IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

PROACTIVE DEFENSE STRAGIES RANSOMEWARE THREATS

Sumithra.G ,Student

Department of Computer Applications

Nehru Arts and Science College ,Coimbatore.

Mr.Sakthikumar T, Student

Department of Computer Applications

Nehru Arts and Science College , Coimbatore.

Araya.M.U,Student

Department of Computer Applications

Nehru Arts and Science College ,Coimbatore.

(UNDER GUIDANCES)

Mrs.B.Jijitha, Assistant professor,

Department of Computer Applications

Nehru Arts and Science College ,Coimbatore.

ABSTRACT:

Attacks using ransomware are still a serious risk to both people and businesses. Conventional reactionary strategies frequently fall short against attackers' developing techniques. This study suggests a proactive protection approach that makes use of Hash Conceal and RanGAN (Ransomware Generative Adversarial Network). Early threat detection is made possible by RanGAN's real-time machine learning detection of ransomware behavior patterns. Conversely, Hash Conceal concentrates on safeguarding data by employing a hashing algorithm to secure important information, making it unusable even in the event of ransomware encryption. Together, these strategies provide a strong security system that reduces data loss and guarantees quick to reaction

Keywords: Data Security, Hash Conceal, Machine Learning, Proactive Defense, Ransomware, and RanGAN

Introduction

The widespread threat of ransomware has resulted in substantial financial losses and interruptions to operations. Attackers use a variety of strategies to break into networks, encrypt important information, and demand ransom payments to unlock it. Conventional security methods, such data backups and incident response procedures, frequently concentrate on reactive measures. These techniques might not be enough to combat highly skilled ransomware strains, though.

This study examines a proactive protection approach that uses cutting-edge technology to detect and neutralize ransomware threats before they have a chance to cause harm.

Ransomware Generative Adversarial Network,

Is a machine learning model that uses ransomware behavior patterns to identify patterns in the power of GANs. RanGAN facilitates early threat detection by studying system activity and identifying abnormalities suggestive of ransomware activity. Hash Conceal: To safeguard important data, this data protection technique makes use of hashing techniques. Data is changed by hashing into an exclusive, unchangeable code. Attackers cannot access the hashed data even if ransomware encrypts it since they do not have the original data or the associated hash key to decrypt it.

Early threat detection using RanGAN

A machine learning model called RanGAN was created expressly to identify ransomware activity. The GAN architecture it employs consists of two neural networks: Generator: Using a dataset of recognized ransomware behavior patterns, this network is trained. It keeps producing fake data that looks and acts like ransomware. Discriminator: This network examines both the artificial data produced by the generator and the actual system activity. The discriminator seeks to discern between the ransomware-simulation patterns and authentic activity. RanGAN enhances its capacity to recognize minute variations in system behavior that can point to a ransomware assault through ongoing training and improvement. Real-time threat detection is made possible by this, enabling prompt action to be taken before any serious harm is done.

Combined Approach: A Proactive Defense System

When combined, RanGAN and Hash Conceal provide a strong security against ransomware attacks. As the first line of protection, RanGAN quickly recognizes unusual activities. The system can take a number of actions after discovery, including: Isolating the compromised system to stop it from moving laterally within the network.Notifying security staff so they can look into and take appropriate action right away. putting automated defenses in place to stop

the threat. Conversely, Hash Conceal offers an extra degree of security for important information. The hashed data is rendered worthless even in the event that ransomware evades RanGAN's detection, hence reducing the likelihood of data loss.

CONCLUSION:

Ransomware evolves, providing a persistent danger to data security. Organizations may greatly improve their ransomware defenses by taking a proactive approach that combines real-time threat detection with data protection techniques. RanGAN provides early threat detection, whereas Hash Conceal protects important data. This integrated approach provides a strong defense system that reduces the impact of ransomware while ensuring company continuity.