GANs: A Deep Learning Algorithm forAdvanced Decoy File

Ashy V Daniel[1], Aslin Monisha V S[2], M S Suvitha[3], S M Ashika[4], Dhanesh M[5]

[1] *Associate Professor/CSE, Lourdes Mount College of Engineering and Technology*

[2,3,4,5] *UG Student /CSE,Lourdes Mount College of Engineering and Technology*

***Abstract*: - Unauthorized removing or moving data is one of the major problem in information theft. Data exfiltration and ransomware attack are the things to be strictly considered. For this, decoy file strategies are used for protecting file and information. We propose GAN, General Adversarial networks which is a deep learning algorithm for decoying the files. This will create a pragmatic decoy files, which can be incorporate in enterprise network to engage the ransom ware threats effectively. This involves continuous monitoring for exceptional interaction and anxious communication. Exact testing against latest ransom ware documents explains over 92% engagement traits and sub-30 seconds response time. This can be used for early detection and prevention of data loss for extortion.**

***Index Terms-D*ata Exfiltration, GAN, decoy file, Ransomware**

I. INTRODUCTION

Ransomware is a type of malicious software (malware) that encrypts files or locks computer systems and demands payment from the victim to restore access. It's a form of cyber extortion where attackers typically demand payment in cryptocurrencies like Bitcoin, which makes it harder to trace. Once ransomware infects a system, it encrypts files using a strong encryption algorithm, making them inaccessible to the victim. The attackers then display a ransom note, usually demanding payment in exchange for a decryption key or tool. Ransomware can spread through various means, including phishing emails, malicious attachments or links, compromised websites, and exploit kits. It can target individuals, businesses, government agencies, and other organizations.

Preventing ransomware attacks involvesimplementing security best practices such as keeping software up to date, using strong passwords, regularly backing up important data, educating users about phishing and other social engineering tactics, and using reputable antivirus and antimalware software. Current network defense mechanism focus on preventing attackers from entering a network, but them exists few defense in place to prevent sensitive data from leaving a network.

Data exfiltration can occur as part of a cyberattack or data breach, where sensitive information such as personal data, intellectual property, financial records, or other proprietary information is stolen or extracted from the victim's systems. Data exfiltration poses significant risks to organizations, including financial losses, reputational damage, and regulatory penalties for non-compliance with data protection laws. To mitigate the risk of data exfiltration, organizations should implement robust security measures such as network segmentation, encryption, intrusion detection systems, data loss prevention (DLP) solutions, employee training on cybersecurity best practices, and continuous monitoring for suspicious activities. Additionally, organizations should have an incident response plan in place to quickly detect and respond to data exfiltration attempts.

Decoy file strategies involves the use of deceptive techniques to protect data and ensure file integrity. These strategies can include creating multiple levels of stacking, monitoring file access, hiding sensitive files with baits, and injecting decoys on to fake system view. Decoy based defense mechanisms, such as honey pots, can be used to detect and remove new forms of internet worms without relying or signatures. The decoy effect is a marketing strategy where consumers change their preferences when presented with a third choice that acts as an asymmetrical dominating bait. In this paper, we introduced Generative Adversarial Network(GAN), a deep learning algorithm for decoy file.

II. RELATED WORK

Ransomware attacks on the Windows platform have been studied by various researchers. Muhammad Salman developed a Bayesian Network model to assess the threat of ransomware attacks by exploiting device vulnerabilities [1]. Tom Meurs et al. analyzed the financial impact of ransomware attacks using a dataset of 453 ransomware attack investigation reports in the Netherlands [2]. Mohd Rafi bin Yaacob applied machine learning techniques to detect ransomware attacks, achieving improved results with feature selection methods. Another study evaluated the performance of machine learning algorithms in detecting ransomware by analyzing PE headers of software [3]. These studies provide insights into the modeling, financial impact, and detection of ransomware attacks on the Windows platform.This paper implements a methodology and countermeasures to prevent and detect data exfiltration attempts [4]. Attacker vector on industrial control system using electromagnetic covert channel. Data exfiltration through wired Ethernet connects without direct physical interactions [5]. Data exfiltration is serious cybercrime affecting organizations worldwide. Current prevention techniques are insufficient due to zero-day vulnerabilities [6].

This paper discusses the effectiveness of true strategies in enhancing the competitiveness of target product it analyzes the performance of different strategic in various product competition and diffusion scenarios [7]. Most prior work on decoy-based detection of ransom ware assume that the decoy object one files that one being monitorial for write access. This paper presents an evaluation on the hest type of file system object to be used as a decoy, as well as the best way to monitor the decoy for the detection of ransom ware [8]. This study implements a honey pot technique, a secret pot mechanism, where decoys one placed in the computer to detect ransom ware. The detection program monitors the decoy used at any time [9]. This paper describes a decoy file system strategy that involves hiding and redacting sensitive files with baits and injecting decoy onto fake system view to product against data theft [10].

III. PROPOSED METHOD

Creating decoy files using generative adversarial networks involves a dynamic interplay between the generator model (G) and the discriminator model (D). These models collaborate to produce decoy files indistinguishable from real data, a crucial strategy in countering advanced ransom ware threats.

The discriminator (D) evaluates data, determining the likelihood of its authenticity, playing a pivotal role in guiding the generator towards producing more realistic outputs. Its function, expressed as

$$D(x) = \text{Prob}_{\text{data is real}}(x)$$

In this equation, D(x) represents the probability assigned to the data being real. D's goal is to accurately distinguish between actual data and decoys generated by G. Trained on real confidential documents, D learns intricate patterns, becoming a reliable judge of data authenticity.

The generator (G) focuses on creating synthetic data realistic enough to fool D. It transforms input noise vectors into decoy documents, refining its process to produce outputs classified as genuine by D, improving the realism of decoy files.

$$G(z;0_g) = \text{Generated data from noise z}$$

Here, $G(z,0_g)$ represents the output of the generator, which, fueled by a noise vector z and controlled by parameters 0_g, crafts a decoy document.

The training objectives are represented mathematically: D maximizes its ability to classify real and fake data, while G minimizes its likelihood of detections by D. This adversarial training continues until G can produce decoy document indistinguishable from real data.

This iterative process ensures that the generated documents are highly convincing, effectively deceiving ransom ware threats. The realistic nature of these decoy files is crucial for early detection and mitigation of ransom ware, especially in scenarios where traditional security measures fall short.

Step 1: Data Preparation

This dataset should consist of various file types (e.g., PDFs, images, documents) along with theirmetadata. The data has to be preprocessed to extract features and convert it into a suitable format for training.

Step 2: Data Preprocessing

The real files dataset undergoes preprocessing to extract features and prepare them fortraining the GAN model.

The below figure shows the architectural diagram for a GAN designed to generate decoy files:

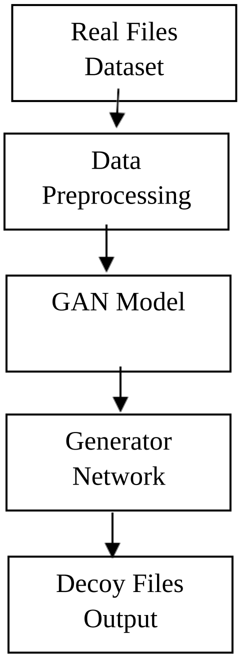

Fig: Architectural diagram for GAN designed to generate decoy files.

File Parsing: Depending on the file types of the dataset, parse each file to extract its content and metadata. Use appropriate libraries or tools to read and extract information from different file formats.

Feature Extraction: Extract relevant features from each file that will be used as input to the GAN model. Features may include textual content, image pixels, metadata attributes (e.g., file size, creation date), or any other characteristics that capture the essence of the file.

Normalization/Standardization: Normalize or standardize the extracted features to ensure they have similar scales and distributions. This step helps stabilize the training process and improve convergence during GAN training.

Data Encoding: Encode the extracted features into a format suitable for feeding into the GAN model. This may involve converting text data into numerical representations (e.g., using word embedding or one-hot encoding) or scaling image pixel values to a range between 0 and 1.

Data Augmentation (Optional): Augment the dataset by applying transformations or adding noise to the extracted features. Data augmentation can help increase the diversity of the training data and improve the robustness of the GAN model.

Data Splitting: Split the preprocessed dataset into training, validation, and test sets. The training set is used to train the GAN model, while the validation set is used for monitoring model performance during training.

Data Serialization: Serialize the preprocessed dataset into a format suitable for storage and efficient access during training. This may involve saving the data as numpy arrays, HDF5 files, or other formats compatible with deep learning frameworks.

By following these preprocessing steps, we can prepare the dataset for training a GAN model to generate decoy files.

Step 3: GAN Model

The GAN consists of generator and discriminator. These networks are trained simultaneously in an adversarial manner. The generator creates synthetic decoy files, while the discriminator evaluates the authenticity of both real and synthetic files.

Step 4: Generator Network

The generator network takes random noise asinput and produces synthetic decoy files. It learns to generate files that mimic the distribution of real files in the training dataset.

Step 5: Decoy Files Output

This represents the output of the GAN, whichconsists of synthetic decoy files generated by the generator network. These files closely resemble real files and can be used as bait or camouflage to deceive potential attackers.

IV TESTING

Testing the effectiveness of GAN-generated decoy files involves assessing various aspects such as realism, resilience against detection, and impact on attacker behavior. Below is a methodology for testing GAN-generated decoy files:

i. Realism Assessment:

Visual Inspection: Evaluate the visual quality and fidelity of the synthetic decoy files compared to real files. Use human judgment to assess how realisticthe decoy files appear.

Statistical Analysis: Measure statisticalproperties of the synthetic files (e.g., pixel distributions for images, word frequency distributions for documents) and compare them to those of real files. Tools like chi-squared tests or kernel density estimation can be helpful.

ii. ***Stress Testing:***

Mimicry Evaluation: Attempt to distinguish between real and synthetic files using various analysis techniques, such as machine learning classifiers or forensic tools. Assess the resilience of the decoy files against detection.

Attack Simulation: Simulate realistic attack scenarios where adversaries interact with the decoy files. Monitor attacker behavior and determine if the decoy files successfully divert or mislead attackers.

iii. ***User Interaction Analysis:***

User Experience: Gather feedback from users who interact with the decoy files to assess their perception of realism and usability. This can provide insights into how effective the decoy files are in practical scenarios.

Behavioral Analysis: Analyze user interactions with the decoy files, such as opening, modifying, or sharing them. Determine if users treat the decoy files differently from real files and identify any suspicious behaviors.

iv. ***Red Team Exercises:***

Penetration Testing: Engage red team members or penetration testers to attempt to infiltrate the system while the decoy files are deployed. Evaluate their success rates and tactics used to bypass security measures.

Scenario-based Testing: Create specific attack scenarios tailored to the organization's threat landscape and assess how well the decoy files withstand sophisticated attacks.

v. ***Monitoring and Alerting:***

Intrusion Detection: Implement monitoring and alerting systems to detect unauthorized access or manipulation of the decoy files. Set up alerts for suspicious activities and investigate any detected incidents promptly.

Incident Response: Develop response procedures for handling incidents involving the decoyfiles. Test the effectiveness of these procedures through tabletop exercises or simulated incident scenarios.

vi. ***Feedback and Iteration:***

Continuous Improvement: Gather feedback from testing activities and use it to refine the GAN model and decoy file generation process. Iterate on thetesting methodology to address any weaknesses or shortcomings discovered during testing.

V. RESULTS

Efficiency of decoy files for selected ransomware is shown below:

Ransomware	Engagement (%)	Detection Accuracy (%)	Response Time (sec)
Avaddon	95	98	26
LockBit	95	98	24
Conti	94	97	27
Babuk	96	96	30
ESXiArgs	94	98	27
Nebula	95	95	25
Yashma	92	98	28

Table 1. Efficiency against some randomware samples of decoy files

The Network scalability and integration is shown below:

Network Environment	Integration Efficiency (%)	Scalability (%)
Small Business	98	94
Medium Enterprise	96	97
Large Enterprise	95	98
Cloud Environment	97	99
Hybrid Environment	92	94

Table 2. Network Scalability and Integration

Graphical representation of Decoy files efficiency, network scalability and integration of sample ransomware are shownbelow.

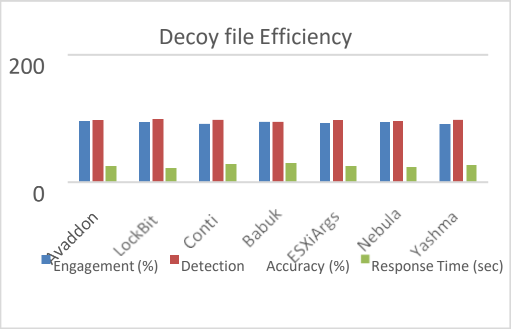

Fig:2 Graphical representation of Decoy files efficiency ofsample ransomware

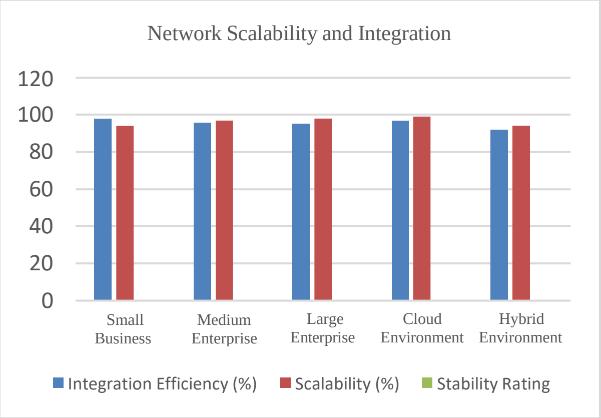

Fig 3: Graphical representation of Network Scalability and Integration

VI. CONCLUSION

Thus our proposed work of decoy file strategy, is customized to identify and counter contemporary ransomware threats aimed at exfiltrating data, was implemented. Utilizing advanced generative adversarial networks (GANs), convincingly authentic decoy documents were strategically inserted throughout enterprise networks to engage potential threats. Continuous surveillance of decoy file access facilitated swift detection of anomalous behaviors indicative of ransomware activity. Additionally, proactive response mechanisms were activated to sever unauthorized connections and disrupt suspicious communications, effectively containing potential data breaches. Thorough testing against recent ransomware strains demonstrated engagement rates exceeding 90% and response times of under 30 seconds. The implementation seamlessly integrated across diverse network infrastructures, maintaining operational efficiency with less than 5% overhead.

REFERENCES

[1] Sulistiadi, Muhammad Salman, “Ransomware Attacks Threat Modeling Using Bayesian Network”, Journal Teknologi Informasi dan Komunikasi Vol: 14 No 01 2023 E-ISSN: 2477-3255 Diterbitkan: 26-05-2023, https://doi.org/10.31849/digitalzone.v14i1.13788

[2] Tom Meurs, Marianne Junger, EricTews, Abhishta Abhishta,“Ransomware: How attacker’s effort, victim characteristics and context influence ransom requested, payment and financial loss”, APWG Symposium on Electronic Crime Research,30 Nov 2022-pp 1-13, 10.1109/eCrime57793.2022.10142138

[3] Haris Uddin Sharif; Mehmood Ali Mohammed; Shahbaz Hassan; Haidar Sharif “Comparative Study of Prognosis of Malwarewith PE Headers Based Machine Leaning Techniques”, 2023 International Conference on Smart Computing and Application (ICSCA), 05 April 2023,DOI: 10.1109/ ICSCA57840.2023.10087532

[4] James King, Gueltoum Bencliab, Nick Savage Stavros, Shiacles., “Data Exfiltration: methods and detection countermeasures” (2021).

[5] Shakthi Sachintha, Nhien- An Le khac, mark Scanion, Asanka sayonkkara., “ Data exfiltration through Electromagnetic covert channel of wired industrial”

[6] Peter S. Nyakomitta, Silvance O. Abeka, A Surrey of Data Exfiltration Prevention Techniques, Journal of Advanted Networking & Application(2020).

[7] Zhen Li, Xiaoyu Bao, Qingfeng Meug, peng- Qun shen, Dimitri volchenkov., Research on the complexity mechanism of Decoy strategies based on multiagent simulation (2020).

[8] B Dehham, DR Thompson- “Analysis of Decoy Strategies for Detecting Ransom ware”, IEEE conference on communication & network security (CNS), (1-6),2023.

[9] Ys Lin, CF Lee- International Journal of network security, “Ransom ware Detection and prevention through strategically hidden Decoy file”, international Journal of network security(2023)

[10] Araujo Frederico, Schales Douglas Leo,stoecklin Marc philippe , Taylor Teryl paul.,Integritytheft protection and cyber deception using a deception based filesystem(2019).