PROACTIVE DEFENSIVE AGAINST RANSOMWARE THREATS

Presented By:

DEVINA S – THE KAVERY ENGINEERING COLLEGE - CSE

edunet foundation

OUTLINE

- Problem Statement
- Proposed System/Solution
- System Development Approach
- Algorithm & Deployment
- Result (Output Image)
- Conclusion
- Future Scope
- References

PROBLEM STATEMENT

- Ransomware attacks have emerged as one of the most pressing cybersecurity threats, causing significant financial losses and data breaches for organizations worldwide. Traditional anti-ransomware solutions often rely on signature-based detection methods, which struggle to keep pace with the rapidly evolving tactics employed by ransomware operators.
- To address this challenge, a novel approach harnessing the power of RanGAN and Hash Concealment has been developed. RanGAN is an advanced machine learning model capable of generating diverse and realistic samples of data, while Hash Concealment techniques aim to obfuscate file hashes to evade detection by ransomware.

PROPOSED SOLUTION

- **RanGAN Integration: RanGAN is integrated into the anti-ransomware solution to generate synthetic data samples that closely mimic the characteristics of legitimate files. By leveraging RanGAN, the solution can create a diverse range of data representations, making it more challenging for ransomware operators to identify and encrypt target files.**
- **Hash Concealment Techniques: Hash Concealment techniques are employed to obfuscate file hashes, rendering them less susceptible to ransomware encryption. By concealing file hashes, the solution adds an additional layer of defense against ransomware attacks, making it more difficult for attackers to identify and encrypt specific files based on their hash values.**

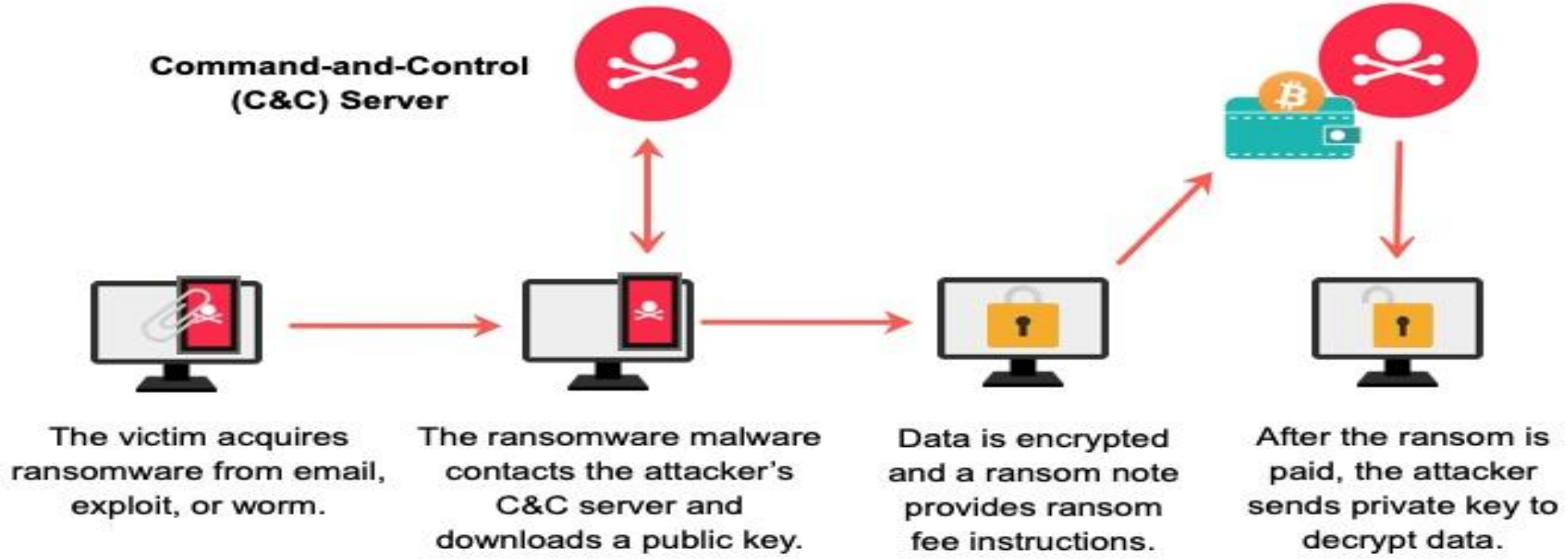
OBJECTIVE

The objective of the project is to presents a proactive defensive strategy harnessing the power of "RanGAN" and "Hash Conceal" technologies to fortify cybersecurity measures against ransomware threats.

- To develop RanGAN technology for early ransomware detection.
- To integrate Hash Conceal for data protection.
- To achieve early threat detection.
- To ensure data protection and concealment.

RANSOMWARE ATTACK

In a ransomware attack, malicious software (malware) is deployed by cybercriminals to infiltrate a computer system or network, encrypt files or data, and demand a ransom payment from the victim in exchange for restoring access to the encrypted data.



SYSTEM APPROACH

- In this project the "RanGAN“ and "Hash Conceal“, is designed to provide a robust and comprehensive defence mechanism

RanGAN Technology Integration:

- RanGAN is a advanced machine learning techniques to actively monitor network and system activities, learning and recognizing ransomware behaviour patterns in real-time

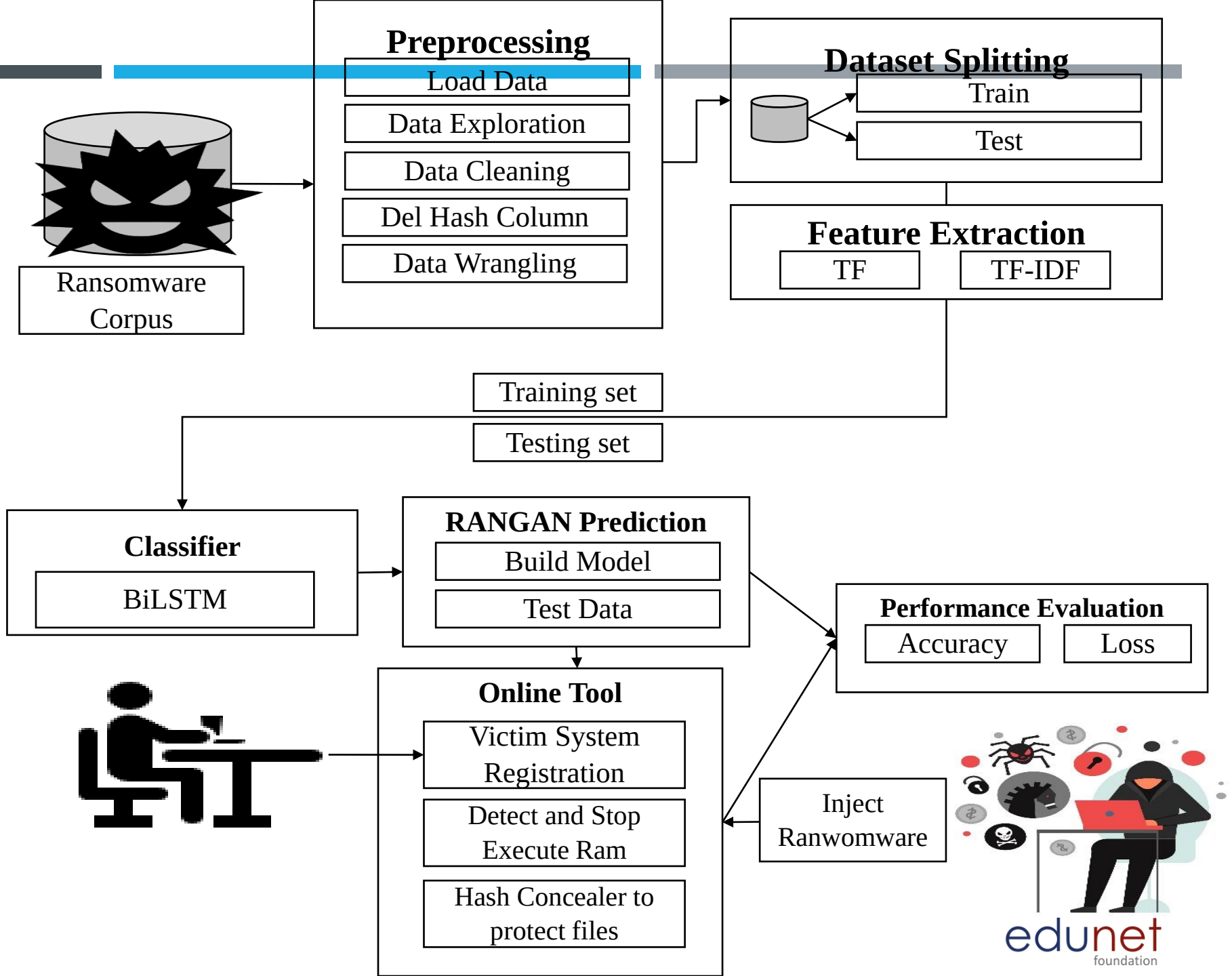
Hash Conceal Implementation:

- Hash Conceal employs advanced cryptographic methods to secure data, rendering it inaccessible to ransomware encryption.

Linker File:

- After the encryption of file user can only able to see the file without decrypting it.

System Architecture Diagram



ALGORITHM & DEPLOYMENT

RanFooler Web Tool

- **In order to simulate a real world scenario, a three-tiered web architecture is developed. This architecture consisted of web-servers, application servers, and a database server.**
- **A front load balancer is tasked with handling and distributing clients requests to the appropriate web servers.**
- **RanFooler can help in protecting the user's device from getting infected with Ransomware and other web security threats.**

Load Dataset

Byte files and Asm files are basically the Ransomware assembly code that contains the information related to the function calls and variable allocation.

Pre-processing

- The byte files are exclusively used for model training and processing, the appropriate files were first separated from the Asm files. The byte files were converted into text files so that the features could be read into the Python code.

.

Feature Extraction

- Shallow deep learning-based feature extraction method (word2vec) is used for representing any given Ransomware based on its opcodes. Each byte file has a varying amount of Ransomware code in it, resulting in different sizes for each file.

Ransomware Build and Train

- The training process involves Bidirectional Long. Such as Short-Term Memory (BiLSTM) and Gated Recurrent Unit (GRU). It will be used to train a subset of the dataset

System Integration

- Behind the scenes, RanFooler integrates the selected configuration settings into the backend, associating the chosen files with the provided MAC ID for the users system.

Continuous Monitoring

- RanGAN continuously monitors the configured systems for any changes or potential
- ransomware activity. Automated alerts and notifications keep users informed about the status of their protected files.

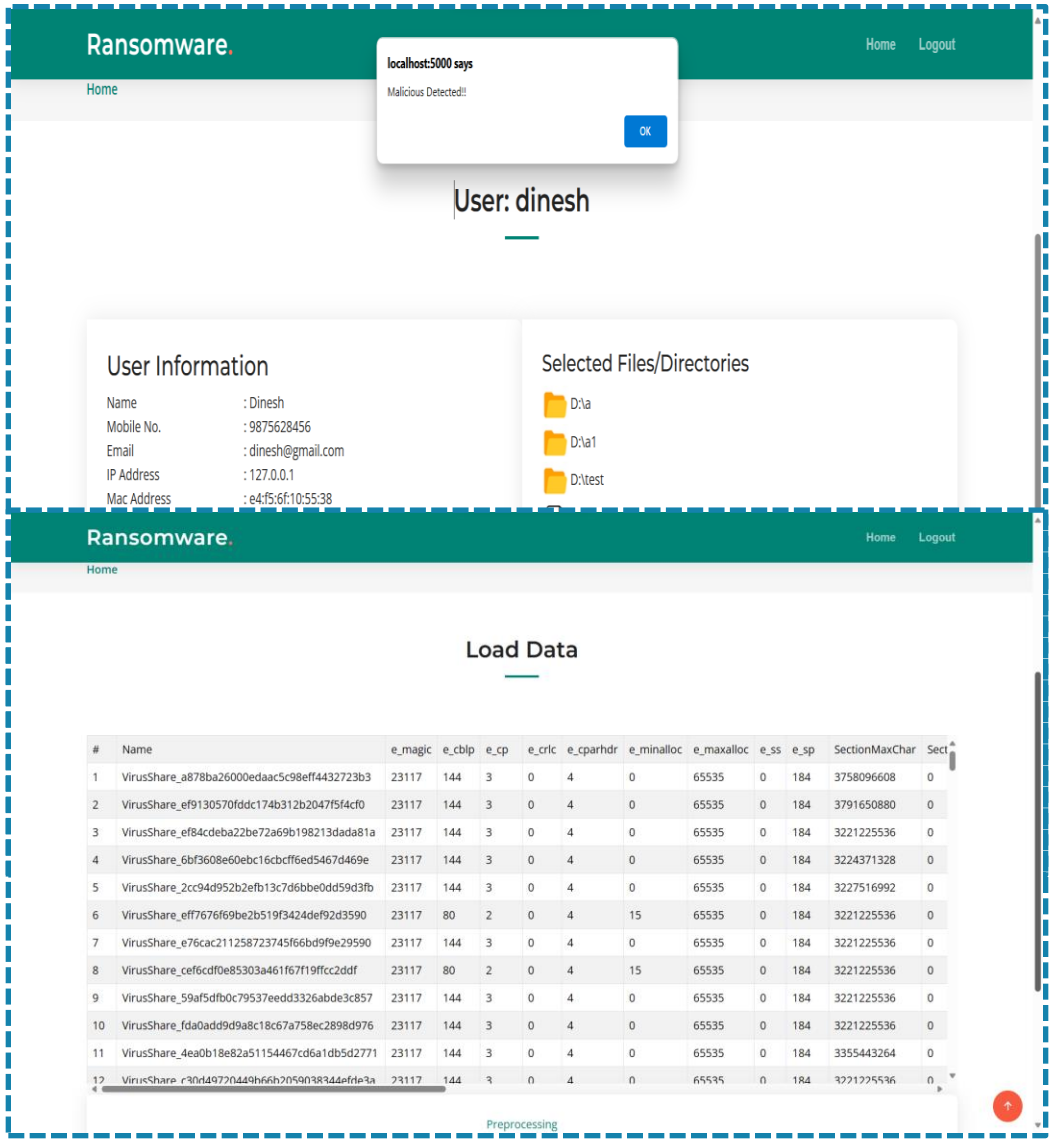
Admin

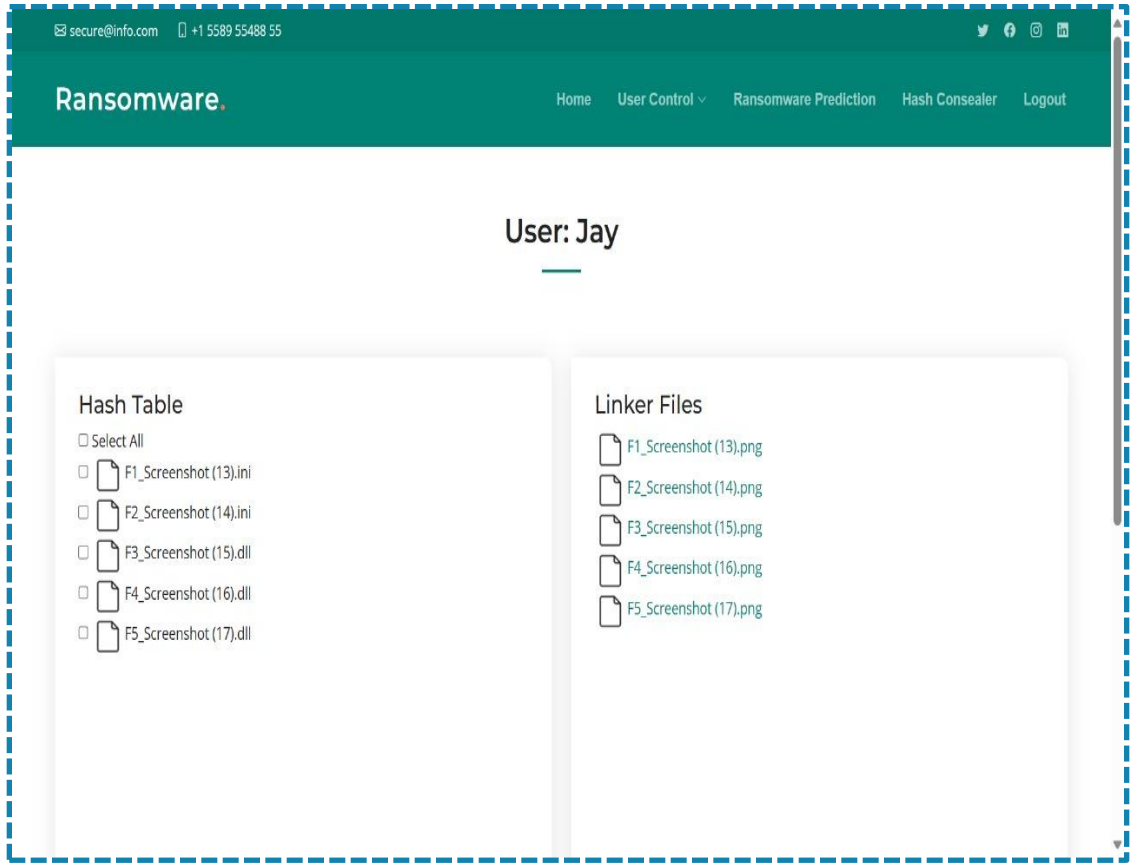
- **Admins initiate their activities by securely logging into the End User Interface, ensuring that only authorized personnel gain access to administrative functionalities. Admins upload datasets, a step in training the RanGAN model. Admins deploy the trained RanGAN model to the RanFooler Web App**

User

- **Users initiate the configuration process by registering with the RanFooler web application. This involves providing necessary details such as username, email, and password. Upon login, users configure their systems by providing the MAC ID of their devices. This step ensures a unique identification for each end-user device.**

RESULT





edunet foundation

CONCLUSION

- In conclusion, the proactive defensive strategy leveraging RanGAN and Hash Conceal marks a shift in combating ransomware threats.
- By integrating with cryptographic concealment, this approach provides a versatile defense against both known and emerging ransomware variants
- This strategy not only detects and mitigates threats but anticipates and prevents potential attacks

FUTURE SCOPE

- As technology and cyber threats continue to evolve, the proactive defensive strategy against ransomware using RanGAN and Hash Conceal is positioned for future enhancements to further strengthen its effectiveness.
- Blockchain Integration for File Tracking
- Investigate the integration of blockchain technology to create an immutable and transparent ledger for file tracking, enhancing the system's ability to trace file access and modifications.

- Quantum-Resistant Encryption
- Anticipate the future threat landscape by exploring quantum-resistant encryption methods to safeguard against potential advancements in quantum computing that could compromise existing cryptographic techniques.

REFERENCES

- J. Choi, J.Lee, G.Lee, J.Yu, and A.Park, " A defense mechanism against attacks on files by hiding files, "J.Korea soc.Ind.Inf.Syst., vol.27, no.2, pp.1–10, 2022, doi:10.9723/jksiis.2022.27.2.001
- 2. J.Yuste and S.Pastrana, "Avaddon ransomware: An in-depth analysis and decryption of infected systems, " Vol.109, Oct.2021, Art.no.102388,doi:10.1016/j.cose.2021102388.
- S. Alzahrani, Y. Xiao, and W. Sun, "An analysis of conti ransomware leaked source codes, IEEE Access, vol.10, pp.100178–100193, 2022,doi: 10.1109/ACCESS.2022.3207757.
- G. Hull, H. John, and B.Arief, Ransomware deployment methods and analysis: Views from a predictive model and human responses, " Crime Sci., vol.8, no. 1, pp.1–22, Feb 2019, doi:101186/s40163-019-0097-9.

THANK YOU

edunet foundation