World Journal of Research and Review (WJRR)
ISSN: 2455-3956, Volume-13, Issue-5, October 2021 Pages 01-03

Ransom-ware Detection by Real Time Android Application

Abhishek Sharma, Ayush Lata

***Abstract*— recently, harm resulting from ransom ware has been growing in PC and Android environments. There are many research into actual-time ransom ware detection due to the fact the most crucial time to save you encryption is earlier than ransom ware is capable of execute its malicious process. Traditional analyses decide a software is ransom ware or now no longer with the aid of using static/dynamic methods. Those analyses can function additives of a technique to hit upon ransom ware in actual time. However, issues can occur together with the incapability to hit upon new/variant/unknown ransom ware. These sorts require signed patches from a depended on birthday celebration that can simplest be created after assaults occur. In a proceeding examine into real-time new/variant/unknown ransom ware detection in a PC environment, crucial documents are monitored and simplest applications which have been formerly analyzed and evaluated as no malicious are allowed. As such, applications which have now no longer been analyzed are confined from gaining access to crucial documents. In an Android environment, this technique may be carried out the usage of Android programs to save you rising threats and confirm consistency with person intent. Thus, this paper proposes a technique of detecting new/variant/unknown ransom ware in actual time in an Android environment**

***Index Terms*— Android; New/Variant/Unknown Ransom ware; Real-Time Detection; Encryption**

I. INTRODUCTION

Ransom ware is turning into an increasing number of problematic, inflicting substantial harm worldwide. Ransom ware—a compound phrase of ransom and software—is used to encrypt and disable a user's precious information, requiring price to get better it. Unlike different malware, the encrypted information cannot be recovered due to the fact handiest the attacker has the decryption key. The unfold of ransom ware is normally facilitated with the aid of using phishing mails, untrusted web sites, and report sharing web sites with social engineering techniques [1].

Recently, Android has emerge as a goal for malware due to the fact it's far an open supply platform with globalization and fragmentation. Additionally, Android lets in customers to install packages from now no longer handiest untrusted web sites however additionally the Google Play Store. This allows hackers to fraud customers [2].

The maximum crucial is to save you information encryption with the aid of using ransom ware. As such, numerous techniques to decide in real time whether or not a software is ransom ware or a normal encryption were studied. Traditional techniques to detect ransom ware packages encompass static analysis [3] and dynamic analysis [4]. However, they're taken into consideration vulnerable and without difficulty circumvented through attackers.

In [5], a 3-step technique is proposed with traditional techniques for detecting ransom ware packages in actual time. The first step in their technique is tracking, the second one is dynamic analysis, and 1/3 is static analysis. However, some issues can arise which include fake detection, in addition to the opportunity of circumvention and vulnerability for new/variant/unknown ransom ware.

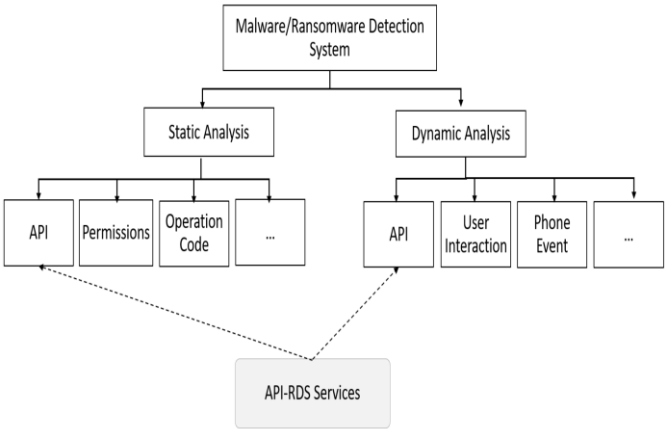

Fig: Ransom ware Detection System

Reference [6] mentioned that strategies to patch information of ransom ware—which include detection primarily based totally on signatures supplied through a depended on celebration—cannot prevent new/variant/unknown ransom ware. This is due to the fact the depended on celebration can simplest get a ransom ware pattern after customers have been attacked. They proposed a technique to discover ransom ware in a Windows surroundings in actual time without patches from a depended on celebration. However, issues can arise

Abhishek Sharma, Ayush Lata, Student at Computer science dept. Vivekananda Institute of Technology, Jaipur.

if this technique is carried out in an Android surroundings due to its Windows additives and outcomes in overall performance overhead through analyzing all get right of entry to operations on tracking process. As such, we want to put in force a comparable technique in an Android surroundings and reduce overhead through decreasing the range of monitored targets.

Section 2 of this paper discusses works associated with ransom ware on Android, ransom ware detection methods, and Shannon entropy. In phase 3, we examine how unique troubles in the preceding research can also additionally occur. In phase 4, we recommend our technique for detecting ransom ware packages in actual time with advanced tracking overall performance in an Android environment. We then define a demand for implementation of our technique in phase 5. Finally, we gift our conclusions and speak destiny paintings to enforce the technique in phase 6.

II. RELATED WORKS

A. *Ransom ware in an Android Environment*

Ransom ware is any form of malware that needs a sum of cash from the inflamed user. On Android, there are two trendy classes of ransom ware: lock-display screen and crypto. In lock-display screen types, the hijacked aid is blocked via way of means of an image that completely covers the screen. Crypto ransom ware encrypts the User's treasured data. Android ransom ware usually suits the popular definition of a Trojan horse. In a few cases, the malicious APKs replica simplest the call and icon of the normal software or hide it as a valid document in an SMS or email. In this way, attackers use social engineering to control sufferers into putting in malicious APKs and executing functions [7]. An instance of ways attackers spread ransom ware as valid applications such assaults may be a hit due to the fact Android gadgets are allowed to put in programs from third-celebration app stores. Additionally, as soon as Google releases a new edition of the OS, manufactures won't improve their OSs immediately, or at all. A tool jogging on an older model of the OS can end result in sure vulnerabilities closing unpatched for an attacker to exploit [10].

B. *Static Analysis*

Static evaluation entails an automatic device that takes the supply code of a software as enter and examines it without executing. It then verifies the code shape and statement sequences, assessments how variables are processed in the course of the extraordinary characteristic calls, analyzes strings in data files— which includes xml—and yields a result. A static evaluation begins off evolved by representing the analyzed app's data to a few abstract fashions primarily based totally at the cause of the evaluation. Those fashions offer a simplified interface for assisting purchaser analyses [3]

C. *Dynamic Analysis*

While static evaluation can rely upon Java byte code extracted through disassembling APKs and does now no longer require code execution, dynamic evaluation can observe all code carried out through an application [11]. This is important due to the fact malware can hide malicious activities in the back of sports that require an interaction with an Android user. Therefore, to check the apps dynamically, a device is required that could simulate those apps to begin their malicious activity. In dynamic analysis, the software is done in a managed environment—including sandbox—and digital system to hint its behaviors [12]

D. *Android ransom ware Detection in Real Time*

In [5], a 3-step evaluation approach is proposed to determine whether or not a utility is ransom ware or not. Whether the user meant for encryption on their tool is a vital element in this approach.

First, for encryption evaluation, essential documents predefined with the aid of using the consumer are monitored and inspected the ones documents had been encrypted the use of Shannon entropy fee in actual time. If an essential report is decided to be encrypted, the method actions to the following step; otherwise, it keeps to monitor. Second, foreground evaluation exams for the encryption software's hobby on the pinnacle of the hobby stack—called Activity Manager. The intention of this step is to make certain that the encryption method is prompted with the aid of using the foreground. That is, it exams that the encryption method is proven at the device's display screen. If the software's hobby is on the pinnacle of the stack, the method actions to subsequent step; otherwise, it stops the software and sends an alarm to the consumer. Finally, in format evaluation records from manifest, format, and xml documents is extracted. It is thought that normal encryption packages display a listing of documents, texts, and buttons with trace strings at the display screen visible with the aid of using the consumer—this will be performed with the aid of using static evaluation. If the software has these components, the step ends and returns to the primary step; otherwise, it stops the software and sends an alarm to the consumer.

III. CONCLUSIONS

In this paper, we analyzed the issues of previous research approximately the way to stumble on new/variant/unknown ransom ware in actual time on Android. Subsequently, we proposed an actual-time ransom ware detection technique in addition to necessities to enforce the technique. This technique can prevent new/variant/unknown ransom ware

with much less performance overhead in an Android environment. We targeted on the primary characteristic of strategies from the Monitoring and Already Analyzed steps. However, how we offer statistics to the consumer within side the Normal step is also important. Thus, extra research approximately how to investigate the programs may be required. In destiny work, implementation of the proposed technique needs to be accomplished with detailed evaluation techniques and evaluated for detection accuracy

REFERENCES

[1] Meet Kanwal, Sanjeev Thakur, and Rishabh Lashkari, "An app based on static analysis for Android ransom ware", 2017 8th International Conference on Computing, Communication and Automation, 2017.
[2] McAfee. Part of Intel Security, "What's on the Horizon for 2016", Mobile Threat Report of Intel Security, 2016.
[3] Li Li, Tegawende F. Biscayne, Mike Papadakos, Siegfried Rasthofer, Alexandrea Bartle, Damien Ocean, Jacques Klein, and Yves Le Traon, "Static Analysis of Android Apps: A Systematic Literature Review", ELSEVIER Information and Software Technology Vol. 88, 2017.08.
[4] Mohammed K. Alzaylaee, Suleiman Y. Yerima, and Sakir Seer, "Improving Dynamic Analysis of Android Apps Using Hybrid Test Input Generation", IEEE International Conference On Cyber Security And Protection Of Digital Services (Cyber Security 2017), 2017.07.
[5] https://builtin.com/artificial-intelligence/artificial-intelligence-future
[6] https://www.sas.com/en_in/insights/analytics/what-is-artificial-intelligence.html [3]https://magazine.startus.cc/growing-role-artificial-intelligence-business/
[7] https://www.sciencemag.org/news/2020/04/artificial-intelligence-evolving-all-itself
[8] https://www.livescience.com/49007-history-of-artificial-intelligence.html
[9] https://becominghuman.ai/introduction-to-artificial-intelligence-5fba0148ec99#:~:text=Artificial%20Intelligence%20is%20an%20approach,study%20outputs%20intelligent%20software%20systems.
[10] https://www.google.com/search?q=artificial+intelligence+images&safe=active&rlz=1C1CHBD_enIN949IN950&sxsrf=ALeKk000L-Lmv3Gbt8ay6l1J3FHn G59AFQ:1624816583916&source=lnms&tbm=isch&sa=X&ved=2ahUKEwiKnby6sbjxAhWkguYKHaDfBJ0Q_AUoAXoECAEQBA&biw=1242&bih=597#i mgrc=WisEJTAPoBXPFM