УДК 004.056.52

А.М. МАХМУТОВ[1], А.А. СКИТЕВ[2]

[1]*ООО «Оу Эйч Ти», Москва*

[2]*Национальный исследовательский ядерный университет «МИФИ», Москва*

АНАЛИЗ ЭФФЕКТИВНОСТИ АППАРАТНЫХ СИСТЕМ ОБНАРУЖЕНИЯ И СМЯГЧЕНИЯ DDOS-АТАК

Проблема безопасности сетевой инфраструктуры становится всё более актуальной. DDoS-атаки представляют серьёзную угрозу для онлайн-сервисов организаций. Анализ существующих аппаратных систем обнаружения атак показал, что они неэффективны против современных DDoS-атак. Для защиты сетевой инфраструктуры необходимы современные алгоритмы, основанные на машинном обучении и энтропии.

Согласно отчету группы компаний «Солар» [1] за первое полугодие 2024 г. на Российские организации было совершено больше на 355 тыс. DDoS-атак чем за весь 2023 г. Средняя мощность атак на Российские компании также выросла с 2.4 Гбит/с за аналогичный период в 2023 г. до 4 Гбит/с.

Критически важно иметь средство обнаружения и смягчения DDOS-атак. Для этих целей был проведен анализ аппаратных решений в области обнаружения атак на предмет возможности их использования в современных реалиях.

В [2] представлен метод вычисления корреляционной меры для сравнения трафика с эталонным. Несмотря на то, что авторами указано, что время определения атаки на их реализации на FPGA составляет менее одной микросекунды, алгоритм требует одну секунду на сбор признаков из трафика. Это не позволяет использовать данный алгоритм для достаточно быстрой реакции на атаку.

В [3] представлен механизм смягчения атаки, основанный на алгоритмах «Hop Count Filtering» [4] и Ingress/Egress-фильтрации. В проведенном эксперименте алгоритм Ingress/Egress-фильтрации сводится к черному и белому спискам. В [3] и [4] трафик для оценки алгоритма был сгенерирован самостоятельно, и авторы не проводят параметры экспериментов, поэтому проведенные эксперименты нельзя воспроизвести точно. Нами проведено моделирование работы алгоритма на наборах данных, используемых для оценки систем обнаружения вторжения. При анализе алгоритма «Hop Count Filtering» на наборе данных, собранном на основе атаки ботнета MIRAI

(2016 г.), удалось получить корректное определение 7% нелегитимного трафика. Результаты представлены на рис. 1. При использовании набора данных CIC-DDoS2019 [5] алгоритм считал все пакеты легитимными.

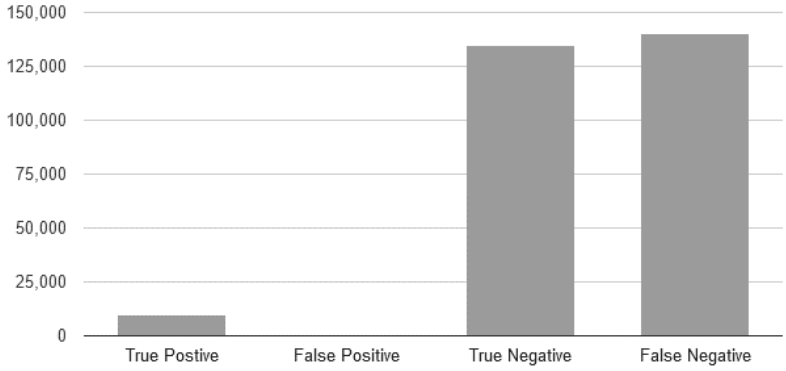

Рис. 1. Результаты HCF на наборе данных ботнета MIRAI

Заключение

Таким образом, на в настоящее время аппаратные системы, представленные в работе, не являются эффективным средством обнаружения и смягчения DDOS-атак. В связи с этим для защиты критически важной сетевой инфраструктуры необходимо использовать современные алгоритмы, основанные на машинном обучении, энтропии. Для того, чтобы справиться с постоянным возрастанием мощности атак, необходимо также использовать специально разработанные аппаратные решения.

Список литературы

1. Отчет о DDoS-атаках на онлайн-ресурсы российских компаний в I полугодии 2024 г. // ГК Солар URL: https://rt-solar.ru/analytics/reports/4677/ (дата обращения: 09.09.2024).
2. Hoque N., Kashyap H., Bhattacharyya D. K. Real-time DDoS attack detection using FPGA. Computer Communications. 2017. Т. 110. С. 48–58.
3. Pham-Quoc C., Nguyen B., Thinh T. N. Fpga-based multicore architecture for integrating multiple ddos defense mechanisms. ACM SIGARCH Computer Architecture News. 2017. Т. 44. №. 4. С. 14–19.
4. Jin C., Wang H., Shin K. G. Hop-count filtering: an effective defense against spoofed DDoS traffic. Proceedings of the 10th ACM conference on Computer and communications security. 2003. С. 30–41.