EasyChair Preprint

№ 15528

A Three-Pronged Approach to Malicious APK: Combining Snort, Wireshark, and Wazuh for Advanced Threat Management

Yi Anson Lam, Siu Ming Yiu and K P Chow

December 4, 2024

A Three-Pronged Approach to Malicious APK: Combining Snort, Wireshark, and Wazuh for Advanced Threat Management

Yi Anson Lam, Siu-ming Yiu, Kam-Pui, Chow

The University of Hong Kong

E-mail: yiansonlam@connect.hku.hk, smyiu@cs.hku.hk,chow@cs.hku.hk

Abstract. In the evolving landscape of mobile security threats, traditional detection methods often struggle to effectively identify and mitigate the risks posed by malicious APKs. This study introduces an integrated approach that combines the strengths of Snort and Wireshark with the dynamic response capabilities of Wazuh Manager. Initially, we leverage Snort's robust network intrusion detection capabilities, enhanced through a custom plugin in Wireshark, to monitor and analyze APK file transfers. This setup allows for effective capture and initial screening of APKs based on known malicious signatures and anomalous network patterns.

Subsequently, Wazuh Manager is employed to facilitate an active response strategy. It automates the response to threats detected by Snort, such as isolating affected systems, alerting administrators, and preventing the execution of suspicious APKs. This proactive approach not only aims to stop malware before it causes harm but also adapts to the evolving threat landscape by continuously updating detection rules and response strategies based on new intelligence.

Our research indicates that an effective defense against malicious APKs involves monitoring, detecting, and actively responding to these threats. The integration of these tools provides a scalable and adaptable framework that can evolve with emerging threats, offering practical solutions for both organizational and individual security needs. This research underscores the potential of combining network analysis tools with active response systems and lays the groundwork for future advancements in mobile security methodologies with the layered defence approach.

1. Introduction

The proliferation of mobile applications has significantly enhanced user experience and productivity, yet it has also escalated the risks associated with malicious software, particularly Android Package Kits (APKs) that can compromise user security. Traditional antivirus and malware detection strategies often struggle to keep pace with the sophistication and rapid evolution of mobile malware. Encrypted traffic limits traditional antivirus from inspecting potential threats, while privacy concerns arise due to extensive permissions and false positives. Consequently, there is a pressing need for innovative approaches that enhance detection capabilities and reduce vulnerabilities. Most existing research on APK analysis employs conventional dynamic and static approaches, focusing predominantly on the detection and post-analysis of APKs once they are suspected or identified as malicious. As mobile applications proliferate, a vast number of APKs are available for download from the internet, often without adequate scrutiny. While there are established methods to scan for malware on computers and

laptops, fewer solutions exist that preemptively scan for malware in APKs before download, or that actively respond to remove already downloaded malicious APKs.

Network-based intrusion detection systems (IDS) such as Snort have been widely employed to monitor network traffic and identify potential threats based on known signatures and anomalous behavior patterns. Similarly, Wireshark, a network protocol analyzer, is extensively used for traffic capture and analysis, offering deep insights into the data packets transmitted across networks. While these tools are powerful for identifying known threats and analyzing network behavior, they often lack the capability to detect new malware variants that do not match existing signatures or behavioral profiles.

In the quest to enhance the security measures against malicious APKs, this study integrates Wazuh Manager, a powerful security management tool that excels in active response capabilities. Wazuh is leveraged to orchestrate a comprehensive defense mechanism against the threats detected during the APK file transfers monitored by Snort and analyzed by Wireshark. Upon detection of a suspicious APK, Wazuh Manager can execute a range of automated responses, from alerting system administrators to executing scripts that block or remove the malicious application from the network. This proactive approach not only mitigates the immediate threat posed by the APK but also contributes to a real-time security posture that adapts to emerging threats dynamically. By automating the response process, Wazuh helps ensure that potential breaches are handled swiftly and efficiently, minimizing the risk of damage or data loss and bolstering the security infrastructure against the increasing sophistication of mobile malware.

This paper introduces a three-pronged approach that combines Snort, enhanced by a custom plugin in Wireshark, with the dynamic response capabilities of Wazuh to remove or deactivate malicious APKs. We begin by discussing the integration of Snort with Wireshark to effectively monitor APK file transfers and capture initial threat data. For malware that may circumvent the network monitoring of Wireshark, the chances are lesser when the malicious packages pass through Snort's detection, as Snort covers signature-based anomalies. Even if the malicious packages are not detected by Snort for an alert, we still have Wazuh's active response, which is an incident-based approach to defense.

We then elaborate on how Wazuh's active response feature can immediately react to the detection of suspicious activities, executing predefined security protocols such as isolating the affected system or blocking the APK download. This proactive strategy not only prevents the execution of potentially malicious APKs but also adapts to new threats dynamically, enhancing overall mobile security.

Finally, we present the findings from our implementation, which demonstrates improved management of security threats and a significant reduction in the window of opportunity for malware to affect systems, providing a robust framework for mobile security in an increasingly threat-prone digital environment.

2. The objective of the study

Cybersecurity has become a critical focus in the digital era, as cyber threats continue to proliferate. While significant research and development efforts have been directed towards intrusion prevention systems for computers, servers, endpoint laptops, and organizational terminals, the protection of end-users at the individual mobile device level has received less attention. The Kaspersky Financial Threats Report 2023 [1] highlights a 32% increase in mobile banking malware like Trojan infection etc, whilst there was a relative decline in financial malware in personal computer when compared to mobile devices at user level.

The reason for this is understandable - solutions sold to corporations are more profitable and in higher demand, as companies must critically protect their digital assets. However, it is more challenging to sell security solutions to retail users, as they represent a large pool of individuals who may not have a strong understanding of the attack landscape in mobile applications or

perceive a pressing need to install such solutions.

This study aims to address this gap by proposing a practical, low-cost solution suitable for small and medium-sized enterprises (SMEs) or individual users, focusing on enhancing security measures before the downloading of Android application packages (APKs). The proposed method not only identifies potentially harmful applications but also integrates an active response mechanism through the Wazuh security platform to mitigate threats effectively.

The overarching goal of this research is to enhance the detection and analysis of malicious APKs through a comprehensive, three-pronged approach. This approach integrates Wireshark's network monitoring technique, Snort's intrusion detection capabilities, and Wazuh's active response features. By leveraging these complementary tools and techniques, the study aims to provide a robust and accessible solution for SMEs and individuals to protect their mobile devices and data from evolving cyber threats.

(i) Integration of Detection Tools: Develop a robust framework that integrates Snort, enhanced with a custom plugin for Wireshark, to enable advanced network monitoring and data capture. This integrated system will utilize network-based, signature-based, and anomaly-based detection methods to identify and flag APK files for further analysis. The objective is to harness these tools to capture a broad spectrum of potential threats at the network level effectively.

(ii) Circumventing Encryption Challenges in Network Traffic: Focus on developing methods to detect malicious APKs that may circumvent traditional detection methods, especially in environments where network traffic is encrypted. Since encryption can obscure the content of network communications, rendering traditional payload inspection ineffective, this objective aims to enhance the capability of the detection system to infer malicious intent from encrypted traffic patterns and other indirect indicators. The integration of active response mechanisms is particularly pivotal here, as it can immediately react to detected anomalies, enhancing threat management without needing payload access.

(iii) Active Response and Real-time Threat Management: Employ Wazuh's active response capabilities to manage and mitigate threats as they are detected. This approach enables immediate automated actions such as isolating affected devices or blocking malicious downloads, thereby preventing the execution of harmful APKs. This proactive strategy not only mitigates the immediate threat posed by malicious APKs but also adapts to new threats dynamically, ensuring a resilient mobile security posture.

3. Related Work

The earlier relevant study in this context is the 2017 paper 'Deep android malware detection and classification' by R. Vinayakumar and his team [2], which focuses on using deep learning to analyze APK files post-collection. Unlike their approach, my proposed integrated method incorporates the collection and analysis phases, utilizing network tools for real-time monitoring and immediate analysis, which enhances the timeliness and accuracy of malware detection. In 2018, The authors introduce DroidCat, a malware detection and categorization system that profiles Android apps at the app-level to identify malicious behavior [3].

In 2019, R. Oak et al. [4] discussed malware detection on highly imbalanced data through sequence modeling, applying sequence modeling to detect malware in APK files. Unlike their approach that solely focuses on machine learning techniques, my proposed integrated method incorporates traditional network monitoring tools, thus providing an initial filtering stage that precedes further analysis.

In 2020, two significant studies were published. The first is "Malware Detection by Eating a Whole APK" by M. Al-Fawa'reh et al.[5], which utilizes a CNN-based model to directly detect malicious content within APK files. My proposed integrated method differs by introducing

a preliminary stage where Snort and Wireshark monitor and analyze the network behavior associated with APK file transfers, providing an early detection mechanism before any in-depth analysis. The second study in the same year is 'Decompiled APK based malicious code classification' by R. Mateless and colleagues [6], focusing on analyzing software's internal features using decompiled APKs. My proposed integrated method enhances this by adding a network analysis layer through Snort and Wireshark, allowing for an initial screening that captures and analyzes APK file transfers.

A. Rahali and M. A. Akhloufi 2023 [7] expand on a BERT-based language model for malware identification, focusing more on machine learning approaches. Unlike this single-layered method, my proposed integrated method combines traditional network monitoring tools with Wazuh's active response capabilities to provide a dynamic defense against APK threats.

QN Nguyen et al. [8] in "XLMR4MD: New Vietnamese dataset and framework for detecting the consistency of description and permission in Android applications using large language models," use LLMs to detect inconsistencies in APK descriptions and permissions. My proposed integrated method incorporates an initial network traffic analysis to identify anomalies during APK file transfers, which supports the dynamic defense mechanism provided by Wazuh.

The literature extensively discusses conventional malware detection tools such as AnalyzePE, chkrootkit, hashdeep, Loki, YARA, and others. These tools primarily employ file signature and network-based approaches, supporting both static and dynamic analysis. Unlike these traditional methods which only usually using one key technology or detection mechanism, the proposed integrated method enhances these capabilities with Wazuh's active response features to dynamically manage and mitigate threats as they are detected. This enhancement is crucial for adapting to the modern landscape of malware dissemination, which has increasingly shifted to APK-based methods. This shift is also evident by the fact that traditionally, the Wazuh agent is mainly installed on laptop devices, with limited use cases in mobile systems where most APKs reside. Another significant difference between previous research and the proposed method is that previous studies focus on post-infection analysis rather than intervening immediately.

4. The Methodology

4.1. The conceptual framework

In this study, we developed a robust methodology to test the effectiveness of a three-pronged approach for detecting and responding to APK-based malware. Due to the scarcity of readily available malicious APK samples from open sources, we created our own test samples. Using AhMyth [8], an open-source tool accessible via GitHub, and some other android malware samples [9-10], we crafted and diversified ten sample malicious APKs. These were developed within a controlled virtual environment operating on Kali Linux, where we also configured a simulated Command and Control (C2) server on the same virtual machine to replicate real-world malware behaviors.

To enhance the realism of our tests and better mimic scenarios where victims are often deceived, we combined some of our malicious APK samples with legitimate applications. For instance, bundling with some banking pure APK which are available online. Adversaries use such strategy to lure victims to install seemingly trustworthy APKs to conceal the malicious components, simulating situations in which users might inadvertently install harmful software, believing it to be safe. We sourced the legitimate APK components from official websites, such as bank sites, to ensure their authenticity. This dual-component setup provides a more comprehensive assessment of our security system's ability to detect and respond to complex threats that merge malicious intent with benign applications.

(i) The malicious APKs developed for this study are programmed with sophisticated capabilities that severely compromise the privacy and security of the affected mobile

devices. These APKs are designed to harvest sensitive information, including contacts and SMS contents, thereby exposing personal and potentially confidential communications. Moreover, the malware has the capability to spoof SMS messages. This function allows it to send deceptive messages to other individuals, impersonating the infected user, which could lead to further spread of the malware or other fraudulent activities under the guise of a trusted identity. Additionally, certain variants of these malicious APKs are equipped with functionality to clandestinely activate the mobile device's cameras—both front and rear. This allows the malware to capture images without the user's knowledge or consent, providing real-time visual data to the attacker. This could lead to serious privacy violations, including the exposure of personal spaces or sensitive situational information. Such features highlight the particularly invasive nature of the malware, illustrating its potential to not only steal personal information but also to enable complex identity theft and surveillance activities.

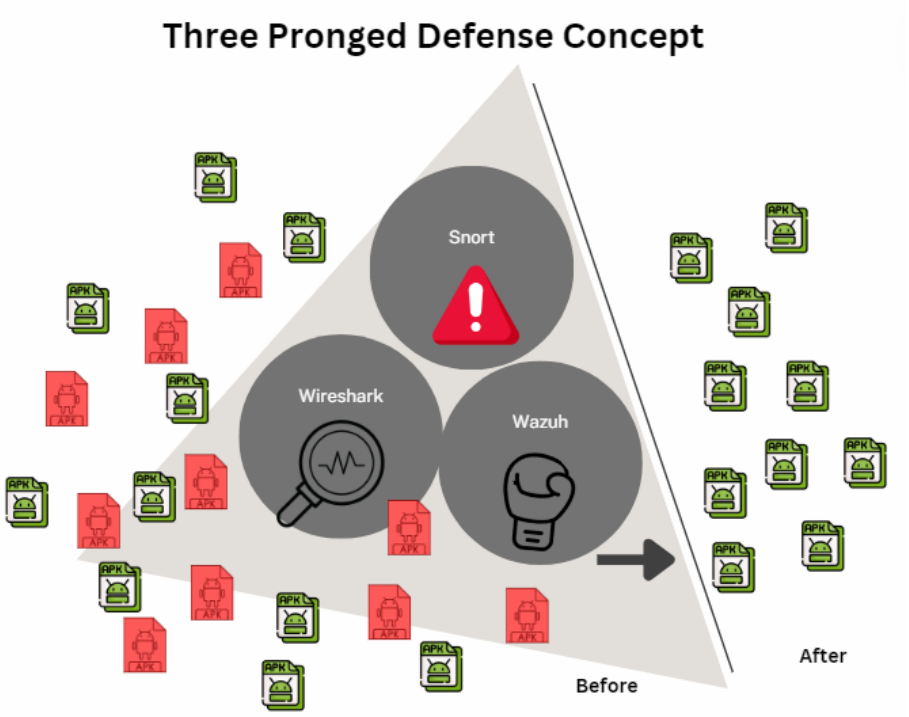

Figure 1. Integrated Defence Concept

(ii) Network Configuration and Monitoring with Snort and Wireshark: The network was configured to route all traffic through an external IP address to simulate an authentic intrusion scenario. This setup involved the integration of Snort[11], a leading intrusion detection system (IDS), which was tasked with monitoring all network traffic for signs of suspicious activities or known malware signatures associated with the test APKs. Snort's real-time traffic analysis capability was essential for the initial detection of potential threats as they traversed the network. Parallel to Snort, Wireshark was employed to capture and analyze packet data within the network. This provided a detailed view of the network interactions and allowed for a deeper examination of the data packets associated with the APK files. Wireshark's comprehensive logging and analysis capabilities helped in verifying and supplementing the detection findings from Snort, offering a granular look at the network traffic and assisting in the identification of any anomalies that Snort might have flagged.

(iii) Active Response with Wazuh: Upon detection of a thre at by Snort, Wazuh—a powerful security monitoring tool—was triggered to manage the response actions [12]. Wazuh was configured to perform automatic responses based on the alerts generated by Snort. These responses included isolating the affected system segment, blocking further downloads of the malicious APK, and initiating scripts to remove the installed APKs from the system. Wazuh's role was critical in actively mitigating the threat in real time, thereby preventing the potential spread or escalation of the malware.

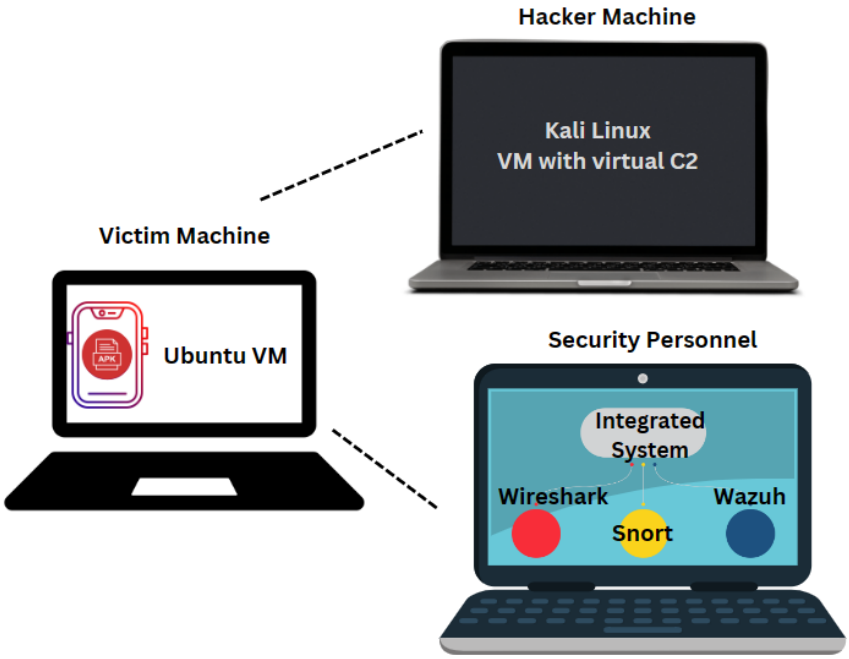

Figure 2. Experiment Set-up Diagram

This comprehensive methodology allowed us to evaluate the effectiveness of integrating Snort, Wireshark, and Wazuh in a unified security framework. The experiment was designed to closely replicate real-world conditions, ensuring that the findings are relevant and applicable in actual operational settings, providing valuable insights into the capabilities and benefits of a three-pronged security approach in combating mobile malware. Below Figure illustrated the security defence concept. Figure 1 showed the advance threat management concept while Figure 2 shows how the experiment is set up.

4.2. Experiment Set-up

(i) Victim Machine (Genymotion 3.6.0 and wazuh agent): Genymotion is an Android emulator used for simulating mobile devices. Set up a virtual device in Genymotion to emulate the desired Android version and device model. Install the Wazuh agent on Ubuntu 22.04.4 LTS. The Wazuh agent will monitor the device for security events and send them to the Wazuh manager for analysis.

(ii) Hacker Machine (Kali Linux): First, install Kali Linux on the hacker machine. Kali Linux is a penetration testing platform that includes various security tools. Second, Use AhMyth and open source toolkit mentioned to build and bind 10 malicious APKs and load into Victim Machine. Set up a virtual C2 server in the Hacker Machine to listen or ex-filtrate

the data from Victim side. For the benign samples, the APK samples are obtained from open source, for example, legitimate banking APK.

(iii) Security Manager Machine (Wazuh Managerin Ubuntu with Wireshark and Snort Plugin together): First, we install the Wazuh manager on Ubuntu 22.04.4 LTS. The Wazuh manager is the central component that receives and analyzes security events from the Wazuh agents. Then we configure the Wazuh manager to receive events from the Wazuh agent installed on the victim machine. Also we have to install the Snort plugin for Wireshark. The Snort plugin enhances Wireshark's capabilities by providing intrusion detection and prevention features. Once the environment is set up, it is use to perform the testing on the total 20 APKs.

4.3. Experiments

A mobile security detection and intervention environment was established by integrating a Snort plugin extension into Wireshark on an Ubuntu machine, also wazuh manager is also installed in the enviroment, forming a integrated threat management system that support not only signature and network-based detection, but also incident based active response. In addition, a Kali Linux Virtual Envirnoment is set up to simulate the C2 Server hosted by the hacker. A Wazuh agent was also deployed on the victim machine, where a mobile visualiser 'Genymotion' is installed, where the bengin and malicious APKs were run in the machine to test the the proof of concept.

The environment was primed for testing by running all 10 sample malicious APKs within this setup. Subsequently, ten sample benign APKs were also executed in the same integrated system to compare their behaviors. Alerts and responses were meticulously recorded for both sets of APKs. A comparative analysis was then conducted between the malicious and benign samples, focusing on the differences in detected activities and the effectiveness of the response actions.

4.4. Evaluation method

Detection Accuracy Evaluation: To assess the accuracy of the integrated mobile security system, we will quantify true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN). True positives and true negatives represent the malicious and benign APKs correctly identified by the system, respectively. Conversely, false positives and false negatives represent benign APKs mistakenly identified as malicious and missed detections of malicious APKs, respectively. From these metrics, we calculate the precision, recall, and F1-score to provide a comprehensive measure of the system's detection accuracy. These statistics will offer insight into the effectiveness of Snort and Wireshark in filtering and identifying APKs, as well as the accuracy of the Wazuh's response configurations.

Response Effectiveness Evaluation: The effectiveness of the system's response to detected threats will be measured by recording the response time and appropriateness. Response time is the interval from when a malicious APK is detected to when Wazuh initiates a response, including alert generation and execution of automated mitigation actions. The appropriateness of the response will be assessed based on whether the actions taken were proportionate to the threat level and successful in mitigating potential damage. This evaluation will help determine the agility and efficiency of Wazuh in managing and neutralizing threats in real-time.

System Robustness Evaluation: The robustness of the system will be tested by conducting stress tests that involve subjecting it to high volumes of APK traffic. This will help us evaluate how the system performs under load and whether there are any degradations in detection or response capabilities. Additionally, the error rate during these tests will be monitored to assess the reliability and stability of the system over extended operational periods. This robustness testing is crucial for understanding the system's performance in realistic scenarios and its ability to function consistently under varying conditions.

5. The Experiments and Result

5.1. Results and Analysis of Malicious APK Samples

In the experiment, the integration of Snort, Wireshark, and Wazuh Manager effectively detected and responded to all malicious APK samples.

During the experiment, problematic traffic was observed, and the APKs were assumed to be known to the security individual monitoring the network, resulting in less harmful actions. However, for the remaining samples, 3 out of 10, the system merely flagged them as bad traffic, entailing that Wireshark's network monitoring alone would not have been able to detect and alert on these samples. Having said that, with the installation of Snort, it successfully identified the malicious traffic with the SID 1:25521 rule. Figure 3 showed the snort alert. Further investigation revealed that Snort detected traffic targeting vulnerabilities in a mobile-based operating system, potentially violating corporate privacy. This alert, categorized under the MITRE ATT&CK Framework as 'Command and Control' tactics using 'Web Protocols' as the attack vector, would alert the security personnel accordingly.

A separate test was conducted using only Wireshark as a conventional monitoring tool to verify harmfulness of using Wireshark alone to monitor the traffic . While it only flagged as some bad traffic, no further information could be revealed due to encryption or lack of detailed information. This further evident the importance of additional defense mechanisms, such as Snort and Wazuh, to effectively detect and respond to malware threats.

Each time a malicious APK was loaded onto the system, the setup successfully triggered alerts and corresponding active response by the Wazuh Manager. It was configured to actively respond to such threats and promptly executed predefined response actions. These actions included setting the rule "firewall drop" to block the Command and Control (C2) IP and using "os.remove()" to uninstall the malicious APKs from the system. Figure 4 shows one of the active response 'firewall drop' after anomaly is detected.

The immediate and automated removal process demonstrated the system's effectiveness in not only detecting but also mitigating potential threats. The ability of Wazuh Manager to execute these actions accurately without manual intervention highlights the practicality of the system for real-time threat management and suggests a high level of reliability in distinguishing between normal and malicious activities.

Malicious APK Samples	Wireshark	Snort	Wazuh
APK 1	Have problematic traffic	Alert Flagged	Threat Removed
APK 2	Indicated bad traffic only	Alert Flagged	Threat Removed
APK 3	Have problematic traffic	Alert Flagged	Threat Removed
APK 4	Have problematic traffic	Alert Flagged	Threat Removed
APK 5	Indicated bad traffic only	Alert Flagged	Threat Removed
APK 6	Indicated bad traffic only	Alert Flagged	Threat Removed
APK 7	Have problematic traffic	Alert Flagged	Threat Removed
APK 8	Have problematic traffic	Alert Flagged	Threat Removed
APK 9	Have problematic traffic	Alert Flagged	Threat Removed
APK 10	Have problematic traffic	Alert Flagged	Threat Removed

Table 1. Alert for Malicious APK Samples

Bengin APK Samples	Wireshark	Snort	Wazuh
APK 1	No problematic traffic	No Alert	No Action
APK 2	No problematic traffic	No Alert	No Action
APK 3	No problematic traffic	No Alert	No Action
APK 4	Indicated bad traffic	No Alert	No Action
APK 5	No problematic traffic	No Alert	No Action
APK 6	No problematic traffic	No Alert	No Action
APK 7	No problematic traffic	No Alert	No Action
APK 8	No problematic traffic	No Alert	No Action
APK 9	No problematic traffic	No Alert	No Action
APK 10	No problematic traffic	No Alert	No Action

Table 2. Alert for Benign APK Samples

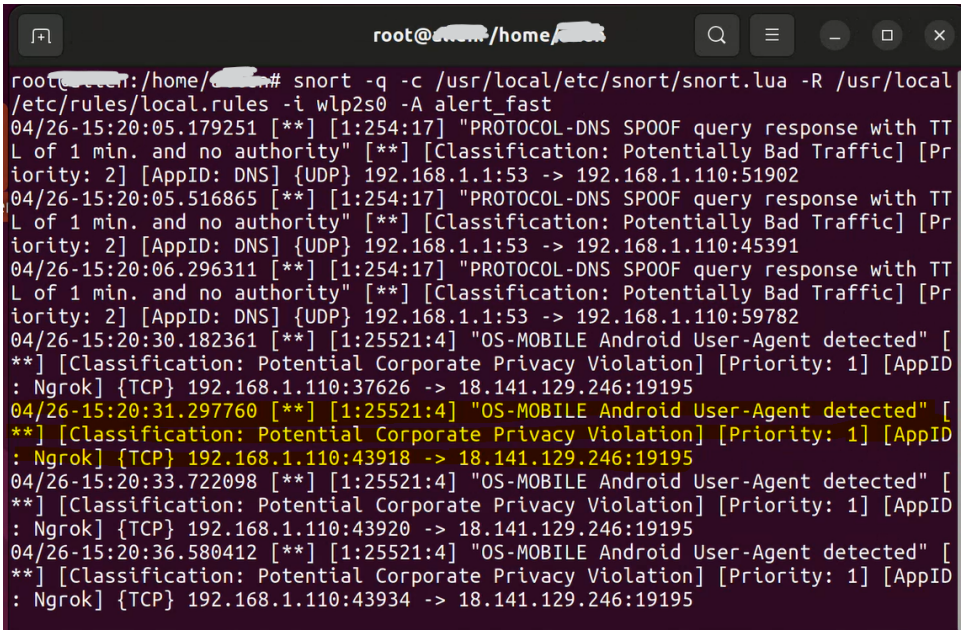

Figure 3. Snort alert upon running a malicious APK

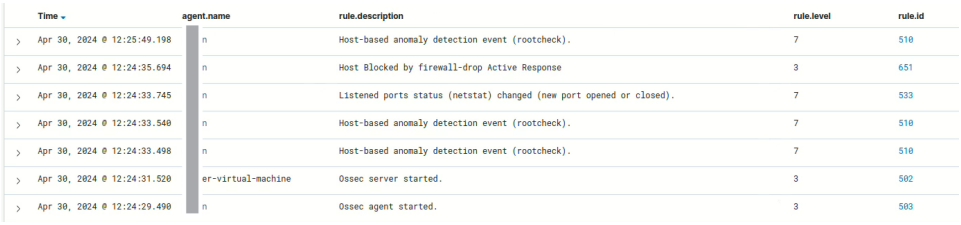

Figure 4. Active Response Taken by Wazuh

5.2. Results and Analysis of Bengin APK Samples

For the benign APK samples, the system also performed as expected. Wireshark was able to capture and analyze the network traffic generated by these APKs, confirming that the network monitoring setup was correctly capturing data traffic. Moreover, even for benign APKs,

sometime due to protocol designed or configure, it may generate some bad traffic. Though these are monitored and highlighted by wireshark, these do not neccessary be suspcious traffic. The information could be treated as an extra piece of information to security personnel, unlike the malicious APKs to require any security action to be taken. Importantly, Snort did not trigger any false alerts during the handling of benign samples, indicating a well-tuned detection configuration that effectively reduces false positives—a common challenge in cyber security. Furthermore, Wazuh did not initiate any response actions for these benign samples, which validates the system's capacity to correctly classify and react to non-malicious software. This aspect of the results is particularly valuable as it shows the system's precision in discerning legitimate software activities from potential threats, thereby preventing unnecessary interventions that could disrupt user experience or system performance.

To calculate accuracy, the formula used was as follows:

$$Accuracy = (TP + TN)/(TP + TN + FP + FN) \quad (1)$$

TP = True Positive, TN = True Negative, FP = False Positive, FN = False Negative

5.3. Overall System Performance

The findings from this study indicate that the integrated system of Snort, Wireshark, and Wazuh Manager is highly effective in the detection and management of APK-based threats. The system demonstrated robust detection capabilities with an optimal balance between sensitivity (detecting all malicious instances) and specificity (avoiding false alarms on benign instances). Such performance is crucial for real-world applications where both security and usability are paramount. The successful implementation and results suggest that this system could serve as a reliable security solution, capable of providing comprehensive protection against APK-related threats in a variety of settings.

Based on the formula for accuracy (Equation 1), if a malware detection system has a 100% accuracy in defending malicious APKs and a 100% accuracy in flagging no false positives in scanning benign APK samples, the accuracy score would be 100% in the experiment.

Despite a small sample with 10 malicious and 10 benign APKs for testing, if the malware detection system achieves 100% accuracy, it means that it correctly identifies all 10 malicious APKs as malicious (True Positives) and correctly identifies all 10 benign APKs as benign (True Negatives). There would be no False Positives or False Negatives in this scenario.

This high level of accuracy is desirable in malware detection systems as it ensures that malicious APKs are accurately identified and flagged, while minimizing the risk of false positives, which could lead to unnecessary alerts or blocking of benign APKs.

Of course it is desirable to test more APK samples, yet the study also focus on showing the proof of concept. It is important to note that the accuracy of a malware detection system can vary depending on various factors such as the dataset used for training and testing, the algorithms and techniques employed, and the evolving nature of malware. Therefore, it is crucial to continuously evaluate and improve the accuracy of malware detection systems to effectively combat the ever-changing landscape of malware threats.

6. Discussion

The integration of Snort, Wireshark, and Wazuh Manager into a comprehensive mobile security framework has demonstrated a promising solution to the pressing challenges posed by malicious APKs. This three-pronged approach provides a robust, one-stop solution for the detection and response to mobile security threats, catering to the needs of a wide range of users from individuals to SMEs. The experimental results have substantiated the efficacy of this integrated system, which combines network monitoring, threat detection, and active response mechanisms.

6.1. Efficiency in Threat Detection and Response
The system's capability to detect all malicious APK samples without fail and initiate an immediate response underscores its reliability and efficiency. By automatically uninstalling malicious APKs upon detection, Wazuh Manager has proven to be an effective tool for mitigating potential damages that could arise from such threats. This automated response is crucial not only in preserving the integrity of the user's system but also in minimizing the window of opportunity for attackers to exploit vulnerabilities, thereby enhancing overall security.

6.2. Reduction of False Positives
One of the most significant outcomes observed during the trials was the absence of false positives when benign APKs were introduced. This result is particularly important as it reflects the system's high specificity and accuracy in threat classification. False positives are a major concern in security systems, as they can lead to unnecessary disruptions and user dissatisfaction. The ability of this integrated approach to discern between harmful and safe applications without error contributes greatly to its usability and reliability, making it a viable option for real-world applications where such precision is indispensable.

6.3. Comparison with Previous Studies
Comparatively, the approach discussed in this study advances beyond traditional methods, which often rely solely on one form of detection and typically do not incorporate an active response mechanism. For instance, previous methods focusing solely on network-based or signature-based detection do not address the challenges posed by new or evolving malware that may elude traditional detection. Furthermore, unlike some advanced machine learning techniques that require extensive computational resources and expertise, our integrated solution balances complexity and accessibility, making it adaptable for smaller enterprises without the resources for complex cyber security setups.

6.4. Practical Implications
The practical implications of these findings are substantial. For businesses, especially SMEs that often operate with limited cyber security budgets and expertise, this integrated solution offers a cost-effective and efficient way to bolster their defenses against mobile threats.

6.5. Stability and flexibility
Additionally, the scalability of this solution allows it to be deployed across various devices and environments, ensuring broad applicability and flexibility. Snort and Wazuh excel in their ability to scale by updating community rules and configuring the Wazuh manager-to-agent settings. Snort is renowned for its customizable rule settings on top of up-to-date community rules, providing a secure default security configuration. Meanwhile, Wazuh offers stateful and stateless active responses that can be adjusted based on the needs of end users or security personnel. These responses can be reverted or halted after a defined period of time, depending on the requirements.

7. Conclusion
The study has successfully demonstrated the effectiveness of a three-pronged approach integrating Snort, Wireshark, and Wazuh Manager for enhancing mobile security through the detection and management of malicious APKs. This innovative framework not only detected all malicious instances with precision but also effectively discriminated between malicious and benign APKs, avoiding false positives which are a common issue in many security systems.

The integration of these tools has shown substantial benefits in real-time monitoring, accurate threat detection, and swift active response capabilities. The automated response system provided by Wazuh Manager, in particular, was crucial in mitigating potential threats by immediately uninstalling detected malicious APKs, thereby minimizing the risk to data leakage and system integrity. Furthermore, the absence of false alerts during the handling of benign APKs highlights the system's reliability and practicality for everyday use.

This research contributes to the ongoing development of mobile security solutions, offering a scalable, efficient, and accessible approach suitable for a wide range of users, from individuals to small and medium-sized enterprises. It addresses critical gaps in current security practices, particularly in providing low-cost, effective defenses against APK-based malware, an increasingly prevalent threat in today's digital landscape.

Future work should focus on expanding the capabilities of this system to include more advanced analytical tools and exploring its applicability in other contexts, such as IoT devices and different operating systems. Enhancing the system's ability to handle zero-day exploits and more sophisticated malware forms will also be crucial for maintaining robust defenses against evolving security threats.

The results of this study underscore the potential of integrated security systems to significantly improve the detection and management of mobile threats, paving the way for safer and more secure digital environments.

References

[1] Kaspersky. Global Mobile Banking Malware Grows 32 Percent in 2023. Available online: https://www.kaspersky.com/about/ press-releases/2024_global-mobile-banking-malware-grows-32-percent-in-2023 (accessed on 15 May 2024).

[2] Vinayakumar, R., Soman, K.P. and Poornachandran, P., 2017. 'Deep android malware detection and classification', *Proceedings of the International Conference on Advances in Computing, Communications and Informatics*, [online] Available at:https://ieeexplore.ieee.org/document/8126084

[3] Cai, H., Meng, N., Ryder, B. and Yao, D., 2018. 'Droidcat: Effective android malware detection and categorization via app-level profiling'. IEEE Transactions on Information Forensics and Security, 14(6), pp.1455-1470.

[4] Oak, R., Du, M., Yan, D., Takawale, H. and Amit, I., 2019. 'Malware detection on highly imbalanced data through sequence modeling', *Proceedings of the 12th ACM Workshop*, [online] Available at: https://dl.acm.org/doi/10.1145/3338501.3357374

[5] Al-Fawa'reh, M., Saif, A. and Jafar, M.T., 2020. 'Malware Detection by Eating a Whole APK', *2020 15th International Conference on Computer Engineering and Systems (ICCES)*, [online] Available at: https://ieeexplore.ieee.org/abstract/document/9351333/

[6] Mateless, R., Rejabek, D. and Margalit, O., 2020. 'Decompiled APK based malicious code classification', *Future Generation Computer Systems*, [online] Available at: https://www.sciencedirect.com/science/article/pii/S0167739X19325129

[7] Rahali, A. and Akhloufi, M.A., 2023. 'MalBERTv2: Code aware BERT-based model for malware identification', *Big Data and Cognitive Computing*, [online] Available at: https://www.mdpi.com/2504-2289/7/2/60

[8] Nguyen, Q.N., Cam, N.T. and Nguyen, K.V., 2024. 'XLMR4MD: New Vietnamese dataset and framework for detecting the consistency of description and permission in Android applications using large language models', Computers & Security, [online] Available at: https://www.sciencedirect.com/science/article/pii/S0167404824001159

[9] VX-Underground. (n.d.). APK Archive. Retrieved from https://vx-underground.org/?value=apk

[10] Abuse.ch Bazaar (n.d.). Retrieved from https://bazaar.abuse.ch/browse/

[11] Snort. 2024. Rule Documentation. [Online] Available at: https://www.snort.org/rule_docs/1-25521

[12] Wazuh 2024 'Active response capabilities' Wazuh documentation. Available at: https://documentation.wazuh.com/current/user-manual/capabilities/active-response/html