**RANSOMWARE PREVENTION ON ANDROID PLATFORM**

Lokesh Patni Pradeep Sharma

[lokeshpatni.cse17@jecrc.ac.in](mailto:lokeshpatni.cse17@jecrc.ac.in) pradeepsharma.it@jecrc.ac.in

Department of Computer Science & Engineering

Jaipur Engineering College and Research Centre

Sitapura, Tonk Road, Jaipur

**Abstract**

The purpose of this paper is to propose a good methodology to stop the attacks of changed ransomware on android platform. The projected technique specifies and intensively monitors processes and specific file directories supported Processor usage and Memory usage in order that the method with abnormal behaviours will be detected. If the method running a suspicious ransomware is detected, the projected system can stop the method and take steps to verify the deletion of programs related to the method from users.

**Keywords**: *ransomware, processes, android platform, intensively monitors, processor usage.*

**1. Introduction**

Ransomware [1] is a kind of malware that uses malicious codes to intrude the system before users notice it, to encrypt important files, to want cash mistreatment encrypted files as a hostage, and to relinquish financial damages to users. The rapid growth of the mobile market has been the main target of hackers to obtain criminal gains by mistreatment ransomware. Compared to different OS like iOS, Windows Phone, or Blackberry, Android holds a high market share near monopoly [2]. The share of the android platform is so high that the platform becomes the main target of ransomware attacks. Traditional immunizing agent system will observe a system if it's infected with ransomware and cure it. However, it cannot forestall attacks by ransomware while not getting data on the ransomware. Additionally, files can't be recovered without the secret writing key as a result of files square measure already encrypted even if the normal immunizing agent system will take away the ransomware[3].However, this methodology has restricted efficaciousness. Existing immunizing agent system will observe ransomware using intrusion detection methodology supported files [4]. However, this approach cannot observe changed ransomware with new patterns as a result of it will solely forestall ransomware based on analysis data of the ransomware. Therefore, an active rather than a passive interference methodology is desperately required.

In this paper, a ransomware hindrance technique on Android platform is projected. The projected technique will monitor file events that occurred, once the ransomware accesses and copies files. This technique will sight and remove the ransomware victimized files by analysing the processor and memory usage. This projected method will sight changed patterns of ransomware while not obtaining info regarding the ransomware. It can be implemented on the kernel and framework level of Android so that it can detect ransomware relatively fast and effectively. Also, it can easily monitor the files and no frequent updating would be required.

**2. Researches**

*2.1.* ***Ransomware****.* Ransomware spreading methods are similar to those of malicious code Trojan Horse[5] that contains malicious routine and pretends as a normal program.

Ransomware intrudes into users’ devices after pretending as a normal application such as Trojan Horse. Ransomware restricts the use of the system in various ways after intruding the system. It is mainly classified into the following three types: Scare ware, Lock-Screen, and Encrypting [6].

(i) *Scare ware*. It informs users that the device has been infected with malicious codes. It suggests the acquisition of fake antivirus programs to treat them. It finally extorts cash from the user.

(ii) *Lock-Screen.* It disables users’ computer in any means. It locks the system so the users aren't able to run the in operation system. Once a user runs his system, it disables the software system and sends the message that your computer has illegitimate contents that you are going to be fined by impersonating Federal Bureau of Investigation or government agencies.

(iii) *Encrypting*. This is the foremost serious form of ransomware. It prevents the utilization of necessary files in your device by encrypting them. It extorts money by encrypting users’ files in PCs and rental users deposit the ransom for files to a virtual account to decode.

Ransomware accesses users and provides injury to them in varied ways that for instance, CryptoLocker [7] will encipher files in computer. Reveton [8,9] can impersonate enforcement agencies like law enforcement agency. Simple Locker [10] targets smartphone users of the mechanical man setting. This ransomware may be serious security threat to cloud computing [11] because it becomes the basic infrastructure of data system.

***2.2. Existing Techniques***

2.2.1. ***Using Hash Information.*** The process methodology of CryptoLocker is to match Hash information. CryptoLocker generates files encrypted with “.encrypted” [12]. The encrypted files are then added to the Hash information. Recovery tools compare Hash information and encrypted files within the information files, ensure the validation of key from key index info hold on in that, and proceed to decoding [13].

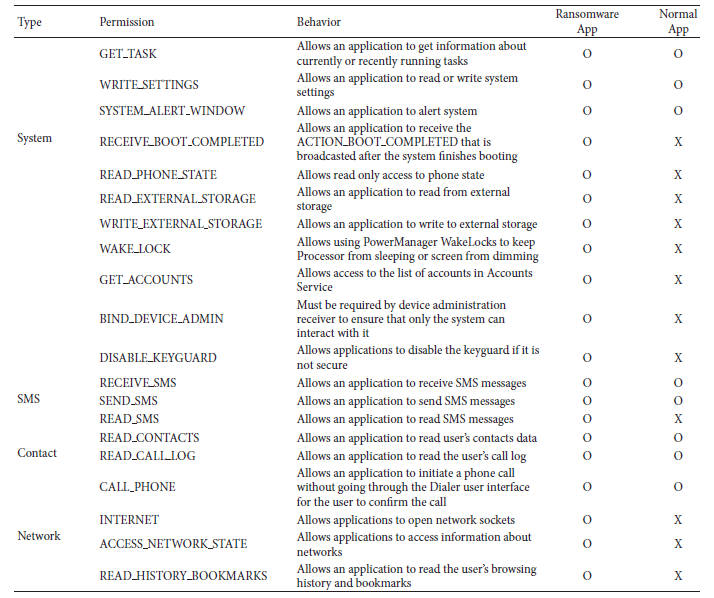
By watching encrypted files’ recovery ways utilized in existing vaccines, a sample is found for the ransomware and decryption is performed using decryption key [14].

There is a risk that once a replacement ransomware seems, users have to wait till a security company finds the coding key value through sample analysis. Intelligent sensing techniques are needed to find new patterns of ransomware as a result of ransomware perpetually threatens the protection of mobile device.

System-based behaviour detection technique [15] is purely based on analysing the different behaviours of the system at a given time. It performs “integrity checking” and “behaviour blocking” [16,17]. Integrity checking is the frequent checking of system to confirm its integrity. So every time it checks the system it maintains a new hash value for it. Behaviour blocking technique monitors all actions within the computer system. When a suspicious action occurs in similar way of malicious infections, this approach tracks the cause of executable file and blocks the execution of a suspicious action so that it has no progress.

2.2.2 ***Application Permissions Analysis.*** Android market applications needs system permissions to perform its operation. Applications registered in an official store show user’s permission requirements when they are downloaded. However, ordinary users may unintentionally download or run applications without carefully looking at them. Ransomware distributors will distribute the ransomware and pretend as a normal application on an official store using this security weakness. Difference in permissions between Ransomware App and Normal App is shown in Table 1. A total of 14 kinds of ransomware that appeared between 2014.01 and 2015.09 based on the

Table 1: Difference in permission between Ransomware App and Normal App [19, 20].



report of virustotal [20] are included in the comparison (Table 1).

The functions of all the permissions are not always safe. These permissions access a lot of information, including the configuration information of the device, the list of applications, resource statistics, and personal information such as location information and SMS information. Normal applications use these permissions. Therefore, users generally agree to install applications without doubt, even when it is the ransomware that requires permissions for the System, SMS, Contact, and Location.

2.2.3 ***CPU Usage.*** Statistical technique is one malware analysis technique that detects abnormal behaviours by analysing the resources of the system. NIDES (Next-generation Intrusion Detection professional System) [18] of SRI (Stanford analysis Institute) International could be a typical system supported applied math techniques. NIDES sets a goal of detecting abnormal behaviours that occurred within the system with an identification technique when assembling Processor usage, I/O rate, Memory usage, and then forth, over a protracted time. However, this system solely operates against the attacks of DDoS. In this paper, a method is proposed to stop the intrusion of ransomware on android platform supported statistical strategies victimisation method, Memory, and Storage I/O usage.

**3. Proposed Technique**

To have an easy implementation, the technique is divided into 3 modules: Configuration, Monitoring, and Processing (Figure 1). Configuration is the initial setup of generating a list of all that process to be monitored. Monitoring module is answerable for watching Processor, Memory, and Storage I/O usages of each method in real time supported statistical techniques. Finally, process module determines the handling of the method suspected as ransomware by the Monitoring module.

All the 3 modules need to be implemented on the kernel level for perfect execution and need to be added to the Android settings and database to get proper results.

The basic algorithm for the process can be understood as:

**begin**

Take ProcessId as input

Get the ProcessInfo from database

**If** Process is from the blacklist

Kill the process

**else**

If Process of not priority **then** Monitor(Process)

**end**

Basic algorithm for proposed system

3.1. ***Configuration Module*** It is the initial step to detect a ransomware. The main role of this module is to specify the location of the files needed to be protected from the attacks of the ransomware. An area of these important files is called priority protection area (hereinafter PPA).It will collect the information of the process and store them in the list for the monitoring module. It will also handle the suspected process. If the user finally determines the process as a ransomware, it stores the information of the corresponding process. Based on the feedbacks the process if found a ransomware kind of process then it will be automatically deleted and if not then its info will be stored in the database.

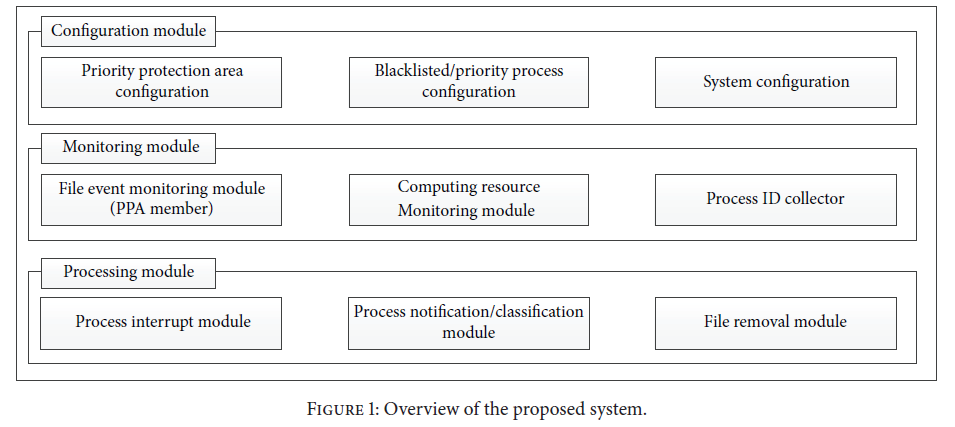
3.2. ***Monitoring Module.*** It is the most important part of the proposed technique as it detects the ransomware by monitoring the PPA area and the process.it comprises of two internal modules.

(i) *File Monitoring Module.* It monitors all the things related to a file i.e. its input/output, open/close, read/write operations and if any ransomware file is found it sends it to configuration module for deletion.

(ii) *Process Monitoring Module*. All the processor related detection are done under this such as identifying the memory usage, the resource usage and I/O usage and any abrupt usage is then send to the configuration module for further handling.

Upon analysing the suspected method, it conjointly handles malicious or exceptional processes within the info applied in the configuration module. For the method registered as a malicious method, the observance module can stop the process at the instant of detection and mechanically delete the process. For the method registered as associate degree exceptional process, it'll enable the conventional execution as a result of it's specified as safe by the user.

**3.3.** ***Processing Module.*** The processing module can anytime stop the process that are seemed to be suspicious in any account in the monitoring module and send a message for it.



The system then enquires about the handling ways. Once the handling is determined, the information of the corresponding process will be stored in the database and used in the configuration module subsequently.

**begin**

Get all the ProcessId

for i=0 to n

**If** ProcessId in PPA then

KillProcess

Send data to Monitor

**else**

Resume Process

**end if else**

Store ProcessInfo in database

**end for**

**end**

Algorithm for process monitoring

It also warns the users about the risk of these ransomware through all the permission analysis and reports.

(i) *System Permission.* The ransomware can invoke any such user’s administrative permissions and manipulate the system. It can easily go through the systems private information and can damage the device.

(ii) *SMS Permission.* Ransomware can easily read your messages can use it for illegal purposes by accessing your SMS permission.

(iii) *Contact Permission.* Permission to access contacts is stored in the device. Typical examples of making ill use of this permission are phishing and smishing.

(iv) *Network Permission.* Ransomware can detect your network and seize you from using it. It has the risk of intercepting user’s personal information stored in the device.

The module inquires of users regarding whether or not to keep or delete the corresponding program once detecting the process suspicious of ransomware. If the user shows his intention to delete the appliance, once an equivalent method appears later, it's mechanically removed while not asking about user’s thoughts as a result of the user acknowledges the corresponding application as ransomware. If he determines the process as normal, its safety is warranted therefore the method will not be forcibly stopped by the planned technique.

3.4. ***Interface****.* In order to provide the features of the system a simple interface is to be designed. It provides users with easy access to the proposed method. It has a basic format of the Android. It provides an interface of the configuration module. The proposed system functions can be turned on and off at any time using the corresponding interface. It can be used for addition and deletion of information further.

**4. Conclusion**

In this paper, a method is proposed to reduce and eliminate the attacks of ransomware on Android devices. The planned technique will effectively cut back injury caused by ransomware with changed or new patterns without getting data on the ransomware. It uses input/output methods, processor usage, and memory usage to detect the ransomware and then eventually eliminate them. It is potential to use the planned technique altogether on Android-based phones as it is based on open source android file. This system is expected to allow users to minimize damage caused by attacks of ransomware that existing systems fail to observe.

**References**

[1] X. Luo andQ. Liao, “Ransomware: a new cyber hijacking threat to enterprises,” inHandbook of Research on Information Security and Assurance, IGIGlobal, 2009.

[2] “Worldwide Quarterly Mobile Phone Tracker,” IDC, August 2015, http://www.idc.com/tracker/showproductinfo.jsp?prodid=37.

[3] TREND Micro, Ransomware Definition—Security Intelligence, TRENDMicro, Irving, Tex, USA, 2015, http://www.trendmicro.com/.

[4] D. Kim and S. Kim, “Design of quantification model for ransomware prevent,”World Journal of Engineering and Technology, vol.3, no. 3, pp. 203–207, 2015.

[5] D. Lim, “Treats and countermeasures of malware,” Journal of IT Convergence Society for SMB, vol. 5, no. 1, pp. 13–18, 2015.

[6] N. Andronio, S. Zanero, and F. Maggi, “HelDroid: dissecting and detecting mobile ransomware,” in Research in Attacks,

Intrusions, and Defenses, vol. 9404 of Lecture Notes in Computer Science, pp. 382–404, Springer, 2015.

[7] A. Beuhring and K. Salous, “Beyond blacklisting: cyberdefense in the era of advanced persistent threats,” IEEE Security & Privacy, vol. 12, no. 5, pp. 90–93, 2014.

[8]P.Ducklin, “Reveton/FBI ransomware—exposed, explained and eliminated,” Naked Security, August 2012, https://nakedsecurity.sophos.com/.

[9] J. Milletary, “Citadel Trojan Malware Analysis,” Dell Secure Works Counter Threat UnitIntelligence Services, Dell Secure Works, September 2012.

[10]T.M.Marengereke and K. Sornalakshmi, “Cloud based security solution for android smartphones,” in Proceedings of the IEEE International Conference on Circuit, Power and Computing Technologies (ICCPCT ’15), pp. 1–6, Nagercoil, India, March 2015.

[11] Y. Liu, Y. L. Sun, J. Ryoo, S. Rizvi, and A. V. Vasilakos, “A survey of security and privacy challenges in cloud computing: solutions and future directions,” Journal of Computing Science and Engineering, vol. 9, no. 3, pp. 119–133, 2015.

[12] Ahnlab Security Issue,How to Attack Us?, Ransomware ‘Crypto- Locker’ThatHit South Korea, 2015 (Korean), http://www.ahnlab.com/kr/site/securityinfo/secunews/secuNewsView.do?menudist=2&seq=23630.

[13] Ahnlab Security Report, “The latest mobile ransomware app and countermeasures,” vol. 65, July 2015 (Korean), http://www.ahnlab.com/kr/site/securityinfo/asec/asecView.do?groupCode=VNI001&seq=23834.

[14] Ahnlab ASEC blog, “The ransomware that impersonate,” NSB (National Security Bureau), Febuary 2015 (Korean), http://asec.ahnlab.com/1025.

[15] M. E.Wagner, Behavior Oriented Detection of Malicious Code at Run-Time, Florida Institute of Technology, 2004.

[16] P. Szor, the Art of Computer Virus Research and Defense, Symantec Press; Addison-Wesley Professional, 2005.

[17] J. Aycock, Computer Viruses and Malware, vol. 22, Springer Science & Business Media, 2006.

[18] D. Anderson, T. Frivold, and A. Valdes, “Next-generation intrusion detection expert system (NIDES): a summary,” Tech. Rep. SRI-CSL-95-07, SRI International, Computer Science Laboratory, 1995.

[19] “System Permissions,” API Guide, Android Developers, http://developer.android.com/intl/ko/guide/topics/security/permissions.html.

[20]virustotal, https://www.virustotal.com/en-gb/.