НБ РАЗДЕЛ. КИБЕРБЕЗОПАСНОСТЬ И КИБЕРПРЕСТУПНОСТЬ

УДК 004

Лобова Анастасия Игоревна,
КФ МГТУ им. Н.Э. Баумана, г. Калуга
Lobova Anastasia Igorevna, KB of BMSTU, Kaluga

Вершинин Евгений Владимирович,
к.ф.-м.н., доцент, КФ МГТУ им. Н.Э. Баумана, г. Калуга
Vershinin Evgeniy Vladimirovich, KB of BMSTU, Kaluga

Фёдоров Виктор Олегович, к.т.н., доцент,
КФ МГТУ им. Н.Э. Баумана, г. Калуга
Fedorov Victor Olegovich, KB of BMSTU, Kaluga

ОБЗОР DDOS-АТАК НА IOT УСТРОЙСТВА
OVERVIEW OF DDOS ATTACKS ON IOT DEVICES

Аннотация: распределенные атаки типа «отказ в обслуживании» становятся одной из самых глобальных угроз в сети Интернет. Растущее число устройств интернета вещей увеличивает множество способов проведения DDoS атак. В данной статье проведен обзор DDoS-атак на устройства интернета вещей и приведены основные рекомендации по защите ИТ-инфраструктур с устройствами IoT.

Abstract: distributed denial of service attacks are becoming one of the most global threats on the Internet. The growing number of IoT devices increases the variety of ways DDoS attacks can be carried out. This article provides an overview of DDoS attacks on IoT devices and provides basic recommendations for protecting IT infrastructures with IoT devices.

Ключевые слова: DDoS, IoT, ботнет, отказ в обслуживании, Mirai.

Keywords: DDoS, IoT, botnet, denial of service, Mirai.

Введение

DDoS-атаки (Distributed Denial of Service – распределённые атаки класса «отказ в обслуживании») – это атаки на вычислительные системы (сетевые ресурсы или каналы связи), имеющие целью сделать их недоступными для легитимных пользователей. DDoS-атаки заключаются в одновременной отправке в сторону определенного ресурса большого количества запросов с одного или многих компьютеров, расположенных в сети Интернет. Если тысячи, десятки тысяч или миллионы компьютеров одновременно начнут посылать запросы в адрес определенного сервера (или сетевого сервиса), то либо не выдержит сервер, либо не хватит полосы пропускания канала связи к этому серверу. В обоих случаях, пользователи сети Интернет не смогут получить доступ к атакуемому серверу, или даже ко всем серверам и другим ресурсам, подключенным через заблокированный канал связи [8].

Иными словами, DDoS-атака – атака, направленная на замедление работы или выведение из строя серверов, сетевой инфраструктуры, а также бомбардировка трафика приложений из нескольких ресурсов. В результате DDoS-атак сайты и приложения становятся заторможенными либо вообще перестают работать. В настоящее время более 30% случаев простоя приложений и серверов вызваны DDoS-атаками [1].

В глобальном масштабе ежедневно регистрируется две тысячи DDoS-атак. Средняя атака DDoS обходится крупной компании в 250 долл. в час [2].

Ботнеты как самый популярный и опасный способ проведения DDoS-атак

Наиболее популярным и опасным способом запуска DDoS-атак является использование ботнетов (BotNets).

Ботнет – это сеть девайсов, инфицированных вредоносным ПО, дающим злоумышленнику доступ к удаленному контролю над ними, к рассылке спама и вирусов, а особенно служащих местом размещения ПО, осуществляющим DDoS-атаки без ведома владельца зараженного гаджета.

Однако, в частности, говоря об «интернете вещей», ботнет – это сеть инфицированных вредоносным ПО IoT устройств [1].

Боты распространяются в сети Интернет различными способами, как правило – путем атак на компьютеры, имеющие уязвимые сервисы, и установки на них программных закладок, либо путем обмана пользователей и принуждения их к установке ботов под видом предоставления других услуг или программного обеспечения, выполняющего вполне безобидную или даже полезную функцию. Способов распространения ботов много, новые способы изобретаются регулярно.

Если ботнет достаточно большой – десятки или сотни тысяч компьютеров – то одновременная отправка со всех этих компьютеров даже вполне легитимных запросов в сторону определённого сетевого сервиса (например, web-сервиса на конкретном сайте) приведет к исчерпанию ресурсов либо самого сервиса или сервера, либо к исчерпанию возможностей канала связи. В любом случае, сервис будет недоступен пользователям, и владелец сервиса понесет прямые, косвенные и репутационные убытки. А если каждый из компьютеров отправляет не один запрос, а десятки, сотни или тысячи запросов в секунду, то ударная сила атаки увеличивается многократно, что позволяет вывести из строя даже самые производительные ресурсы или каналы связи [8].

DDoS-атаки на IoT устройства

Случаи бурного роста числа и тяжести DDoS атак, зарегистрированные в 2016-2017 годах, вызваны широким внедрением технологии Internet of Things (IoT) [1].

IOT – это развивающаяся технология, которая объединяет обычные устройства с Интернетом. После подключения к сети IoTD (устройства интернета вещей) могут обмениваться данными друг с другом, веб-службами и приложениями. Интернет вещей используется для обеспечения человека такими удобствами, таких как автоматическое или удаленное управление умными домами, эффективная инфраструктура с низким уровнем отходов, а также сбор и анализ биометрических данных в реальном времени с помощью носимых технологий.

Хотя устройства Интернета вещей (IoTD) приносят пользу во многих аспектах жизни, эти устройства также создают риски безопасности в виде уязвимостей, которые дают хакерам миллиарды новых многообещающих целей. Например, ботнеты использовали недостатки безопасности, характерные для IoTD, для получения несанкционированного контроля над сотнями тысяч хостов, которые затем использовали для проведения массовых разрушительных распределенных атак типа «отказ в обслуживании» [3].

На данный момент концепция IoT опирается на две технологии:

1) Радиочастотная идентификация – метод распознавания объектов, при котором благодаря использованию радиосигналов происходит записывание и считывание имеющихся данных;

2) 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 [4].

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.

Ботнеты для IoT отличаются от аналогов на базе Windows тем, что они построены из взломанных IoT-устройств и могут распространяться на огромное количество устройств, используя обширную сеть IoT. Более того, в отличие от обычных ботнетов, которые, в основном, используются для рассылки спама, ботнеты IoT могут нанести гораздо больший ущерб, воздействуя на доступную для устройств IoT физическую среду.

Например, атака ботнетов IoT на светофоры может создать хаос в городе и разрушать интеллектуальную городскую инфраструктуру. Аналогичным образом хакеры способны увеличить температуру в умных домах и искусственно повысить спрос на нефть или газ.

В отличие от персональных компьютеров и серверов, которые защищены фильтрующими функциями файерволов и детекторами вредоносных программ, IoT-устройства становятся для ботнетов привлекательными целями, поскольку они обычно не используют такие расширенные функции безопасности.

Угроза для кибербезопасности, связанная с распространением ботсетей IoT, была предсказана в 2016 году, но специалисты по безопасности в Интернете не уделили достаточно внимания этой проблеме. В то время эта угроза представлялась довольно ограниченной. Однако вскоре появился набор инструментов, позволяющих ботнетам пользоваться уязвимостью в незащищенных устройствах IoT. Атака Mirai в октябре 2016 года стала ключевым поворотным моментом в развитии IoT.

Злоумышленникам не так интересны IoT девайсы в качестве «жертвы». Цель хакеров – захватить устройство, чтобы добавить его к ботнету, который и используется для DDoS-атак.

Безопасность «интернета вещей» в целом недооценивается и даже игнорируется не только обычными пользователями, но и целыми компаниями. Именно из-за уязвимости IoT устройств и их растущего количества данная область интернета интересна хакерам [1].

Вместе с ежегодным ростом количества IoT устройств, растет потенциальное количество уязвимостей во встроенном программном обеспечении этих устройств. От того насколько быстро будет обнаружена уязвимость, зависит скорость выпуска патча, закрывающего эту уязвимость, следовательно существует потребность в повышении эффективности процесса выявлении уязвимостей во встроенном программном обеспечении устройств интернета вещей [5].

Интернет вещей присутствует в различных устройствах: в бытовой технике, смартфонах, умной одежде, носимых устройствах (браслеты, очки виртуальной реальности и т.д.), смарт-телевизорах, игровых консолях, транспортных системах, зданиях (камеры видеонаблюдения), кондиционирование воздуха, контроль доступа и т. д.), общественные инфраструктуры (мосты, шоссе, парки и т. д.), общественные услуги, промышленные компоненты (например, системы SCADA), системы транспортировки и т. д.

По мере увеличения сбора и анализа информации с различных устройств, не только промышленный сектор и сектор услуг, но и вся технологическая инфраструктура, на которой основано общество, подвергается опасности, что увеличивает риски безопасности, где объем данных растет со все возрастающей скоростью, превышающей несколько эксабайтов. Несанкционированный доступ организованной преступности к системам прогнозирования в промышленной, военной, финансовой, медицинской и иной инфраструктуре может быть критичен и практически непоправим [6].

Не каждая компьютерная система в доме содержит сканер вирусов: в современном доме вы легко найдёте больше десятка устройств на базе Linux и процессоров ARM или MIPS, – телевизоры, работающие под управлением смарт-систем, сетевые устройства, такие как точки доступа и адаптеры Powerline, интернет-радио и Raspberry Pi.

Отсутствие программного обеспечения безопасности и, в частности, отсутствие мер безопасности, интегрированных в Linux, повышают привлекательность для хакеров. Поскольку вредоносное ПО обычно запускается и удаляется, то есть исчезает после перезапуска, ни анализ образа операционной системы, ни проверка существующих файлов не помогают.

Mirai как один из самых опасных ботнетов, нацеленных на IoT

Mirai – это вредоносная программа, которая заражает интеллектуальные устройства, работающие на процессорах ARC, превращая их в сеть удаленно управляемых ботов или «зомби». Эта сеть ботов часто используется для запуска DDoS-атак.

Mirai сканирует Интернет на предмет устройств IoT, работающих на процессоре ARC. Этот процессор работает под управлением урезанной версии операционной системы Linux. Если комбинация имени пользователя и пароля по умолчанию не изменена, Mirai сможет войти в устройство и заразить его.

Mirai со временем мутирует. Злоумышленники, пользуясь его исходным кодом, оставшимся в сети, разработали и продолжают разрабатывать другие ботнеты, такие как Okiru, Satori, Masuta и PureMasuta.

Мутации Mirai начали появляться буквально ежедневно, и то, что у них сохранялась способность размножаться и наносить ущерб с помощью тех же методов, что и у оригинала, указывает на хроническое пренебрежение производителей устройств Интернета вещей простейшими методами защиты. Как ни странно, при этом ботнеты, образованные из таких устройств, исследовались слабо, несмотря на опасность того, что все более сложные атаки на их базе потенциально способны подорвать всю инфраструктуру Интернета [7].

Особенность сканирования устройств ботнетом Mirai заключается в словаре логинов и паролей, которые бот использует при попытках подключения к устройству. Так, например, автор оригинального Mirai включил в процесс сканирования относительно небольшой список логинов и паролей для подключения к различным устройствам. Однако в настоящее время зафиксировано значительное расширение этого списка за счет логинов и паролей «по умолчанию» от различных IoT-устройств, что говорит о появлении модификаций данного бота.

Существует также недавно обнаруженный и мощный ботнет, получивший различные прозвища IoTrooper и Reaper, который может взламывать устройства Интернета вещей гораздо быстрее, чем Mirai. Reaper способен нацеливаться на большее количество производителей устройств и имеет гораздо больший контроль над своими ботами [7].

Традиционные стратегии обнаружения DDoS-атак

1) Обнаружение на основе подписи. Существует два распространенных подхода к обнаружению продолжающихся DDoS-атак: на основе сигнатур и на основе аномалий. Обнаружение на основе сигнатур обычно пытается сопоставить доступные данные с известными шаблонами атак. Пример этого можно увидеть в Captcha, которая представляет собой соединение систем с задачей, которую легко решить для человека, но которая превосходит возможности современных компьютерных программ. Этот подход имеет преимущество простоты; при обнаружении новой атаки можно идентифицировать уникальные характеристики ее активности и добавить их в базу данных сигнатур.

Ботнет Mirai, например, представляет отличительные сигнатуры сетевого трафика на этапах сканирования и заражения, что делает его сильным кандидатом для обнаружения на основе сигнатур.

2) Обнаружение аномалий. Обнаружение на основе аномалий идентифицирует атаки, основанные на отклонении от нормы. Типичная реализация этой стратегии заключается в том, что механизм обнаружения изучает нормальное состояние системы, наблюдая за ним в течение длительного периода времени. Когда он обнаруживает необычную активность, он поднимает тревогу. Распространенной стратегией для обнаружения аномалий является статистическое моделирование работы системы, создание математической основы для определения того, что является нормальным, а что нет. Поскольку этот метод не использует узкую сигнатуру для обнаружения атак, он может идентифицировать атаки нулевого дня, замечая странную активность в системе, которую он отслеживает.

К сожалению, обнаружение аномалий тоже не лишено недостатков. Хотя система может столкнуться с очень необычным состоянием, это не обязательно означает, что она находится под атакой.

Системы обнаружения аномалий по своей природе имеют тенденцию к чрезмерному усердию при обозначении активности как атаки, что приводит к тому, что они характеризуются высоким уровнем ложных тревог [3].

Несмотря на то, что полностью искоренить угрозу бот-сетей невозможно, все еще есть способы ограничить воздействие и масштабы этих атак, приняв превентивные меры. Один из них – размещение устройств Интернета вещей в сегментированной сети, защищенной от внешнего трафика. Также крайне важно начать мониторинг систем и инвестировать в разработку процессов обнаружения вторжений, которые будут иметь большое значение для предупреждения пользователя о том, что система взломана.

Помимо сегментации и тестирования сети, не стоит забывать о фундаментальных мерах безопасности, таких как своевременное обновление прошивки и программного обеспечения, а также возможность контролировать, кто может получить доступ к определенному устройству [9].

Основные рекомендации по защите ИТ-инфраструктур в эпоху IoT

Защита от DDoS и других типов кибератак начинается с понимания сложности современных угроз безопасности. Интернет Вещей представил новые проблемы безопасности для обоих предприятий, которые делают связанные гаджеты частью своих ИТ-инфраструктур и компаний, которые управляют всеми видами веб-решений, включая корпоративные веб-сайты, CRM-системы и настраиваемые социальные сетевые решения.

Следуя этим общим, но эффективным, советам, вы сможете значительно снизить риски безопасности, связанные с IoT, и обеспечить безопасность ИТ-инфраструктуры:

• Никогда не забывайте переустанавливать пароли по умолчанию и обновлять прошивку. Использование паролей устройств IoT по умолчанию является основной причиной, по которой произошла атака Mirai. 47% ИТ-отделов добавили новые подключенные гаджеты в свои корпоративные сети, не изменяя пароли, установленные производителями устройств. Если вы перейдете в интерфейс управления и обнаружите, что пароли по умолчанию не могут быть изменены, не стесняйтесь удалять гаджеты из корпоративной сети, а лучше вообще не приобретать такие устройства. То же самое касается обновлений прошивки, которые должны выполняться автоматически или, по крайней мере, требуют небольшого надзора со стороны ИТ-команды.

• Не выставляйте устройства напрямую в Интернет – решения IoT, которые обрабатывают большие объемы данных и, следовательно, требуют высокоскоростной полосы пропускания – например, камеры видеонаблюдения, которые составляют большую часть армии бота Mirai, – всегда должны быть защищены брандмауэром. Кроме того, вы можете использовать сторонний порт и решения сканирования трафика, такие как BullGuard, чтобы определить, публично ли открыт IP-адрес и обнаружить устройства с открытыми портами.

• Работа с надежными поставщиками IoT. Наиболее известные уязвимости устройства IoT, в том числе неправильное использование механизмов аутентификации и авторизации, отсутствие шифрования транспортного уровня и проблемы с исправлением прошивки, обусловлены плохими решениями, принятыми в ходе разработки программного обеспечения IoT. Если вы рассматриваете возможность внедрения стороннего или настраиваемого подключенного решения на рабочем месте, обязательно обратитесь к компаниям с проверенной репутацией в разработке решений IoT.

• Укрепление безопасностью веб-приложений. Плохая новость об атаках, вызванных IoT-атак, заключается в том, что любая компания или физическое лицо, независимо от того, используют ли они решения IoT для деловых целей или нет, могут легко попасть под огонь. Существует несколько способов защиты ваших веб-приложений от бот-сетей IoT. Во-первых, вы можете реализовать решение VPN для маскировки своего веб-трафика. Во-вторых, используйте безопасные готовые плагины CMS и другие программные компоненты с открытым исходным кодом без документированных уязвимостей безопасности. И, наконец, вы никогда не должны идти на компромисс по обеспечению качества [10].

• Отключайте функции, которые не будут использоваться.

• Отслеживайте журнал работы. Например, что делал регулятор тепла, пока вас не было дома.

• Используйте специально разработанные для умного дома антивирусные программы, которые защитят ваши устройства от атак ботнетов.

• Если вы используете управление через голосовые команды, то пробуйте иногда менять фразы для их активации.

• Отключите протокол UPnP (Universal Plug & Play). UPnP находит схожие устройства и подключается к ним. Однако такой протокол вредоносное ПО также может взламывать ввиду наличия уязвимостей. То есть если предмет умного дома соединен с другим предметами, то они также будут заражены.

Выводы

С распространением технологии Интернета вещей компьютерные сети быстро увеличиваются в размерах. Хотя устройства Интернета вещей приносят пользу во многих аспектах жизни, они также создают риски безопасности в виде уязвимостей, которые дают хакерам миллиарды новых целей. Именно поэтому необходима защита устройств Интернета вещей не только со стороны разработчиков программного обеспечения, но и, главным образом, со стороны пользователей. Следуя общим, но эффективным правилам, пользователи могут значительно снизить риски безопасности, связанные с IoT, и обеспечить безопасность как отдельных устройств, так и всей ИТ-инфраструктуры.

Список литературы:

1. Баженов А.С. Обзор DDoS атак на IoT устройства // Наука настоящего и будущего. 2019. Т. 1. С. 122-125.

2. Горев А.В. Интеллектуальный анализ DDoS-атак ботнета на IoT устройства при помощи Sap Analytics Cloud // Безопасность информационного пространства. Сборник трудов XIX Всероссийской научно-практической конференции студентов, аспирантов и молодых ученых. Екатеринбург, 2021. С. 10-14.

3. Оралбаев Е.А. Обнаружения DDoS-атак ботнетов в сетях доступа IoT // Актуальные вопросы современной науки и образования. Монография. Пенза, 2021. С. 190-200.

4. Савченко Е.В., Ниссенбаум О.В. Ботнет-атаки на устройства интернета вещей // Математическое и информационное моделирование. сборник научных трудов, электронный ресурс. Тюмень, 2018. С. 347-356.

5. Тавасиев Д.А., Команов П.А., Ревазов Х.Ю., Семиков В.С. Анализ методов выявления уязвимостей во встроенном программном обеспечении IoT устройств // Международный научно-исследовательский журнал. 2020. № 1-1 (91). С. 34-37.

6. Díaz J. Internet of Things and Distributed Denial of Service as Risk Factors in Information Security: [Электронный ресурс]. URL: https://www.intechopen.com/chapters/73910. (Дата обращения: 25.10.2021).

7. What is the Mirai botnet?: [Электронный ресурс] // Cloudaflare. URL: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/. (Дата обращения: 20.11.2021).

8. DDoS-атаки и как от них защищаться. Систематизация мирового и российского опыта: [Электронный ресурс] // Nag. URL: https://nag.ru/material/16862. (Дата обращения: 10.11.2021).

9. IoT Botnets and DDoS Attacks: Architecting Against Disaster: [Электронный ресурс] // IoT for all. URL: https://www.iotforall.com/iot-botnets-ddos-attack-architecture. (Дата обращения: 15.11.2021).

10. Взгляд внутрь инициированных IoT DDoS-атак и защита ИТ-инфраструктур: [Электронный ресурс] // SecurityLab. URL: https://www.securitylab.ru/blog/personal/bezmaly/344271.php. (Дата обращения: 11.11.2021).