iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 6 **Issue:** IV **Month of publication:** April 2018

DOI: http://doi.org/10.22214/ijraset.2018.4631

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 6.887
Volume 6 Issue IV, April 2018- Available at www.ijraset.com

Using Software- Defined networking for Ransomware Mitigation: A case of Cryptowall

Shirsat Harshad Jayavant[1], Pawar Vishal Waman[2], Walnekar Priyanka Deepak[3], Renuka Deshpande[4]
[1, 2, 3]*Undergraduate Student, Department of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Dombivli, Maharashtra, India*
[4]*Assistant Professor, Department of Computer Engineering, Shivajirao S. Jondhale College of Engineering, Dombivli, Maharashtra, India*

Abstract: The making of crypto-ransomware` affected the world. A crypto-ransomware locks documents by encrypting them and requests for payment in turn for decryption key. Discovery of ransomware relies upon how rapidly and deliberately the framework logs can be dug to scan for pernicious exercises and stop assault. We set up a domain to gather action logs of ransomware tests. We found a typical behavioural example of various ransomware as they utilize distinctive algorithms. We could distinguish ransomware based on pattern recognition test. We at that point take note of all the samples inside various ransomware families which can be utilized for identifying ransomware family to build insight about risk and danger profile of a given target.

Keywords: Ransomware, security, attack, encryption, detection.

I. INTRODUCTION

Ransomware is a kind of noxious code from crypto virology that debilitates to distribute the casualty's information or never-endingly square access to it unless a payment is paid. While some straightforward ransomware may secure the framework a way which isn't troublesome for an educated individual to turn around, further developed malware utilizes a strategy called encryption, in which it encrypts the casualty's data, making them impossible to use it, and requests a payment in turn for decryption key for decrypting the files. Ransomware assaults are normally done utilizing a Trojan that is veiled as an authentic document that the client is deceived into downloading or opening when it touches base as an email connection. In any case, one prominent illustration, the "WannaCry worm", exchanged consequently between PCs without client connection.

II. ORIGIN OF RESEARCH PROBLEM

With increase in cyber-crimes, attacker came with better and more efficient ways to exploit the organisations or individual victims. Ransomware is a way to ask for ransom payment for giving the victim their precious data back. There have been a lot of ransomware attacks in India itself. Once the attacks made the ATM services all over India to be closed for several days, so we decided to contribute our part to the anti-ransomware research with our project.

III.OBJECTIVE OF WORK

Our objective of work is to secure the systems from ransomwares attacks that are happening all over the world. Our application will make sure to detect the ransomware and to take the necessary actions needed to prevent it from locking the files from encrypting. When a ransomware is executed then there is a sudden spike in RAM and Processor usage, our system will also check monitor for such uneven spikes in usage.

IV.LITERATURE SURVEY

A. Francesco Mercaldo, Vittoria Nardone, Antonella Santone, [1] "Ransomware Inside Out".

Android is at present the most generally utilized versatile condition. This pattern urges malware journalists to create specific assaults focusing on this stage with dangers intended to secretively gather information or financially blackmail casualties, the supposed ransomware. In this paper we utilize formal strategies, specifically display checking, to naturally dismember ransomware tests. Beginning from manual review of few examples, we define an arrangement of lead with a specific end goal to check whether the practices we find are illustrative of ransomware functionalities.

B. Krzysztof Cabaj and Wojciech Mazurczyk, [2] "Utilizing Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall".

Right now, unique types of ransomware are progressively undermining Internet clients. Present day ransomware encodes critical client information, and it is just conceivable to recuperate it once a payment has been paid. In this article we demonstrate how programming characterized systems administration can be used to enhance ransomware relief. In more detail, we investigate the conduct of prevalent ransomware — CryptoWall — and, in light of this information, propose two constant alleviation strategies. At that point we portray the plan of a SDNbased framework, actualized utilizing OpenFlow, that encourages a convenient response to this danger, and is a vital factor on account of crypto ransomware. What is critical is that such a plan does not essentially influence general system execution. Test comes about affirm that the proposed approach is attainable and effective.

C. Kanwalinderjit K Gagneja, [3] "Knowing the Ransomware and Building Defense Against it – Specific to HealthCare Institutes".

In the human services field the patient information is extremely touchy. So the healing centers ought to have some intend to ensure it also. Be that as it may, in only us various clinics are assaulted by cybercriminals through ransomware malwares to make oodles of cash. The healing centers ought to be readied when given such circumstance where they need to pay cash to recover their information. Presently the inquiry emerges would it be advisable for them to pay the payment? Now and again a healing facility might not have a decision, if their reinforcement system is broken. This paper presents different advances that ransomware takes after to scramble the imperative documents on the casualties arrange, at that point requests cash and once it gets the cash, at that point discharges the information records. The paper likewise introduces different advances those could be taken after to ensure against such assaults.

D. Mattias Wecksten, Jan Frick, Andreas Sjostrom, Eric Jarpe, [4] "A Novel Method for Recovery from Crypto Ransomware Infections".

Blackmail utilizing computerized stages is an expanding type of wrongdoing. A generally observed issue is coercion as a contamination of a Crypto Ransomware that encodes the documents of the objective and requests a payoff to recoup the bolted information. By dissecting the four most regular Crypto Ransomwares, at composing, a reasonable powerlessness is recognized; all diseases depend on apparatuses accessible on the objective framework to have the capacity to keep a straightforward recuperation after the assault has been identified. By renaming the framework device that handles shadow duplicates it is conceivable to recoup from contaminations from every one of the four of the most widely recognized Crypto Ransomwares. The arrangement is bundled in a solitary, simple to utilize content.

E. Text FMarzieh Ahmadzadeh, Sajad Homayoun, Ali Dehghantanha, Sattar Hashemi, Raouf Khayami, [5] "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence".

Rise of crypto-ransomware has fundamentally changed the digital risk scene. A crypto ransomware evacuates information caretaker access by scrambling profitable information on casualties' PCs and solicitations a payment instalment to reinstantiate overseer access by unscrambling information. Opportune identification of ransomware especially relies upon how rapidly and precisely framework logs can be mined to chase variations from the norm and stop the abhorrence. In this paper we first setup a domain to gather movement logs of 517 Locky ransomware tests, 535 Cerber ransomware tests and 572 examples of TeslaCrypt ransomware. We use Sequential Pattern Mining to discover Maximal Frequent Patterns (MFP) of exercises inside various ransomware families as applicant highlights for grouping utilizing J48, Random Forest, Bagging and MLP calculations. We could accomplish 99% precision in identifying ransomware examples from goodware tests and 96.5% exactness in recognizing group of a given ransomware test. Our outcomes show handiness and common sense of applying design mining procedures in identification of good highlights for ransomware chasing. Also, we demonstrated presence of particular continuous examples inside various ransomware families which can be utilized for recognizable proof of a ransomware test family to build knowledge about danger performers and risk profile of a given target of Entire Document.

V. BACKGROUND OVERVIEW

A. Existing System

'Ransomware' is a kind of malware that endeavors to blackmail cash from a PC client by tainting and taking control of the casualty's machine, or the records or archives put away on it. Ordinarily, the ransomware will either 'bolt' the PC to avoid ordinary use or encode the archives and records on it to forestall access to the spared information. The decryption key can be broken utilizing brute

force and such other secret word breaking attacks, yet it will take a very long time to locate the right blend, as the key is long and complex. Aggressor often requests for emancipate cash in untraceable advanced monetary standards, for example, Bitcoin. Aggressors can't be trusted even after casualty pays the payment, its exceedingly conceivable that the assailant will request more in future.

B. Disadvantages

Framework isn't secure, and information isn't protected. All records on framework can get encoded after a ransomware is executed on a framework. Aggressor can request emancipate installment which leaves negative effect on organization's picture and in addition the budgetary status. Likewise, in the wake of paying payoff no one can guarantee if assailant will give a decryption key or interest for additional.

C. Proposed System

We will utilize Kali Linux to code and convey the ransomware on target frameworks. After focusing on a framework, we at that point contemplate the assault and endeavor to locate a conceivable arrangement and make a rundown of things that will be done to keep the ransomware assault. We will think about the assault's conduct and figure out how to ensure the administrations that are utilized by this ransomware. This framework will recognize the assault, till the assault is been distinguished a few documents may get encoded yet once the assault is being identified it will keep whatever is left of the framework from encryption. We will give a free module which must be introduced on the framework and it will keep the framework from ransomware assaults.

VI. INCIDENT RESPONSE DIAGRAM

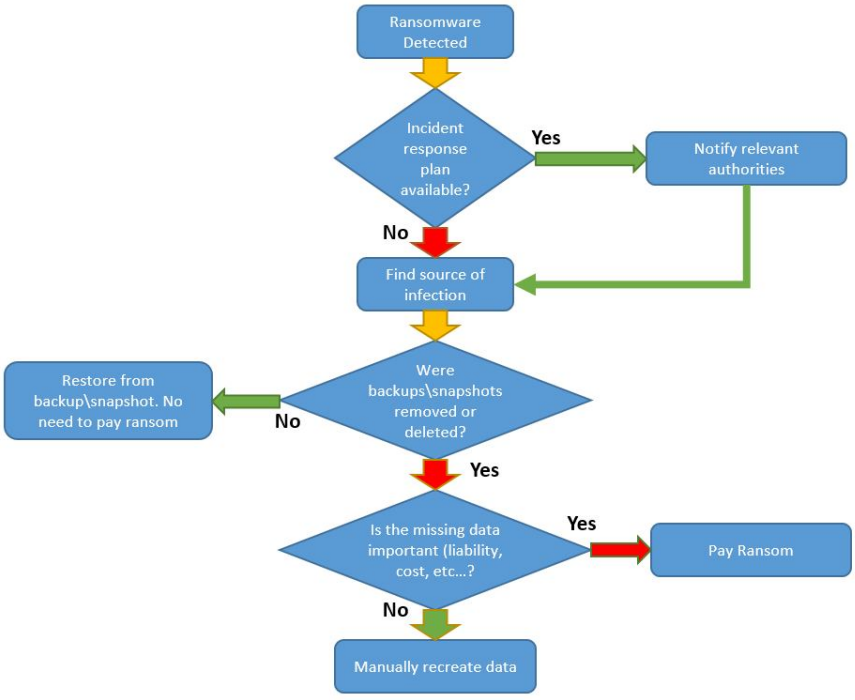


Fig.1: Incident response diagram when ransomware attack occurs

A. The following are the brief explanations of the working of incident response plan to a ransomware attack

When a ransomware is detected, it checks for an incident response plan, if it is available then it notifies the relevant authorities who investigates it and find the source of infection. If there is no incident response plan available, then it should directly find the source of infection. After this step, it checks if there were backups of the removed or deleted data. If there is a backup it would restore it and not pay the ransom amount. If there are no backups, we must see if the lost files are that important. If they are very important then we can manually try to recreate similar data, and if we can't recreate it and it is also important then we must pay the ransom to get the key and decrypt the system to usable state. This is the normal procedure if you don't have our program sunning, while these things can be avoided if you install our program.

B. Algorithms used by Ransomwares

1) Symmetric-key algorithm- Computations for cryptography that use the same cryptographic keys for both encryption of plaintext and deciphering of ciphertext. The keys may be undefined or there may be a clear change to go between the two keys

2) RSA algorithm- RSA gets its security from the trouble of calculating substantial whole numbers that are the result of two expansive prime numbers. Increasing these two numbers is simple yet deciding the first prime numbers from the aggregate - calculating - is viewed as infeasible because of the time it would take notwithstanding utilizing the present super PCs.

3) AES algorithm- Each figure encrypts and decrypts information in squares of 128 bits utilizing cryptographic keys of 128-, 192- and 256-bits, separately.

4) Blowfish algorithm- Blowfish is a symmetric piece figure that can be utilized as a drop-in swap for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it perfect for both local and exportable utilize.

There are many such encryption algorithms used in ransomwares to encrypt the files on victim system.

VII. REQUIREMENTS

A. Software Requirements

1) *Operating system:* Kali Linux, Ubuntu, Windows 7, Windows 10.

2) *Tools used:* Bash, text editor

B. Hardware Requirements

1) *Processor:* Pentium 4 equivalent or higher

2) *Motherboard:* Any

3) *RAM:* Minimum 2 GB

4) Hard Disk: 80 GB

C. Functional Requirements

1) Program will detect the execution of a ransomware code based on pattern.

2) After execution and detection, the processes and services used by ransomware will be stopped/paused to avoid further damage.

3) System will be functional with only a few files encrypted until the detection.

D. Non-Functional Requirements

1) An Anti-virus software installed on system.

2) System with Internet connection.

3) Administrative privileges on the system.

VIII. METHODOLOGY

The following will be development steps so as to achieve the working Model of the above proposed system…

1) Defining the Problem,

2) Understanding the Need & Usability in industry and society (Market Analysis),

3) Developing Block Diagram

4) Studying ransomware samples,

5) Listing the behaviour of different samples,

6) Creating set of rules to be applied on system,

7) Developing Flowchart for the entire working,

8) Writing actual Software Program,

9) Compilation,

10) Testing and Debugging,

11) Finally Running the system and

12) Updating.

IX. FEATURES

The Following are the prominent features of the above discussed system:

A. It will block the execution of the ransomware.

B. It will monitor the file system for abnormal patterns for detection of ransomware

C. It will safeguard the system from getting encrypted by attackers.
D. The monitoring system keeps scanning files constantly making older systems a bit slow.

X. SCOPE AND APPLICATIONS

A. Scope of Our Project Are

1) Our project will safeguard users from ransomwares for free.
2) Once you install it on your system, it will even remove ransomware after you try to execute the program.

B. Applications of Our Project Are

1) It can be used at schools, and such other organizations,
2) It can also be installed on ATM systems to safeguard system from ransomware attacks.

XI. FUTURE SCOPE

There is always chance to improve the any system as research & development is an endless process. Our system is no exception to this phenomenon. The following improvements can be done:

1) We will keep updating more behavioural patterns as we study,
2) Also, we will add some features for organisations where they can monitor all system's status from one server.

XII. CONCLUSIONS

By the realization of the above proposed system one can understand how security is a necessity and it is very important to safeguard ourselves from the hackers who might be targeting our valuable data in the virtual world. Data might be some confidential organizational data or someone's personal files. It is of utmost priority to keep our systems away from Ransomware attacks and such other attacks.

XIII. ACKNOWLEDGMENT

We sincerely wish to thank our project guide Prof. Renuka Deshpande for her ever encouraging and inspiring guidance helped us to make our project a success. Our project guide makes us endure with her expert guidance, kind advice and timely motivation which helped us to determine about our project.

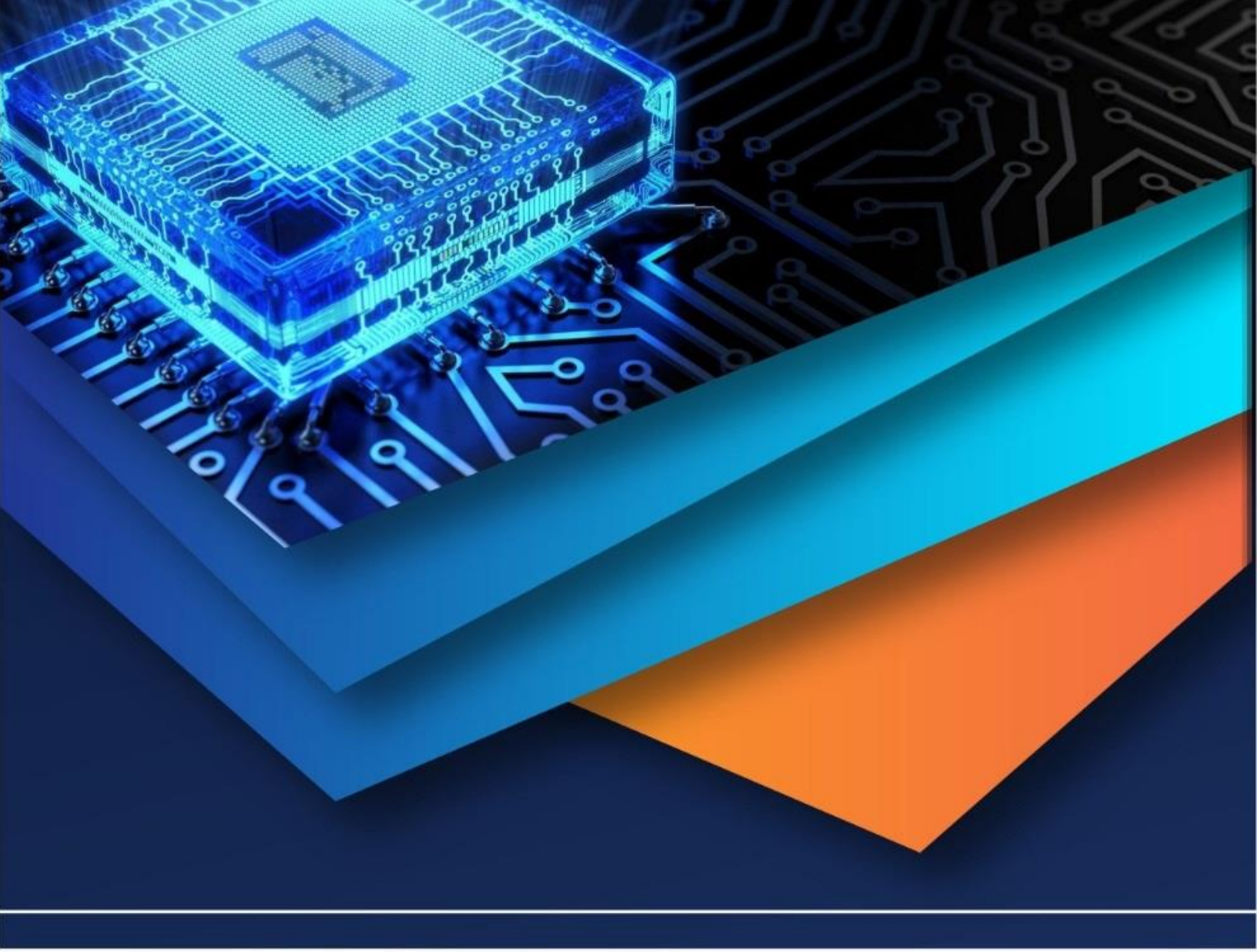
We would like to thank our project coordinator Prof. Uttara Gogate for all the support we needed from her for our project.

We also express our deepest thanks to our H.O.D. Prof. P. R. Rodge whose benevolent helps us making available the computer facilities to us for our project in our laboratory and making it true success. Without his kind and keen co-operation our project would have been stifled to standstill.

Lastly, we would like to thank our college principal. Dr. J. W Bakal for providing lab facilities and permitting us to go on with our project. We would also like to thank our colleagues who helped us directly or indirectly during our project.

REFERENCES

[1] Krzysztof Cabaj, and Wojciech Mazurczyk, "Using Software-Defined Networking for Ransomware Mitigation: The Case of CryptoWall", IEEE Network, Volume:30, Issue: 6, November-December 2016, pp. [1–19].
[2] Francesco Mercaldo; Vittoria Nardone; and Antonella Santone; "Ransomware Inside Out", Availability, Reliability and Security (ARES), 2016 11th International Conference on, 31 Aug.-2 Sept. 2016, pp. [1–9].
[3] Kanwalinderjit K Gagneja, "Knowing the ransomware and building defense against it - specific to healthcare institutes", Mobile and Secure Services (MobiSecServ), 2017 Third International Conference on, November-December 2016, pp. [1–4].
[4] Mattias Weckstén; Jan Frick; Andreas Sjöström; and Eric Järpe, "A novel method for recovery from Crypto Ransomware infections", Computer and Communications (ICCC), 2016 2nd IEEE International Conference on, 14-17 Oct. 2016, pp. [1-4]..
[5] Marzieh Ahmadzadeh; Sajad Homayoun; Ali Dehghantanha; Sattar Hashemi; and Raouf Khayami, "Know Abnormal, Find Evil: Frequent Pattern Mining for Ransomware Threat Hunting and Intelligence", IEEE Transactions on Emerging Topics in Computing, Volume: PP, Issue: 99, 26 September 2017, pp. [1–10].
[6] Nolen Scaife; Henry Carter; Patrick Traynor; and Kevin R. B. Butler, "CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data", Distributed Computing Systems (ICDCS), 2016 IEEE 36th International Conference on, 27-30 June 2016, pp. [1–9].
[7] Rhythima Shinde; Pieter Van der Veeken Stijn Van Schooten; and Jan van den Berg, "Ransomware: Studying transfer and mitigation", Computing, Analytics and Security Trends (CAST), International Conference on, 19-21 Dec. 2016, pp. [1–4]
[8] www.wikipedia.com



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY