RANSOMWARE IMPLEMENTATION AND DETECTION

CYBER SECURITY

CDAC, Noida

CYBER GYAN VIRTUAL INTERNSHIP PROGRAM

Submitted By:

SHASHWAT MISHRA

Project Trainee, (July-August) 2024

BONAFIDE CERTIFICATE

This is to certify that this project report entitled <RANSOMWARE IMPLEMENTATION AND DETECTION> submitted to CDAC Noida, is a Bonafede record of work done by <SHASHWAT MISHRA>under my supervision from <06/12/2024> to <20/12/2024>

Declaration by Author(s)

This is to declare that this report has been written by me. No part of the report is plagiarized from other sources. All information included from other sources have been duly acknowledged. I aver that if any part of the report is found to be plagiarized, I'll take full responsibility for it.

Name of Author(S): SHASHWAT MISHRA

TABLE OF CONTENTS

ACKNOWLEDGEMENT

I would like to express my heartfelt gratitude to our CDAC faculty for their invaluable guidance, encouragement, and support throughout this project on ransomware implementation and detection. Their expertise and insights have been instrumental in shaping the direction and outcome of this work.

I extend my sincere thanks to all the batchmates for their continuous support and constructive feedback, which have greatly contributed to the successful completion of this project.

Lastly, I am grateful to my family for their unwavering support and understanding during the course of this research.

Thank You CDAC

-SHASHWAT MISHRA

RANSOMWARE IMPLEMENTATION AND DETECTION

PROBLEM STATEMENT: Ransomware encrypts victim's data, demanding payment for decryption keys. It spreads via phishing emails, malicious attachments, or websites. The rise of cryptocurrencies facilitates anonymous ransom payments, escalating the threat. Effective detection requires robust cybersecurity, user education, and regular backups to mitigate these attacks.

Learning Objective:

1. Understand Ransomware Mechanisms: Gain insights into how ransomware functions, its types, and methods of propagation.

2. Implement Ransomware Attack: Learn the process of designing and executing a ransomware attack in a controlled environment for educational purposes.

3. Detection Techniques: Explore various tools and strategies to detect ransomware activities effectively.

4. Mitigation Strategies: Develop skills to create effective countermeasures and response plans to minimize the impact of ransomware attacks.

5. Ethical Considerations: Recognize the ethical implications of cybersecurity practices and ensure compliance with legal standards.

APPROACH: The approach of the project on ransomware implementation and detection involves a comprehensive methodology: start with a literature review to understand existing ransomware types, propagation methods, and detection techniques. Set up a controlled lab environment using virtual machines for safe experimentation. Develop a ransomware prototype for educational purposes, simulating real-world attacks. Implement and test various detection tools and strategies, analyzing their effectiveness. Develop countermeasures and response plans, including backups, user training, and security protocols. Finally, evaluate the effectiveness through rigorous testing and document the findings in a detailed report.

IMPLEMENTATION: For implementation of ransomware attack first we'll install the tool SARA in our KALI LINUX machine using GitHub link. Now when we'll run the tool it will ask about whick type of ransomware you are trying to apply, in this project we'll apply screen lock ransomware in which when any user install any app or run any extention in his system his screen will be encrypted and user will be unable to use his device, for unlocking it he will have to decrypt it for decryption he'll need decryption key

that we have entered while creating a ransomware application.

CONCLUSION & RECOMMENDATIONS: Ransomware is a growing threat that endangers data security. Detection techniques proved crucial for early identification and response. It is recommended to enhance security measures, educate users, perform regular backups, deploy robust detection tools, and develop a comprehensive incident response plan to mitigate ransomware impacts.

LIST OF REFERENCES:

1- **For installing the Tool (SARA)-** GitHub - termuxhackers-id/SARA: SARA - Simple Android Ransomware Attack
2- **For Application And Website Security Test-** Website Security Test | ImmuniWeb
3- **For Google Play Protection Service-**Android Apps on Google Play