ФГБОУ ВПО "Алтайский государственный университет"
Терновой Олег Степанович
начальник отдела корп. сети и комп. классов

Средство обнаружения аномального трафика сетевых атак направленных на отказ в обслуживании

В докладе рассказывается о создании средства информационной безопасности по выявлению и противодействию DDOS атакам. По итогам научных изысканий было разработано программное средство. В настоящий момент получено свидетельство о государственной регистрации программного продукта. Сам продукт, отвечает требованиям «открытого исходного кода», внедрен на нескольких площадках Алтайского края.
В свете крупных DDOS атак осуществляемых на сайты таких крупных информационных агентств Алтая, как Атмосфера, Амител, БанкФакс, программный продукт является востребованным и весьма актуальным.
Результаты научного исследования и созданный программный продукт отмечены дипломами и наградами различных уровней и научных конференций.
По мотивам научных исследований и программной реализации выпущен цикл статей с конкретными рецептами, для системных администраторов, позволяющий реализовать данную разработку на собственной площадке для любой платформы и с использованием любого языка разработки.

Введение

DDOS атака – распределенная атака направленная на отказ в обслуживании. В результате атаки такого типа, атакуемый сетевой ресурс получает лавинообразное количество запросов, которые не успевает обработать. Источником вредоносных запросов являются так называемее зомби сети, состоящие большей частью из компьютеров обычных пользователей, в силу каких-то причин зараженных вредоносным ПО.

DDOS атаки являются оружием массового поражения. Крупным DDOS атакам подвергаются сайты правительства и органов власти, сайты ведущих IT корпорация Amazon, Yahoo, Microsoft и т.д. Эти мощные корпорации, имеющие огромные ресурсы не всегда могут справиться с атаками, и отразить нападение.

Однако в большинстве своем DDOS атаки направленные на вывод из строя небольших интернет ресурсов: интернет магазинов, сайтов СМИ, интернет представительств имеют низкую или же среднюю степень интенсивности. Применять для противодействия таким атакам корпоративные средства, связанные с внедрением дополнительных серверов или внешней фильтрацией трафика, экономически нецелесообразно. Рынок же средств противодействия атакам средней и малой эффективности представлен крайне скудно. И в большинстве случаев, системные администраторы таких ресурсов противостоят атакам самостоятельно не использую специализированных средств.

Сегодня для фильтрации вредоносного трафика с успехом используют принципы машинного обучения. Однако для успешной реализации таких фильтров необходимо иметь две актуальные обучающие выборки. Одну соответствующую вредоносному трафику, другую благонадежному.

При отражении атаки, многие системные администраторы для обучения классификаторов вынуждены подготавливать обучающие выборки вручную.

Этот способ достаточно трудоемкий и долгий. Кроме того, злоумышленник уже в процессе атаки может менять поведение запросов и таким образом вынуждать администратора заново подготавливать обучающие выборки. В этой ситуации злоумышленник работает на опережение, успевая вызывать перебои в работе сервера.

В данной работе, автор ставит перед собой цель разработать алгоритм противодействия HTTP-flood DDOS атакам, средней и малой интенсивности. Алгоритм должен отвечать следующим требованиям:

- Кросс платформенность
- Быстрота развертывания
- Работа в автоматическом режиме
- Работа только с теми данными, которые имеются в наличии администратора web ресурса
- Приемлемая стоимость внедрения

Основная часть

Для получения актуальной выборки соответствующей благонадежному трафику, оптимально использовать алгоритм раннего обнаружения DDOS атак, учитывающий сезонные колебания нагрузки на сетевой ресурс. Использование данного алгоритма позволяет достаточно точно оценить момент начала атаки. А так же определить начало атаки на ранних периодах, когда злоумышленник может дозировано начать подмешивать вредоносный трафик, для негативного обучения фильтров.

Суть алгоритма обнаружения начала атаки сводиться к расчету среднеквадратичного отклонения основных количественных свойств сетевой активности и последующего сравнения прогнозного и фактического значений. Для расчета среднеквадратичного отклонения используются последние n периодов, актуальных сезонов. Например, период с 8-00 до 9-00, каждого понедельника.

Точное определение начала атаки позволяет отнести весь предшествующий трафик к благонадежной выборке.

Трафик приходящий после начала атаки будет включать в себя как вредоносный, так и легитимный трафик.

В первом приближении выделить злонамеренный трафик можно с помощью алгоритма кластеризации k-means. Данный алгоритм позволяет проводить кластеризацию при заранее известном числе кластеров.

Суть метода заключается в том, что на каждой итерации перевычисляется центр масс для каждого кластера, полученного на предыдущем шаге, затем векторы разбиваются на кластеры вновь в соответствии с тем, какой из новых центров оказался ближе по выбранной метрике.

Шаг завершается, когда на какой-то итерации не происходит изменения кластеров. Это происходит за конечное число итераций, так как количество возможных разбиений конечного множества, конечно, а на каждом шаге суммарное квадратичное уклонение уменьшается, поэтому зацикливание невозможно.

В случае анализа лог-файлов, кластеризацию можно проводить отдельно по каждой группе данных. Например, по количеству запросов с определенного адреса и по количеству запросов к определенной странице. В этом случае окончательная выборка будет представлять собой запросы, попадающие в пересечение различных групп данных, по каждому кластеру.

Для дальнейшего уточнения выборки с вредоносным трафиком предлагается использовать наивный Байесовский классификатор. Критериями работы первичной кластеризации и классификатора будут являться:

- Количественная оценка полученной выборки. Если количество запросов в наблюдаемый период составило n, среднее количество запросов характерное для благонадежного трафика m. То количество вредоносных запросов можно оценить как n-m.
- Качественная оценка полученной выборки. Выборка благонадежного трафика полученная после начала атаки должна максимально соответствовать выборке благонадежного трафика, полученного до начала атаки.
- Центр масс выборки благонадежного трафика полученного после начала атаки должен соответствовать усредненному центру масс аналогичных сезонных выборок предшествующих началу атаки.

Реализация программной части.

В качестве источника анализируемых данных выступает стандартный access log, одного из самых популярных web-серверов – Apache.

%h %l %u %t \"%r\" %>s %b \"%{Referer}i\" \"%{User-Agent}i\"

В котором:

- **%h** — хост/IP-адрес, с которого произведён запрос к серверу;
- **%t** — время запроса к серверу и часовой пояс сервера;
- **%r** — тип запроса, его содержимое и версия;
- **%s** — код состояния HTTP;

- **%b** — количество отданных сервером байт;
- **%{Referer}** — URL-источник запроса;
- **%{User-Agent}** — HTTP-заголовок, содержащий информацию о запросе (клиентское приложение, язык и т. д.);
- **%{Host}** — имя Virtual Host, к которому идет обращение.

Для удобства обработки и хранения. Данные из лог файла с интервалом в одну минуту экспортируются в базу данных.

В качестве сервера баз данных используется mySQL. На сегодняшний момент это один из самых распространенных и доступных серверов баз данных доступных на подавляющем количестве хостингов web-сайтов.

В качестве среды разработки был выбран PHP. Данное средство разработки выбрано не случайно. Во-первых, PHP является одним из самых популярных средств разработки. Возможность исполнения php-скриптов есть практически на каждом сервер предоставляющем услуги хостинга. Значит, у системного администратора не будет проблем с внедрением данного решения. Во-вторых, данный язык имеет, богаты инструментарии, позволяющий гибко обрабатывать полученные данные.

Алгоритм работы программы

1. Программа постоянно анализирует поступающий трафик на предмет начала атака.
2. В случае начала атаки. Фиксируется точка начала атаки и в базе данных создаются две дополнительные таблицы соответствующие благонадежному трафику и трафику, пришедшему после начала атаки.
3. С помощью алгоритма k-means трафик пришедший после начала атаки делиться на две группы.
4. На основании вредоносного трафика создаются необходимые запрещающие правила для firewall’a.

Апробация результатов

Для апробации работы средства противодействия, на базе компьютерных классов Алтайского Государственного Университета создан аналог DDOS сети. В качестве клиентов сети и атакуемого сервера выступают физические компьютеры, имеющие следующие технические и системные характеристики:

- процессор: Celeron Dual 2600 MHz;
- размер оперативной памяти: 2Gb;
- размер жесткого диска: 250Gb;
- сетевой адаптер: 100 Mb/s;
- операционная система: Windows XP Professional, Service pack 3.

Использование в качестве клиентов зомби-сети физических компьютеров позволило получать более точные данные, по сравнению с данными получаемыми в сетях, состоящих из

виртуальных компьютеров запущенных на одной физической платформе. На каждом зомби-компьютере запущена консольная версия программа Apache JMetr, для операционной системы Windows XP. Посредством данной программы была создана и проведена серия нагрузочных тестов, имитирующих DDOS атаку средней эффективности.

Вывод

Полученное средство противодействия соответствует целям поставленным во введении.

Работа данной программы, равно как и теоретическая часть алгоритма, были апробированы в лабораторных условиях с использованием данных, соответствующих реальным DDOS атакам. Использование данного средства позволило уменьшить время реакции на атаку в 5 раз. И увеличить точность обнаружение вредоносного трафика в 3 раза. По сравнению с реакцией системного администратора на DDOS атаку в ручном режиме.