УДК 004.49

АНАЛИЗ СУЩЕСТВУЮЩИХ АЛГОРИТМОВ РАННЕГО ВЫЯВЛЕНИЯ И БЛОКИРОВАНИЯ РАСПРЕДЕЛЕННЫХ АТАК НА ОТКАЗ ОТ ОБСЛУЖИВАНИЯ

Бисенбаева Назерке Кобыландиевна
n.kobylandievna@gmail.com
Докторант 2-курса специальности 8D06104 -Вычислительная техника и программное обеспечение, ЕНУ им. Л.Н.Гумилева, Нур-Султан, Казахстан
Научный руководитель – Д. Сатыбалдина

Аннотация. Статья посвящена анализу существующих алгоритмов раннего выявления и блокирования распределенных атак на отказ от обслуживания и актуальности новых эффективных алгоритмов. Объект исследования: компьютерные сети и распределенные атаки, направленные на отказ в обслуживании осуществляемые в этих сетях. Предмет исследования: алгоритмы и методы обнаружения распределенных атак, направленных на отказ в обслуживании.

Введение.

Распределенная атака типа «отказ в обслуживании» (Distributed Denial of Service, DDoS) – это попытка снизить производительность веб-сервера или онлайн-системе, завалив их данными [1]. В результате атаки полностью блокируется обслуживание обычных пользователей, законных ресурсов, других систем, так как серверные оборудования, обслуживающие сайт (онлайн-система), вынуждены обрабатывать большое количество ложных запросов, организованные ботнетами, в связи с чем сайт становится недоступным для легитимного пользователя.

DDoS-атаки в основном осуществляются ботнетами – большой группой распределенных вычислительных машин, которые осуществляют действие согласованно друг с другом – одновременно рассылают спам-запросы на веб-сайты или на онлайн-системы.

Злоумышленники используют вредоносное программное обеспечение (ПО) или незащищенные уязвимости устройств, систем для установки программного обеспечения Command and Control (C2) для использования его ресурсов как ботнетов (см. Рисунок 1).

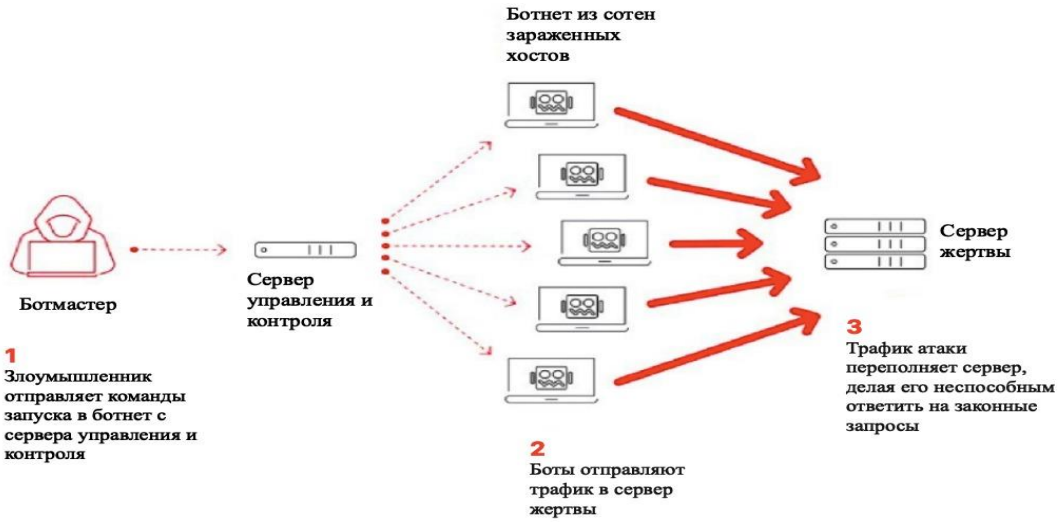

Рисунок 1. Для получения максимального эффекта в основном злоумышленники используют боты для запуска DDoS-атак.

Такого вредоносного ПО (Malware) с открытым исходным кодом много, и любой желающий интернет-пользователь может построить собственный такой ботнет, так как уязвимых систем и IoT-устройств во всем мире очень много. Они работают по простой схеме: как только ботнет будет готов, злоумышленники (ботмастеры) отправляют команду запуска на все свои узлы ботнета и ботнеты в свою очередь отправляют запрограммированные запросы на целевой сервер. Если атака проходит внешнюю защиту, она быстро перебивает большинство систем, вызывает перебои в обслуживании и в некоторых случаях приводит к сбою сервера. Конечный результат DDoS-атаки – это прежде всего потеря производительности или прерывание обслуживания - клиенты не смогут пользоваться услугами поставщика или открыть веб-сайт [2].

Опубликованный индекс цен Dark Web за 2020 год показывает текущие средние цены на ряд продуктов и услуг доступных по запросу связанных с киберпреступностью. В Европе и США базовая целевая атака вредоносным ПО стоит 300 долларов, а таргетированная распределенная атака типа отказ в обслуживании (DDoS) стоит всего 10 долларов в час или 60 долларов в течение 24 часов. «Продавцы» даже предлагают оптовые скидки, что делает такие атаки обычным оружием для вымогательства в Интернете [3].

Согласно отчету Nexusguard об угрозах за 2020 год, в первом квартале этого года количество DDoS-атак увеличилось более чем на 278% по сравнению с первым кварталом 2019 года и более чем на 542% по сравнению с предыдущим кварталом [4].

Согласно исследованию Gartner, средняя стоимость простоя для малого и среднего бизнеса составляет 5600 долларов за минуту [5].

DDoS-атака может быть неизбежной, особенно если бизнес работает в отрасли с высоким уровнем риска. Тем не менее, все организации должны включить процедуру реагирования на DDoS-атаки в свои официальные планы обеспечения непрерывности бизнеса.Согласно исследованию Ponemon Institute, фирмы, которые могут быстро отреагировать на инцидент безопасности и локализовать ущерб, могут сэкономить 26% или более от общих затрат на ликвидацию последствий инцидента [6].

«Одна из причин, по которой DDoS-атаки так дешевы, заключается в том, что все больше и больше людей, предлагающих услуги DDoS-атак, используют масштаб и пропускную способность публичных облаков», - сказала Юта Гуринавичюте, технический директор NordVPN. «Поскольку удаленная работа становится новым стандартом, и особое внимание уделяется домашнему интернет-подключению на небывало высоком уровне, надлежащие меры безопасности для предотвращения этих атак как никогда важны» [7].

Злоумышленники DDoS внедрили сложные методы искусственного интеллекта (далее

- ИИ) и машинного обучения. Например, ботнеты DDoS применяют методы машинного обучения для проведения сложной сетевой разведки с целью поиска наиболее уязвимых систем. Также с помощью ИИ они время от времени изменяют стратегий атаки и перенастраивают себя.

В сентябре 2016 г. был создан ботнет Интернета вещей на базе Mirai, вредоносное программное обеспечение, со скоростью 600 Гбит/с, нацеленное на Брайана Кребса в его блог об информационной безопасности (krebsonsecurity.com) [10]. Принцип работы Mirai достаточно просто: он использует список из 62 общих имен пользователей по умолчанию и пароли для доступа в основном к домашним маршрутизаторам, сетевым камерам и цифровым видеомагнитофонам, которые обычно имеют менее надежную защиту, чем другие потребительские устройства IoT. В том же месяце компания Mirai устроил атаку на французский веб-хостинг OVH, и эта атака побила рекорд для самой крупной зарегистрированной DDoS-атаки со скоростью не менее 1,1 Тбит/с, и возможно даже до 1,5 Тбит/с [11]. Такая скорость атак мотивирует исследователей вводить новаторские методы чтобы смягчить угрозу. Атакующий контролирует большой набор компьютеров для выполнения запросов. Число и размер сетевых журналов также чрезвычайно велик, это будет занимать десятки терабайт, то есть большие данные. Если для анализа этого сетевого журнала использовать традиционные методы анализа то потребуется значительное количество времени для анализа и обнаружения DDoS-атак. В итоге использование технологии и методов больших данных действительно важна для этого типа задач.

Обзор методов раннего выявления и блокирования распределенных атак на отказ от обслуживания.

Информационная безопасность компьютерной сети (далее - КС) – это любая деятельность, предназначенная для защиты удобства использования и целостности вашей сети и данных. Она включает в себя аппаратные и программные технологии. Другими словами, это защищенность сети от случайного или преднамеренного вмешательства в нормальное состояние ее функционирования, а также от попыток хищения, изменения или разрушения циркулирующей в сети информации. Сетевая безопасность начинается с авторизации доступа к данным в сети, которая контролируется сетевым администратором. Пользователи выбирают или получают логин и пароль или другую аутентифицирующую информацию, которая позволяет им получать доступ к данным и программам в пределах своих полномочий в сети. [8]

Обнаружение DDoS – это процесс, позволяющий отличить атаки распределенного отказа в обслуживании (DDoS) от обычного сетевого трафика, чтобы обеспечить эффективное смягчение атак [9].

Первым шагом в предотвращении или прекращении DDoS-атаки является знание того, что атака происходит. Чтобы обнаружить атаку, нужно собрать достаточную информацию о сетевом трафике, а затем выполнить анализ, чтобы выяснить, является ли трафик легитимным. Этот процесс может быть выполнен вручную или в автоматическом режиме. Обнаружение DDoS является ключом к быстрой остановке или смягчению атак, и для того, чтобы это произошло, необходимо выполнить два критерия успеха: 1) скорость обнаружения и 2) точность обнаружения. Таким образом, методы обнаружения являются ключевым фактором при разработке надежной защиты от DDoS.

Выявление DDoS-атак были исследованы путем предложения схемы, известной как Connection Score [12]. Авторы работы определили оценку для любого соединения на основе статистического анализа в нормальных условиях. Анализ показал, что связи противника дают низкие оценки. В работе [13] предложен метод обнаружения DDoS-атак в сети, в частности в тяжелой магистральной сети.

Еще в одном исследовании сконструировали частотный вектор в реальном времени (RFV) как набор моделей, которые будут использоваться при обнаружении DDoS-атак. Их архитектура была построена на трех модулях, включая датчик головной станции, модуль обнаружения и фильтр трафика, который пропускает законные запросы. Они показали

эффективность своего метода по результатам экспериментов по моделированию реальных данных. Но эти методы были направлены только на DDoS-атаки на уровне приложений [14].

Авторы работы [15] провели исследование со статистическими данными информационной базы управления SNMP (MIB) вместо необработанных пакетных данных из сети. Лучшие характеристики переменных SNMP MIB были выбраны с помощью метода выбора функций, а для обнаружения атак использовался метод машинного обучения, известный как машина опорных векторов (SVM). Также, был предложен гибридный метод с использованием SVM и вейвлет-теории функций ядра [16] и был назван в качестве Admissive опорных векторов ядра. Обоснованность предложенного метода была оценена с помощью имитационных экспериментов. В ходе которых на данных реальных экспериментов показано, что предложенные методики способны обнаруживать DDoS-атаки только в оффлайн режиме.

Методы теории игр в обнаружении DDoS-атак был реализован в [17]. Ученые смоделировали DDoS-атаку как одноразовую, некооперативную игру с нулевой суммой. Результаты моделирования подтвердили точность их модели с использованием NS2.

В другом исследовании искусственная иммунная система (AIS) использовалась в качестве метода обнаружения DDoS-атак на основе аномалий [18]. Используя AIS, чтобы улучшить частоту обнаружения и набор данных DARPA, авторы модифицировали структуру «Отрицательный отбор» и «Клональный отбор», чтобы получить высокий уровень истинного положительного результата и низкий уровень ложного положительного результата.

Обнаружение DDoS-атаки также было исследовано в [19] с использованием метода фильтрации. Точность результатов исследования доказана на практике, но их метод подходит только для облачной среды.

В работе [20] предложен масштабируемый одноранговыйй механизм обнаружения на основе MapReduce, Botcloud, который сочетает сетевые и хостовые подходы. По этому методу сначала генерируется большой объем данных Netflow, а затем применяется алгоритм PageRank, чтобы дифференцировать зависимость подключенных хостов для обнаружения ботнетов. На основе MapReduce Алгоритм PageRank показал эффективность на кластере.

Ли и несколько ученые предложили механизм обнаружения атак на основе Hadoop, который реализует на платформе распределенных вычислений алгоритм обнаружения HTTP GET flooding с использованием MapReduce [21]. Метод на основе счетчика подсчитывает общий трафик: получен или запрос веб-страницы от клиентов. На основе этого задано пороговое значение, при превышении порогового значения сервер подает сигнал тревоги. Этот метод, основанный на шаблонах, предполагает, что клиенты, зараженные одним и тем же ботом, ведут себя одинаково, таким образом можно отличить злоумышленника от обычного клиента. Недостаток предложенного метода в том, что предлагаемая структура поддерживает автономную только пакетную обработку трассировок трафика.

Apache Hadoop разделяет данные на несколько одинаковых блоков одинокого размера и распределяет их в кластере, который необходимо обработать независимо. Но это может нарушить структуру трафика. Чтобы решить эту проблему, в работе [22] предложен Hashdoop фреймворк MapReduce для обнаружения аномалий сети. Разработанная хеш-функция разделяет трафик сети на блоки, сохраняющие особые и временные структуры трафика. Это помогает фреймворку MapReduce для эффективного обнаружения аномалий.

Суфиан и Усман [23] предложили метод HADEC, основанный на Hadoop фреймворк Live DDoS Detection эффективно используя MapReduce для защиты от атак злоумышленника. Они реализовали алгоритм обнаружения DDoS атак на основе счетчика для обнаружения атак типа TCP-SYN, HTTP GET, UDP и ICMP.

Заключение

Анализ научных работ из индексируемых международных рейтинговых изданий показывает, что предложение метода обнаружения DDoS-атаки с высокой точностью и низким уровнем ложной тревоги все еще является интересным исследованием, так как существующие методы обнаружения DDoS атак имеют задержку по времени и низкую

частоту обнаружения, также возможности существующих систем и методов защиты во многом не удовлетворяют требованиям практики. Одним из существенных их недостатков выступает невысокая адаптивность к изменяющимся условиям и видам угроз.

Список использованных источников

1. Zhijun W. et al. Low-rate DoS attacks, detection, defense, and challenges: a survey //IEEE Access. – 2020. – T. 8. – C. 43920-43943.
2. C. Douligeris and A. Mitrokotsa, DDoS attacks and defense mechanisms: classification and state-of-the-art //Comput. Networks –2004. –vol. 44, no. 5, 643–666.
3. https://www.privacyaffairs.com/dark-web-price-index-2020/
4. https://www.businesswire.com/news/home/20200630005295/en/DDoS-Attacks-Increase-542-Quarter-over-Quarter-Pandemic-Nexusguard/?feedref=JjAwJuNHiystnCoBq_hl-V2wqxRmnpgZtOypyHtjMYiqcp-o_pnudlUwsb5apQ1S4gUE65BTfjH3-pSuqdv0gW3cb3F4oTIgUqCPafFkgu4s9L7CzgBlYMXxVoyWhzlQ
5. https://blogs.gartner.com/andrew-lerner/2014/07/16/the-cost-of-downtime/
6. https://www.csoonline.com/article/3203705/what-is-incident-response-and-how-to-build-an-ir-plan.html
7. https://www.missioncriticalmagazine.com/articles/93185-the-dark-web-ddos-attacks-sell-for-as-low-as-10-per-hour
8. J. Kizza, System intrusion detection and prevention //A Guid. to Comput. Netw. Secur. London Springer, – 2009. 273–98.
9. B. K. Sy, “Integrating intrusion alert information to aid forensic explanation: An analytical intrusion detection framework for distributive COB,” //Inf. Fusion, – 2009. –vol. 10, no. 4, 325–341.
10. KrebsOnSecurity Hit with Record DDoS, – 2016.
11. US Computer Emergency Readiness Team, Heightened DDoS Threat Posed by Mirai and Other Botnets, alert TA16-288A, – 2016; www.us-cert.gov/ncas/alerts/TA16-288A.
12. H. Beitollahi and G. Deconinck, Tackling Application-layer DDoS Attacks //Procedia Comput. Sci., – 2012. – vol. 10, 432–441.
13. http://ipmeasurement.org/index.php?option=com_con.
14. Wei Zhou , Weijia Jia, Sheng Wen Yang Xiang, Wanlei Zhou “Detection and defense of application-layer DDoS attacks in backbone web traffic” //Future Generation Computer Systems – 2014. 36–46
15. J. Yu, H. Lee, M.-S. Kim, and D. Park, Traffic flooding attack detection with SNMP MIB using SVM //Comput. Commun., – 2008. – vol. 31, no. 17, 4212–4219.
16. M. YANG and R. WANG, DDoS detection based on wavelet kernel support vector machine //J. China Univ. Posts …, – 2008. – vol. 15, no. September, 59–63.
17. T. Spyridopoulos, G. Karanikas, T. Tryfonas, and G. Oikonomou, A game theoretic defence framework against DoS/DDoS cyber attacks //Comput. Secur., – 2013. – vol. 38, 39–50.
18. U. Akyazı and A. Uyar, Detection of DDoS attacks via an artificial immune system-inspired multiobjective evolutionary algorithm //Appl. Evol. Comput., – 2010.
19. “The CAIDA UCSD Anonymized Internet Traces 2013 Dataset http://www.caida.org/data/passive/passive_2013_dataset.xml,” – 2013.
20. Jerome Francois, Shaonan Wang, Walter Bronzi, R State, and Thomas Engel. Botcloud: Detecting botnets using MapReduce. In Information Forensics and Security (WIFS) //2011 IEEE International Workshop, – 2011. 1-6.
21. Yeonhee Lee and Youngseok Lee, Detecting DDoS attacks with Hadoop //In Proceedings of The ACM CoNEXT Student Workshop, – 2011.1-2.
22. Johan Mazel Romain Fontugne and Kensuke Fukuda, Hashdoop: A MapReduce framework for network anomaly detection //IEEE Conference (INFOCOM WKSHPS), – 2014. 494-499.
23. Sufian Hameed, Usman Ali ,On the Efficacy of Live DDoS Detection with Hadoop //IEEE Access. –2015.