Обнаружение источников вредоносного трафика DDOS атак методами статистического анализа

О.С. Терновой
АлтГУ, г. Барнаул

Рассматриваются атаки, направленые на отказ в обслуживании (DDOS атаки), которые представляют серьезную угрозу для многих сетевых ресурсов. Для предотвращения атак такого типа необходимо выявить и блокировать источники вредоносного трафика – компьютеры участники зомби-сети. Обнаружение вредоносного трафика реализуется различными методами – математическими, поведенческими и т.д. Среди математических методов особый интерес представляют методы статического анализа. Каждый источник трафика характеризуется определенными значениями параметров сетевой активности. Анализируя эти параметры можно сделать вывод о принадлежности источника к зомби сети. С помощью среднеквадратичного отклонения можно рассчитать допустимые границы для этих параметров. В случае нарушения одним или несколькими параметрами этих границ можно сделать вывод о начале DDOS атаки или появление вредоносного трафика и принадлежности источника.

На основании этих методов создан алгоритм по обнаружению DDOS атаки и выявлению вредоносного трафика. Апробация и исследование алгоритма проведена в условиях соответствующих данным сетевой активности реальных DDOS атак. Для снижения ошибки, обнаружения источников вредоносного трафика, подобным способом, предлагается учитывать сезонные колебания значений сетевой активности.

В результате исследования, выявлены наиболее важные параметры сетевой активности, отклонение по которым однозначно может свидетельствовать о принадлежности источника к зомби-сети. Выявлена зависимость между различными параметрами сетевой активности. Доказана эффективность учета сезонности.

При проведении исследований создана распределенная сеть для проведений нагрузочных тестов с использование программы Apache JMetr. В рамках указанной сети происходит имитация DDOS атак различного уровня сложности. Атаки максимально приближены к реальным DDOS атакам. Сценарии проведения атак создаются на основании лог-файлов реальных серверов подвергшихся нападению. Это позволяет в лабораторных условиях моделировать, повторять и изучать реальные атаки и новые приемы, которыми пользуются злоумышленники.