Е.В. Савченко, О.В. Ниссенбаум

Тюменский государственный университет, г. Тюмень

УДК 004.7

БОТНЕТ-АТАКИ НА УСТРОЙСТВА ИНТЕРНЕТА ВЕЩЕЙ

Аннотация. В статье представлен обзор концепции Интернета вещей, активно развивающейся в настоящее время, а также проблемы безопасности «умных» устройств и примеры атак на них.

Ключевые слова: интернет вещей, IoT, Internet of Things, уязвимости интернета вещей, атаки на интернет вещей, ботнет, botnet.

Интернет вещей (Internet of Things, IoT) – научная концепция о способах взаимодействия физических объектов, устройств и систем между собой и с окружающим миром с применением различных технологий связи и стандартов соединения. Благодаря IoT работают фитнесс-трекеры, системы умного дома, умные часы, веб-маячки и множество других устройств [1].

Строение сети Интернета вещей

На данный момент концепция IoT опирается на две технологии [2]:

- радиочастотная идентификация - метод распознавания объектов, при котором благодаря использованию радиосигналов происходит записывание и считывание имеющихся данных;
- беспроводные сенсорные сети - наличие множества датчиков и исполнительных устройств, объединенных с помощью радиосигнала, область покрытия которого находится в диапазоне от нескольких метров до пары километров.

Архитектура IoT предполагает наличие следующих уровней: сеть датчиков, шлюз, управление, приложение. Большинство сервисов IoT основано на обработке информации от множества узлов, что принципиально отличается от архитектур классических сетей. Поэтому необходимы специальные протоколы для обеспечения взаимодействия устройств друг с другом и верхними уровнями.

Для обеспечения связи между сенсорными узлами и датчиками используется протокол DDS (Data Distribution Service) [3], реализующий шаблон публикации-подписки для отправки и приема данных, событий и команд среди конечных узлов [4].

Для связи сенсорного узла с сервером используются протоколы [4]:

- CoAP (Constrained Application Protocol) – протокол передачи для сетей и устройств с ограниченными ресурсами [3];
- XMPP (Extensible Messaging and Presence Protocol) – используется в интернете для передачи сообщений в режиме реального времени [4];
- MQTT (Message Queue Telemetry Transport) – собирает данные от множества узлов и передает их на сервер, основан на модели издатель-подписчик с промежуточным сервером – брокером [4];
- STOMP – Simple (или Streaming) Text Oriented Message Protocol – протокол обмена сообщениями, предполагает взаимодействие со многими языками, платформами и брокерами [3].

Для передачи данных от сервера к приложению в IoT используется протокол SOAP (Simple Object Access Protocol), так как у него выделен механизм доступа RPC (Remote Procedure Call) для удаленного вызова функций [3].

В IoT применяются технологии построения сетей передачи данных по линиям электропередачи и технологии беспроводных вычислительных сетей физических предметов с низким энергопотреблением [5].

Чаще всего в IoT используются следующие протоколы [6]:

- ZigBee - стандарт стека протоколов для беспроводных сенсорных сетей от альянса ZigBee, создан на основе стандарта IEEE 802.15.4, описывающего физический уровень и уровень доступа к среде для беспроводных сетей передачи данных на небольшие расстояния (до 75 м) с низким энергопотреблением, но высокой надежностью передачи сообщений;
- Bluetooth v.4.0 – Bluetooth с низким энергопотреблением (Bluetooth low energy, Bluetooth LE, BLE) – версия спецификации Bluetooth,

дающая возможность поддержки широкого диапазона приложений и позволяющая уменьшить размер конечного устройства;

- IEEE 802.11 (WiFi) – благодаря высоким скоростям передачи, беспроводные сети WiFi применяются, когда необходимо передавать большие объемы информации в режиме реального времени.

Уязвимости и атаки в Интернете вещей

Одной из основных причин уязвимости информационных систем в сети Интернет, в том числе IoT, являются слабости сетевого протокола IP стека протоколов TCP/IP, который служит основой сетевых коммуникаций [7].

Кроме того, слабыми местами Интернета вещей являются [8]:

- стандартные учётные записи от производителя, слабая аутентификация;
- отсутствие поддержки со стороны производителя для устранения уязвимостей;
- использование текстовых протоколов и наличие ненужных открытых портов;
- использование незащищённых мобильных технологий;
- использование незащищённой облачной инфраструктуры;
- использование небезопасного ПО.

С использованием уязвимостей IoT осуществляются атаки [9]:

- DoS-атаки в Интернете вещей – с использованием протокола SNMP осуществляется особая форма DoS-атак, позволяющая злоумышленнику захватить незащищенные сетевые устройства с ограниченными вычислениями и памятью: датчики, камеры, принтеры, роутеры и т.д., которые в дальнейшем используются как боты для атаки на третьих лиц;
- прослушивание в IoT - если злоумышленник получит доступ к определенной инфраструктуре, то он может восстановить информацию, проходящую через нее;

- узел захвата в IoT - хакер может нацелиться на инфраструктуру, используемую для хранения или обработки данных организации: в распределенной среде IoT для создания и обработки информации используются различные объекты, что увеличивает количество затрачиваемых на атаку времени и сил, однако если злоумышленники заинтересованы только в части информации, они могут использовать узконаправленные атаки на системы, управляющие конкретными данными;
- атаки на физическую безопасность датчиков - с помощью специального оборудования для обнаружения различных электронных сигналов злоумышленник может определить расположение датчиков, а затем физически отключить, уничтожить или украсть.

Значительная часть атак на Интернет вещей происходит из-за небрежности владельцев «умных» вещей, которые не меняют пароли и не устанавливают контроль номеров доверенных лиц, так что отключить «умную» сигнализацию может любой человек, знающий модель системы и телефонный номер установленной в ней карты [10].

Ботнет

Самым распространенным использованием уязвимостей IoT является захват устройств в ботнет – сеть компьютеров, зараженных вредоносной программой – ботом, позволяющим удаленно управлять зараженными машинами без ведома пользователя. Управление может быть прямым и опосредованным. В случае прямого управления злоумышленник может установить связь с инфицированным компьютером и управлять им, используя встроенные в тело программы-бота команды. В случае опосредованного управления бот сам соединяется с центром управления или другими машинами в сети, посылает запрос и выполняет полученную команду [11].

Часто киберпреступники стремятся заразить вредоносными программами и взять под контроль тысячи, десятки тысяч и даже миллионы компьютеров и таким образом свободно управлять большой зомби-сетью. В

некоторых случаях злоумышленники создают большую сеть зомби-компьютеров, а затем продают доступ к ней другим преступникам или сдают ее в аренду [12].

Известны следующие типы архитектуры ботнетов [11]:

- с единым центром – самый распространенный тип – все зараженные компьютеры соединяются с одним центром управления (C&C, Command&Control Centre), который ожидает подключения новых ботов, регистрирует их в своей базе, следит за их состоянием и выдает им команды;
- децентрализованные, или P2P-ботнеты («peer-to-peer», «точка-точка») - каждый новый зараженный компьютер получает список тех ботов, с которыми он будет связываться в зомби-сети - «соседей», команды передаются от бота к боту: при получении команды, компьютер передает ее остальным.

Ботнеты выполняют следующие функции [13]:

- распределяют нападения типа DoS (Distributed DoS, DDoS);
- открытые SOKS-прокси на заражённых компьютерах позволяют рассылать спам;
- выуживание информации, рентабельность которой превышает рентабельность спамовых электронных писем в 1000 раз;
- создание фишинговых сайтов, которые могут располагаться на компьютерах пользователей по всему миру;
- кража программного обеспечения.

Пожалуй, самым известным в настоящее время ботнетом является Mirai –программа, которая взламывает онлайн-устройства и использует их для проведения DDoS-атак. По одной версии, программа использует почтовые вирусы, чтобы заразить домашний компьютер, а потом все подключенные к нему устройства – видеорегистратор, телеприставку, роутер. По другой версии, Mirai непрерывно сканирует устройства IoT и заражает их, используя таблицу устанавливаемых производителем имен пользователей и паролей. Устройство остается зараженным до первой перезагрузки, если

после пароль не был сменен, то устройство заражается снова. Получив тем или иным способом доступ к устройствам интернета вещей, Mirai создает из них ботнет [14].

Примеры атак

Начиная с сентября 2016 года было совершено несколько сильнейших в истории DDoS-атак. Суммарная мощность двух из них достигала рекордных 1 Тбит/с [15]. Все началось 10 сентября с DDoS атаки на блог специалиста по безопасности Брайана Кребса. На пике мощность атаки составила около 140 гигабит в секунду. На некоторое время блог ушел в офлайн, но вскоре возобновил работу – благодаря компании Akamai, которая в течение четырех лет бесплатно защищала его от DDoS-атак. Однако злоумышленники не прекратили атаку, и 20 сентября пик атаки составил уже 665 гигабит в секунду. Akamai, одна из крупнейших компаний по обеспечению работы сайтов, отказалась продолжать обслуживать блог, поскольку из-за силы атаки начались проблемы у платных клиентов. Как сообщили Akamai, эта атака была в два раза мощнее всех известных ранее.

Позже выяснилось, что атака на блог Кребса велась при помощи взломанных IoT-устройств — IP-камер, роутеров и другого оборудования, на которых остались стандартные пароли [16]. В атаке участвовало около 1,5 миллионов устройств Интернета вещей.

Еще одним примером DDoS атаки с применением «умных» устройств является атака на DNS-серверы компании Dyn, произошедшая 21 октября 2016 года. Во время атаки часть пользователей не могла зайти в Twitter, Spotify, Reddit и на ряд других сайтов. В атаке был задействован трафик сотен тысяч устройств Интернета вещей – камер наблюдения, видеорегистраторов и других приборов. Хакеры использовали ботнет Mirai [17].

В начале 2017 года специалисты по информационной безопасности компании Radware обнаружили зловред BrickerBot, который не объединяет «умные» устройства в ботнет, а делает невозможным их использование [18].

Атаковать гаджеты это зловредное ПО начало с 20 марта [19]. На первом этапе атаки BrickerBot действует так же, как и другие IoT-зловреды, включая Mirai. Сначала проводится брутфорс-атака по Telnet, с подбором доступа к функциям управления атакуемого устройства. После того, как зловред получил доступ в систему, начинаются попытки вывода гаджета из строя. Скомпрометированный гаджет прекращает работать всего через несколько секунд после заражения.

После раскрытия BrickerBot, его автор Janit0r обратился в Bleeping Computer и объяснил, что считает BrickerBot "Интернет-Химиотерапей" и что он создал вредоносное программное обеспечение как способ саботировать уязвимые устройства, прежде чем они были заражены вредоносным программным обеспечением Mirai [20].

Заключение

На данный момент ведутся активные разработки в сфере обеспечения информационной безопасности IoT. Разрабатываются новые модели и протоколы, рассматриваются способы применения шифрования и более защищенных протоколов. Владельцам «умных» устройств для защиты необходимо:

- менять пароли на всех устройствах;
- проверять количество установленных сетевых подключений и удалять подозрительные;
- регулярно обновлять операционную систему и основное программное обеспечение;
- отключить разрешения на стороннее внедрение в ОС.

СПИСОК ЛИТЕРАТУРЫ

1. Джурко А. Как появился Интернет вещей? // Новости Интернета вещей – 2016 – 27 июня [Электронный ресурс] URL:

https://iot.ru/promyshlennost/istoriya-interneta-veshchey (дата обращения 15.03.2018)

2. Интернет вещей - что это такое? Развитие интернета вещей в России // Новостной портал FB.RU – 2016 – 9 июня [Электронный ресурс] URL: http://fb.ru/article/251264/internet-veschey---chto-eto-takoe-razvitie-interneta-veschey-v-rossii (дата обращения 14.03.2018)

3. Гойхман В., Савельева А. Аналитический обзор протоколов Интернета вещей // Технологии и средства связи. – 2016. – №4. – С. 32-37 [Электронный ресурс] URL: http://www.tssonline.ru/articles2/reviews/analiticheskiy-obzor-protokolov-interneta-veschey (дата обращения 25.03.2018)

4. Протоколы передачи данных IoT // Новости Интернета вещей [Электронный ресурс] URL: https://iot.ru/wiki/protokoly-peredachi-dannykh-iot (дата обращения 25.03.2018)

5. Ткаченко В. IoT - современные телекоммуникационные технологии // ОБУЧЕНИЕ В ИНТЕРНЕТ – 2016 – 29 августа [Электронный ресурс] URL: http://www.lessons-tva.info/articles/net/013.html (дата обращения 18.03.2018)

6. Росляков А.В., Ваняшин С.В., Гребешков А.Ю. Интернет вещей: учебное пособие – Самара: ПГУТИ, 2015. – 200 с.

7. Уязвимости основных сетевых протоколов // Хелпикс.Орг - Интернет помощник [Электронный ресурс] URL: http://helpiks.org/6-60723.html (дата обращения 28.03.2018)

8. Информационная безопасность интернета вещей (Internet of Things) // TAdviser - портал выбора технологий и поставщиков – 2018 – 22 марта [Электронный ресурс] URL: http://www.tadviser.ru/index.php/Статья%3AИнформационная_безопасность_интернета_вещей_%28Internet_of_Things%29 (дата обращения 23.03.2018)

9. Alsaadi E., Tubaishat A. Internet of Things: Features, Challenges, and Vulnerabilities // International Journal of Advanced Computer Science and Information Technology (IJACSIT) – 2015 - V. 4, №. 1 - P. 1-13 [Электронный

ресурс] URL: http://elvedit.com/journals/IJACSIT/wp-content/uploads/2015/02/internet-of-things.pdf (дата обращения 23.03.2018)

10. Еще один взгляд на безопасность Интернета вещей // Geektimes – 2015 - 17 декабря [Электронный ресурс] URL: https://geektimes.ru/company/iridiummobile/blog/267760/ (дата обращения 29.03.2018)

11. Что такое ботнет // WEBTUN.COM – веб обозреватель – 2012 – 27 октября [Электронный ресурс] URL: https://webtun.com/others/3706-chto-takoe-botnet.html (дата обращения 13.04.2018)

12. Что такое ботнет? // Лаборатория Касперского [Электронный ресурс] URL: https://www.kaspersky.ru/resource-center/threats/botnet-attacks (дата обращения 13.04.2018)

13. Что такое ботнеты? // Мельница web services [Электронный ресурс] URL: http://melnyca.ru/chto-takoe-botnety/ (дата обращения 13.04.2018)

14. Чехова П. Как понять, что твой компьютер стал частью ботнета? // Новостной портал SmartBabr – 2016 – 31 октября http://smartbabr.com/?doc=784 (дата обращения 13.04.2018)

15. Григорьев Д. Атака «умных» вещей // Новостной портал NAG.RU – 2016 – 25 октября [Электронный ресурс] URL: https://nag.ru/articles/article/30371/ataka-umnyih-veschey.html (дата обращения 29.03.2018)

16. Цыбульский В. Специалист по безопасности раскрыл организаторов DDoS-атак — и ему отомстили: блог Брайана Кребса атаковали так, как никого и никогда // Новостной портал MEDUZA – 2016 - 26 сентября [Электронный ресурс] URL: https://meduza.io/feature/2016/09/26/spetsialist-po-bezopasnosti-raskryl-organizatorov-ddos-atak-i-emu-otomstili (дата обращения 02.04.2018)

17. Красильникова Ю. Интернет вещей открыл новую эру кибератак // Новостной портал Хайтек – 2016 – 25 октября [Электронный ресурс] URL: https://hightech.fm/2016/10/25/ddos_2016 (дата обращения 02.04.2018)

18. Новое вредоносное ПО BrickerBot превращает IoT-устройство в «кирпич» // Новостной портал SecurityLab – 2017 – 7 апреля [Электронный ресурс] URL: https://www.securitylab.ru/news/485811.php (дата обращения 03.04.2018)

19. Зловред BrickerBot превращает IoT-гаджеты в «кирпич» // Geektimes 2017 – 8 апреля [Электронный ресурс] URL: https://geektimes.ru/post/287844/ (дата обращения 03.04.2018)

20. Cimpanu C. BrickerBot Author Retires Claiming to Have Bricked over 10 Million IoT Devices // BleepingComputer.com - News, Reviews, and Technical Support – 2017 - December 11 [Электронный ресурс] URL: https://www.bleepingcomputer.com/news/security/brickerbot-author-retires-claiming-to-have-bricked-over-10-million-iot-devices/ (дата обращения 03.04.2018)