УДК 004.056.5

О. С. Терновой

Методика и средства раннего выявления и противодействия угрозам нарушения информационной безопасности в результате DDOS атак

O. S. Ternovoy

Methods and Means for Early Detecting and Countering Threats to Information Security Breaches as a Result of Ddos Attacs

Представлен оригинальный алгоритм по классификации вредоносного и благонадежного трафика. В основе алгоритма лежит использование статистических методов: метод k-means, теоремы Байеса и Байесовского классификатора. Использование данного алгоритма позволяет точно фиксировать начало атаки, а также получать обучающие выборки, которые могут быть использованы для обучения нейронных сетей и других различных классификаторов, в том числе для фильтрации нежелательного трафика.

На базе алгоритма реализовано программное средство по обнаружению начал атаки и классификации вредоносного трафика.

Программное средство прошло апробацию в рамках специализированной нагрузочной сети, созданной на базе компьютерных классов АлтГУ.

Ключевые слова: DDOS атака, бот сеть, аномальный трафик, DDOS, k-means, статистический анализ.

DOI 10.14258/izvasu(2013)1.2-24

The paper presents an original algorithm for the classification of bad traffic and legitimate traffic. Algorithm is based on the use of Bayes' theorem and Bayesian classifier. The use of this algorithm allows to obtain training samples, which can be used for training neural networks and various other classifiers, as well as to filter out unwanted traffic.

On the basis of the algorithm software the tool for the detection and classification of attacks is implemented.

The software tool has been tested in the stress-network established on the basis of the ASU computer classes.

Key words: DDOS attack, bot network, traffic anomaly, DDOS, k-means, statistical analysis.

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 называемые зомби сети, состоящие большей частью из компьютеров обычных пользователей, в силу каких-то причин зараженных вредоносным ПО [1].

Крупным DDOS атакам подвергаются сайты правительства и органов власти, сайты ведущих IT корпораций Amazon, Yahoo, Microsoft и т. д. Эти мощные корпорации, имеющие огромные ресурсы, не всегда могут справиться с атаками и отразить нападение [2].

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 используя 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 [3].

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 у 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 также определить начало атаки на ранних периодах, когда злоумышленник может дозированно начать подмешивать вредоносный трафик для негативного обучения фильтров.

Суть алгоритма обнаружения начала атаки сводится 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 [4].

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 [5].

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. Качеством работы первичной кластеризации и классификатора будут являться следующие критерии.

Количественная оценка полученной выборки. Если количество запросов в наблюдаемый период составило n, а 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 произведен 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 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 сервере, предоставляющем услуги хостинга. Значит, у системного администратора не будет проблем с внедрением данного решения. Во-вторых, данный язык имеет богатый инструментарий, позволяющий гибко обрабатывать полученные данные [6].

Алгоритм работы программы. Программа постоянно анализирует поступающий трафик на предмет начала атаки.

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.

С помощью алгоритма k-means трафик, пришедший после начала атаки, делится на две группы.

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, была апробирована в лабораторных условиях с использованием данных, соответствующих реальным DDOS атакам.

Предварительно данные были проанализированы и в ручном режиме выделены:

— точка начала атаки;
— вредоносные запросы.

С этими данными сравнивались результаты работы разработанного средства. Также для подтверждения актуальности и конкурентности разработанного средства результаты его работы сравнивались с результатами работы сходных средств:

— Snotr;
— Symantec;
— Kaspersky Anti-Haker.

Результаты экспериментов представлены в сводной таблице.

Результаты экспериментов испытаний различных средств, проведенных в нагрузочной сети

Система	Ложные срабатывания, %	Не обнаруженные вредоносные запросы, %	Среднее время между началом и обнаружением атаки
Kaspersky Anti-Haker	0,7	11	44 мин.
Snort	3,8	10,9	17 мин.
Symantec	4,3	8,4	12 мин.
Разработанное средство	3,8	8,1	4 мин.

.

Библиографический список

1. DDOS атаки [Электронный ресурс]. — URL: 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. — URL: http://www.cisco.com/web/RU/products/ps5887/products_white_paper0900aecd8011e927_.html.

3. Методы защиты от DDOS нападений [Электронный ресурс]. — URL: http://www.securitylab.ru/analytics/216251.php.

4. Терновой О. С., Шатохин А. С. Снижение ошибки обнаружения DDOS атак статистическими методами при учете сезонности // Ползуновский вестник. — 2012. — №3/2.

5. k-means [Электронный ресурс]. — URL: http://ru.wikipedia.org/wiki/K-means.

6. Бенкен Е. С. PHP, MySQL, XML. Программирование для Интернета. — СПб., 2011.