LAGO

A Generative Adversarial Network (GAN) Solution for Synthetically Generated Botnet Attacks Data Samples

Nikolaos Peppes[1], Theodoros Alexakis[1], Emmanouil Daskalakis[1], Evgenia Adamopoulou[1] and Konstantinos Demestichas[2]

1. School of Electrical and Computer Engineering, National Technical University of Athens
2. Department of Agricultural Economy and Development, Agricultural University of Athens

Abstract: The trend of digitization in almost every aspect of daily human life has raised serious concerns about security in the digital world. With new technologies, solutions, and tools emerging daily, new vulnerabilities also arise. Botnets are among the most widespread cyber-threats in the modern digital landscape, as they can breach and affect entire organizations or domains by infecting just a single device in a network. This study involves the design and implementation of a Generative Adversarial Network (the so-called ZDGAN) to synthetically generate botnet attack data samples, which are assessed for both quality and quantity using specific data quality indicators. The quality assessment results show that the produced data are very similar to the original ones. Therefore, the significance of GANs in data generation processes is almost undeniable. Furthermore, increasing the volume of annotated data can lead to the improvement and enhancement of AI-based cybersecurity solutions that heavily rely on data availability.

1. Introduction

The widespread adoption of digital services in people's daily lives has resulted in an increased demand for cybersecurity. With the proliferation of new software and hardware, detecting known vulnerabilities and zero-day exploits has become a daunting task for cybersecurity professionals. Botnets are one type of software vulnerability and attack that can have disastrous consequences [1]. These attacks allow attackers to remotely control infected machines. To combat these infections, cybersecurity experts are developing proactive systems that utilize machine and deep learning technologies. However, the lack of available training data often hinders the development of these systems. To address this issue, a new study proposes a methodology for generating botnet-type data in a tabular format. This methodology involves the use of Generative Adversarial Networks (GANs) [2] with varying parameterizations to determine the most efficient and reliable way to generate synthetic data with high accuracy while minimizing computational costs. The generated samples will be assessed using a wide range of Graphical Data Quality Indicators, such cumulative sums, absolute log mean and STD diagrams, correlation matrices, and heatmaps.

2. Proposed solution

Generative Adversarial Networks (GANs) [1] utilize an architecture that generates new data based on input data and random noise. GANs consist of two components: the generator and discriminator. The generator uses random noise to create realistic data, while the discriminator classifies input samples as either real or fake. Both components are optimized based on the discriminator's ability to accurately classify real and fake data.

This study aims to evaluate the effectiveness of different GAN architectures [2] in generating synthetic data that accurately represents malicious cyber-attacks, specifically botnet attacks. To accomplish this, the study compares the performance of different GAN architectures for both the generator and discriminator, using the CTU-13 dataset [3] from the Stratosphere IPS. This dataset includes captures of diverse malware samples and normal traffic, with 32 million packets. The training dataset has 216,352 records, with 140,849 marked as "0" for malware and 75,503 labeled as "1" for legitimate. The evaluation dataset has 88,258 records without any labels.

The study utilizes the ZDGAN model architecture [4], which is designed to generate 1D synthetic data from the input dataset. The model was implemented using Tensorflow 2.0 and Keras API. The proposed ZDGAN architecture utilizes the sequential API to stack the different layers of the deep neural network. The generator component includes an input layer that accepts scaled random noise, nine hidden layers activated by the 'ReLU' function, and an output layer activated by the 'linear' function, with the same dimension as the (preprocessed) dataset, i.e., nine feature columns. The discriminator model is also a sequential model with four dense layers.

The first three layers are activated by the 'ReLU' function, and the output layer is activated by the 'sigmoid' function to distinguish input samples as real or fake. A dropout rate of 20% was applied to the visible and two hidden layers of the discriminator model.

After detailing the generator and discriminator models, the proposed ZDGAN model is characterized as a sequential model that integrates these components in an adversarial manner. Figure 1 illustrates how the ZDGAN model uses (preprocessed) botnets data samples to generate synthetic, tabular data.

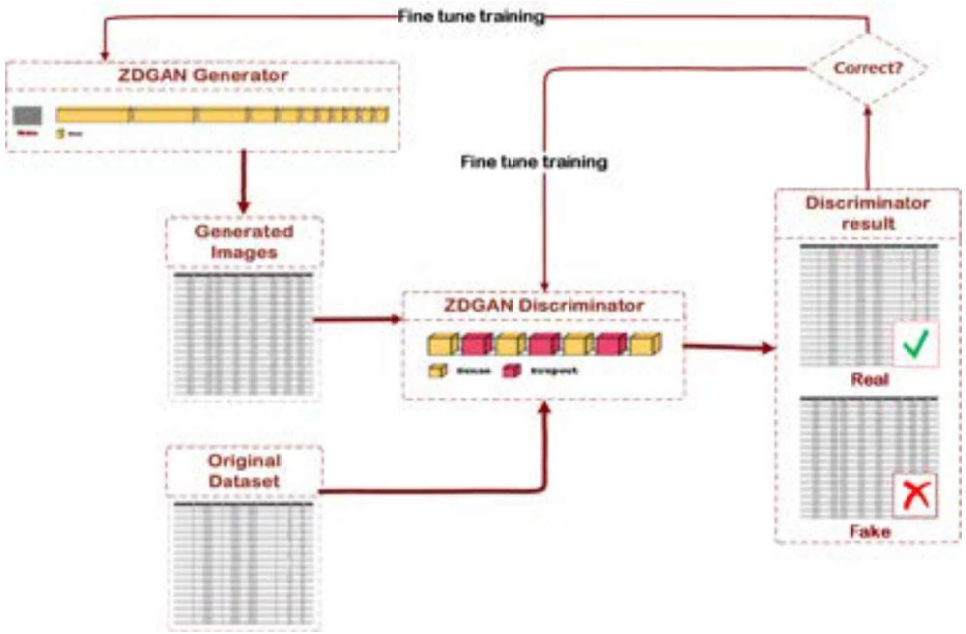

Figure 1. *ZDGAN Model Implementation*

3. Conclusions and Future Work

In conclusion, as digital tools continue to evolve and become more prevalent, the need for effective cybersecurity measures has become increasingly critical. The primary objective of this study is to outline a comprehensive methodology for generating synthetic data for botnet attacks using Generative Adversarial Networks (ZDGAN). The generation process utilizes an open-source dataset, the CTU-13 dataset [3], provided by Stratosphere IPS, which is a collection of network traffic captures that has been widely used in the field of cybersecurity research. This tabular format data is used as input for the suggested ZDGAN architecture [4]. The ZDGAN model generates over 200,000 new botnet data samples that closely resemble the original data. Subsequently, the generated botnet data samples are evaluated using a wide range of Graphical Data Quality Indicators, including cumulative sums, absolute log mean and STD diagrams, correlation matrices, and heatmaps, to assess the quality of the generated data. Overall, this proposed methodology provides a promising approach to improving botnet attack detection and prevention.

Acknowledgements

The work described in this paper is performed in the Horizon Europe project LAGO ("Lessen Data Access and Governance Obstacles"). This project has received funding from the European Union's Horizon Europe research and innovation program under grant agreement No 101073951.

References

1. Shinan, K.; Alsubhi, K.; Alzahrani, A.; Ashraf, M.U. Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review. Symmetry 2021, 13, doi:10.3390/sym13050866.
2. Randhawa, R.H.; Aslam, N.; Alauthman, M.; Rafiq, H.; Comeau, F. Security Hardening of Botnet Detectors Using Generative Adversarial Networks. IEEE Access 2021, 9, 78276–78292, doi:10.1109/ACCESS.2021.3083421.
3. García, S.; Grill, M.; Stiborek, J.; Zunino, A. An Empirical Comparison of Botnet Detection Methods. Computers & Security 2014, 45, 100–123, doi:https://doi.org/10.1016/j.cose.2014.05.011.
4. Peppes, N.; Alexakis, T.; Adamopoulou, E.; Demestichas, K. The effectiveness of Zero-Day Attacks Data Samples Generated via GANs on Deep Learning Classifiers; MDPI Sensors, 2023; ISSN 1424-8220.