ANDROID PROJECTS ON ANDROID ATTACK APPLICATION

Zainab Rustum Mohsin[1], Auhood Mukr Dayish[2], Baida Abdulredha Hamdan[3]

[1,2,3] *Department of Computer Science, College of Pure Science, Thi-Qar University, Thi-Qar, Iraq.*

Abstract **–Built up an assault android application. It is intended for individuals who are under assault. They would press a catch on their telephone and it will accumulate their present area and begin recording a 5-second video with sound. This will at that point naturally send the area and video straight to the police or companion. The application additionally can actuate U.**

Android Attack application - A major application worked for android handheld gadgets. It is an application that utilizations administrations of the camera, SMS, email, contacts, GPS, It sends recordings to present area coordinates for use by police or companions.

Android applications are traditionally weak across malicious applications. This is an unclassified category of attacks of android which let the user use a sly site in the android browser and do not need the user to install malicious applications. This is known as online injection attacks (or W2AI), that creates differences between various kinds of W2AI and its side effects. For estimating its prevalence, an automated W2AI scanner was offered for determining and confirming the weaknesses in W2AI. The apps from the official Google Play store were analyzed and found to have 286 points in 134 unique applications. The outcomes suggested that these attacks are widespread, and developers do not appropriately protect applications against them. A new mix of Static analysis was employed by our tools, testing and implementing a symbolic dynamic. This design was experimentally shown to enhance the accuracy of detection specifically in comparison to the present sophisticated analysis.

Keywords: **Android, applications, google, android attack, gadgets**

I. INTRODUCTION

Since all ubiquitously digital and physical applications depend primarily on the Internet, these applications can be accessed and controlled via web services and programs. Attackers attempt to breach them with various exploitation techniques to target individuals or organisations for various incentives, such as, stealing valuable information and disrupting computational resources. As a result, a considerable growth of web attacks targeting different web services and applications have been observed. Attacks on web applications have been studied and analysed for many years. The different types of attacks on web applications pose several challenges for cyber-security experts [1,2].

The different types of attacks on web applications pose several challenges for cyber-security experts. There are some attacks like SQL injection and Cross-Site Scripting (XSS) which have been tackled by mitigations that mostly rely on automated technical countermeasures, whereas other attacks such as phishing, which involve technical subterfuge in conjunction with social engineering techniques, that have been attempted to be mitigated using automated detection as well as awareness mechanisms to educate users. Most automated detection techniques rely on extracting features from the URLs and content of webpages before Using automated learning classification techniques them as malicious or genuine [3].

In 2018, a negative record was set where 3.2 million new Android malware samples were discovered by G DATA analysis. Around 11,700 new malware samples were counted per day for the popular operating system by the researchers. An increase of over 40% has been observed than the last year (2,258,387). In 2016, this number has increased to this point. A new level of threat has been introduced in android these days. These threats include malware missing updates from smartphones [6].

II. REVIEW OF LITERATURE

The answer to the question of android is not easy. The market shares suggested that around 80% of global smart phone users have android devices. The high rate of distribution has a direct relation with the smartphone's price purchase. Decent devices of android can be got at relatively low prices [7].

As android has a struggle with outdated devices, Google had begun addressing issues back in 2017. The company incorporated an option under Project Treble in android 8 and that made the fast update possible [8]. G DATA security analysis blog was reported about this issue. Only one in five devices installed android 8 after its launch in August 2017. The latest version has a rate of distribution less than 0.1%. The path of protecting smartphones and tablets better depend on the latest updates on securities on time. Device providers and security researchers are needed to maintain higher standards [9].

The report from Technology portal; The Verge stated that, for the last two years, this summer Google has been contractually obliging manufacturers of popular Android smartphones for providing security updates. Mobile phones must receive at least four updates on Google Security in the first year according to the terms. The updates should be regularly received in two years. Devices must be protected against every vulnerability each month, which was discovered more than 90 days ago. But there are various limitations in contractual regulation. Around 100,000 users have activated it in smartphones [10, 11]. Additionally, the contract is applicable to devices that were introduced in the market after 31st January 2018. A huge portion of this legislation were supposed to be implemented by 31st July, but a grace period has been given till 31st January 2019.
The Linux kernel area has an urgent backlog. Based on the Greg Kroah-Hartman, there are few android smartphones which will use the latest Linux kernel. Googlee's "Pixel" is an internally developed has an updated system. Aside from the "Pixel" devices, all android phones are vulnerable towards attacks. It is because the attackers need to check if there is unpatched vulnerabilities left by the kernel developers and if the source software is posted publicly [12].

Uncertainty is caused by the present coverage related to spyware for android smartphones. Whatsapp chats can be read by the copy of a host of private data by the malware. Another cause behind uncertainty is the present coverage of spyware of android smartphones. Whatsapp chats can be read from a smartphone by copying the private data in a host by the malware. The threat is recognized under the name of android by G DATA Internet Security. According to Trojan-Spy. Buhsam. A [13], Smartphones especially hold a wide range of important private data on a device. For example, protection against threats is provided on a mobile device. For Google, the danger from malware is a necessary matter. IT Security industry experts meet annually at the conference of Virus Bulletin Trade. Google researchers gave two talks on the subjects of apps of android malware. Maddie Stone, the analyst, presented a sophisticated strains of malware which go to unusually massive strengths for being founded by automated systems [14].
Security expert, Łukasz Siewierski, spoke about a campaign including pre-installed malware on Android smartphones in the second Google Talk. The malware is installed during the actual development stage according to the analysis [15].

Android registers Digital signature application when you install it for the first time and the security model is formed for this purpose. All updates to this application must be signed by the author himself in order to verify that they have not been manipulated. The ability to modify legally signed applications means an attacker could trick users to install fake updates to their applications already installed have access to all data that is potentially stored by these applications. If the targeted ones are system applications, such as applications that are installed by previous manufacturers, even malicious code in rogue updates can perform system privileges. "It's a different approach to achieving the same goal with previous exploitation," said Bau Oliva, a mobile security engineer at ViaForensics Security. Oliva Fora has created a proof-of-concept exploit of the signature verification file discovered by Bluebox. The researcher did not have time to make a same exploit for the new case, but see the technical details [16].

The new effects enable hackers in inserting code to specific files in APK files, particularly in their head to go beyond verification of signature. The target files must be less than 64 kilobytes (KB) by limiting the attack to an extent. According to Olivia, the detection method is easy or this kind of APK applications, but they vary from altered applications from exploiting the past vulnerability. It is a reasonable ad credible method and possesses the same effect as the main key (Android Key) by Bluebox, "However, Bluebox is familiar with different, more comprehensive ways with fewer limitations than those that were technically explained in that publication," said Jeff Forsthal, chief technology officer at Bluebox Security. This most comprehensive approach has been unveiled by Bluebox to Google, with proper correction. "Implementing the released AOSP [Android Open Source Project] will result in protection against either method" [17].

The technical details have been blocked for allowing enough time for the manufacturers to come up with the patch version. Google with Bluebox security version indicated that application can be detected by Google Play which try to disrupt the newly affected ones. According to Forrestal, no test has been performed by Bluebox to confirm it [18].

It can provide weaknesses that allow modifying APK files without legitimate failure to verify the digital signature of the Android benefits for cybercriminals. Trying to pass harmful applications Koab common and other applications are known for as long as the technique used by the authors of malware in Android to distribute their creations. Probably you will not receive any of the affected devices to the problem of the vulnerability of this correction because it reached the end of support. However, if Google Play has already discovered these exploits, we must protect users who do not demonstrate applications from alternative sources such as application stores, third-party [19].

III. DISCUSSION

Describe the surface of the attack.

Surface Attack	Describe
Internet	Unsafe protocols, for example, HTTP, incorrect HTTPS, and so on sent sensitive information over the Internet
Third Party	Third-party servers store the sensitive information
Bluetooth	You can sniff or inject sensitive information that is collected by health devices that support Bluetooth technology
Logging	Sensitive information is placed in system logs where it is not locked
SD Card Storage	The SD Card does not encrypt the stored sensitive information and can be accessed generally by another application
Exported Components	Components of android app, designed to be private, are set to export, making them accessible by other apps
Side Channel	A malicious application derives sensitive information containing side channels, for example, packet size, serialization, timing, etc.

In 2018, The total count of mobile malware increased around 40%. Around 3,2 million malicious apps were determined by G DATA Analysis by the end of the third quarter of 2018.

This represents an increase of over 40% in comparison to the same period last year (Q3 2017: 2,258,387 malware samples). Cyber criminals are increasingly focusing on mobile devices, especially those with Android operating systems. The cause behind this is that, eight out of ten people globally use a smartphone with the popular OS, because these are often cheap to buy. This makes it all the more important to use a security app [20].

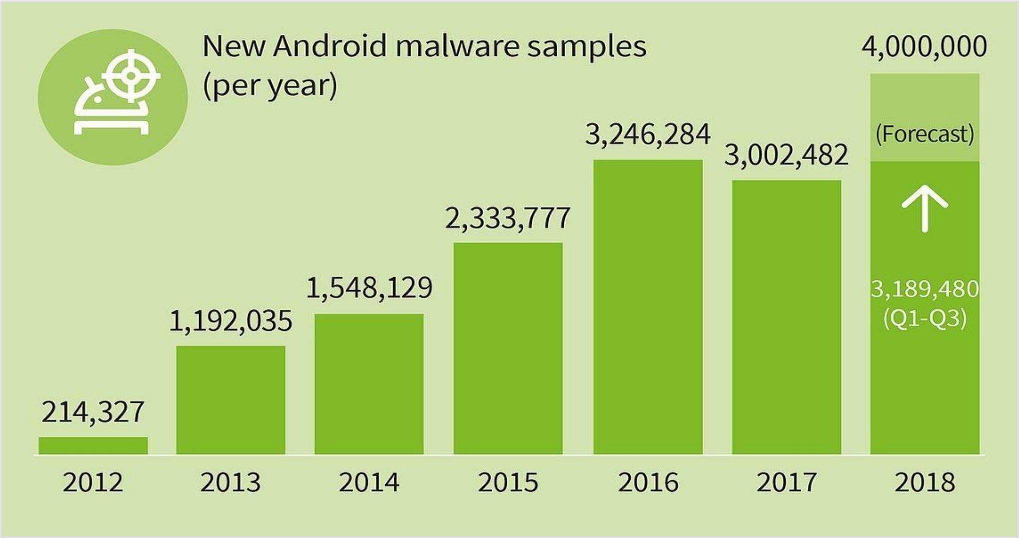

Fig 1. The total count of mobile malware rises about 40 percent in 2018. G DATA Analysts have identified around 3,2 million malicious apps by the end of the third quarter of 2018 [21].

IV. CONCLUSION

The continued development and rapid change of the smartphone market has helped to increase the number of services and applications offered. With the integration of these devices in everyday user activities, they become very attractive targets for Internet criminals. In this sense, malicious software (malware has become) a major security problem in this area. Although malware is not a new problem in the IT industry, the differences between computers and smart devices make smart devices different security problem associated with special features for portable devices. Moreover, the large number of stakeholders ranging from hardware manufacturers to telecommunications equipment and providers of telecommunications services creates a highly heterogeneous environment where it becomes the penetration of a very complex task attacks. In this context, this chapter aims to provide an overview of the basic aspects of the analysis and detection of Android malware.

As can be seen from the information discussed above, there is generally a core set of analysis techniques and resource data used in multiple research methodologies to identify and detect malware. This observation may be obvious because the specific features are key elements of the Android security architecture, although there is no full agreement in better technology or procedures to detect malware effectively. It is important to note that the automated learning plays an important role in most of the approaches discussed in the latest case of malware analysis, and in some cases the results reported seem very promising, but there is always a problem and there is a limited problem. The number of samples to test all potential threats. In addition, In addition, with the enormous current set of analysis and reverse engineering set of tools, which are implemented in the framework of different techniques and methods of analysis, a very difficult task of integration seems to be achieved. Furthermore, the availability of multiple different tools and multiple levels of automation. However, the need to automate most of the process is still an important issue because most of the analysis in the identification of new threats continues to be a humanitarian mission. Finally, the information provided in this chapter is expected to help readers gain an overview of the Android malware analysis and detection area where they can or can see new ways to search.

G DATA Internet Security for Android obtained full marks in the latest comparison test by AV-TEST. The smart security app detected 1005% of all malware and obtained the highest marks for no less than the ninth time in a row. A total of 20 security products for Android were examined by AV-TEST, this time. All of the security solutions had to demonstrate their capabilities using all of their protection and functionality levels. G DATA Internet Security for Android impressed in every category and obtained a detection rate of around 100%. The second gap was determined that can be used to modify Android applications without breaking digital signatures that have been publicly documented.

REFERENCES

[1] Aafer, Y., Du, W., & Yin, H. Droidapiminer: Mining api-level features for robust malware detection in android. In International Conference on Security and Privacy in Communication Systems.2013; pp. 86--103.

[2] Arp, D., Spreitzenbarth, M., Hubner, M., Gascon, H., Rieck, K., & Siemens, C. DREBIN: Effective and Explainable Detection of Android Malware in Your Pocket. In Network and Distributed System Security.2014; 14, 23--26.

[3] Arsene, L. Android Adware Breakdown: Benign Vs. Aggressive. https://hotforsecurity.bitdefender.com/blog/androidadware-breakdown-benign-vs aggressive-3188,2012.

[4] Backdoor. Retrieved from https://www.f-secure.com/v-descs/backdoor.shtml,2018 .

[5] Bermejo, L., Pan, J., & Pernet, C. Android Backdoor GhostCtrl can Silently Record Your Audio, Video, and More,2017 https://blog.trendmicro.com/trendlabs-securityintelligence/android-backdoor-ghostctrl-can-silentlyrecord-your-audio-video-and-more/.

[6] Botnets. Retrieved from https://www.fsecure.com/en/web/labs_global/botnets,2018.

[7] Brenner, B. Mobile security vendor: DroidDream pulling Android into botnet army. https://www.csoonline.com/article/2134637/dataprotection/mobile-security-vendor--droiddream-pullingandroid-into-botnet-army.html,2011.

[8] Buczak, A. L., & Guven, E. A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials.2016; 18(2), 1153-1176.
[9] Cimpanu, C. Koler Android Ransomware Targets the US with Fake PornHub Apps. https://www.bleepingcomputer.com/news/security/kolerandroid-ransomware-targets-the-us-with-fake-pornhubapps/.2017.
[10] Collier, N. Yet more mobile adware found in Google Play. https://blog.malwarebytes.com/cybercrime/2017/10/yetmore-mobile-adware-found-in-google-play/,2017.
[11] Constantin, L. Self-propagating SMS worm Selfmite targets Android devices.https://www.computerworld.com/article/2491339/malware-vulnerabilities/self-propagating-sms-worm-selfmitetargets-android-devices.html,2014.
[12] Coogan, P. Android RATs Branch out with Dendroid. https://www.symantec.com/connect/blogs/android-ratsbranch-out-dendroid,2014.
[13] Donohue, B. First Ever Android SMS Trojan Targeting U.S. Users. https://www.kaspersky.com/blog/fakeinst-targets-ususers/4601/,2014.
[14] Enck, W., Ongtang, M., & McDaniel, P. On lightweight mobile phone application certification. In Proceedings of the 16th ACM Conference on Computer and Communications Security,2009; pp. 235--245.
[15] FakeToken Android Banking Trojan Returns as a Ridesharing App. Retrieved from https://www.trendmicro.com/vinfo/us/security/news/mobil e safety/faketoken-android-banking-trojan-returns-as-aride-sharing-app,2018.
[16] Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., & Rajarajan, M. Android security: a survey of issues, malware penetration, and defenses. IEEE Communications Surveys & Tutorials.2015; 17(2), 998--1022.
[17] Feizollah, A., Anuar, N. B., Salleh, R., Suarez-Tangil, G., & Furnell, S. Androdialysis: Analysis of android intent effectiveness in malware detection. Computers & Security.2017; 65, 121--134.
[18] Felt, A. P., Chin, E., Hanna, S., Song, D., & Wagner, D. Android permissions demystified. In Proceedings of the 18th ACM Conference on Computer and Communications Security.2011; pp. 627--638.
[19] Global mobile OS market share in sales to end users from 1st quarter 2009 to 2nd quarter. Retrieved from https://www.statista.com/statistics/266136/global-marketshare-held-by-smartphone operating-systems,2017.
[20] Goodin, D. Menacing Android botnet still thrives 16 months after coming to light. https://arstechnica.com/informationtechnology/2018/01/menacing-android-botnet-still-thrives16-months-after-coming-to-light,2018.