise.jsp
Home Page
Admin
User
Search our site
Sidebar Menu
Admin Home
LogOut
Back

View All Users Advertisement Details...

Sl NO	Advertised User	Advertisement Category	Advertisement Name	Company Name	Advertisement Image	Advertisement Rank	Advertisement Rating
1	raj	Products	Sony2	Sony		0	


Admin Authorize Users
localhost:8084/Understanding_In-app_Ads_and_Detecting/A_AuthorizeUsers.jsp

View and Authorize Users...

ID	User Image	User Name	Email	Mobile	Address	Account Type	Status
1	Submit	Rakesh	tmksmanju13@gmail.com	9535866270	#55, 8th main,3rd cross, Vijayanagar Banglore	Malacious	Authorized
2	Submit	omkar	tmksmanju13@gmail.com	9535866270	#66, 3rd main, 8th cross, jayanagar	Normal	Authorized
3	Submit	ramesh	tmksmanju13@gmail.com	9535866270	#55, 5th main ,8th cross , Rajajinagar Banglore	Malacious	Authorized
4	Submit	mahesh	tmksmanju13@gmail.com	9535866270	#66, 8th block Jayanagar Banglore	Normal	Authorized
5	Submit	Raju	tmksmanju13@gmail.com	9535866270	#8928,3rd Cross,Rajajinagar	Normal	Authorized
	Submit						

8. CONCLUSION

In order to curb malware and scam attacks on mobile platI forms it is important to understand how they reach the user. In this paper, we found 242 ad libraries and explored the appI web interface, wherein a user may go from an application to a Web destination via advertisements or Web links embedded in the application. We used our implemented system for a period of two months to study over 600,000 applications in two continents and identified several malware and scam campaigns propagating through both advertisements and web links in applications. With the provenance gathered, it was possible to identify the responsible parties (such as ad networks and application developers). Our study shows that that should such as system be deployed, the users can be offered better protection on the Android ecosystem by screening out offending applications that embed links leading to malicious content as well as by making ad networks more accountable for their ad content. A regulatory authority like CNCERT(National Internet Emergency Center) could use our tool to understand the prevailing trends in mobile malvertising and hold the ad networks accountable. Similar techniques could also be used by the ad networks themselves to find malvertising in their own networks (note that this is a non-trivial issue due to multiple ad networks involved in serving a single ad).

9. FUTURE SCOPE

The future scope for unveiling in-app ads and uncovering covert attacks via mobile app-web interfaces is promising and essential in addressing evolving challenges in digital security and privacy. With increasing concerns about data privacy, there's a growing demand for transparency in advertising practices within mobile apps. By leveraging advanced detection techniques, collaboration among industry stakeholders, and continuous monitoring and analysis, businesses can enhance the integrity and security of their mobile app-web interfaces. Moreover, user education and awareness play a critical role in empowering individuals to make informed decisions about their digital security. Overall, by addressing these challenges effectively, organizations can strengthen user trust, comply with regulatory requirements, and safeguard against emerging threats in the digital landscape.

10. REFERENCES

[1]“Smartphoneosmarketshare,q12015,”http://www.idc.com/prodserv/smartphone-os market-share.jsp.

[2]“Malware infected as many android devices as windows laptops in 2014,” http://bgr.com/2015/02/17/android-vs-windows-malware-infection/.

[3]“Androidphoneshitby‘ransomware’,”http://bits.blogs.nytimes.com/2014/08/22/androi d-phones-hit-by-ransomware/?r=0.

[4] A. Zarras, A. Kapravelos, G. Stringhini, T. Holz, C. Kruegel, andG. Vigna, “The dark alleys of madisonavenue: Understanding malicious advertisements,” in Proceedings of the 2014 Conference on Internet Measurement Conference. ACM, 2014, pp. 373–380.

[5] Z. Li, K. Zhang, Y. Xie, F. Yu, and X. Wang, "Knowing your enemy:understanding and detecting malicious web advertising," in ProP ceedings of the 2012 ACM conference on Computer and Communications Security. ACM, 2012, pp. 674–686.

[6] A. Z. Broder, "On the resemblance and containment of documents,"in Compression and Complexity of Sequences 1997. Proceedings, Jun 1997, pp. 21–29.

[7] J. Buhler, "Efficient large-scale sequence comparison by localitysensitive hashing," vol. 17, no. 5, pp. 419–428, 2001.

[8] V. Rastogi, R. Shao, Y. Chen, X. Pan, S. Zou, and R. Riley, "Are theseads safe: Detecting hidden attacks through the mobile app-web interfaces,"2016.

[9] W. Zhou, Y. Zhou, M. Grace, X. Jiang, and S. Zou, "Fast, scalabledetection of piggybacked mobile applications," in Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013, pp. 185–196.

[10] V. Rastogi, Y. Chen, and W. Enck, "AppsPlayground: Automatic Security

Analysis of Smartphone Applications," Proceedings of ACM CODASPY, 2013.

[11] "Selendroid: Selenium for android," http://selendroid.io/.

[12] V. Rastogi, Y. Chen, and W. Enck, "Appsplayground: automatic security analysis of smartphone applications," in Proceedings of the third ACM conference on Data and application security and privacy. ACM, 2013, pp. 209– 220.

[13] "Celery: Distributed task queue," http://www.celeryproject.org/.in

[14] N. Viennot, E. Garcia, and J.Nieh, "A measurement study of google play," in The 2014 ACM international conference on Measurement and modeling of computer systems. ACM, 2014, pp. 221–233.

[15] Symantec, "Airpush begins obfuscating ad modules,"November 2012, http://www.symantec.com/connect/blogs/airpush-begins-obfuscating-ad modules.

[16] http://forums.makingmoneywithandroid.com

[17]http://www.androidauthority.com/armor-for-android-342192/.in

[18]“Reputationofamarktflow.com,”https://www.mywot.com/en/scorecard/amarktflow.c om.

[19] “Free iPad mini scam spreads via facebook rogue application,” https://nakedsecurity.sophos.com/2012/10/31/free-ipad-mini-facebook/.

[20] “Apple iPad scam,” http://blog.spamfighter.com/software/apple-ipad scam.html.

[21] “How to spot a ‘free iPhone or iPad’ scam: Why ’free iPhone’and ’free iPad’ stories are always bogus, and how to avoid getting ripped off,” http://www.macworld.co.uk/feature/iphone/free-iphone-ipad-scam-fake-auction-site facebook-3608522/.

[22] B. Liu, S. Nath, R. Govindan, and J. Liu, “Decaf: detecting and characterizing ad fraud in mobile apps,” in Proc. of NSDI, 2014. [23] J. Crussell, R. Stevens, and H. Chen, “Madfraud: Investigating ad fraud in android applications,” in Proceedings of the 12th annual international conference on Mobile systems, applications, and services. ACM, 2014, pp. 123– 134.