Hailey Stewart (A20483446), Amir Stephens (A2039928), Alec Donald (A20489762)

Improving Botnet Detection and Mitigation Techniques Using Machine Learning.

Overview

Botnets have become a major threat to network security, using armies of compromised devices to carry out large-scale attacks like Distributed Denial of Service (DDoS) and spamming. As botnets grow more sophisticated, traditional detection methods - like signature-based and behavior-based techniques - are struggling to keep up.

In this project, we will focus on setting up a practical environment to study and analyze botnet activity using existing tools. We'll simulate botnet attacks, analyze network traffic, and experiment with detection rules to see how well traditional techniques perform in real time. Using tools like Wireshark or Scrapy, we aim to detect malicious traffic patterns and refine rule-based detection methods and train classification algorithms.

Our goal is to highlight both the strengths and limitations of traditional detection techniques, as well as explore how they could be improved. From there we would like to build upon the traditional detection methods, with more advanced topics like various machine learning algorithms, like Naive Bayes or a Decision Tree.

Background

Botnets, networks of compromised devices controlled by a single attacker, have become increasingly prevalent and dangerous in the digital world. These networks can be used to launch Distributed Denial of Service (DDoS) attacks, distribute spam, and conduct other malicious activities at scale. Botnet operators continuously adapt their tactics, making it difficult for traditional detection methods, like signature-based and behavior-based systems, to keep pace.

Most botnets rely on a command-and-control (C&C) structure, where compromised devices (bots) communicate with a central server to receive instructions. The centralization of botnets has led to several detection strategies, including monitoring traffic for known patterns or signatures of botnet communication. However, as botnets evolve—adopting decentralized architectures or employing encryption to hide their activities—these traditional methods struggle to detect new variants.

In response, more advanced techniques have been developed, such as anomaly-based detection, which monitors network traffic for unusual patterns that could indicate botnet activity. These methods have improved detection rates but can generate a significant number of false positives, especially as normal network traffic becomes more complex.

In this project, we will focus on understanding and analyzing the communication methods and attack strategies used by botnets. By simulating these attacks and testing detection techniques in a controlled environment, we aim to evaluate the effectiveness of traditional rule-based detection systems alongside machine learning models such as Naive Bayes. This background sets the stage for our exploration into real-world botnet detection challenges, as well as potential future improvements.

Project Outline

We propose two types of analysis for the project: analytic and experimental

Phase I: Understanding Botnet Architecture and Existing Detection Methods: Outline the fundamentals of botnet architecture, including the communication methods (C&C channels) and

their attack strategies (DDoS, spamming, etc.). Survey existing detection techniques, such as signature-based, behavior-based, and anomaly-based methods.

Phase II: Implement a Network Traffic Analysis System: Set up a simulated environment using existing tools like Wireshark to monitor and analyze network traffic. Focus on identifying botnet activity using rule-based and heuristic approaches rather than developing machine learning models.

Phase III: Experimenting with Detection Rules: Experiment with creating and refining detection rules and signatures for known botnets. Compare their effectiveness in detecting botnet activity in simulated environments, focusing on minimizing false positives and negatives.

Phase IV: Challenges of Botnet Detection: Identify the limitations of rule-based botnet detection and explore how machine learning could enhance detection capabilities in the future.

References

1. Kim, Jiyeon, Minsun Shim, Seungah Hong, Yulim Shin, and Eunjung Choi. 2020. "Intelligent Detection of IoT Botnets Using Machine Learning and Deep Learning" Applied Sciences 10, no. 19: 7009. https://doi.org/10.3390/app10197009
2. Shinan, Khlood, Khalid Alsubhi, Ahmed Alzahrani, and Muhammad Usman Ashraf. 2021. "Machine Learning-Based Botnet Detection in Software-Defined Network: A Systematic Review" Symmetry 13, no. 5: 866. https://doi.org/10.3390/sym13050866
3. Taşcı, Burak. 2024. "Deep-Learning-Based Approach for IoT Attack and Malware Detection" Applied Sciences 14, no. 18: 8505. https://doi.org/10.3390/app14188505
4. Nazir, Ahsan, Jingsha He, Nafei Zhu, Ashsan Wajahat, Xiangjun Ma, Faheem Ullah, Sirajuddin Qureshi, and Mohammad Salman Pathan. “Advancing IOT Security: A

Systematic Review of Machine Learning Approaches for the Detection of IOT Botnets." Journal of King Saud University - Computer and Information Sciences, December 6, 2023. https://www.sciencedirect.com/science/article/pii/S1319157823003749#sec3.

5. Shareef, SK Khaja, R. Krishna Chaitanya, Srinivasulu Chennupalli, Devi Chokkakula, K. V. D. Kiran, Udayaraju Pamula, and Ramesh Vatambeti. "Enhanced Botnet Detection in IOT Networks Using Zebra Optimization and Dual-Channel Gan Classification." Nature News, July 26, 2024. https://www.nature.com/articles/s41598-024-67865-2#Sec10.