EnNos Mobile Application for Automated Malware Tracking on Android

Martin Loh Zhuan Jie
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
TP050925@mail.apu.edu.my

Julia Juremi
Forensics & Cybersecurity Research Center (FSEC)
Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur, Malaysia
julia.juremi@staffemail.apu.edu.my

***Abstract*— Individuals are the victims of most cybercrimes because they are unaware of them, despite the fact that there is a plethora of news and publications concerning cybercrime. This is because they continuously consider themselves fortunate and assume that they will be spared from attacks by hackers, especially for senior citizens and teenagers. Based on the research, people can see that most of the cyber-attacks are target on Android devices. This is because Android devices are built on open-source software, which means that users may alter the operating systems of their phones and tablets. In this project, the proposed application can assist senior citizens and teenagers in avoiding cybercrime by tracking malware in their mobile phones, which includes scanning emails, applications, websites, and more. Once the application has detected malware, it will notify users and automatically remove it from their devices.**

Keywords—android, malware, vulnerabilities, VirusTotal

I. INTRODUCTION

Nowadays, the mobile phone has become a necessity, people would like to use their phone social, business, learning and more. Therefore, people will leave all their personal information on their phones, and it has become a way to let the hacker hijack their phones to get important information. Besides, most of the organization has started the mobile initiatives. According to all of the research show that to process mobility can help to improve their operations and efficiency (Gontovnikas, 2021).

Therefore, a mobile phone can bring users a lot of benefits, it can let the life of users become more convenient and wonderful. However, it also can let the user be at risk when using the phone, which is been attacked by hackers. The most common type of mobile security risks is mobile application security threats, web-based mobile security threats, mobile network security threats, and mobile device security threats (Gartner, 2021).

For mobile application security threats, which will happen in downloading applications from unsafe platforms. This kind of application is looked to be genuine but is really skimming data from the smartphone of users. The web-based threats have always been ignored by users. This is because they will only happen when the users are browsed or visit the insecure website. Therefore, when users visit the website, they might immediately download harmful information to their smartphones.

The mobile network security threats are the most common and risky. This is because while the users are connected to public WiFi networks, the hacker can easily steal the unencrypted data. For the mobile device security threats, they can refer to the loss or theft of their devices. Also, this kind of threat is the most dangerous threat because the hacker can directly access the devices, and easy to locate the important data.

II. MOBILE APPLICATION

The first mobile application on the worldwide network supplied general-purpose information and information services, such as calendar, email, classifieds, stock market, and weather information (Pham, 2021). However, the need for mobile applications, as well as the capacity to build them, has spread to other areas, such as industrial automation, GPS, mobile gaming, and so on. The growth in the quantity and variety of applications has spawned a plethora of new fields. Many services, such as detecting location and online banking, monitoring, purchasing tickets, and even mobile medical services, increasingly rely on mobile application technology.

Mobile application has been classified into three types which are native apps, hybrid, and web apps.

1. Native application

Native applications are any apps that are designed for a certain mobile platform. Professionals utilize best-in-class user interface components while creating native apps. This results in improved performance, consistency, and a positive user experience. Users also have access to a broader range of application programming interfaces and have unrestricted access to all apps on the device. They can also seamlessly transition from one app to the next. The example of the native application which are dictionary apps, offline mobile game and more (Services, n.d.).

2. Web-based application

The web-based applications have similar speed to a web application running in a browser, which can be considerably slower than a native application. Also, it does not have as many functions as the original application on computer. HTML, CSS, and JavaScript are the standard web technologies used to create a web-based software. When opposed to offline usage, internet connectivity is usually necessary for appropriate behavior or to be able to use full

functionalities. Besides, most the data that stored by web-based application is in cloud (os-system,2020).

3. Hybrid application

The hybrid application is coded by using HTML, CSS and Java Script and it is performed on mobile WebView. The hybrid application is a combination of native and web-based apps. This category includes apps made with Apache Cordova, Sencha Touch, Xamarin, React Native and other platforms.

III. MOBILE SECURITY

Due to the increased business data on mobile devices attracts hackers, who can use mobile malware to attack both the device and the back-end systems. Therefore, the mobile device security is becoming increasingly essential. Malware assaults are a major security problem for mobile devices. According to experts, Android smartphones are the most vulnerable, but other platforms that incorporate near-field communications and other mobile payment technologies might also attract financially motivated thieves (Posey, Wigmore, & Westervelt, 2021). Due to the lack of mobile security, data of users might be compromised. For example, the user has lost or stolen his or her mobile phone, the user personal data can be put on risk.

To have a mobile security can help users to get less chance be target by hackers. This is because mobile security can help users to protect themselves. Also, mobile device security guards against unknown or hostile outsiders gaining access to critical corporate information (VMware, n.d.). For the services that mobile security which have including:

- BYOD (bring your own device)
- Observance of regulations
- Enforcement of security policies
- Updates to devices can be controlled remotely
- Controlling the application
- Automatically done device registration
- Data backup

Mobile security threats are attacks aimed at compromising or stealing information from mobile devices such as smartphones and tablets (Shyamsundar, 2020). For the mobile security threats which can be classification into two groups, which are:

1. Application-based threats
2. Web-based threats

Mostly, the application-based threats will be happened when the user downloaded malicious applications on their devices. This kind of applications will look like safe to download, but they are made with the intention of defrauding people. The application-based threats can be classified into 3 categories, which are:

• Malware - It is a piece of software that, once installed on your phone, conducts harmful operations.

• Spyware – It is intended to gather and utilize personal information without knowledge of users or consent.

• Vulnerable application – It is an application with security vulnerabilities that can be used for nefarious purposes.

Web-based attacks represent a continuous concern for mobile devices since they are always linked to the Internet and regularly used to access web-based services. This type of threats can be divided into 3 categories:

• Phishing attack – Basically, the hacker will send a phishing link to victim by using the email, messages or more to persuade the victim to provide information such as, account and password.

• Drive-by download – It will be happened when the victim is visiting the websites that design by hackers, and it will automatically download an application on the devices.

• Browser exploits – To exploit flaws in mobile web browser or browser-launched applications such as Flash player, PDF reader and more.

IV. ENNOS APPLICATION

EnNos application is a mobile antimalware software which is developed for senior citizen and teenagers. The core functions of EnNos are App scanning, APK scanning, custom scanning and real-time scanning.

For the App scanning, EnNos will scan all the applications on the mobile phone. After scanning, EnNos will list out all the result of the applications. The result will base on the application permission required. If the application has required more sensitive permissions, the application will be list as dangerous.

Next, if users want to know whether or not APK files are secure, EnNos offers APK scanning, which is used to scan APK files. Users must first choose the APK file in EnNos, after which it will automatically scan the APK files and display the result, such as secure score, sha256 and application permissions.

Moreover, custom scanning may be performed if consumers just want to scan a single application. If custom scanning is performed, EnNos will only present the selected application as a result. The security score, sha256, and permissions of the application will also be included in the report.

When the users lunch the application, EnNos will run the real-time scanning automatically. Real-time scanning is a backend service that will operate in the background on mobile devices. As a result, the application is constantly able to identify mobile activities. For example, when a user downloads a new app, EnNos will automatically scan it and display a message regarding the app's safety. Users may, however, turn off the real-time scanning capability in the settings if they do not want it.

In addition, EnNos will categorize the scanned application based on permissions required for secure scoring. The application will be classed as safe if the score is less than 0.5. In addition, if the score falls between 0.5 and 0.75, the application will be classed as high-risk. The application will be labelled as dangerous if the score is more than 0.75. Furthermore, the developer has created a basic graphic user interface for the system. Based on public research, the decision to utilize a basic visual user interface will be made. According to the research, most respondents prefer a basic and

straightforward user interface. Also, by employing a basic visual user interface, which is better suited to senior citizens, since most of them will only be able to identify functions based on a single icon.

Finally, EnNos is linked to an API called Virus Total API. This is due to the fact that the Virus Total API has a well-developed backend system for identifying viruses all around the world. As a result, the Virus Total API has been integrated into EnNos, and the API is linked to the core functions of App scanning, APK scanning, custom scanning, and real-time scanning. The advantage of integrating with the Virus Total API, which may assist EnNos in detecting malicious applications, is also more exquisite.

The system architecture design in Fig. 1. shows that the application is developed with 5 elements, such as Presentation Layer, Business Layer, Data Layer and API. The presentation layer the developer will need to consider about the application user interface design and user interface process.

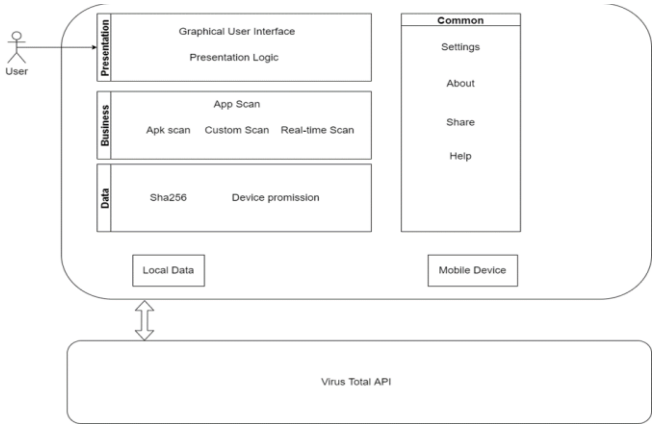

Fig. 1. System Architecture Design of EnNos

Since EnNos is a mobile antivirus application, the key parts will identify malware on a mobile phone. As a result, the business layer contains aspects such as App scan, APK scan, Custom scan, and Real-time scan. In addition, the business layer has included the service layer, commonly known as the common application function. "Settings," "About," "Share," and "Help" are the application's most common functions.

The data layer, on the other hand, is concerned with secure data exchanges. It has included data access ingredients, data services and operators. As a result, Sha256 and device permission were incorporated as application components in the data layer. During malware scanning, Sha256 data and device permission will be used. The hash value and device permission of the application, for example, will be detected by the application.

Lastly, the EnNos application has a connection to Virus Total API, a third-party backend service. When the API is integrated, it will be used to perform the application's fundamental purpose, which is malware detection. EnNos will submit the mobile phone's local data to the Virus Total backend service for malware detection, and the result will be sent back to the mobile phone.

Upon launching the EnNos, it will load the loading page before going to the main page. For the loading page, it will show the EnNos' logo as shown in Fig. 2.

Fig. 2. EnNos Loading Page

After loading the loading page, EnNos will bring the user to the main menu as show in Fig. 3. As we can see the interface is designed in simple user interface. When entering the main menu, the real-time protection will be launched automatically and pop out a message as highlighted in the figure. Besides, user can also check the last scan date and time as shown.

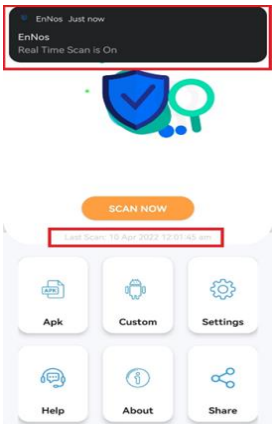

Fig. 3. EnNos Main Page

To perform App Scan, the user just needs to click the "SCAN NOW" button as shown in Fig. 4. EnNos will automatically scan the all the applications on mobile phone. During the scanning, EnNos will show the progress, such as percentage. Also, the user also can stop the process, if they do not want to launch the process.

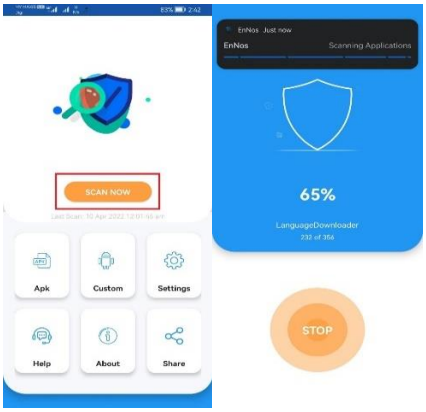

Fig. 4. App Scan

After scanning, EnNos will list out all the result as shown in Fig 5. The result will be categorized into 4 parts, which are Safe, Risky, Dangerous and Unknow. If the user wants to get more detail information, the user can click the application to get more information. Also, if the user wants to uninstall the dangerous application, user can click the "UNINSTALL"

button to uninstall it. To process APK scan, the user will need to click the “Apk” button as highlighted in Fig. 5.

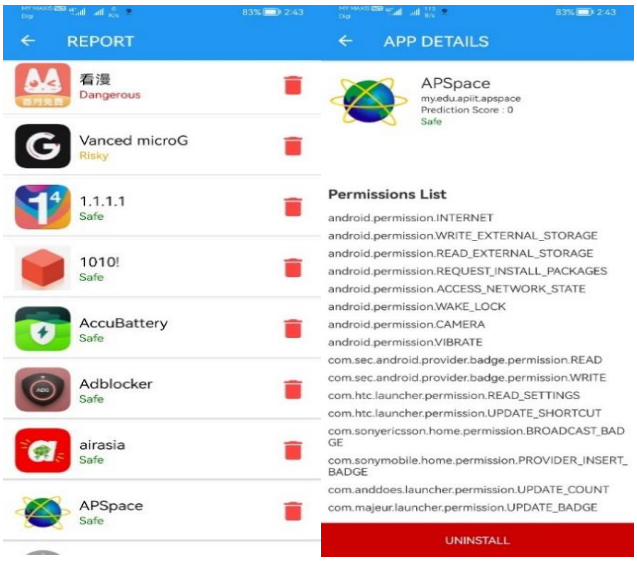

Fig. 5. Result of App Scan

Fig. 6. APK Scan

Once clicked the button, EnNos will ask the user to locate the APK file as shown in Fig. 7.

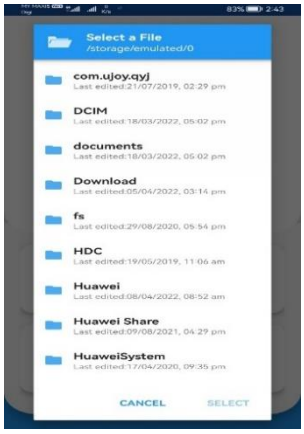

Fig. 7. Select File Location

When the user finds the APK file, the user just needs to select it and press the “SELECT” button as shown in Fig. 8 for scanning process.

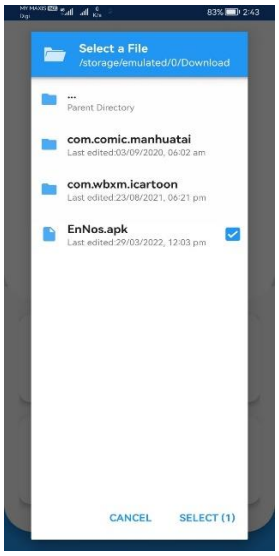

Fig. 8. Select APK File

Once done the scanning, EnNos will automatically show the result as shown in Fig. 9. Therefore, the user will be able to check the application’s hash value, result, name, and permissions list.

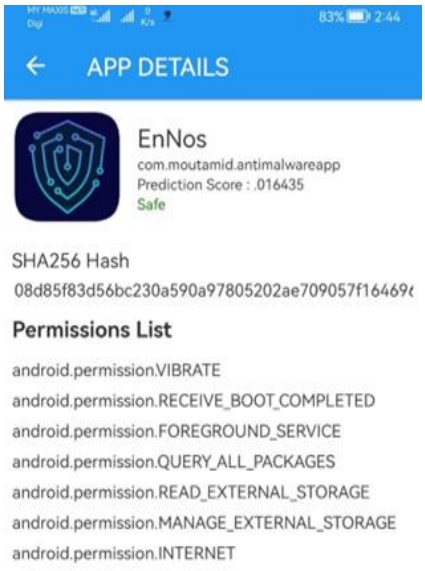

Fig. 9. APK Result Page

Custom scan option allows the user to select a single application for scanning process. Once the user has selected an application, EnNos will scan the application automatically. Then, the user will be able to check the result or uninstall the application, similarly like the usual scan option.

For the Help function, when the user clicks the button, the application will bring the user to check the system’s guideline as show in Fig. 10. For this function which can help the user to learn how the system process, such as malware scan engine.

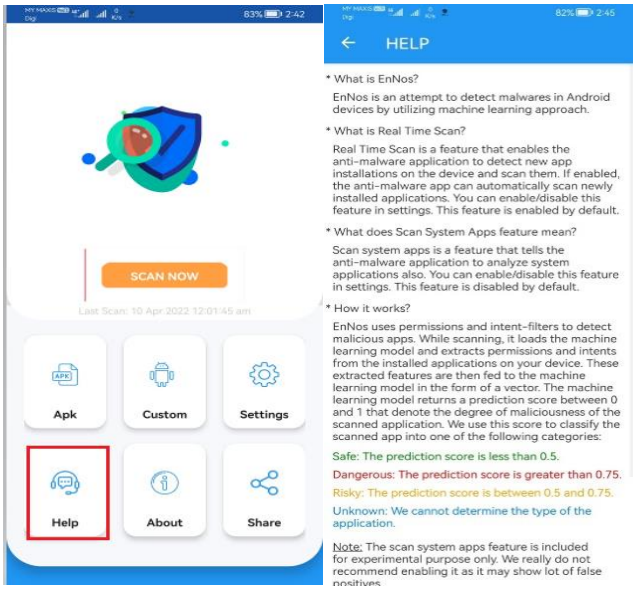

Fig. 10. EnNos Help Page

EnNos Settings function is used for editing the system's function. When the user login to the settings page, it will show all the function of the application, such as real-time protection and scanning applications functions. The real-time protection will be turn on by default and the scan applications function will be turn off by default. User can also find the system's version and feedback form on the settings as named as "Rate the app".

V. Conclusion and Outcomes

An application of automated tracking malware can provide a secure environment to users when they are using their phones. It will help to track and block all the malware if the application is being updated from time to time. For example, if the user has downloaded a malware application, it will directly remove the application and warning the user. EnNos is designed and developed on an Android platform so it can assist senior citizens and teenagers in monitoring malware on their phones. While EnNos has been installed, it will automatically run at the background of the android mobile system, scanning all data to track down and remove malicious data. If EnNos has tracked a critical malware, and the user has been involved in the cybercrime, EnNos will help the user to report the incident to forensic investigators. EnNos will provide evidence to forensics investigators during the forensic investigation. Therefore, the forensic investigators can do their job easily.

References

Gontovnikas, M. (2021, June 25). The 9 Most Common Security Threats to Mobile Devices in 2021. Retrieved from Auth0: https://auth0.com/blog/the-9-most-common-security-threats-to-mobile-devices-in-2021/

Gartner. (2021). Secure Web Gateway. Retrieved from Gartner: https://www.gartner.com/en/information-technology/glossary/secure-web-gateway

os-system. (2020, October 27). Mobile App Architecture-How to Design it? Retrieved from os-system: https://os-system.com/blog/mobile-app-architecture-how-to-design-it/

Pham, L. (2021, March 10). Mobile application: Definition, Technology, types and example 2021. Retrieved from magenest: https://magenest.com/en/mobile-application/

Posey, B., Wigmore, I., & Westervelt, R. (2021, May). Mobile Secuirty (Wireless Security). Retrieved from TechTarget: https://whatis.techtarget.com/definition/mobile-security

Services, A. W. (n.d.). What is Mobile Application Development? Retrieved from Amazon Web Services.Inc: https://aws.amazon.com/mobile/mobile-application-development/

Shyamsundar, T. (2020, October 22). Today's Mobile Security Threats: What Are They and How Can You Prevent Them? Retrieved from Okta: https://www.okta.com/blog/2020/10/mobile-security-threats-and-prevention/

VMware. (n.d.). What is mobile device security? Retrieved from vmware.com: https://www.vmware.com/topics/glossary/content/mobile-device-security