6. Евсютин О.О. Использование клеточных автоматов для решения задач преобразования информации [Текст] / О.О. Евсютин, С.К. Росошек // - Доклады ТУСУРа. — 2010. — № 1(21), часть 1. — С. 173–174.
7. Евсютин О.О. Шифр на основе обратимых клеточных автоматов на разбиении [Текст] / О.О. Евсютин, С.К. Росошек // - Безопасность информационных технологий. — 2007. — № 4. — С. 27–31.
8. Евсютин О.О. Приложения клеточных автоматов в области информационной безопасности и обработки данных [Текст] / О.О. Евсютин, А.А. Шелупанов // - Доклады ТУСУРа. — 2012. — № 1(25), часть 2. — С.119–125.
9. Мещеряков Р.В., Крайнов А.Ю., Шелупанов А.А. Модели надежности передачи информации в защищенной распределенной телекоммуникационной сети [Текст] /Р.В. Мещеряков, А.Ю. Крайнов, А.А. Шелупанов// - Известия Томского политехнического университета. Том 313 N5, 2008.- С. 60-63.

***Евсютин О.О.**, аспирант каф. КИБЭВС ФГБОУ ВПО ТУСУР, **Миронова В.Г.**, аспирант каф. КИБЭВС ФГБОУ ВПО ТУСУР*

УДК 004.056.5

СНИЖЕНИЕ ОШИБКИ ОБНАРУЖЕНИЯ DDOS АТАК СТАТИСТИЧЕСКИМИ МЕТОДАМИ ПРИ УЧЕТЕ СЕЗОННОСТИ

О.С. Терновой, А.С. Шатохин

В статье рассматривается задача раннего обнаружения DDOS атак с использованием статистических методов при учете сезонности, в работе сетевого ресурса. Предложена гипотеза раннего диагностирования DDOS атаки. Гипотеза апробирован на данных соответствующих реальным DDOS атакам, полученным из лог файлов различных web серверов. Для апробации алгоритма разработан программный комплекс, в который входят: база данных, программа для экспорта лог файлов в базу данных, программа детектор, которая проводит анализ и диагностирует начало DDOS атаки, различными способами.

Ключевые слова: DDOS атака, распределенная атака, отказ в обслуживании, зомби сеть, BOT сеть, среднеквадратичное отклонение, статистический анализ, ранее обнаружение, Hypertext Preprocessor, сезонность

Введение

DDOS атаки – распределенные атаки направленные на отказ в обслуживании, продолжают оставаться, одной из важнейших угроз в сети. Атаки такого типа могут быстро истощить сетевые ресурсы или мощности сервера, что приведет к невозможности получить доступ к ресурсу, и вызовет серию негативных последствий: упущенная прибыль, невозможность воспользоваться услугами и произвести различные транзакции и т.д[1].

В DDOS атаке в роли атакующего выступает так называемая бот сеть или «зомби» сеть. Зомби сеть может насчитывать от нескольких десятков до тысяч хостов. Обычно это нейтральные компьютеры, которые, в силу каких-то причин (отсутствие файрвола, устаревшие базы антивируса, и т.д.), были заражены, вредоносными программами. Программы, работая в фоновом режиме, непрерывно посылают запросы на атакуемый сервер, выводя его таким образом из строя [2].

В настоящий момент не существует какого-то универсального средства для противодействия DDOS атакам. Даже такие крупные компании как Microsoft, eBay, Amazon, Yahoo страдают от DDOS атак и не всегда могут с ними справиться [2].

Постановка задачи

Для противодействия распределенным атакам, направленным на отказ в обслуживание, требуется выполнение двух основных задач [3].

1. Диагностировать DDOS атаку на самых ранних стадиях. Чем раньше будет обнаружена DDOS атака, тем раньше сможет включиться в игру сетевой администратор и тем раньше можно будет начать проводить анти DDOS мероприятия. Кроме того при обнаружении DDOS атаки, можно будет не дожидаясь реагирования администратора, автоматически запустить мероприятия по противодействию атаки: задействовать резервные каналы связи, включить фильтры, и т.д.
2. Вторая задача связанна с разделением общего потока трафика на вредоносный и обычный. Поняв, какие из клиентских запросов являются результатом DDOS атаки, можно будет создать соответствующие правила для межсетевого экрана или ACL правила для маршрути-

затора, или же в случае масштабной атаки, передать эти данные на вышестоящие маршрутизаторы.

Первая из этих задач является достаточно новой. Несколько лет назад, основной являлась именно задача по «сортировке» трафика. Однако злоумышленники постоянно совершенствуют способы проведения атак такого типа. И современные атаки отличаются сложностью и наличием этапа подготовки. Во время подготовительного этапа злоумышленник пытается выявить наиболее уязвимые для атаки места. Например, для web сервера такими местами могут быть определенные скрипты, которые совершают большое количество запросов к базе данных или чрезмерно используют процессорное время. Для выявление этих мест злоумышленник может совершать серию мини DDOS атак, на различные скрипты, отслеживая при этом время ответа сервера и время выполнения скрипта. Найдя уязвимое место, злоумышленник сможет парализовать работу сервера используя бот сеть меньшего размера. С другой стороны, если диагностировать атаку удастся уже на этом этапе, можно будет задействовать автоматические средства предотвращения атаки, а у системного администратора будет время подготовиться - оптимизировать скрипты чрезмерно загружающие ресурсы компьютера, создать фильтры и т.д.

На сегодняшний день для обнаружения DDOS атак, и создания специальных фильтров для отсечения вредоносного трафика, применяются разнообразные методы и подходы.

Среди основных методов, можно выделить методы базирующиеся на статистическом анализе. Это количественный анализ, анализ среднеквадратичных отклонений, кластерный анализ и т.д. Все эти виды анализа могут оценивать различные параметры сетевой активности, и диагностировать начало атаки либо определять вредоносный трафик.

Основными параметрами, по которым проводится анализ, могут быть:

- Количество запросов за определенный период
- Скорость поступление запросов
- Количество запросов с определенного источника или из определенной сети
- Количество запросов к определенному пункту назначения (для web сервера, это может быть конечный скрипт)
- Время между запросами
- Другие различные параметры сетевой активности

С помощью среднеквадратичного отклонения, можно рассчитать допустимую границу для одного из параметров сетевой активности. Например, для количества запросов за какой-то период времени. В случае если, граница будет нарушена, это может стать свидетельством начала атаки. Так как в разное время нагрузка на сетевой ресурс, так же может быть разной, то для раннего обнаружения атаки необходим постоянный мониторинг и пересчет границ для каждого временного шага. Это позволит определить атаку, если она начнется в период небольшой сетевой активности. Или если злоумышленник ищет потенциально уязвимые места на сервере, проводя мини ddos атаки и изучая поведения сервера. В случае если верхняя граница задана строго, и злоумышленник проводит мини атаки в период наименьшей сетевой активности, он может не нарушать заданную границу и его действия будут не обнаружены. Атака будет обнаружена тогда, когда злоумышленник найдет потенциально уязвимое место, и предпримет на него атаку. Постоянный мониторинг активности и перерасчет допустимых границ позволяет этого избежать. В период меньшей сетевой активности, верхняя граница снизиться. Однако и этот метод имеет ряд минусов.

Во-первых. Злоумышленник может начать атаку постепенно. Показатели активности на каждом шаге будут плавно повышаться, но при этом не будут нарушать границ. Так как при расчете среднеквадратичного отклонения используются последние n интервалов, в том числе и те которые уже содержать данные атаки, то злоумышленник постепенно увеличивая интенсивность атаки сможет отодвигать границу.

Во-вторых. Выбор размера периода n, для расчета среднеквадратичного отклонения, не является однозначным.

Если n будет слишком велико, полученная граница, будет слишком высоко, если используется малое значение n, то возможны частые срабатывания. Выбрать же оптимально значение n в этой ситуации будет не возможно, так как любое его значение может захватывать два разных периода. Например, даже малое значение n, рассчитываемое в начале рабочего дня, будет захватывать данные и ночного периода, связанного с низкой активностью и дневного периода, который характеризуется большей нагрузкой на сетевые ресурсы.

Для того, чтобы в этом случае, предотвратить ложное срабатывание, связанное, с

началом рабочего дня, потребуется использовать такое значение n в котором будут данные за несколько дней. Либо контролировать сразу несколько временных периодов – при срабатывании на минутных интервалах, рассмотреть часовые или суточные периоды. Но это в свою очередь приведет к уменьшению точности и атака будет определена с опозданием[4].

Учет сезонности при обнаружении DDOS атак

В качестве гипотезы можно предположить, что более высокую точность, в этих случаях может дать учет различных периодов активности, и сравнение сходных между собой периодов.

Пусть xi количество запросов к серверу за один час. Сервер испытывает сравнимую суточную нагрузку. Количество суточных периодов n. Тогда запросы к серверу можно записать в виде матрицы:

x1 1, x1 2 , x1 3 …x1 24
x2 1, x2 2 , x2 3 …x2 24
……
xn 1, xn 2 , xn 3 …xn 24

Каждая строка матрицы включает в себя суточные данные о количестве запросов. Первая строка отражает данные текущих суток, в этой связи она может быть, заполнена не до конца. Расчет среднеквадратичного отклонения, в этом случае может проводиться двумя способами [5].

Обычным способом, с учетом определенного числа последних значений, например, так:

x2 1, x2 2 , x2 3 …x2 24, x1 1, x1 2 , x1 3 ,x1 4

В этом случае, значения берутся из строк матрицы.

С учетом, сезонности. В этом случае расчет можно проводить по столбцам.

xn 1,… x2 1, x1 1

Если мы находимся в i периоде, можно рассчитать границу для i+1 периода. Используя значения i+1 столбца. Если сетевой ресурс испытывает нагрузку, связанную с недельными или суточными циклами, то в этом случае необходимо, исключить строки, которые соответствуют праздничным и выходным дням. Или даже использовать только каждую седьмую строку, то есть сравнивать, например, только период с 11:00 до 12:00, для каждого понедельника и т.д.

Проверка гипотезы

Апробация данной гипотезы проведена на реальных данных, полученных из лог файлов различных web сайтов, которые содержат в себе нормальные данные и данные соответствующие DDOS атакам.

Список рассматриваемых сайтов:
http://ankt.ru
http://www.corrupcia.net/
http://litm.ru

Лог файл представляет собой, стандартный файл access_log web сервера Apache.

Предварительно данные из лог файлов были обработаны вручную и проанализированы. В результате были выделены сезонные периоды, а так же точно обозначено время начала атак.

Диагностирование DDOS атаки проводилось различными методами:

Анализ сходных сезонных периодов

Анализов последних n периодов, при различных значениях n

Анализ последних n периодов, различной размерности(минуты, часы и т.д.), для разных значений n

В связи с тем что лог файлы имеют свой специфичный формат, их анализ стандартными методами является затруднительным. Для проведения анализа был создан скрипт извлекающий из лог файла необходимые данные и экспортирующий их в базу данных. Скрипт был реализован с помощью языка PHP (Hypertext Preprocessor). Предпочтение данному языку программирования было отдано в связи с наличием богатого инструментария по работе со строками и регулярными выражениями [6]. В качестве системы управления базами данных была выбрана свободно распространяемая СУБД MySQL версии 5.5.23. Использование СУБД позволило ускорить процесс обработки и анализа данных и сделать его более гибким.

Для проведения собственно самого анализа так же была разработана отдельная программа. Язык реализации программы PHP, в данном случае его использование позволило выдержать созданный программный комплекс в одном ключе, и дало возможность реализовать web интерфейс. Web интерфейс может быть доступен для системного администратора с любого компьютера и позволяет в удаленном режиме диагностировать атаку и выявлять во входящем трафики различные аномалии. В дальнейшем планируется доработать программу для работы в полностью автоматическом режиме. В этом случае данные из лог файла должны экспортироваться в базу данных в режиме реально-

го времени. Анализ должен происходит после каждого нового добавления данных. В случае диагностирования начала атаки, программ будет рассылать необходимые уведомления и автоматически задействовать мероприятии по противодействию атаке.

Выводы

Метод анализа с учетом сезонности, показал более высокую точность обнаружения DDOS атаки, и более короткое время, которое прошло с момента начала атаки и до её диагностирования. На графике отражается количество запросов к серверу за секунду, соответствующие периоду начала DDOS атаки. Ось X – временной интервал. Одно деление соответствует 10 минутам. Ось Y - количеству запросов к серверу за секунду. На основании IP адресов, принадлежащих компьютерам бот сети, которые были выявлены при анализе лог файлов, удалось точно установить момент начала атаки. На графике он соответствует 24 периоду. Учет сезонности помог выявить DDOS атаку уже в 31 периоде. Другие методы показали худшие результаты. При слишком больших значениях n атаку удалось диагностировать только на 42 периоде, при малых происходило ложно срабатывание в 14 периоде.

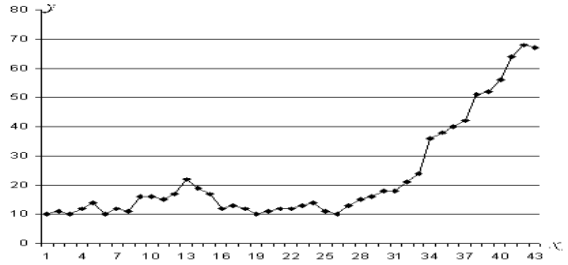

Рисунок 1 - Количество запросов в период начала DDOS атаки, 10 минутный интервал

На основании IP адресов, принадлежащих компьютерам бот сети, которые были выявлены при анализе лог файлов, удалось точно установить момент начала атаки. На графике он соответствует 24 периоду. Учет сезонности помог выявить DDOS атаку уже в 31 периоде. Другие методы показали худшие результаты. При слишком больших значениях n атаку удалось диагностировать только на 42 периоде, при малых происходило ложно срабатывание в 14 периоде.

В среднем по всем тестам, время обнаружение DDOS атаки, методами с учетом сезонности, сократилось в 4 раза. Так же сократилось число ложных срабатываний.

Достаточно большой сложностью, возникающей при использовании данного метода, является правильный выбор сходных между собой периодов. Для апробации были выбраны данные с таких серверов, периоды работы которых однозначно определялись и не вызывали сомнения. Однако определить различные периоды в работе, например, крупного магистрального маршрутизатора, может быть сложно. Его активность может не подчиняться суточным или недельным периодам. Но так же иметь свои периоды, которые могут представлять из себя сложные периоды, получаемые в результате сложения, активности различных групп пользователей. Например, пользователей из разных часовых поясов. Кроме того уже существующие сезонные периоды, могут изменяться, к ним могут добавляться новые периоды. Поэтому при постоянном мониторинге трафика, необходимо будет проводить его кластеризацию и выявлять новые сезонные периоды в работе.

СПИСОК ЛИТЕРАТУРЫ

1. DDOS атаки [Электронный ресурс] / Режим доступа: http://localname.ru/soft/ataki-tipa-otkaz-v-obsluzhivanii-dos-i-raspredelennyiy-otkaz-v-obsluzhivanii-ddos.html
2. Предотвращение атак с распределенным отказом в обслуживании (DDoS) : [Электронный ресурс] / Официальный сайт компании Cisco. – Режим доступа: http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927.html
3. Методы защиты от DDOS нападений [Электронный ресурс] / Режим доступа: http://www.securitylab.ru/analytics/216251.php
4. Терновой О.С. Ранее обнаружение DDOS атак методами статистического анализа [Текст] /О.С. Терновой/ Перспективы развития информационных технологий. – Новосибирск, изд. «Сибпринт», С. 2012 – 212
5. Боровков А.А., Математическая статистика. Оценка параметров проверка гипотез [Текст] / А.А. Боровков - М.: «Наука», 1984 - 280 с.
6. Бенкен Е.С, PHP, MySQL, XML. Программирование для Интернета [Текст] / Е.С. Бенкен – Санкт-Петербург: «БХВ-Петербург», 2011 – С. 336.

*Аспирант **О.С. Терновой** – Алтайский Государственный Университет, каф. Вычислительной техники и электроники, Физико-технического факультета, (3852)36-35-71, ternovoi@vc.asu.ru; к.т.н., доцент. **А.С. Шатохин** – Алтайский Государственный Университет, заведующий каф. Вычислительной техники и электроники, (3852)36-86-40, sas@asu.ru;*