УДК 004.91

О.Д. Смоктій[1], К.В. Смоктій[1], О.В. Іванченко[2]

[1] *Донецький національний університет імені Василя Стуса, Вінниця*
[2] *Університет митної справи та фінансів, Дніпро*

АНАЛИЗ МЕХАНИЗМА И ПОСЛЕДСТВИЙ ВОЗДЕЙСТВИЯ DDOS-АТАК НА ЭТАЛОННУЮ МОДЕЛЬ ВЗАИМОДЕЙСТВИЯ ОТКРЫТЫХ СИСТЕМ OSI

В статье рассмотрен механизм воздействия DDoS-атак на облачные серверы на прикладном и инфраструктурном уровнях модели OSI, приведены основные направления атак данных уровней. На каждом из OSI-уровней проведен анализ последствий и выработаны рекомендации по ослаблению воздействияDDoS-атак.В работе приведены данные исследований основных направлений атак, мотивации атакующих и применяемых ими техник атак. Сделаны выводы относительно наиболее уязвимых для атак злоумышленников протоколов передачи данных и самых распространенных направлений DDoS-атак.

***Ключевые слова**: DDoS-атаки, распределенный отказ в обслуживании, модель OSI, атаки прикладного уровня, атаки уровня инфраструктуры, SYN-флуд, HTTP-флуд, облачный сервер.*

Введение

Постановка задачи. Современные условия применения интернет-технологий требуют обеспечения высокоэффективной защиты информационного пространства, являющегося важнейшим фактором влияния на национальную безопасность государства. На сегодняшний день одной из актуальных проблем в национальном кибернетическом пространстве является защита киберактивов различных инфраструктурных образований, включая активы отдельных предприятий, от воздействия DDoS-атак.

Фактически DDoS-атака (Distributed Denial of Service) представляет распределённый отказ в обслуживании вычислительных мощностей, вызванный действиями злоумышленников. Это один из многих возможных способов несанкционированного захвата компьютерных систем, который занимает ведущее место по численности попыток совершения взломов в силу гибкости и высокой степени безотказности его применения в компьютерных сетях любой архитектуры. Поэтому DDoS-атаки являются серьезной угрозой как для информационного пространства отдельных предприятий, поскольку наносят им серьёзный материальный ущерб, так и для глобального интернет пространства, т.к. воздействующий вредоносный трафик снижает скорость и эффективность работы корневых интернет серверов.

Известные методы защиты инфраструктуры от DDoS-атак направлены на максимальное её ослабление. К сожалению,в силу несовершенства механизмов воздействия на кибернетических злоумышленников спрогнозировать и полностью предотвратить атаку практически невозможно.

Анализ последних исследований и публикаций. Одним из основных инструментариев реализации DDoS-атаки является бот (Bot), представляющий собой вредоносную программу, которая имитирует действия пользователя в сети Интернет и работает автоматически по заданному графику [1]. Это подтверждается исследованиями, проведёнными компанией Imperva. В отчёте компании сказано, что за 3 месяца 2016 года соотношение числа пользователей случайно выбранного домена к количеству ботов того же домена составляет один к трём [2]. Исходя из этого, аналитики компании сделали вывод, что бот-атаки менее опасны, чем направленные DDoS-атаки. Тем не менее, для небольших слабо защищенных сайтов бот-атаки представляют серьезную угрозу, поскольку по данным компании из 100000 случайно выбранных доменов 94% хотя бы один раз в три месяца отказывали в обслуживании, подвергаясь воздействию этого вида атак.

На рис. 1 представлена диаграмма наиболее распространенных технологий совершения взломов компьютерных сетей по данным компании Hack mageddon за январь 2017 года [3].

Из рис. 1 видно, что DDoS-атаки составляют 5,6% от общего числа атак. Кроме того, по данным компании Hackmageddon мотивацией злоумышленников к нанесению DDoS-атак служит в основном стремление получить выгоду от совершённогокибер-преступления, в первую очередь, от взлома финансовых систем, а также хакерство – как применение техник взлома новых защитных механизмов и изучение принципов их работы (рис. 2).

Наибольший интерес для атаки отказа в обслуживании представляют облачные сервисы, поскольку используются крупными корпорациями и финансовыми организациями для хранения данных и осуществления электронной коммерции. Облачные хранилища наиболее уязвимы при работе UDP-протокола, по которому происходит обмен сообщениями между хостами.

Рис. 1. Наиболее распространенные техники атак злоумышленниками вычислительных систем

Рис. 2. Мотивация DDoS-атакующих по данным на январь 2017 г.

Поэтому чрезвычайно важно при реализации соответствующих мер защиты контролировать входной облачный трафик и осуществлять мониторинг активности действий поставщика данных. В качестве превентивных мер защиты рассматривается вариант «самоконтроля» и «арбитражного контроля» со стороны поставщика данных [4]. На рис. 3 представлен рейтинг основных направлений DDoS-атак по данным компании Imperva [5].

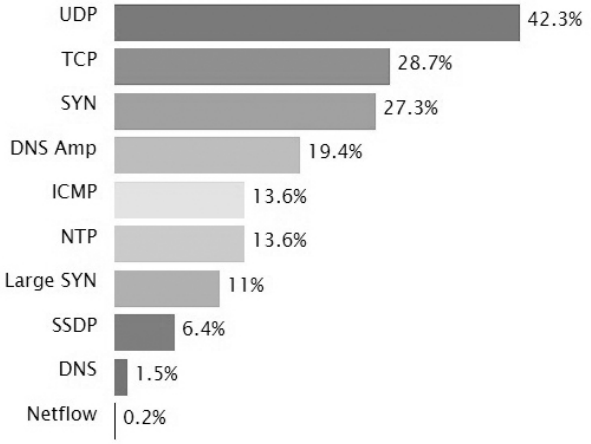

Рис. 3. Распределение DDoS-атак по основным протоколам 2016 г.

Одним из первых шагов по ослаблению DDoS воздействия является идентификация атаки, а именно: выявление источника; определение типа, масштаба атаки; оценка возможных последствий. В работах [6-8] предложены методы выявления DDoS-атак на основе методов MapReduce, искусственных нейронных сетей, аппарата нечеткой логики.

Основные уязвимости, на которые направлены действия DDoS-атак, а также меры по ослаблению атак исследованы в работах [9, 10].

Формулировка цели статьи

К облачным вычислениям, как и к любой сетевой инфраструктуре, применима модель OSI (Open Systems Interconnection), которая условно разделяет коммуникацию на семь уровней. На каждом уровне модели применим свой механизм ослабления DDoS-атаки, учитывающий разную природу и особенности вредоносного воздействия.

Целью статьи является рассмотрение механизма реализации DDoS-атак на каждом из OSI-уровней, анализ последствий и выработка рекомендаций по ослаблению их воздействия.

Изложение основного материала

На протяжении последних четырех лет атаки отказа в обслуживании были сосредоточены на трех уровнях: сетевой (3), транспортный (4) и прикладной (7).

Атаки третьего и четвертого уровней – инфраструктурные атаки, которые нацелены на перегрузку пропускной способности сети путем отправки большого количества фальшивых запросов (ICMP флуд, SYN флуд, Smurf-атака). Атаки седьмого уровня – прикладные атаки – преследуют цель нарушить работу приложений и критически важного программного обеспечения, тем самым вывести из строя серверы и другие обеспечивающие работу

сети устройства (GET запросы, HTTP GET, HTTP POST и т.д.).

Наиболее популярными направлениями инфраструктурных DDoS-атак являются такие направления [10]:

- DNS-отражение;
- TCP SYN флуд;
- UDP флуд;
- ICMP флуд.

Первое направление, к которому относятся DNS-отражение или DNS-усиление заключается в том, что злоумышленник посылает на DNS-сервер жертвы запрос небольшого размера, в котором изменен IP-адрес отправителя на IP-адрес компьютера-жертвы (так называемый IP spoofing). DNS-сервер отвечает на запрос сообщением гораздо большего размера и посылает его на IP-адрес компьютера-жертвы. Схема повторяется до тех пор, пока сеть не заблокируется вследствие перегрузки DNS-запросами.

Второе направление TCP SYN флуд работает с механизмом трехкратного обмена сообщениями (“рукопожатиями”) между сервером и клиентом перед установкой TCP соединения. Злоумышленник имитирует запрос на установку соединения от клиента серверу с отметкой SYN. На этот запрос сервер отвечает сообщением SYN-ACK клиенту, после чего клиент должен закрыть соединение, отослав серверу ACK-сообщение. Поскольку в роли клиента выступает злоумышленник, то он не закрывает соединение, тем самым оставляя серверу «полуоткрытое» соединение. Таких соединений устанавливается столько, сколько требуется для блокировки работы сети.

Третье направление UDP флуд – наиболее распространенный вид инфраструктурной DDoS-атаки, поскольку работает через UDP-протокол (User Datagram Protocol), который использует простую модель передачи сообщений, без обменов сообщениями и сеансов. Достаточно направить большое количество UDP-пакетов хосту-жертве, на каждый из которых атакуемый хост должен отправить ответ, и сеть окажется перегруженной. Если подменить IP-адрес отправителя UDP флуда, то злоумышленник сохранит анонимность и не подвергнется ответному потоку сообщений.

Четвёртое направление CMP флуд или PING флуд – простой способ DDoS-атаки, при котором на компьютер-жертву посылается большое количество ICMP-пакетов с целью блокировать TCP/IP стек.

На прикладном уровне действие DDoS-атак направлено на захват управления или вывод из строя программного обеспечения удаленного компьютера. Облачные вычисления особенно подвержены таким атакам в силу их веб-ориентированности. При DDoS-атаке на седьмой уровень OSI сеть не перегружается избыточным трафиком, тем самым снижается вероятность обнаружения взлома.

Основные инструменты, которые используются при атаках прикладного уровня, - это запросы HTTP, GET, DNS, SIP INVITE, отправленные на сервер-жертву. Эти запросы дают сверхнагрузку на текущую сессию сервера, блокируют его процессы и переполняют ресурсы.

Отдельно следует обратить внимание на атаку прикладного уровня типа DNS-усиление (DNS Amplification).

Ее принцип заключается в том, что атакующий посылает запрос просмотра DNS имен на открытый DNS сервер с IP-адресом источника равном IP-адресу жертвы. DNS сервер посылает ответ вместо источника атакуемому серверу. Таким образом на сервере создается избыточное количество пакетов от DNS до тех пор, пока работа сервер не блокируется из-за нехватки ресурсов. Такие атаки ослабляются ограничением количества принимаемых пакетов от DNS-сервера.

В табл. 1 представлено краткое описание возможных DDoS-атак на каждом из уровней OSI, протоколы, которые подвержены действиям злоумышленников, основные инструменты атакующих и методы, направленные на смягчение действий атаки.

Выводы из данного исследования и перспективы дальнейшего развития

Несмотря на то, что DDoS-атаки составляют 5,6% от общего количества известных атак, они оказывают разрушительное воздействие на кибернетические активы инфраструктурных образований и отдельных предприятий.

Мотивацией злоумышленников в подавляющем большинстве случаев является получение личной выгоды от атаки. Облачные вычисления подвержены DDoS-атакам наиболее часто по протоколам UDP иTCP – протоколам обмена сообщениями между хостами.

Атаки, направленные на 2-4 уровни OSI, ослабляются и предупреждаются настройками роутера или свитча (использование линейных списков контроля доступа, ограничение скорости канала и др.); атаки 5-7 уровней – конфигурацией брандмауэра и операционной системы сервера (использование UDP-,ICMP-экранов, ограничения сеансов, SYN cookie; использование брандмауэров с динамической проверкой и др.).

Первый уровень OSI защищается использованием качественного оборудования и мониторингом работы физического сетевого оборудования.

Таблица 1

Методы смягчения DDoS-атак на каждом уровне модели OSI

Уровень модели OSI	Задействованные протоколы	Инструменты DDoS	Возможные последствия атаки	Методы, смягчающие действие атаки
Прикладной уровень (7)	FTP, HTTP, POP3, SMTP, DNS и шлюзы, которые их используют	PDF GET запросы, HTTP GET, HTTP POST	Достижение предела по ресурсам сервисов атакуемого ресурса	Использовать мониторинг приложений для выявления 0day-уязвимостей приложений. Идентифицировав такие атаки, их можно раз и навсегда остановить и отследить их источник. Использовать коммерческие продукты, такие как ArborPeakflow SP и ArborPeakflow SP TMS, которые созданы для глобального анализа трафика инфраструктуры [1]. Использовать проксирование трафика.
Представительский уровень (6)	Протоколы шифрования и кодирования ASCII, EBCDIC, SSL, HTTPS, SSH	Подложные SSL запросы,THC-SSL-DoS атаки,HTTPS флуд	Не принимаются SSL соединения; автоматическая перезагрузка сервера	Проверка трафика приложений на предмет атак или нарушения политик на платформе приложений. Распределение шифрующей SSL инфраструктуры: размещение SSL на отдельном сервере, если это возможно. Использование протокола шифрования TLS (SSL-3), который защищает от атак типа man-in-the-middle.
Сеансовый (5)	Протоколы входа/выхода (RPC, PAP)	Слабые места программного обеспечения Telnet-сервера на свитче	Свитч не доступен администратору	Использование надежной аппаратной части – свитчей, маршрутизаторов и т.д.
Транспортный (4)	TCP, UDP	SYN флуд, Smurf-атака (атакаICMP-запросами с измененными адресами)	Достижение пределов по пропускной способности канала или по количеству допустимых подключений	Использовать фильтрациюDDoS-трафика, известная как blackholing[11]. Однако этот подход делает атакуемый ресурс недоступным как для трафика злоумышленника, так и для легального трафика пользователей. Тем не менее, блокировка доступа используется в борьбе с DDoS-атаками для защиты от таких последствий, как замедление работы сетевого оборудования и отказ работы сервисов.
Сетевой (3)	Протоколы IP, ICMP, ARP, RIP и роутеры, которые их используют	ICMP флуд, UDP флуд, DNS отражение	Снижение пропускной способности атакуемой сети и возможная перегруженность брандмауэра	Ограничение количества обрабатываемых запросов по протоколу ICMP, запрет ICMP форвардинга. Ограничение скорости для трафика UDP, защита прокси-серверов и настройка маршрутизатора для остановки передачи по прямому IP-адресу [1].
Канальный (2)	Протоколы 802.3, 802.5, контроллеры, точки доступа, мосты, которые их используют	MAC-флуд – переполнение пакетами данных сетевых коммутаторов	Потоки данных от отправителя получателю блокируют работу всех портов	Ограничить количество MAC адресов надежными, которые проходят проверку аутентификации, авторизации и учета на сервере (протокол AAA) и в последствии фильтруются. Для настройки фильтрации MAC-адресов используются конфигурируемые свитчи моделей, выпущенных в последние 5 лет. Наиболее эффективна фильтрация MAC-адресов в проводных сетях.

Окончание табл. 1

Физический (1)	Протоколы 100BaseT, 1000 Base-X, а также концентраторы, розетки, патч-панели	Физическое разрушение, физическое препятствие работе	Физическое сетевое оборудование приходит в негодность	Использовать систематический подход к мониторингу работы физического сетевого оборудования.

Многообразие механизмов реализации соответствующих стратегий DDoS обуславливает индивидуальные подходы к ослаблению атак на каждом уровне OSI модели.

Приведенные в статье методы ослабления действий DDoS-атак не являются исчерпывающими, что подтверждает необходимость дальнейших исследований механизмов и инструментариев противодействия DDoS-атакам.

Список литературы

1. Rashmi V. Deshmukh. Understanding DDoS Attack & its Effect in Cloud Environment / Rashmi V. Deshmukh, Kailas K. Devadkar // Procedia Computer Science, 2015. - Tokyo, Japan. - Vol. 49. - P. 202-210.

2. Bot Traffic Report 2016 [Electronic resource] / Access regime: https://www.incapsula.com/blog/bot-traffic-report-2016.html.

3. Hackmageddon Information Security Timelines and Statistics [Electronic resource] / Access regime: http://www.hackmageddon.com/

4. Gartner: Start security monitoring in the public cloud [Electronic resource] /Access regime: http://www.networkworld.com/article/2167209/security/gartner--start-security-mo-nitoring-in-the-public-cloud.html.

5. Global DDoS Threat Landscape Q1 2016 [Electronic resource] / Access regime: https://www.incapsula.com/ddos-report/ddos-report-q1-2016.html.

6. Головін А. Виявлення DDoS-атак прикладного рівня шляхом використання моделі Map Reduce / А. Головін // Інформаційні технології та безпека. - К.:Ін-т спец. зв'язку та захисту інформації Нац. техн. ун-ту України "Київ. політехн. ін-т", 2015. - Том. 3, вип. 2 (5). - С. 117-124.

7. Jie-Hao C. DDoS defense system with test and neural network / C. Jie-Hao, Z. Ming, C. Feng-Jiao, Z. An-Di // Proceedings of the IEEE International Conference on Granular Computing, 2012. - Hangzhou, China. - P. 38-43

8. Shanmugam B. Improved Intrusion Detection System using Fuzzy Logic for Detecting Anamoly and Misuse type of Attacks / B. Shanmugam, N. Idris // Proceedings of the International Conference of Soft Computing and Pattern Recognition, 2009. - Malacca. - P. 212-217.

9. Рубан І.В. Исследование удаленных атак на распределительно вычислительные сети / І.В. Рубан, С.С. Сєров // Системи обробки інформації. - Х.: Харьковский университет Воздушных Сил им. И. Кожедуба, 2013. - Вип. 5 (112). - С. 118-120.

10. FuiFui Wong. A survey of trends in massive ddos attacks and cloud-based mitigations / FuiFui Wong, Cheng Xiang Tan // International Journal of Network Security & Its Applications (IJNSA), 2014. - Vol. 6, No. 3. - P. 57-71

11. Види DDoS-атак та алгоритми виявлення DDoS-атак типу Flood-Attack / Н.В. Багнюк, В.М. Мельник, О.В Клеха, І.А. Невідомський // Науковий журнал "Комп'ютерно-інтегровані технології: освіта, наука, виробництво", 2015. - Луцьк. - Вип. 18. - С. 6-12

Надійшла до редколегії 30.01.2017

Рецензент: д-р техн. наук, с.н.с. С.Г. Семенов, Національний технічний університет «Харківський політехнічний інститут», Харків.

АНАЛІЗ МЕХАНІЗМУ І НАСЛІДКІВ ВПЛИВУ DDOS-АТАК НА ЕТАЛОННУ МОДЕЛЬ ВЗАЄМОДІЇ ВІДКРИТИХ СИСТЕМ OSI

О.Д. Смоктій, К.В. Смоктій, О.В. Іванченко

У статті розглянуто механізм впливу DDoS-атак на хмарні сервери на прикладному та інфраструктурному рівнях моделі OSI, наведені основні напрямки атак даних рівнів. На кожному з OSI-рівнів проведено аналіз наслідків і вироблені рекомендацій щодо ослаблення впливу DDoS-атак. В роботі наведені дані досліджень основних напрямків атак, мотивації атакуючих і використаних ними технік атак. Зроблено висновки щодо найбільш вразливих для атак зловмисників протоколів передачі даних і найпоширеніших напрямків DDoS-атак.

***Ключові слова**: DDoS-атаки, розподілена відмова в обслуговуванні, модель OSI, атаки прикладного рівня, атаки рівня інфраструктури, SYN-флуд, HTTP-флуд, хмарний сервер.*

ANALYSIS OF MECHANISM AND CONSEQUENCES OF DDOS-ATAKS ON THE STANDARD OPEN SYSTEMS INTERACTION OSI-MODEL

O.D. Smoktii, K.V. Smoktii, O.V. Ivanchenko

The article the DDoS-attacks mechanism on the application and infrastructure levels, gives recommendations for mitigating the effects of DDoS attacks.

The article shows the mechanism of the DDoS attacks impact on cloud servers via the application and infrastructural OSI-model levels, gives the main directions of attacks on these levels. At each of the OSI-levels, an analysis of the consequences and recommendations for DDoS-attacks mitigation are given. The paper presents research data of the main attacks directions, the attackersmotivationand the techniques they are using. The paper consists conclusionsabout the most vulnerable protocols for attacks and the most common directions for DDoS attacks.

***Keywords**: DDoS attacks, distributed denial of service, OSI model, applicationlevel attacks, infrastructure level attacks, SYN flood, HTTP flood, cloud server.*