УДК 004.056.5

МЕТОДЫ ЗАЩИТЫ ОТ DDOS-АТАК В СЕТИ УСТРОЙСТВ IOT. ИХ ДОСТОИНСТВА И НЕДОСТАТКИ

© 2024 В. В. Гордиенко[1], М. А. Печурин[2]

[1] кандидат технических наук, доцент кафедры информационной безопасности
e-mail: vika.gordienko.1973@ mail.ru
[2] студент 1 курса магистратуры, направления подготовки
«Информационно-коммуникационные технологии в образовании»
e-mail: maxim.pechurin@mail.ru

Курский государственный университет

В статье рассматриваются основные методы защиты от DDoS-атак в сети устройств IoT, анализируются их достоинства и недостатки в контексте текущих угроз кибербезопасности. Представлены технические и поведенческие подходы к предотвращению атак, включая обучение пользователей, механизмы аутентификации, использование программного обеспечения, защищающего от DDoS-атак, и многое другое. Авторы предлагают читателям более глубокое понимание эффективных методов защиты, которые могут помочь предотвратить серьезные последствия DDoS-атак в современном мире цифровых технологий.

Ключевые слова: DDoS-атака, интернет вещей (IoT), информация, метод, злоумышленник, ботнет.

METHODS OF PROTECTION AGAINST DDOS ATTACKS IN THE NETWORK OF IOT DEVICES. THEIR ADVANTAGES AND DISADVANTAGES

© 2024 V. V. Gordienko[1], M. A.Pechurin[2]

[1] Candidate of Engineering Sciences,
Associate Professor, Department of Information Security, KSU
e-mail: vika.gordienko.1973@ mail.ru,
[2]1st year student of the master's degree in the field of training "Information and communication technologies in education",
e-mail: maxim.pechurin@mail.ru

Kursk State University

This article discusses the main methods of protection against DDoS attacks in the network of IoT devices, analyzing their advantages and disadvantages in the context of current cybersecurity threats. It discusses technical and behavioral approaches to preventing attacks, including user training, authentication mechanisms, the use of software that protects against DDoS attacks, and much more. The author offers readers a deeper understanding of effective protection methods that can help prevent serious consequences of DDoS attacks in the modern world of digital technologies.

Keywords: DDoS attack, Internet of Things (IoT), information, method, attacker, botnet.

Современный мир все более часто использует IoT-устройства (Internet of Things), либо же умные вещи. Миллионы гаджетов заменяют собой обычные вещи. Однако все потребительские умные вещи, от часов до планшетов, термостатов и даже умных

игрушек, являются лишь крохотной частью по сравнению с миллионами новых коммерческих устройств, подключаемых к Интернету ежедневно.

Область применения таких устройств затрагивает все сферы человеческой жизни, включая медицину, промышленность, сельское хозяйство и городскую среду, но для злоумышленников все они представляют собой лишь неисчерпаемый источник приумножения своих сил [1].

До недавнего времени атаки на IoT-устройства были направлены в первую очередь на хищение данных пользователей, однако сейчас злоумышленников больше интересует контроль над устройством с целью включения его в ботнет и осуществления DDoS-атак. Причин, по которым преступники выбирают для взлома именно IoT-устройства, несколько:

1) многие из них постоянно доступны из сети Интернет, но так как не обладают высокой вычислительной мощностью, лишены встроенных средств защиты;

2) такие устройства чаще всего настраивают один раз при установке, а потом про их настройку забывают. Пользователь не знает обо всех функциях безопасности, не обновляет программное обеспечение – эти факторы повышают риск взлома;

3) пользователь не меняет заводские логины и пароли, которые легко можно найти в Интернете для любого устройства [2].

DDoS-атака (Distributed Denial of Service) – это форма кибератаки на веб-системы с целью вывести их из строя или затруднить доступ к ним для обычных пользователей. Атакующие зачастую используют распределенную сеть множества устройств, одновременно отправляющих запросы на сервер жертвы до его перезагрузки. Такие кибератаки наиболее распространены, потому что могут довести до отказа любую систему без должной защиты, не оставляя юридически значимых улик [3].

Схожий метод можно проиллюстрировать ситуацией, когда множество людей скапливается у входа в магазин, препятствуя подход другим посетителям. В результате магазин теряет доходы и вынужден предпринимать какие-либо меры для того, чтобы устранить скапливание людей.

Ботнеты – это сети, состоящие из компьютеров, захваченных киберпреступниками, которые те используют для различных махинаций и кибератак. Организация ботнета обычно является начальным этапом многоуровневой схемы. Боты служат инструментом массированных автоматизированных атак, цель которых – похищение данных, вывод из строя серверов и распространение вредоносного ПО [4].

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

1) изучить возможности устройства по обеспечению безопасности перед покупкой;
2) провести аудит уже имеющихся в сети устройств;
3) использовать уникальные пароли для доступа на устройство и подключения к сети Wi-Fi (не использовать admin, root, password, 123456 и т.п.);
4) использовать надежные методы шифрования при подключении к Wi-Fi (WPA);
5) отключить неиспользуемые сетевые функции устройства;
6) отключить Telnet-доступ и использовать SSH;
7) отключить удаленный доступ к устройству, если он не используется;
8) регулярно обновлять встроенное ПО с сайта производителя;
9) уделить внимание настройкам безопасности устройства в соответствии с требованиями;
10) использовать проводное соединение вместо Wi-Fi, где это возможно [5].

В 2016 г. трое молодых американских хакеров, не так давно начавших свой путь в данной сфере, создали ботнет под названием Mirai, с помощью которого на протяжении долгого времени атаковали крупнейшие медиа, веб-сайты и компании. Принцип работы вредоносного ПО заключался в том, что Mirai ищет подключенные к Интернету IoT-устройства, работающие на процессоре ARC. Причем в объектив попадают процессоры, на которых установлена урезанная версия ОС Linux. Вирус взламывает доступ путем подбора имени пользователя и пароля, установленных по умолчанию (если те не были изменены). По оценкам экспертов, в ботнете Mirai было задействовано порядка 145 000 IoT-устройств. Хоть создатели этого вредоносного ПО были найдены и осуждены, Mirai все еще остается опасным ботнетом по причине того, что исходный код вируса продолжает жить и приобретать новые и более опасные формы [6].

DDoS-атаки можно разделить на низкоуровневые и высокоуровневые. К низкоуровневым относятся атаки на Сетевой и Транспортный уровни модели OSI, к высокоуровневым атакам относятся атаки на Сеансовый и Прикладной уровни модели OSI.

Рассмотрим низкоуровневые атаки. Основная цель атак на сетевом уровне – исчерпание пропускной способности на всех уровнях и этапах. Сетевой уровень считается легкой мишенью для киберпреступников, поскольку для организации DDoS-атаки даже не нужна установка TCP-соединения с атакуемыми ресурсами. Атаки представляют из себя «засорение» канала. Примером могут быть CMP-flood, ICMP-flood и др.

Атаки транспортного уровня могут быть направлены на недостатки в процессе установления соединения, управления сессией или завершения соединения. Транспортные DDoS-атаки могут вызвать чрезмерное потребление ресурсов, блокировку доступа к сервисам или сбои в работе сетевого оборудования. Примером могут быть SYN-flood, Smurf-атака, «Ping-of-Death».

Перейдем к высокоуровневым атакам. На сеансовом уровне атакам подвергается сетевое оборудование. Используя уязвимости программного обеспечения Telnet-сервера на свитче, злоумышленники могут заблокировать возможность управления свитчем для администратора. К таким атакам можно отнести также SYN-flood, UDP-flood, Словарную атаку (атака, при которой происходит попытка подобрать пароль пользователя), ARP- и ICMP-атаки на Telnet-сервер.

В конечном итоге переходим на атаки на уровне приложений – это виды кибератак, которые направлены на приложения, в особенности на их программный код, AIP, протоколы и технологии, такие как базы данных и скрипты. Причем они могут задействовать не только HTTP, но и, например, HTTPS, DNS, VoIP, SMTP, FTP. Сейчас атак на уровень приложения становится больше, их количество в объеме DDoS-атак постоянно увеличивается. Причем опасность таких кибератак не только в сложности их отражения, но и в том, что они часто комплексные, включая:

1) медленные атаки малого объема;
2) атаки с применением массивов произвольных «мусорных» запросов;
3) атаки, которые имитируют поведение реальных пользователей.

Примерами атак на уровне приложений могут являться следующие: SQL-инъекция, XSS, HTTP-flood, HTTPS-flood, DNS-атаки [7].

Для каждого вида атаки выработаны свои методы защиты и профилактики. Они включают в себя различные меры и технологии, направленные на предотвращение атак со стороны злоумышленников. Ниже приведены основные технические методы защиты от DDoS-атак в сети устройств IoT с веб-приложением в форме управления умными устройствами:

1) использовать подготовленные выражения и параметризованные SQL-запросы;
2) использовать экранирование специальных символов в SQL-запросах;
3) фильтровать IP других стран;
4) использовать проверку входных данных на соответствие ожидаемому формату;
5) использовать преобразование специальных символов в безопасные эквиваленты;
6) ограничить источники, из которых разрешено загружать ресурсы;
7) использовать HTTPOnly и Secure флаги для Cookie;
8) использовать безопасные API;
9) использовать уникальные токены;
10) настраивать XML-парсер так, чтобы он не обрабатывал внешние сущности;
11) двухфакторная аутентификация [8].

Изучая существующие методы борьбы с DDoS-атаками в сети устройств IoT, нужно однозначно понимать, что у каждого из них существуют свои определенные достоинства и недостатки, и для полноценного анализа стоит в них разобраться.

К достоинствам существующих методов защиты точно стоит отнести такие характеристики, как: снижение нагрузки на сервис (веб-приложение); ускорение работы в связи со снижением нагрузки; защита компьютеров и сетей от вредоносных программ, что уменьшает риск заражения и утечки данных; предоставление многофактурной аутентификации дополнительного уровня безопасности за счет требования ввода дополнительных данных для входа в систему.

Хотя существуют различные методы защиты от DDoS-атак в сети устройств IoT, они не лишены недостатков. Вот некоторые из них:

1) недостаточная осведомленность пользователей;
2) сложность обнаружения новых методов атак;
3) непостоянство уровня защиты;
4) недостаточная интеграция различных методов защиты;
5) сложность поддержания актуальности защиты.

Подводя итог, можно отметить, что существует ряд эффективных методов защиты от DDoS-атак в сети устройств IoT, которые могут значительно уменьшить риск попадания в ловушку злоумышленников. Однако каждый из них имеет свои достоинства и недостатки.

Например, обучение сотрудников признакам DDoS-атаки и проведение регулярных тренингов может повысить уровень осведомленности персонала, но требует времени и ресурсов на его реализацию. Технические меры, такие как внедрение защитного кода в состав приложения и фильтров, обеспечивают неплохую защиту от зловредного программного обеспечения, но не всегда эффективны против продвинутых, современных и новореализуемых атак.

Таким образом, оптимальная стратегия защиты от DDoS-атак в сети устройств IoT включает в себя сочетание различных методов, учитывающих как человеческий фактор, так и технические аспекты, комплекса аппаратной защиты и встроенного защищающего кода. Важно постоянно совершенствовать свои знания и применять новейшие технологии для обеспечения безопасности информации, личных данных и средств.

Библиографический список

1. *Зараменских, Е. П.* Интернет вещей. Исследования и область применения / Е. П. Зараменских, И. Е. Артемьев. – М.: ИНФРА-М, 2020.

2. Как ботнеты «похищают» умные устройства (IoT) [Электронный ресурс]. – URL: https://botfaqtor.ru/blog/iot-botnets/ (дата обращения: 12.04.2024).

3. *Бирюков, А.А.* Информационная безопасность: защита и нападение. – М.: ДМК-Пресс, 2013. – 474 с.

4. Что такое DDoS-атаки и как от них защититься [Электронный ресурс]. – URL: https://yandex.cloud/ru/docs/glossary/ddos (дата обращения: 21.04.2024).

5. Взгляд внутрь инициированных IoT DDoS-атак и защита ИТ-инфраструктур [Электронный ресурс]. – URL: https://www.securitylab.ru/news/549362.php (дата обращения 09.04.2024).

6. Чудовище из американского подвала: краткая история мегаботнета Mirai [Электронный ресурс]. – URL: https://www.securitylab.ru/news/543680.php (дата обращения: 05.04.2024).

7. Классификация DDoS: полное руководство по типам атак [Электронный ресурс]. – URL: https://ddos-guard.net/ru/blog/classification-of-ddos-attacks (дата обращения: 20.04.2024)

8. Методы защиты от DDoS нападений. [Электронный ресурс]. – URL: https://www.securitylab.ru/analytics/216251.php (дата обращения 21.04.2024).