Анализ DDoS атак, проводимых с помощью устройств IoT

М. Жакиш[1], Е. Н. Созинова[2], А. Д. Бондарева[3]
Санкт-Петербургский национальный исследовательский университет
информационных технологий, механики и оптики
[1]zhakishmadina@gmail.com, [2]s.ekaterina-nik@mail.ru, [3]Bondareva.AD@yandex.ru,

Аннотация. **В статье описывается наиболее распространенная угроза информационной безопасности Интернета вещей – DDoS атака. Описываются и анализируются наиболее часто используемые схемы DDoS атак, которые проводятся с помощью устройств IoT. Рассматривается современное состояние проблемы и приводятся рекомендации.**

Ключевые слова: информационная безопасность; Интернет вещей; DDoS атаки

Интернет вещей (IoT) начинает играть все большую роль на IT-рынке и в жизни общества, а скоро и вовсе станет неотъемлемой частью повседневной жизни множества людей. В связи с этим тема безопасности IoT все чаще оказывается в центре внимания – благодаря тому, что злоумышленники активно используют уязвимости умных устройств для проведения резонансных атак. На данный момент наиболее распространены атаки нового, ранее неизвестного типа: взломщики действуют не через компьютеры непосредственно, а обращаются к «подключенным системам» – web-камерам, элементам умных домов и гаджетам, – собирая из них ботнет или получая через эти устройства доступ к персональной информации. Объекты, входящие в IoT защищены куда слабее, чем непосредственно компьютеры, а доступ к ним дает потенциально не меньше возможностей, чем традиционный взлом. [1] Основываясь на этом можно сделать вывод, что защищенной экосистемы IoT на сегодняшний день не существует. Безопасность многих IoT-устройств сохраняется лишь потому, что на данный момент владелец не представляет интерес для киберпреступников. Можно сделать вывод, что особая опасность от IoT исходить в контексте распространения целевых атак.

Проблема атак на устройства IoT существует достаточно давно, но чаще всего речь шла об устройствах автоматизации дома и домашней безопасности. Сегодня политика злоумышленников приняла другую форму, направленную на добавления устройства к ботнету, большинство которых используются для выполнения DDoS атак. Таким образом, можно сделать вывод, что одна из самых распространенных целей взлома устройств IoT – проведение DDoS атак. Распространение всевозможных подключаемых к Интернету устройств дает злоумышленникам возможности по созданию ботнетов огромных размеров, с помощью которых можно атаковать даже очень крупный сервис.

Дословно с английского термин DDoS атака переводится – «отказ в обслуживание», то есть целью такой атаки является создание условий, при которых рядовым пользователям будет затруднён или полностью ограничен доступ к системе. [2] DDoS атаки распространены в современном мире. Для людей, занимающихся незаконной деятельностью в Интернете, это один из традиционных инструментов, применяемых для взлома или выведения из строя серверов сайтов и организаций. При этом злоумышленники маскируют обратный адрес, чтобы исключить возможность блокировки по IP.

Часто DDoS атака может быть просто инструментом для проведения дальнейших противоправных действий, например, злоумышленники могут провести DDoS атаку как отвлекающий манёвр во время проведения таргетированной атаки на предприятие.

Разновидностей DDoS довольно много, далее необходимо рассмотреть большинство типовых атак.

1. TCP SYN Flood

Цель атаки SYN Flood – вызвать перерасход ресурсов системы. Принцип атаки заключается в том, что злоумышленник, посылая SYN-запросы, переполняет на сервере очередь на подключения. При этом он игнорирует SYN+ACK пакеты цели, не высылая ответные пакеты, либо подделывает заголовок пакета таким образом, что ответный SYN+ACK отправляется на несуществующий адрес. В очереди подключений появляются так называемые полуоткрытые соединения, ожидающие подтверждения от клиента. По истечении определенного тайм-аута эти подключения отбрасываются. Задача злоумышленника заключается в том, чтобы поддерживать очередь заполненной таким образом, чтобы не допустить новых подключений. Из-за этого клиенты, не являющиеся злоумышленниками, не могут установить связь, либо устанавливают её с существенными задержками. Защита от типа атак SYN Flood осуществляется средствами DPI-систем, которые способны анализировать и контролировать проходящий через них трафик.

2. Fragmented UDP Flood

Используется UDP протокол, где не требуется установление сессии с отправкой любого типа ответа. Отличается тем, что для атаки используются пакеты максимального допустимого размера, чтобы заполнить

канал минимальным количеством пакетов. Поскольку эти фрагменты пакетов являются фальсифицированными и не имеют никакого отношения к реальным данным, сервер-жертва, принимая их, будет резервировать ресурсы для того, чтобы восстанавливать несуществующие пакеты из поддельных фрагментов. Рано или поздно это приведет или к исчерпанию системных ресурсов и отказу сервера, или к переполнению каналов. Так же, как и UDP флуд, такую атаку сложно фильтровать, и риск переполнения канала много выше. Наиболее простой способ защиты от такого типа атак – это блокирование UDP трафика.

3. Атака широковещательными ICMP ECHO пакетами (Smurf-атаки)

Реализуется такая атака путем отправки ICMP ECHO запросов с подмененным адресом источника (вместо которого указывается адрес сервера-жертвы) на широковещательный адрес маршрутизатора крупной сети. Задумка состоит в том, что ICMP ECHO запрос, пришедший на широковещательный адрес, будет разослан всем устройствам сети, каждый из которых в свою очередь ответит на этот запрос. Таким образом, образуется поток ICMP ECHO ответов, направляемых серверу-жертве, который способен частично или полностью исчерпать канальные и вычислительные ресурсы целевого сервера. В настоящее время атаки этого вида происходят редко, т.к. заводские настройки большинства современных маршрутизаторов не предусматривают обязательную рассылку каждому устройству сети пакетов, пришедших на широковещательный адрес. Однако, в сетях все еще встречаются устаревшие модели сетевого оборудования, а также с неактуальной версией ПО или некорректной настройкой политик обработки пакетов, которые могут быть использованы злоумышленниками для реализации таких атак. Среди рекомендуемых способов защиты можно назвать тщательную настройку правил обработки пакетов, пришедших на широковещательный адрес сети, на маршрутизаторе.

4. DNS Flood

Разновидность UDP флуда, нацеленная на DNS сервис. В процессе DNS флуда на атакуемый DNS сервер направляется огромное количество DNS запросов с широкого диапазона IP-адресов. Сервер-жертва не в состоянии определить, какой из пакетов пришел от реального клиента, а какой нет, и отвечает на все запросы. Таким образом, DNS флуд занимает все сетевые ресурсы и полосу пропускания DNS-сервера, вызывая его отказ. DNS флуд является очень продуманным видом DDoS атак: содержимое пакетов организовано точно так, как в реальных DNS запросах. Такую атаку невозможно отследить с помощью глубокого анализа: каждый запрос будет выглядеть легитимным. С большим диапазоном атакующих IP-адресов мошенник может с легкостью обойти большинство алгоритмов обнаружения аномалий трафика.

5. HTTP-флуд (HTTP Flood, Excessive VERB)

Атакующий бот генерирует большое количество HTTP запросов к серверу жертвы. В большинстве случаев это GET запросы на получение максимально больших элементов сайта. Каждый бот может генерировать большое количество легитимных запросов (более 10 раз в секунду). Таким образом, злоумышленнику не нужно иметь большую армию ботов для осуществления данного вида атаки. VERB атаки осуществляются ботами с реальных IP-адресов, поэтому количество адресов источников сопоставимо количеству используемых ботов. Кроме GET запросов также могут посылаться POST запросы и осуществляться другие HTTP действия, приводящие к одному и тому же результату – перегрузке веб-сервера жертвы и его недоступности. Среди способов возможных способов защиты стоит отметить следующие: настройка ограничений клиентских сессий; установка дорогостоящих аппаратных комплексов анализа и очистки трафика. [3]

6. Атака с использованием ботнета

Злоумышленники обычно стараются заполонить полосу жертвы большим количеством пакетов или соединений, перегружая сетевое оборудование. Такие объемные атаки проводятся с использованием множества скомпрометированных систем, являющихся частью ботнет. При проведении атаки такого типа пользователю нет нужды скрывать IP-адрес каждой машины, и благодаря большому числу участвующих в атаке компьютеров, такие действия ведут к значительной нагрузке на сайт. Причем обычно злоумышленники выбирают наиболее ресурсоемкие запросы.

DDoS атаки с помощью IoT появились относительно недавно. В июне 2016 года был обнаружен ботнет из более чем 25 тысяч городских и частных камер наблюдения и цифровых видеомагнитофонов, созданный группой хакеров для совершения DDoS атак, а уже к осени стали известны случаи, когда в состав зараженной сети входило до миллиона устройств. И хотя вычислительные мощности, доступные устройствам такого рода, достаточно невелики по сравнению с компьютерными, будучи объединенными в систему таких масштабов они становятся по-настоящему угрожающей силой.

Сентябрь 2016 года, возможно, стал знаковым для всего современного интернета. Начиная с 16 сентября, неизвестными злоумышленниками было совершено несколько сильнейших в истории DDoS атак. Суммарная мощность двух из них достигала рекордных 1Тбит/с. Всё началось с атаки на ресурс известного в IT-среде журналиста Брайана Кребса, который в одном из своих расследований вскрыл деятельность хакерской группы V-Dos, специализирующейся на организации заказных DDoS атак. Вскоре злоумышленники были арестованы, а на Кребса посыпались угрозы и шквал рекордных по мощности DDoS атак. Проанализировав инциденты, специалисты пришли к выводу, что основной ударной силой атак были IoT-устройства: роутеры, IP-камеры, DVR и другие. Все они были объединены в различные ботнеты. Всего же с 2016 сентября было зафиксировано уже 14 DDoS атак мощностью более 200 Mbps.[4]

Также в 2016 году были совершены атаки на крупные сайты вроде Twitter или Spotify, которые временно вывели их из строя. Эта атака достигла рекордных показателей по

объему генерируемого трафика. Для этого использовался ботнет Mirai, объединяющий 400-500 тысяч устройств интернета вещей.

Вне всякого сомнения, 2016 год стал годом DDoS атак, приведших к крупным техническим сбоям, масштабных и оказавших заметное влияние на повседневную жизнь пользователей. Но с каждым годом данный способ атаки никуда не уходит, а только набирает силу.

В своем отчете компания Nexusguard прямо указывает на проблему незащищенных IoT-сетей, актуальность которой возросла в течение последних нескольких лет. Тенденция касается множества устройств, задействованных в потребительских и промышленных целях, подключаемых к сети без соблюдения должных мер безопасности. В последние годы хакеры начали использовать большее количество уязвимых устройств для создания масштабных ботнетов из тысяч и миллионов зараженных девайсов: маршрутизаторов, Smart-TV и так далее.[5] Уязвимость IoT-устройств подтверждается и в отчете «Лаборатории Касперского». Кирилл Илганаев, руководитель отдела защиты от DDoS атак в «Лаборатории Касперского», заявил: «Учитывая эффективность IoT-ботнетов, а также растущее число слабо защищенных IoT-устройств, мы можем обоснованно прогнозировать увеличение числа таких атак, а также их мощности и сложности».

По данным статистики компании Corero Network Security:

- В третьем квартале 2017 года организации испытали в среднем 237 попыток атаки DDoS в месяц, равных восьми в день.
- В третьем квартале 2017 года ежемесячные попытки атаки DDoS увеличились на 35% по сравнению с Q2 и на 91% по сравнению с Q1.
- Растущая доступность услуг DDoS for-hire и распространение небезопасных интернет-устройств Things (IoT) привели к увеличению числа атак DDoS в 2017 году. [6]

Из всего вышесказанного можно сделать вывод, что DDoS атаки через IoT-устройства выгодны и достаточно легки в реализации, что влечет за собой их неумолимое развитие.

Чтобы минимизировать риск взлома IoT-устройств, а следовательно – предотвратить атаки злоумышленников на общедоступные сайты, необходимо произвести несколько простых действий:

- Изучить возможности устройства по обеспечению безопасности.
- Провести аудит уже имеющихся в сети устройств (настройки безопасности, актуальные версии ПО).
- Использовать уникальные пароли для доступа на устройство и подключения к сети Wi-Fi (нельзя использовать admin, root, password, 123456 т. п.).
- Использовать надежные методы шифрования при подключении к Wi-Fi (WPA).
- Отключить неиспользуемые сетевые функции устройства (сетевая печать, интернет-облако и т. п.).
- Отключить Telnet-доступ и использовать SSH.
- Отключить удаленный доступ к устройству, если он не используется.
- Регулярно обновлять встроенное ПО с сайта производителя.
- Уделить внимание настройкам безопасности устройства в соответствии с требованиями.
- Использовать проводное соединение вместо Wi-Fi, где это возможно.

Сейчас основной целью взлома IoT-устройств является именно организация DDoS атак, но с ростом мощности оборудования цели преступников могут поменяться и под ударом окажется финансовый сектор, промышленные предприятия и крупные компании. Кража данных или взлом систем управления таких организаций может причинить значительно больший ущерб, нежели простое ограничение доступа к сайту в сети Интернет. И любое домашнее устройство может стать участником этих преступлений. [7]

Согласно опросу A10 Networks, в этом году тип атак DDoS of Things достиг критической массы – в каждом случае нападения задействованы сотни тысяч устройств, подключенных к интернету. Борьба с этим явлением только начинает разворачиваться – хотя поставщики IoT-оборудования крайне медленно реагируют на угрозы, определенные успехи в борьбе с DDoS of Things уже были достигнуты. Счётная палата США в мае выпустила отчет об оценке IoT-технологий, во многом сосредоточенный на уязвимости систем перед кибератаками. Среди основных факторов, сопутствующих распространению угроз, названы отсутствие контроля безопасности из-за невозможности спрогнозировать потенциальные проблемы, а также применение идентичного ПО в различных устройствах, что увеличивает эффективность эксплуатации технических уязвимостей. В связи с этим управление рекомендует разрабатывать IoT-устройства с обязательной возможностью обновления, причем в доступной форме, а не посредством ложного для пользователя процесса.

В ходе проведенной работы было рассмотрено распространение проблемы уязвимости IoT к DDoS атакам, и можно сделать вывод, что ни одна система IoT не достаточно безопасна, чтобы защититься от них. Так как существует множество схем DDoS атак, которые проводятся с помощью устройств IoT и имеющие успех в данное время. Операторы связи и интернет-провайдеры со своей стороны организуют мероприятия по защите от них. Лучшие специалисты отрасли и правительственные структуры работают над протоколами кибербезопасности

интернета вещей, для безопасного использования данных устройств необходимо лишь следовать им.

Список литературы

[1] Опасные предметы: кто и зачем взламывает интернет вещей и как с этим быть [Электронный ресурс] Режим доступа: https://apparat.cc/world/internet-of-things/, свободный. (Дата обращения: 18.03.2018 г.).

[2] DDoS атака. [Электронный ресурс] Режим доступа: https://ru.wikipedia.org/wiki/DoS-%D0%B0%D1%82%D0%B0%D0%BA%D0%B0, свободный. (Дата обращения: 19.03.2018 г.).

[3] Типы DDoS атак. [Электронный ресурс] Режим доступа: https://DDoSguard.net/ru/terminology, свободный. (Дата обращения: 19.03.2018 г.).

[4] Атака "умных" вещей. [Электронный ресурс] Режим доступа: https://nag.ru/articles/article/30371/ataka-umnyih-veschey.html., свободный. (Дата обращения: 19.03.2018 г.).

[5] Овчинский В.С.. Криминология цифрового мира. Учебник для магистратуры.. Москва: НОРМА ИНФРА-М, 2018. 111 с.

[6] DDoS attacks increased 91% in 2017 thanks to IoT [Электронный ресурс] Режим доступа: https://www.techrepublic.com/article/DDoSattacks-increased-91-in-2017-thanks-to-iot/, свободный. (Дата обращения: 21.03.2018 г.).

[7] DDoS атака с IoT устройств. [Электронный ресурс] Режим доступа: https://vasexperts.ru/blog/DDoSataka-s-iot-ustrojstv/, свободный. (Дата обращения: 21.03.2018 г.).