УДК 004.7

# ИССЛЕДОВАНИЕ РАСПРЕДЕЛЕННЫХ ИНФОРМАЦИОННЫХ АТАК И МЕТОДОВ БОРЬБЫ С НИМИ

**Дядин И.П., магистрант; Червинский В.В., к.т.н., доц.**
*(Донецкий национальный технический университет, г. Донецк, Украина)*

Одной из самых актуальных задач в сфере услуг предоставления информации является DDoS-атака (от англ. Distributed Denial of Service, распределённая атака типа «отказ в обслуживании»). Суть таких атак сводится к тому, чтобы всеми доступными способами уменьшить количество полезной нагрузки на ресурс, или вовсе сделать его недоступным. Отказ в обслуживании может быть достигнут при разных условиях, причинами могут служить: ошибки в программном обеспечении которое работает на атакуемом сервисе, недостатки сетевых протоколов и ограничения в пропускной способности канала связи, а так же непродуманная сетевая инфраструктура. Обычно DDoS-атака ведется с так называемого ботнета, это достаточно большое количество компьютеров, а также смартфонов, зараженных вредоносным программным обеспечением.

По данным аналитического отчета компании «Лаборатория Касперского» – «DDoS-атаки второго полугодия 2011 года» очевидно, что лидерами по количеству источников DDoS-атак являются Россия и Украина. Отсюда можно сделать вывод, что вирусная активность и количество зараженных компьютеров в этих странах находятся на высоком уровне, так же это означает, что используется достаточно большое количество устаревшего программного обеспечения и злоумышленники могут использовать его критические уязвимости. Данные показатели так же обеспечиваются еще ростом количества семей, у которых появился доступ в Интернет и низкой компьютерной грамотностью.

По данным компании Arbor 35% процентов атак были спровоцированы по идеологическим или политическим причинам, 31% были обоснованы как нигилизм (примером может послужить атаки на государственные ресурсы МВД Украины, администрации президента и других после закрытия ресурса ex.ua). Атакам так же подвергаются сервисы провайдеров услуг мобильной связи такие как электронная почта, доступ в интернет, были зарегистрированы атаки на клиентские устройства.

Что касается каналов связи, новым стандартом в скорости поступления неполезной нагрузки на ресурсы стала скорость 10 Гбит/с. Максимальные зарегистрированные неполезные нагрузки 60 Гбит/с и 100 Гбит/с. Также в последнем отчете была выявлена первая атака с использованием протокола IPv6.

Для выявления DDoS-атак используются следующие методы: статистический – основан на анализе отклонения статистических параметров трафика от средних значений; статический – основан на черных и белых списках, в том числе формируемых пользовательскими приложениями через API; поведенческий – основан на анализе соблюдения или несоблюдения спецификаций прикладных протоколов; сигнатурный: основан на анализе индивидуальных особенностей поведения ботов.[3]

По сложности подавления, а так же по мотивации проведения DDoS-атаки можно разделить на такие категории как: вандализм – обычно это не распределенные атаки, а атаки которые ведутся с одного-двух хостов, злоумышленник скорее всего не получает от этого какой-либо выгоды, а делает это из-за обиды на владельцев какого-

либо ресурса, знания его в этой области ограничены простыми методами атак найденные в сети Интернет. Данные атаки отражаются достаточно легко, так как тоже не требуют высокой квалификации в области защиты компьютерных сетей от внешних атак, и зачастую решается блокированием конкретного IP или простой фильтрацией пакетов по замеченной закономерности; нигилизм – по сути, причины фактически идентичны причинам при вандализме, но действия происходят более целенаправленно, и это уже распределенная атака. В ней участвует группа людей, которая недовольна теми или иными информационными поводами. Обычно это простой bat-скрипт, в котором используется команда ping с большим размером проверочного пакета и перечислены атакуемые ресурсы, никаких знаний от пользователя не требуется, достаточно лишь запустить скрипт. Блокируется такая атака обычно достаточно легко, блокируется вся нагрузка полученная по протоколу ICMP; бизнес – злоумышленники используют данный вид атак, не только как средство для собственного обогащения, но и предоставляют DDoS-атаки как услугу.

Рассмотрев причины возникновения и проблемы, которые нужно решать при борьбе с данным видом атак, можно определить методы решения данных проблем. Весь рынок решений по защите от DDoS-атак можно разделить на три части: программные решения – самое распространённое на рынке, зачастую представляет собой набор правил фильтрации трафика, которые составлены разработчиком на личном опыте. Так же существуют решения с открытым исходным кодом (например DDoS Deflate), но имеет очень простой статический метод фильтрации (белые и черные списки) по IP, на основе количества соединений от одного IP. Данное решение достаточно просто установить прямо на сервер на котором работает ресурс и поможет только от малозаметных атак вида вандализм. Решение совершенно неэффективно в масштабе дата-центров; аппаратные решения – используется для защиты масштабных сетевых инфраструктур, таких как: точки обмена трафиком, дата-центры и т.д. Типичная схема работы подобных решений представлена на рис.1.

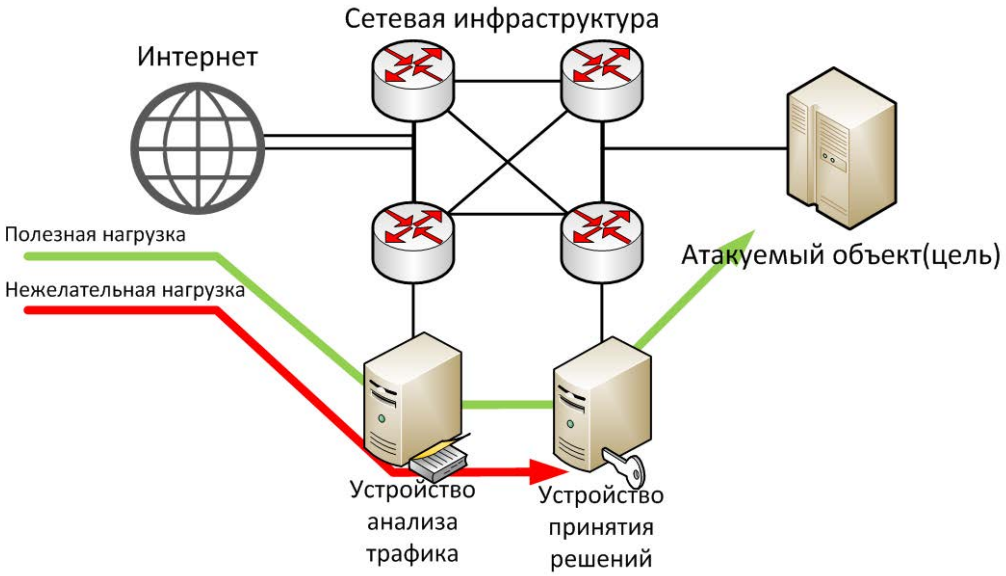


Рисунок 1 – Стандартная схема аппаратного решения защиты от DDoS-атак.

Обычно схема состоит из двух устройств: это устройство анализа трафика, на которое дублируется весь трафик, который приходит в дата-центр, и устройство принятия решений, которое блокирует нежелательную нагрузку, на основе анализа данных полученных устройством сбора информации. Иногда данные решения

сочетаются в одном устройстве как например решения от Cisco, которое при отсутствие активных атак, работает в режиме накопления информации о полезной нагрузке, а в случае возникновения вредоносной активности изменяется маршрутизация и начинается фильтрация трафика.

Поскольку анализ трафика и принятие решений является достаточно сложной задачей, некоторые компании запатентовали свои алгоритмы, например компания «Black Lotus» запатентовала алгоритм «Анализ поведения человека»(Human Behavior Analysis), который определяет кто генерирует данный трафик, человек или бот. Так же интересны решения от компании «Arbor», а именно продукт« PeakFlow» который кроме стандартных решений имеет сигнатурный подход к фильтрации нежелательного трафика, то есть устройства PeakFlow могут обмениваться между собой данными об атаке, такими как источники атаки, способы и какие-либо закономерности. Это позволяет решать данную проблему не на уровне дата-центра, а, например, на уровне провайдера, который предоставляет каналы данному дата-центру; облачное решение — данный вид решений включает в себя как программные так и аппаратные решения, но так же использует все виды защит от DDoS-атак.

Рассмотрим его на примере продукта «Лаборатории Касперского» – «Kaspersky DDoS Prevention». Данное решение является шлюзом, через который будет проходить весь трафик, который идет на Интернет-ресурс. Поскольку это облачное решение, это означает, что увеличение скорости атаки, не является проблемой(тогда как в аппаратных решениях, она упиралась в скоростные ограничения сетевой инфраструктуры в которой была установлена) так как решение масштабируется в случае увеличения неполезной нагрузки. Другое преимущество данного решения это алгоритмы которые принимают решение о том, что делать с той или иной нагрузкой не только на основе статистики, которая была накоплена за время атак, но и на основе того, что алгоритм знает об источниках DDoS-атак и их функционале.

Выводы

В статье рассмотрены причины возникновения DDoS-атак, их мотивация и способы создания, показано, что данная проблема на сегодняшний день актуальна и хоть существуют уже лидеры рынка в данной области, они предоставляют закрытые решения, которые защищены патентом или совсем не разглашаются. В отличие от решений с закрытым исходным кодом, открытые рекомендации позволяют привести методики и алгоритмы к единому стандарту, что позволит производителям оборудования и программных решений обмениваться средствами более эффективного решения данной проблемы.

Перечень ссылок

1. Arbor Networks. (2012). Stopping & Preventing DDoS Attacks. Retrieved 4/9/2012, from DDoS Attack Protection | Stop DDoS Attacks | Arbor Networks: http://www.arbornetworks.com/stopping-&-preventing-ddos-attacks.html

2. Black Lotus. (2012). Behavior analysis techniques in DDoS mitigation. Retrieved 4/9/2012, from Black Lotus DDoS Mitigation Technology: http://www.blacklotus.net/learn/behavior-analysis-techniques

3. ЗАО «Лаборатория Касперского». (2011). DDoS-атаки второго полугодия 2011 года - Securelist. Получено 9/4/2012 г., из http://www.securelist.com/ru/analysis/208050745/DDoS_ataki_vtorogo_polugodiya_2011_goda

4. Arbor Networks, "Worldwide Infrastructure Security Report 2011 Volume VII", 2011. – 72 с.