Survey on Malware Detection for Smart Devices

Shewale Harshali Kailas[1], Pawar Namrata Sanjay[2]

[1]*Research Student, Department of Master of Computer Application, Asm Imcost, Thane*

[2]*Research Student, Department of Master of Computer Application, Asm Imcost, Thane*

Abstract - *Smartphones are the third revolution in this digital era, following the computer and internet, and they enable ubiquitous computing. Nowadays the use of mobile phones is common among people and people are storing a large amount of data in mobile. Because of its widespread use, Android has become a top target for hackers and online attackers. Cyberattacks of many different kinds are frequently directed at the Android environment. These frequently used gadgets store private information that is sensitive and are therefore increasingly being targeted by harmful malicious software. This essay focuses on the ideas and dangers connected to malware and examines current methods and tools for malware detection in terms of their evaluation metrics, accompanying datasets, and methodology. Android offers flexibility and personalization. Users can unintentionally allow malicious software access, which would destroy their sensitive data. IoT devices that are connected to networks are frequently used by people, which has increased Android and iOS usage. Cyberattacks have increased as a result of the use of mobile devices for business data, private areas, text messaging, and contacts.*

***Key Words*:** Cyberattacks, android, network, intrusion detection, cybersecurity,

1.INTRODUCTION

To make living easier, mobile phones were widely used in daily life. Because they are simple to use and affordable, consumers typically recommend Android and iOS based operating systems. However, because of their widespread use, Android devices have become the most desirable targets for cybercriminals. Data theft, hacking, and other cyberattacks of various kinds are directed at Android, and technically, malware serves as a platform for many or most of these cyberattacks.iOS and Android operating systems With a 72.3% market share compared to iOS's 27%, Android has retained its position as the top mobile OS. An application (app) for mobile devices is a program created to carry out a certain function.

2.RELATED WORK

There are numerous mobile platforms available for smartphones, including Symbian, Blackberry, Windows, Android, and iOS. The market share of each mobile operating system (OS) from 2009 to 2020 is shown in the table below. Due to their improved features and growing user appeal, Android (72.95%) and iOS (26.27%) are well-known. The combined market share of Google's Android and Apple's iOS will make up 99% of all smartphone platforms by the year 2020, despite the existence of other platforms; for this reason, this study focuses on Android and iOS.Also evident is that Android is more widely used than iOS. In 2019, there were 2.5 billion active Android devices, making Android the most popular mobile OS overall, according to ZDNet. In contrast, Apple has 1.4 billion customers who use its whole product line, which includes iOS and macOS computers. the data for global mobile app downloads from 2018 to 2024, arranged by the app store. According to predictions, 139 billion mobile applications will be downloaded from the Google Play Store by mobile users in 2024, up from 102 billion in 2019 The aforementioned factors are responsible for Android's popularity in the smartphone market.

In our daily lives, smartphones have become a necessity. Every day, we use them to communicate by making calls, sending messages, checking emails, taking pictures, and browsing the web. Numerous

functions on cell phones are supported, including texting, taking pictures and videos, and doing financial transactions. Using a smartphone for networking, education, and gaming is also possible. Smartphones globally outnumber both desktop and tablet PCs in terms of numbers sold and use However, because of their widespread use, Android devices have become the most desirable targets for cybercriminals. Data theft, hacking, and other cyberattacks of various kinds are directed at Android, and technically, malware serves as a platform for many or most of these cyberattacks.

According to research from "Pulse Secure", 97% of all mobile malware is created for Android smartphones, making Android the most often targeted operating system (OS) among all other mobile and smart device OS. Throughout this decade, there has been a sharp rise in malware infections. Malware will interrupt several activities soon, ranging from individual to organizational effects on banking, email, and the transmission of sensitive information. Smartphones offer a wide range of services, but some of them also store a lot of valuable data, posing serious security and privacy risks. Mobile malware, for instance, can infect smartphone devices to steal sensitive data, share and track actions, and carry out numerous functions, like placing unauthorized calls. Therefore, protecting against such malware is a crucial task, and methodologies and techniques to identify and stop malware infections of mobile devices have drawn growing interest in both academic and professional circles. Malware packages and mobile device malware threats are both on the rise. Stalkerware is spyware software that steals personal data including images, movies, and GPS coordinates while disguising itself as a parent application.

3. ANDROID MALWARE AND TYPES

Malware is dangerous software that can be used to get beyond security measures, obstruct the functionality of any apps, or find and acquire private data without the users' knowledge. Additionally, malicious software is referred to as "badware." There are various types of malware, including ransomware,worms, trojan horses, rootkits, and botnets. A Trojan horse for Palm devices, F-Secure was the first malware in the history of malware. The first virus to target Android smartphones was Fake Player, which was released in early August 2010 with the primary goal of taking up immediate memory space. According to applications, the first Android virus developed in Russia was ANDROIDS_DROIDSMS, a scam app that charges users to send SMS. A trojan horse game called TapSnake that uses the hypertext transfer protocol to query the Global Position System (GPS) application was introduced to track the GPS location. First, in August 2010, iOS-based malware was released. It uses the Secure Shell (SSH) password to replicate other iPhones that have been jailbroken . Furthermore, according to Trend Micro research , Zeus malware was able to bypass the two-way authentication method on a mobile banking site. Following that, the capability of Android continued to increase quickly, and hackers exploited a weakness to compromise the devices. One such malware is DroidDream , it can reach the root of android smartphones. This sort of malware not only gains International Mobile Station Equipment identity (IMEI) and International mobile Subscriber identity (IMSI),but also installs more obscure malware to collect other information from devices. Google‟s release the google security tools to clean the devices, which is done by the malware writer, take the advantage and release different tools, by which cybercriminals gain information and find the backdoor activities. At present scenario, a lot of malicious android apps are there, which are used to send premium SMS, GPS location spyware and Google+ application to monitor telephone conversation etc. Kaspersky released a report, 1,319,148 harmful programmes have been identified in mid- 2017. Moreover, in year Q4 2016, Mobile ransomware was 200,054, ransomware rapidly expanded in every past year to reach up to 3.5 million in 2017.Currently, RedDrop is android based malware, it has fifty three Androids application packages (APKS) automatically download 7 additional dangerous programmes.

3.1 DIFFERENT TYPES OF ATTACKS ON THE ANDROID ENVIRONMENT.

1. **Data theft**

Most smartphone users have a wealth of personal and financial data. Impact Direct financial and reputational harm. accessible options Monitoring, Anti-theft scanning, and verified apps

2. **Identity theft**

Many online services that use NFC, OTP, and other methods of authentication also use smartphones. Using an Android-powered smartphone, the attacker

gains access to the victim's mobile device and assumes their identity. Although just confined to the attacker, impact losses can be very significant.
Available Solutions Avoid installing dodgy apps, avoid jailbreaking, Monitoring

3. Remote Access

A large amount of personal and financial information is stored on most smartphones. Impact harm to reputation and finances directly.available alternatives Verified apps, monitoring, and anti-theft scanning. impact Innocent users may be found guilty of attacking while the actual attacker is beyond

4. Bloatware

Applications that are pre-installed can be good or bad. Impact Resource usage varies depending on the type of malware. Available Options Avoid dodgy apps and monitoring

3.2. TYPES OF MALWARE

1. virus

A virus is a piece of code that replicates itself and spreads across an application. Viruses spread by attaching an executable file, spreading throughout the system via script code, documents, and online applications. The purpose of a viral attack is to snoop on information, steal money, and destroy the target host . The most common examples of viruses in Android include the Universal Cross-Site Scripting (UXSS) Attack, malware hiding in downloaded apps, Lasco, Command and Control (C & C), CardBlock, CardTrap Android Installer Hijacking, and crossover .

2. Worm

A worm is a piece of computer code that has the capacity for automatic reproduction and distribution among connected devices . The "payload" of the worm, which is intended to disrupt the network's capacity by causing congestion on the web server, is included therein. Additionally, worms use their "payload" to steal information and erase files from their target systems. The primary method of worm transmission across a network is opening infected email attachments. ADB.Miner Android [Gdata link] is the most well-known example of a worm in Android.

3. Trojan

It is a specific kind of malware that manifests itself when a web application is opened for download and installation.Using remote access to the target computer, the attacker can change files, steal information, and keep track of user activity and logs. MasterKey, FakePlayer, GantSpy, DownAPK, and other well-known trojan examples are among the most common ones.

4. Spyware

The malware is the kind that is used without the user's consent, observe user activity. Attackers steal account information and gather key logs.etc. The most important objective of spy software.

5. Botnet

It is a piece of code that is used to hack the device to build the bot, so that remote Without the user's permission, a server called Bot-Master. The number of devices is under Bot-Master's control. A botnet is a type of hacker network. the server data by a web crawler, gather data by spam bots. The most well-known examples of botnets on Android devices are Beanboot, DoubleDoor, and Geinimi .

6. Rootkit

This particular trojan aims to gain remote control. access and controls on the gadget. Rootkit profits administrative rights to use several malicious apps to take the data, carry out the wrongdoing, and modify the Configuration of the system. Rootkits conceal themselves within the system. It stays in the system for a very long time. with the aid of obfuscation. Rootkit Is most prevalent examples in Androids are Godless, HummingBad, and Checkpoint. .

7.Backdoor:

Malware that serves as a backdoor for other malware and can open any port for other applications is considered to be the most hazardous type of malware. Backdoors make it possible for another malicious programme to exploit a weakness in the easiest possible way. Brador is the most well-known example of backdoor malware.

8.Key-loggers

Keyloggers are essentially programmes that are installed on the victim's system. This kind of malware keeps track of all keyboard activity by recording it in the Key-Loggers programme, together with any Key-Stork recordings that the user may have. The two most popular Android keylogger malware programmes are FlexiSpy and mSpy.

9.Ransomware

It is a form of malware that locks down computer resources until the victim pays with cryptocurrency. Malware that demands money will be removed from the system. A 36% increase in ransomware attacks and the introduction of hundreds of new malware

variants were reported in the year 2017 by a semantic report . The most well-known Android malwares include adultPlayer, Simplelocker, FakeDefender, and Xbot .

4.ANDROID MALWARE DETECTION TECHNIQUES

Techniques for detecting Android malware fall into two categories:

1) Signature-based detection and

2) NonSignature-based detection.

These detection methods can also be divided into static analysis and dynamic analysis groups. The next section provides a detailed explanation of these strategies with references to related literature.

4.1 Signature based detection

The signature is used in signature-based detection to identify malicious programs. A signature is a collection of bytes taken from known malware. While dynamic signature-based detection runs the program in a secure environment while checking for the signature, static signature-based detection does not. When dealing with "zero-day" and "unknown" malware, signature-based detection completely fails but performs better when dealing with known malware. The signature database, which necessitates a regular updating of newly formed signatures and requires storage space proportional to the number of signatures, is the only source of signature-based detection.DroidEagle is a tool that looks through an app's layout resources to identify aesthetically comparable apps. RepoEagle and HostEagle are two subsystems of DroidEagle that are used to scan and identify visually comparable applications on the host computer and in app repositories, respectively. The scientists claim that combining structural and behavioral data produces a unique fingerprint for a specific Android application and increases OpSeq's overall recall rate. Although it uses a signature-based approach, it can only identify known malware and is effective against obfuscation techniques. The DroidMOSS method uses fuzzy hashing to measure similarity to locate and identify repacked applications with high accuracy . In this work, authors conducted a systematic analysis of six well-known third-party Android app marketplaces and discovered that 5% to 13% of the apps hosted on these third-party marketplaces are repackaged to achieve various goals, such as stealing or rerouting ad revenues and injecting various types of malware. To obtain two fingerprints for each application to identify repacked applications, context-triggered piecewise hash (CTPH) is employed twice (T-CTPH). The hash similarity calculation algorithm, which maximizes process efficiency, is also optimized by the authors. A dynamic malware detection method for Android apps was recently proposed by Vidal et al. (2018). Because this dynamic technique is based on the comparison of sequences in a significant amount of data, it has the advantage of reducing computation costs. The outcome of using the boot procedure was to cut down on the amount of search space In the end, pattern recognition prevented the malicious application from being installed. This pattern recognition system relies on observation, analysis, and judgment to function.

In their rapid and application store independent technique, Gurulian et al. (2016) proposed that the adversary be prevented from copying the pieces without also significantly reducing the attack potential. This method allows the client to start the detecting process before an installation. When the attacker just copies the Android application's name and icon, the strategy works. To close the gap between the technique's implementation and resource-based repackaging detection, Gadyatskaya et al (2016) note that the resource-based approach detection approach is particularly effective at identifying apps that have been stolen. The results of the experiment indicate that the approach is effective if the various file types are used independently. The main dex code file, the manifest file, and the built resources (such as strings) are the resource file types that are altered the most frequently when repackaging multimedia files, libraries, raw resources, and images. The reliability of the majority of Android malware analysis tools, and in particular static ones, has been questioned due to the widespread use of obfuscation in Android malware. Most of these tools rely on static features that are derived from the source code and are negatively impacted by even minor source code changes. They are therefore not resistant to transformational attacks. Obfuscation has also shown to be a new safeguard for Android users, therefore spotting it is essential to comprehend the semantics of malware specimens at their core.

4.2 Non-Signature based detection

The limitations of signature-based detection can be overcome by non-signature-based detection. Malware-specific signatures are not used in the non-Signature-based detection. This detection approach creates a regular profile and treats any deviation from the normal profile as malicious. The term "machine learning" and "deep learning" are both terms used to describe artificial intelligence (AI), which has a significant impact on cybersecurity. Attackers attempt to employ artificial intelligence (AI) in cybercrime to take advantage of the Android application's user and creator. The AI was crucial in identifying the virus that infected Android devices. Each Android application's manifest file declares and stores the information on permissions and intentions. To create malware classifiers or any other ML-based classifiers, many earlier works (Di Cerbo et al, 2010; Geneiatakis et al., 2015; Sanz et al, 2012) have employed permissions and intentions as features. The creators of CLANdroid use information retrieval techniques and five semantic anchors to find related apps: identifiers, Android APIs, intents, permissions, and sensors . CLANdroid is primarily focused on the detection of similar apps that do not necessarily need to be repackaged. For instance, similarity is the search for apps that are similar to vehicle booking services, while repackaging is the distribution of the same gaming apps by altering the developers' information or substituting the advertisement channel code, etc.

5. CONCLUSIONS

We have covered one of the most important cyber threats to Android security and malware in this review article. We've talked about the security of the Android platform and Google's services for it. There is offered a thorough review of major Android malware variants. Numerous defenses, such as signature-based and non-signature-based detection of Android malware, are also thoroughly covered based on the literature that is currently accessible. Many of these methods for protecting against Android malware are effective, however, the majority of them either target a particular kind of Android malware or address a particular issue. Some solutions have inherent limits, such as the inability of signature-based detection to identify "zero day" malware, and others have resource consumption restrictions, which are crucial for smartphones. For a large number of works to be debated in future review works, we have only mentioned a few carefully chosen works in this work with different parameters. After conducting multiple experiments, a sample test result of various techniques based on a common malware dataset can be provided. This will give a clear picture of the state of those techniques and make it easier to compare and choose the best ones.

6. RESULTS AND DISCUSSIONS

Authors have suggested a method to gauge app similarity based on reported behavior in one of their works The information retrieval method was utilized to retrieve the raw features, which were then enhanced with ontological analysis and used as attributes to describe the apps. The apps were clustered utilizing the agglomerative hierarchical clustering algorithm. 17,877 apps that were harvested from the BlackBerry and Google app stores were used in the experiments. For the Blackberry and Google shops, respectively, the proposed strategy raises the existing categorization quality from 0.02 to 0.41 and from 0.03 to 0.21.

REFERENCES

[1] D. Kornack and P. Rakic, “Cell Proliferation without Neurogenesis in Adult Primate Neocortex,” Science, vol. 294, Dec. 2001, p. 2127-2130, doi:10.1126/science.1065467.

[2] M. Young, The Technical Writer’s Handbook. Mill Valley, CA: University Science, 1989.

[3] R. Nicole, “Title of paper with only first word capitalized,” J. Name Stand. Abbrev., in press.

[4] K. Elissa, “Title of paper if known,” unpublished

[5] Symantec,T ISTRI InternetT SecurityT ThreatT Report,T 2017. 33. J.T Buntinx,T TopT 4T typesT ofT androidT ransomware,T 2017,T JanuaryT 20,2017;T AvailableT from:T https://themerkle.com/top-4-types-ofandroidransovmware/..

[6] F-Secure,T Brador.T AvailableT from:T https://www.f-secure.com/vdescs/brador.shtm

[7] Symantec,T Android.GolddreamT AvailableT from:T https://www.symantec.com/security-center/writeup/2011-070608-4139-99 38. KevinT Sun,T SecurityT IntelligenceT ,T AvailableT from:T https://blog.trendmicro.com/trendlabs-security-integence/ghostteamadware-can-steal-facebook-credentials/