International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-9 Issue-1, May 2020

A Proposed Methodology to Prevent a Ransomware Attack

Salunke M.D, Kumbharkar P.B., Yogesh Kumar Sharma

Abstract- RANSOMWARE as malware, increasing threat, three techniques-prevent, detect and mitigate, backup, software updates, educating users, network protection, software optimization, antivirus solution, don't pay ransom, RDP (remote desktop protocol), disabling macros, principle of least privilege, software restriction policies(SRP), Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), Domain Keys Identified Mail (DKIM), administrative rights, network segmentation.

I. INTRODUCTION

Ransomware is a kind of malware that is aimed at targeting your important data, critical files and vital system settings for the purpose of extortion. It generally creates fear in the mind of the owner of the system of losing their critical files or disclosing the classified documents for the sole purpose of extorting some amount of ransom.[2] Ransomware thus is very much notorious and our systems need to be protected from it to avoid financial losses.

Ransomware are the fastest growing malwares, targeting users of all types—from the home user to the corporate network. There are more than 4,000 daily ransomware attacks that have occurred since January 1, 2016. This includes a 300-percent increase over the approximately 1,000 attacks per day seen in 2015. There are different yet very effective prevention and response actions that can significantly mitigate the risk posed to your organization. [1]

Ransomware is frequently delivered through phishing emails. Once the user is locked out of the data or system, the cyber criminal demands a ransom payment for retrieving back our data. Upon receipt of payment, the cyber criminal assures to provide an avenue to the victim to regain access to the system or data. [2]

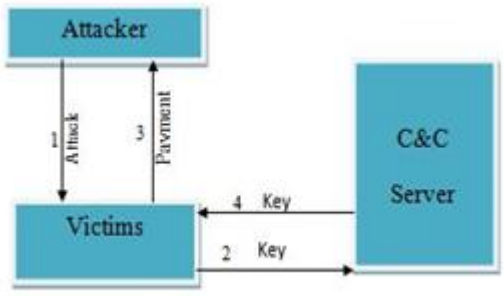

Fig 1: Working of Ransomware Attack

Manuscript received on April 30, 2020.
Revised Manuscript received on May 06, 2020.
Manuscript published on May 30, 2020.
* Correspondence Author
Salunke M.D., PhD scholar, Shri. JJT University,
Dr. P.B. Kumbharkar, Shri JJT University
Dr. Yogesh Kumar Sharma, Shri JJT University

Previously our defensive strategies were very much passive and we relied on the attacker to attack and then to mitigate the attack and secure our system, but this type of approach is ineffective and time consuming , also there is data risk and privacy violations.

So to counter this we need active protection and defensive mechanisms. So in this we build our mechanism based on three different aspects corresponding to the behavior of ransomware.

1. Those three aspects are -: Prevent, Detect, Mitigate

These aspects provide complete foundation of our defensive mechanism in the act of countering ransomware attacks.

Fig 2: Security aspects [2]

We confine ourselves to knowing details of prevention techniques in this paper as what are the different methods through which we can prevent the attack of ransomware. By doing this we ensure to keep our data and privacy secured.

II. LITERATURE REVIEW

Juan A. Herrera Silva et. al., (2017), they developed a model for Ransomware prevention and detection by using machine learning algorithm on Windows platform to analyze non-structured data collected by using EcuCERT logs. These logs help for selecting features that decide the attack. These logs are generated with the help of machine learning approach by discovering behavioural pattern of treats under cognitive security. [3]

Jordan W. Han et. al., (2017), they created a solution for prevention of Ransomware attack. The system that is extension to the browser work as anti-virus like extension that gives security strategy and awareness policies that allows user to surf web or Internet and get warning about danger or most common Ransomware attacks. [4]

Daniel Gonzalez et. al., Author investigates or discusses most common types of crypto Ransomware families and their methods of attacks, their infection types, what type of files are affected, typical behavior of crypto Ransomware attack. It also listed prevention methods from crypto Ransomware attack. [5]

Ganesh Gupta et. al., (2017), authors discuss Ransomware attack, working of ransomware attack, impact of attack and prevention techniques of ransomware attack. [6]

Manveer patyal et. al. (2017), they proposed multilayer prevention and detection defence architecture to defeat ransomware attack. Define policies, recursive folder, monitoring file activity; backup and recovery are the four layers of multilayered architecture. [7]

Ronny Richardson and Max North (2017), author discussed history of ransomware, the preventive measure of ransomware attack that can prevent you from attack that is best practices. Lastly author discuss about the big question related to ransomware to pay or not to pay the ransom. [8]

Jinal P. Tailor and Ashish D. Patel (2017), author discussed about modern ransomware families, life cycle and time line of windows based ransomware attack and finally discuss about some detection and prevention methodologies of ransomware attack such as regular back up, spam mails, hyperlinks, anti-virus and Anti-malware [9]

Dae-Youb Kim et. al., (2018), authors proposed a method that is White list-based Ransomware detection system that can detect or block Ransomware to encrypt the files of user in real time by applying an access control scheme to user's application on user's system. The proposed system can detect new as well as variant of Ransomware family as it allows white list-based application to run. [10]

III. PROPOSED PREVENTION TECHNIQUES

There are some basic steps that need to be followed every time to safeguard our system and data.

1. Backup -: Well taking backup of your data is your best weapon to safely counter the threat. Backups should be scheduled regularly and their frequency should be decided on the importance of data being backup-ed. It is also important to check that the backup of data taken is correct and right data is stored by restoring backups on a regular basis.[5] Also backup of data should be stored offline so that it is not compromised during a certain kind of ransomware attack. We also should follow the 3-2-1 backup rule wherein we make 3 copies of data of which at least 1 is stored offline. Verifying the integrity of backup data is also important in this process.[3]

Fig 3: Preventive Measures [12]

Software updates -: Attackers find loopholes in the software and design malwares based on those loopholes. So to avoid damage we can cover these loopholes by regularly updating our system and applying various kinds of patches. Inconsistent patching and outdated software will leave your system and data exposed. Use a centralized patch management system.[3][4][5]

Educating users -: Security awareness training must be conducted regularly to educate end users about the ransomware threats and how to avoid them. Users must be able to suspect the phishing emails and report them to take necessary actions. Humans are the weakest link in security mechanisms, they easily fall prey to phishing mails or attractive advertisements on the web, and once clicked on the link your security is compromised. Slight mistakes from a single user of a connected network may risk security of all connected firmware. Train employees to avoid opening of unknown links or attachments in emails.[2][4]

Network protection -: This includes various steps such as deploying a layered protection firmware or laying down strong firewalls. The network security software should be robust so that it can even handle unforeseen threats along with the known ones partially or fully. We can also imply network segmentation by logically separating network access and limiting accessible network volume. If you are not accessing the RDP them you must disable Remote Desktop protocol (RDP). Keep a check on network activity of all the users and try to gain in depth network visibility this will help uncover the route through which the attack is done.[2][5]

2. Software Optimization -: Developing an inbuilt function to block malicious websites, spam mails will help a lot; this might be using a strong filter for such a purpose. Enforce serious software restriction policies that will restrict users on your network from accessing sensitive information. Make use of some technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and Domain Keys Identified Mail (DKIM) to prevent email spoofing. Implement Software Restriction Policies (SRP) for better access control and Least Privilege principle for control over accessibility of files, directories and network sharing.[3][5] Check administrative powers of each system and verify their credentials so as to avoid silent installations and modifications of any programs over the whole network. You can also disable macros as most ransomware attacks require macros to be enabled to function as desired.

3. Anti-Virus Solution -:

To protect from threat you must have a tool that will help you combat the threat and get rid of it, antivirus solutions help here a lot. There are many real time threat detection solutions available that must be used to get real time threat detection and control. Perform regular scans of your data and system settings using these solutions. [1][4] Keep your antivirus optimized and updated.

We must also conduct security assessments to regularly check security vulnerabilities; this can be done in virtualized environments thus verifying security integration. Don't pay Ransom -: According to cyber experts 1 out of 5 users who pays the ransom gets its data back.
Be aware that there is no promise made that you will be granted access back. Contact the authorities instead and refrain from funding these cybercriminals.[5]

Fig 4: Avoid Ransom Payment

IV. RESULT

As a result of proposed methodology that is preventive measures is best approach to avoid the risk of ransomware attack. So by applying these preventive measures one can prevent the ransomware attack risk.

V. CONCLUSION

So, here in the epilogue, we must remember that Proactive Prevention is the best form of Defense against the ransomware attack. We must know our attack surface and try to reduce or cover it to protect our system from any threats. We must also identify vulnerabilities of our system and must timely correct them. Prevention is better than cure. It may be trite but it is truth.

REFERENCES

1. Sonu B. Surati, Ghanshyam I. Prajapati. "A Review on Ransomware Detection & Prevention". IJRSI, ISSN-2321-2705
2. F-secure white paper, "RANSOMWARE HOW TO PREDICT, PREVENT, DETECT & RESPOND".
3. Juan A. Herrera Silva "Large Scale Ransomware Detection by Cognitive Security", 978-1-5386-3894-1/17/$31.00 ©2017 IEEE.
4. Jordan W. Han "A Conceptual Security Approach with Awareness Strategy and Implementation Policy to Eliminate Ransomware", 2017 Association for Computing Machinery. ACM ISBN 978-1-4503-5392-2/17/12.
5. Daniel Gonzalez "Detection and Prevention of Crypto-Ransomware", 978-1-5386-1104-3/17/$31.00 ©2017 IEEE.
6. Ganesh Gupta "STUDY ON RANSOMWARE ATTACK AND ITS PREVENTION", International Education & Research Journal [IERJ], E-ISSN No: 2454-9916, Volume: 3, Issue: 5, May 2017,
7. Manveer patyal , "Multi-layered defense architecture against ransomware", International Journal of Business & Cyber Security (IJBCS) Vol. 1 Issue 2
8. Ronny Richardson and Max North, "Ransomware: Evolution, Mitigation and Prevention", International Management Review Vol. 13 No. 1 2017
9. Jinal P. Tailor and Ashish D. Patel (2017), "A Comprehensive Survey: Ransomware Attacks Prevention, Monitoring and Damage Control", International Journal of Research and Scientific Innovation (IJRSI) | Volume IV, Issue VIS, June 2017 | ISSN 2321–2705
10. Dae-Youb Kim "White List-based Ransomware Real-time Detection and Prevention for User Device Protection", 2018 IEEE International Conference on Consumer Electronics (ICCE), 2018 IEEE
11. Ransomware Prevention and Response Checklist by Data Security Plus.
12. The Ultimate Checklist for Preventing and Fighting Ransomware Attacks by Cisco.
13. How to protect your Networks from ransomware by the US government.

AUTHORS PROFILE

Salunke M.D. ME Computer Network, PhD Scholar

Dr. P.B. Kumbharkar, PhD Computer Engineering