IJCSE International Journal of Computer Sciences and Engineering Open Access

Review Paper Vol.-6, Issue-5, May 2018 E-ISSN: 2347-2693

Ransomware: Detection And Prevention

Annu[1*], Monika Poriye[2], Vinod Kumar[3]

[1]Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India
[2]Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India
[3]Department of Computer Science and Applications, Kurukshetra University, Kurukshetra, India

Corresponding Author: annuraj789@gmail.com,

Available online at: www.ijcseonline.org

Accepted: 23/May/2018, Published: 31/May/2018

Abstract— Now a day everyone wants data to be secure from malicious users. What happens when data is hijacked? Ransomware hijacks user data on different OS like the window, Android, Mac etc. Ransomware is most popular and destructive malware in the cyber world. It can be dispersed via affected spam emails, infected application, infected external storage device and negotiated sites. Ransomware blocks system in a different way. One way to lock the system and another is (crypto ransomware which) to encrypt the data. After encrypting/locking the system data ransom money will be demanded and time is allotted by the hacker for decryption/unlocking. The main goal of Ransomware is always force to pay money not like other types of attack. Ransom money is in the form of bitcoin because it is harder to trace. There are some tools are invented to prevent system from attack like heldroid, honeypot, and wannakiwi etc. This paper focuses on ransomware prevention technique which helps you to detect and remove ransomware from the system.

Keywords— encryption, decryption, malware, hijack, ransom, bitcoin, EternalBlue, IDS.

I. INTRODUCTION

Ransomware is destructive malware on the computer network and it is formed by two word 'Ransom' and 'ware'. Here 'Ransom' stands for an oversized amount of money is demanded in exchange of data which is hijacked by the hacker and 'Ware' means conscious so that ransomware means money is demanded by the hacker to release of data [1]. The computer affected by Ransomware is locked after the system install or open files which have this malware. In the beginning it is installs into the system and then start scanning all the storage except external storage (this was scanned after all system has been locked). The main aim of ransomware is always nearly monetary, the targeted system is expressed that an exploit has occurred and Instructions are given for how to recover from the attack. Payment is informed of bitcoin so that hackers are not exposed. There is usually a time limit assign an alert message to a user that after the time limit has expired their data are deleted permanently [2].There is a loss of data if ransom amount is not paid and loss of money if ransom paid. Ransomware not only affect local storage, but also affects external storage, Server, NAS (network attached storage) which was connected to the system [3].

First time Ransomware come into existence in 1989 named AIDS Trojan (also known as pc cyborg) which was developed by Dr. Joseph Popp and spread via floppy disk of size 5.25 inch. Original ransomware holder floppy disk is attached to the system than it copies all into the floppy disk and return autoexec.bat files on that place. Whenever the system is booted this will be tracked. When boot score is 90 then this malware (pc cyborg) starts its working and encrypts that drive completely, after that display ransom pay message on system screen to decrypt files [2].

The authors elaborate a brief introduction about the common type of ransomware attack and discourse about trending prevention and detection techniques. Cyber security Foresee ransomware compensation will charge the world $5 billion in 2017 and rise to $11 billion in 2019.Those are up formed just $325 million in 2015.The regularity of attacks is growing loss of money [5].

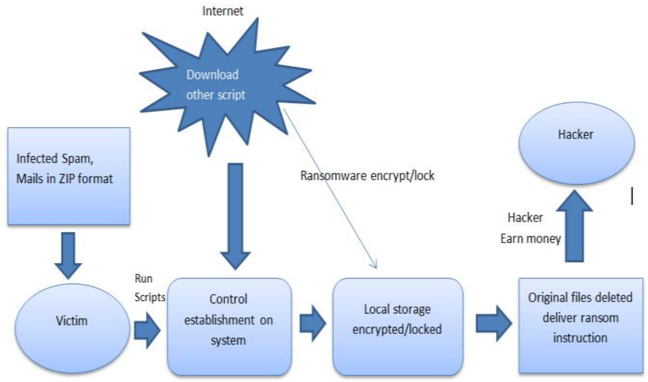
The detection of fraud generated by Ransomware can be removed by using Anti-ransomware tools like AVAST software, AVG technology, ESET, Wannakiwi, BitDefender and Trend Micro lock screen ransomware tools etc. In which some tools are capable to decrypt only some variant of ransomware [6]. The ransomware detection is sophisticated because of morphic nature. There are not any patterns are present for detecting ransomware. Sometime this attack will be detected by using some extension like .locky, .wcry,

.encrypted,and .wnry etc. These different extensions depend on its variant [7].

A.) Origin of Ransomware infection:

Ransomware generally infect system through Email and compromised site because Emails are most commonly used mechanism for information exchange and compromised sites contain malicious advertisement that divert control to attackers website [8].Once the Ransomware is downloaded by victim unwarily. Then it will start scanning and encrypting files. Ransomware has been detected when any abnormal action like file renames and creation of the new file with the same extension made in window OS. The following steps define all working of ransomware:

- Ransomware entered into system form infected spam mail or via the Negotiated site in Zip format.
- Install Scripts and establish control on the system.
- Download another script from internet using list of domain and C&C server (handled by cyber criminals) and change registry key for making permanent.
- Scanning all local storage system and start encrypting files.
- It encrypts all files, entire hard disk including cloud accounts (Google Drive, Dropbox).
- After encrypts or lock original file are deleted from the system and deliver a ransom alert on system window.
- The encryption key is deleted from the system and sends that key to the system attacker [9].


Internet
Download other script
Infected Spam, Mails in ZIP format
Ransomware encrypt/lock
Hacker
Hacker Earn money
Run Scripts
Victim
Control establishment on system
Local storage encrypted/locked
Original files deleted deliver ransom instruction

[10]Figure 1 Ransomware process.

Now it totally depends on victim whether to pay money or not to pay it. If the victim decides not pay money to hacker then they will not regain access to encrypted data [2]. There is no assurance that after payment you gain full access to your data or attackers not demand more money[11].This describe about how exploited process are interacts with file system when system under ransomware attack. It is usually harms to the files like PDF, Word, and Excel etc. which have user's important information.

Rest of the paper are organized in a way: Section I contains Introduction and origin of infection, Section II discuss about Common variant of ransomware, Section III defined Failed ransomware attack, Section IV describe Detection Technique, Section V disclose about Prevention Technique, Section VI concludes the study of paper with Future Scope.

II. COMMON VARIANT OF RANSOMWARE:

There are two common types of Ransomware:

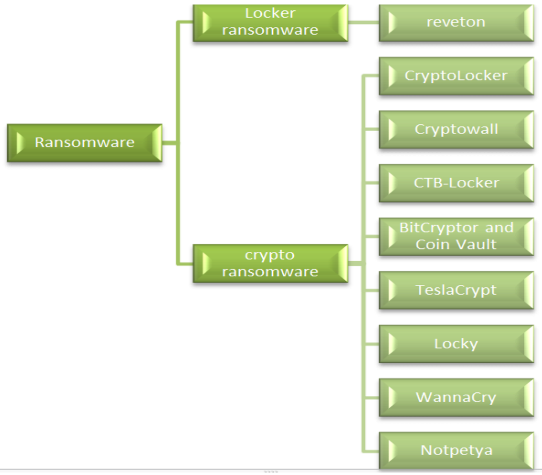
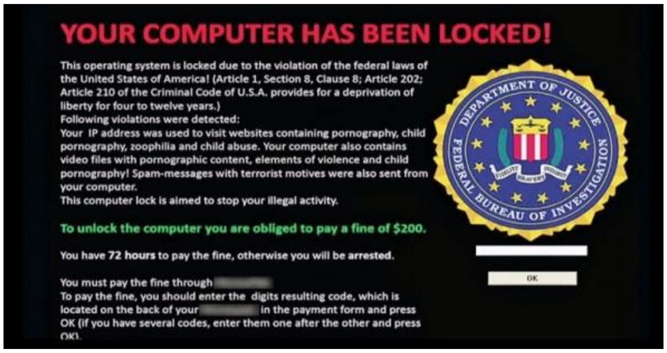


Figure 2.Varient of Ransomware

1. Locker Ransomware:

Locker Ransomware is those which lock system until a ransom is paid to regain access to the system. The system is in that state which allows the user to interface with ransomware and pay it. This type of attack mostly impact on wearable device and IoT (internet of things), results of that connected device are possibly in danger [1, 2, 12]



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).

[13]Figure3. Locker Ransomware

- *Reveton:*

Reveton ransomware has appeared in last of 2012. This type of ransomware mainly circulates itself using Pornography sites. It locked personal system of a user's by controlling from logging in and show an alert of display advising [14].

2. *Crypto Ransomware:*

Crypto Ransomware is those which encrypt all files of local storage using vigorous cryptography. When all files are encrypted this conveys a message to users to pay ransom for freeing data [2, 15].There are some most popular Crypto ransomware types:

- *CryptoLocker:*

CryptoLocker first appears in 2013.It follows the different path for encrypting files by creating a random symmetric key for each file. After that for decryption public asymmetric key is required. If payment is not made within given time limit then the symmetric key will be deleted and if you try to remove CryptoLocker from the system then the asymmetric key is deleted[14,16].

CryptoLocker is disappeared in 2014 when it was taken down by U.S Department of Justice Operation [2, 14, and 16].

- *CryptoWall:*

CryptoWall will appear after CryptoLocker in 2014.CryptoWall are present in different versions like CryptoDefence, CryptoBit, CryptoWall2.0, 3.0, and 4.0. In which Hacker suggest free single file decryption for a single file to justify to a victim that they keep decryption key[11,14].

CryptoWall version 4.0 comes in 2015.In which filename of file are encrypted to make it difficult to detect encrypted files; this is innovation of CryptoWall Version 4.0 [14, 16, and 17].

- *CTB-Locker:*

CTB-Locker one more name is Critorni. It is a greatly complex type of Ransomware.CTB made by three different words that are Curve, TOR, and Bitcoin. In CTB-Locker attacker location are not declared. This is as much as closer to CryptoWall. Both needs TOR browser for making payment and for communication, protocols is changed from HTTP (plaintext) to HTTPS (encrypted) [2].

- *BitCryptor and CoinVault:*

BitCryptor and CoinVault have infected thousands of system before the author was jailed in 2015. After inspection Kaspersky gain of 14,000 decryption keys used to decrypt user data. A tool made by Kaspersky for a release of data by BitCryptor and CoinVault [14].

- *TeslaCrypt:*

TeslaCrypt is released in 2015 and for encryption AES algorithm is used .Which was dispersed through exploited kit Angler this especially attack Adobe weaknesses. Taking advantages of flaws, In Microsoft temp folder TeslaCrypt installs itself.

In 2016, attacker release master decryption key and it is spread by ESET to recover encrypted data and stop distribution [16].

- *Locky:*

Locky is first time emerging in 2016, and it is a complex type of ransomware which affects system through malicious Microsoft office attachment to emails. After open office file prompt appears that indirectly allow malware file run. Once encryption process is completed, ransom message is displayed.TOR browser is downloaded for ransom pay [16].

- *WannaCry:*

WannaCry ransomware is most popular nowadays and it behaves like the worm. It infects 100,000 systems in May 2017 by taking benefit of unpatched Microsoft windows (MS17-010). It spread with help of EternalBlue exploit, which was developed by NSA (National Security Agency) and discloses by Shadow Brokers group on April 14, 2017, earlier month to the attack. Weakness in window implementation of SMB (Server Message Block).Microsoft patched system on March 13, 2017 month before the WannaCry attack but some system stays unpatched and formed attack. Microsoft discloses emergency patches and found kill switch that stops propagating WannaCry further [18].

Wannacry ransomware software is those which block access to a system and taking ownership of data using encryption until pay ransom to take decryption key [19].

- *Notpetya:*

Notpetya was encountered on June 27, 2017. Master Boot record (MBR) of window's system is modifies by this and causing system crash. When system reboots it presents ransom prompt demanding money. This was also spread via EternalBlue exploit [20].

In reaction to incrementing a count of ransomware attacks, users are guided to generate the backup of their important data. Absolutely, having a genuine data backup policy decrease of infected with ransomware [5].To prevent form WannaCry and Notpetya attack you have to be updating your system regularly.

III. FAILED RANSOMWARE ATTACK:

There are some failed ransomware attacks which are detected by researcher because they found decryption key for decrypts data [21].

- *Hitler ransomware:*

Hitler ransomware are those which were invented by AVG malware analyst Jokub Kroustek. It display Hitler on lock screen and convey that files are encrypted. Then shows to put cash code for 25 Euro Vodafone card for payment to decrypt files. This malware will not decrypt files instead of that this will remove file extension in different directory and also show one hour time duration. After one hour system dumped and reboot will delete all file [22].

- *Fake window 10 lock screen:*

Fake window 10 lock screen tell user that license has been invalid, and hidden decryption key inside code. When Researcher uses Reverse engineering the code, they originate decryption key (8716098676542789) in simple text [21].

- **'***PowerWare' and 'Bart':*

Another name of 'PowerWare' is 'PoshCoder'. Researcher found some fault in malicious software so that this will be broken. Bart have week encryption algorithm so decryption tool are easily invented by company [23].

- *Chimera ransomware:*

Chimera ransomware are encrypting file in compromised system. Decryption key are also created by Rival ransomware gang named Janus [21].

IV. DETECTION TECHNIQUE:

Now a day's healthcare, government, university, Manufacturing, technology, and banking sector etc. like everywhere security of data is the main concern [6]. Everyone is maintaining our data in digital form like on a cloud or on a hard disk. So cyber security is required to secure data from an intruder. The present portion deals with the experiment made by the researcher in the area of the variant of ransomware and its detection techniques.

Chris Moore 2016, in which author creates a honeypot to identify ransomware activity. There are two select point options in which Microsoft File Server Resource manager using File Screening service and for controlling the security logs of window EventSentry are used. The research developed a staged response to attack to the system along with thresholds when there were triggered. There were no agreements that malware would attempt to occupy these areas and the disadvantage of honeypot technique is restricted system view. In which a message from attack free honeypot is not specifying that this will not targeted other area [7].

S. Zanero, F. M. B 2015, Author defines technique that exposes ransomware pattern. Heldroid is a fast, powerful and fully automatic way that detectsfamiliar and unfamiliar security software. The author said that this approach is using 'Bulding block' which naturally used for making mobile ransomware application. If any application is encrypting or locking device then this will work in a generic way without user interaction [24].

Monika, Pavol Zavarsky et.al 2016, Author analyzing seventeen windows and eight Android ransomware variant. From that author finalized that all variant are behaved in an analogous fashion but using the dissimilar payload. Results of this experiments revel that possibilities of ransomware attack are decreases when permission requests are observed [25].

Muhammet Baykara and Baran Sekin 2018, the author presents Novel approach to design safe zone system. When data is encrypted by the attacker and reestablish coded data only possible when a user has a particular key to decrypt data. Ransom money is demanded in return for release of data and this is not sure that after monetary more payment are not demanded. The author creates a method to overcome this problem and to decrease data damage. In that way to do, an area created is called Safe Zone and to secure from other nasty software transfer essential data in that particular area [11].

Tianliang Lu and Lu Zhang et al. 2017,Author motivated by a biological immune system, Introduce detection method situated on V-detector negative selection algorithm with mutation optimization. The author states that behaviour of ransomware is derived by dynamic analysis as per hard disk reading and writing, file encryption and deletion. For upgrade accuracy and efficiency boost detector's space distribution via replica and mutation. This will increase coverage of non-self-space and decrease overlapping between detectors [26].

V. PREVENTION TECHNIQUE:

There are some researcher article and research work for preventing from ransomware attacks. For preventing user private data to be discovered to intruder user should take backup data online as well as offline. Avoid all spam e mails and turnoff java and javascript. The user should up-to-date all software patches and blocks so system faults are not exposed [27].

The research article by Saggeun Song et.al 2016, Focuses on a new effective method to prevent attacks of advanced ransomware on android platform. The previous system is exposed to newly advanced pattern ransomware because they only sense previous pattern ransomware. The proposed method diminishes harms affected by an attack with reform or creating new patterns. This process needs information of file input/output events and processor status regarding ransomware behaviour those are not like previous that uses information of ransomware. This technique reduces destruction of data because it is affixed in the open source of Android source file that why author use it in Android smart phone [28].

Amin Kharaaz and W. Robertson, Author describes various aspects. There is 1359 sample are found 2006 to 2014 from different ransomware generations. Author advice that controls over advanced ransomware is not as complicated as this will be disclosed previously by other researchers. A Convenient observation on file system activities advises that Master File table (MFT) in the NTFS should be safe from this. Author assumes that this process is feasible for detection and prevention from Zero day ransomware attacks [29].

S. Mahmudha Fasheem et al.2017, this paper proposes ATPG (automatic test packet generation) model which was used for compose a minimal set of test packet on the network. The test packet is sent infrequently over a network and detects failures alert a definite procedure to localize the fault. It originates a device-independent model and read router configuration so that prevent user from arriving ransomware attack in the system [16].

Daniel Gonzalez and Thaier Hayajneh, Focuses of this research are to help from preventing next victim by using the method of infection a technology behind it. In which examine types of crypto-ransomware, different payload method of infection, nature, and approaches how the attack is carried out [2].

Azad Ali, The main aim of this paper is to share previous research finding of ransomware, describe the most used format by researcher and specialist clarify personal experience about ransomware [1].Another author evaluating the file action process of the Operating system and implementation an access control pattern on file action process is the new way to identify/block ransomware [30].

VI. CONCLUSION & FUTURE SCOPE:

Ransomware variants are increasing day by day. They usually target user wise (Average user, Business, Emergency service, Banking) and system wise (Personal Computer, Mobile Device, server).The main aim of ransomware is to take currency from the victim. Detecting this attack researcher used various techniques like V-detector negative selection algorithm, creating a safe zone to secure data, heldroid, honeypot, Cryptolock, and sand-box etc. There is distinct model invented by the researcher to protect from malicious activities like ATPG model collect a nominal set of test packet, protect MFT file, patched software, backup important data regularly and ignore spam emails.

Researchers discuss some fact about to secure system from attack and set some parameters to save data from attack in future. Just because of Ransomware are Malware and Trojan type attack so Anomaly-based IDS may be used in future for detecting abnormal behaviour of the network. Some data mining technique is used for detecting the activity of attack.

REFERENCES

[1] Azad Ali, "*Ransomware: A research and a personal case study of dealing with this Nasty Malware*" Issues in Information Science +Information Technology, Vol. 14, 2017.

[2] Daniel Gonzalez and Thaier Hayajneh, "*Detection and prevention of Crypto-ransomware*," IEEE, 978-1-5386-1104-3/17, 2017.

[3] Timothy Gallo, Allan Liska, "Ransomware" published by O'Reilly Media, Inc., ISBN: 9781491967874,Release Date: December 2016.

[4] "*Ransomware holding your data hostage*," Deloitte Development Lcc, issue date: August 12, 2016, Serial: W-TS-EN-16-00734.

[5] Amin Kharraz "*Techniques and Solutions for Addressing ransomware Attacks*", College of Computer and Information Science Northeastern University, July 2017.

[6] Nadeem Shah and Mohammed Farik, "*Ransomware-Threats, Vulnerabilities And Recommendation*", International Journal Of Scientific & Technology Research(IJSTR), ISSN:2277-8616, Vol. 6, Issue.06 June, 2017.

[7] Chris Moore, "*Detecting ransomware with Honeypot technique*", CyberSecurity and Cyberforensic conference IEEE,978-1-5090-2657-9/16,2016.

[8] Lam Zhanhui and Nor Azlina Adb Rahman,"*A Review on ransomware Trend of Attacks and Prevention*", International Journal of Applied Engineering Research, ISSN:0973-4562, Vol. 12, No. 16, pp.6201-6210, 2017.

[9] Sherya Chadha and Utham Kumar , "*Ransomware : Let's Fight Back !*", International Conference on Computing, Communication and Automation (ICCCA2017).ISBN:978-1-5090-6471-7/17 IEEE 2017.

[10] Sonu B. Surati, Ghanshyam I. Prajapti , " *A Review on Ransomware detection and prevention*" International journal of research and Scientific Innovation, Vol. 5, Serial no 9 Sept, 2017 ISSN:2321-2705

[11] Muhammet Baykara and Baran Sekin, "*A Novel Approach to Ransomware: Designing a Safe Zone System*", ISBN: 978-1-5386-3449-3, 2018 IEEE.

[12] Kevin Savage, Peter Coorgen, and Hon Lau "*The evolution of Ransomware*", Security Response, Symantec, version 1.0 August 6, 2015.

[13] Adam Alessandrini "RANSOMWARE Hostage Rescue Manual" published by Knownbe4, Tel: 855-KNOWBE4 (566-9234)

[14] Dr.P.B.Pathak, "A Dangerous Trend of Cybercrime: Ransomware Growing Challenge", International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), ISSN: 2278-1323,Volume 5, Issue 2, February 2016.

[15] Nolen Scaife,Henry Carter,Patrick Traynor and Kevin R.B. Butler, "*CryptoLock (and Drop It):Stopping Ransomware Attacks on User Data* ", ISSN NO-1063-6927,IEEE 2016.

[16] S.Mahmudha Fasheem, P.Kanimozhi, and B.AkoraMurthy,"*Detection and Avoidance of Ransomware*", International Journal of Engineering Development and Research, Volume 5, Issue 1, ISSN: 2321-9939, 2017.

[17] K. Cabaj and W. Mazurczyk, "*Using Software-Defined Networking for ransomware mitigation: The case of cryptoWall*", ISSN: 0890-8044, Vol. 30, No. 6, pp. 14-20, Dec 2016, IEEE.

[18] K.V.G.N. Naidu and P. Sireesha "*A Study on WannaCry Ransomware Attack* ", International Journal of recent innovation in engineering and Research.e-ISSN:2456-2084,2017.

[19] Savita Mohurle and manisha Patil, "*A brief study of Wannacry Threat: Ransomware Attack 2017*", International Journal of advanced Research in Computer Science, ISSN No: 0976-5697, Vol. 8, No. 5, May 2017.

[20] The computer emergency Response team Mauritius (CERT-MU), "*The Petya Cyber-attack*", Whitepaper .June 2017.

[21] Segun I. Popoola, Ujioghosa B. Iyekekpolo, Samuel O. Ojewande, Faith O. Sweerwilliams, Samuel N. John, and Aderemi A. Atayero, "*Ransomware: Current Trend, challenges, and Research Directions*", World congress on Engineering and Computer Science, Vol.1, ISSN. 2078-0958, ISBN: 978-988-14047-5-6, Oct 2017, WCECS.

[22] POPOOLA, Segun Isaiah, "Ransomware :Most Recent Threat to Computer Network Security", 2017 CU EIE Seminar on Computer Network Security, Ota, Covenant University, DOI:10.13140/RG.2.2.31592.67841.

[23] Lucian Constantin, "*Researchers Release Free Decryption Tools for Powerware and Bart Ransomware*", PC Word from IDG, July 22, 2016.

[24] S. Zanero and F. M. B, "*HELDROID: Dissecting and Detecting Mobile Ransomware* ", pp. 382-404, 2015

[25] Monika, Pavol Zavarsky and Dale Lindskog,"*Experimental Analysis of Ransomware on Windows and Android Platforms: Evolution and Characterization*", International Workshop on Future Information Security, Privacy & Forensics for Complex Systems, ISSN. 1877-0509, doi: 10.1016,2016 ELSEVIER.

[26] Tianliang Lu, Lu Zhang, Shunye Wang and Qi Gong,"*Ransomware Detection Based on V-detector Negative Selection Algorithm*", ISBN: 978-1-5386-3016-7, IEEE 2017.

[27] A. K Maurya, N. Kumar, A. Agrawal and R. A. Khan, "*Ransomware: Evolution, Target and Safety Measures*", International journal of Computer Science and Engineering, Vol.6, Issue.1,E-ISSN:2347-2693, 2017.

[28] Sanggeun Song, Bongjoon Kim, and Sangjun Lee,Research Article "*The Effective ransomware prevention Technique using process Monitoring on Android platform*" Vol no 2016, Article Id.2946735 Hindawi Publishing Corporation Mobile Information Systems.

[29] Amin Kharaaz, W. Robertson, D. Balzarotti, L. Bilge, and E. kirda,"*Cutting the Gordian knot: A look under the hood of ransomware attacks*", 12th conference on detection of Intrusion and malware &vulnerability Assessment (DIMVA 2015), July 9-10, 2015, Milan Italy.

[30] Dae-Youb Kim, Geun-Yeong Choi, and Ji-Hoon Lee, "*White List-based Ransomware Real-time Detection and Prevention for User Device Protection*", ISSN: 978-1-5386-3025-9-18,2018 IEEE.

Authors Profile

Miss. Annu pursed B.tech form MDU University of Rohtak, in 2015 and Diploma in Computer Scinece and Engineering form HSBTE, Panchkula, in 2012. I am currently pursuing M.tech from Kurukshetra University, Kurukshetra Department of Computer Science and Applications.

Mrs Monika Poriye is currently pursuing Ph.D. and currently working as Assistant Professor in Department of Computer Science and Applications, Kurukshetra University, Kurukshetra.Her main research work focuses on Security in wireless Sensor Netwrok.