УДК 004.056

РАЗРАБОТКА МЕТОДИКИ ОБНАРУЖЕНИЯ БОТНЕТОВ НА ОСНОВЕ АНАЛИЗА ДАННЫХ DNS-ЗАПРОСОВ С ИСПОЛЬЗОВАНИЕМ ГЛУБОКОГО ОБУЧЕНИЯ

Као.Н.Т.[1]

Научный руководитель – старший научный сотрудник, кандидат технических наук, Канжелев.Ю.А. [1]

[1]Университет ИТМО

Введение

В последние годы ботнеты считаются одной из основных угроз безопасности информационных систем, подключенных устройств и пользователей Интернета. Это связано с тем, что ботнеты напрямую связаны со многими типами атак и злоупотреблений в Интернете, такими как крупномасштабные распределенные атаки типа «отказ в обслуживании» (DDoS), рассылка спама, передача и распространение вредоносного кода, создание фальшивых кликов и лайков, а также кража конфиденциальная информация. Кроме того, опасные атаки, поддерживаемые ботнетами, также включают подмену URL-адресов, подмену системы доменных имен (DNS), атаки с использованием вредоносного кода в веб-приложениях и сбор информации от пользователей. Вот почему обнаружение, удаление ботнетов и устройств, зараженных вредоносным программным обеспечением, очень важно. Разработано множество научных публикаций и методов обнаружения ботнетов, но они все еще имеют некоторые ограничения и потенциал для дальнейшего развития. С точки зрения точности обнаружения ботнетов, методы глубокого обучения демонстрируют преимущество. В моем исследовании также используется глубокое обучение, но в гибридном варианте, сочетающем различные алгоритмы глубокого обучения для повышения точности обнаружения ботнетов.

Основная часть

В рамках исследовательской работы решаются следующие основные задачи:

1) Обзор ботнетов и ботнетов DGA – общее представление о проблеме; принципы функционирования ботнетов; определение DGA-ботнетов; обоснование того, почему набор данных DNS-запросов является подходящим и эффективным для обнаружения ботнетов;

2) Аналитический обзор современной литературы по тематике исследования – анализ актуальной литературы по проблеме исследования с целью выявления существующих методов, их преимуществ и недостатков, а также определения нового направления решения;

3) Разработка методики обнаружения ботнетов на основе анализа данных DNS-запросов с использованием глубокого обучения – разработка методов обнаружения ботнетов с использованием методов глубокого обучения, таких как CNN-1D и LSTM, помогает лучше улавливать информацию из доменных имен, тем самым повышая возможности обнаружения;

4) Экспериментальная проверка и оценка результатов полученного решения по сравнению с другими передовыми решениями – использование наборов данных из надежных источников, таких как Alexa и Netlab 360, для обучения и тестирования модели. Применение показателей эффективности – Accuracy, Precision, Recall и F1-score – для оценки результативности модели. А также сравнение его с другими решениями.

Выводы

Был предложен новый метод обнаружения ботнетов, основанный на анализе DNS-запросов с использованием комбинации алгоритмов глубокого обучения, таких как

одномерная сверточная нейронная сеть (1D-CNN) и сеть долгой краткосрочной памяти (LSTM). Экспериментальные результаты показали высокую способность к классификации нормальных доменных имен и доменных имен, генерируемых ботнетами, с точностью более 98%.

Литература

1. MANASRAH, Ahmed M.; KHDOUR, Thair; FREEHAT, Raeda. DGA-based botnets detection using DNS traffic mining. Journal of King Saud University-Computer and Information Sciences, 2022, 34.5: 2045-2061.
2. Zhou, Shaofang, et al. "CNN-based DGA detection with high coverage." 2019 IEEE international conference on intelligence and security informatics (ISI). IEEE, 2019.
3. Selvaraj, Sarojini, and Rukmani Panjanathan. "WordDGA: Hybrid Knowledge-Based Word-Level Domain Names Against DGA Classifiers and Adversarial DGAs." Informatics. Vol. 11. No. 4. MDPI AG, 2024.
4. Namgung, Juhong, Siwoon Son, and Yang-Sae Moon. "Efficient deep learning models for DGA domain detection." Security and Communication Networks 2021.1 (2021): 8887881.
5. Harishkumar, S., and R. S. Bhuvaneswaran. "Enhanced DGA detection in Botnet traffic: leveraging N-Gram, topic modeling, and attention BiLSTM." Peer-to-Peer Networking and Applications 18.1 (2025): 55.
6. Zang, Xiaodong, et al. "BotDetector: a system for identifying DGA-based botnet with CNN-LSTM." Telecommunication Systems 85.2 (2024): 207-223.
7. Domain generation algorithm [Электронный ресурс]. – 2023. – URL: https://en.wikipedia.org/wiki/Domain_generation_algorithm.

Обучающийся _____ Као Нгок Туан
(Фамилия И.О.)

Научный руководитель _____ Канжелев Юрий Алексеевич
(Фамилия И.О.)