МЕТОДЫ АКТИВНОЙ И ПАССИВНОЙ ЗАЩИТЫ ОТ АТАК ТИПА BADUSB НА ОСНОВЕ ЭМУЛЯЦИИ HID-УСТРОЙСТВ

Погирейчик В.В., студент гр.361402

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Мокеров В.С. – ассистент каф. ЗИ

Аннотация. Статья посвящена исследованию методов активной и пассивной защиты от атак типа BadUSB, основанных на эмуляции HID-устройств. Анализируются достоинства и недостатки существующих подходов к обнаружению подмены класса USB-устройства. Рассматриваются пассивные методы, включающие анализ дескрипторов устройств и мониторинг событий ввода, а также активные меры, такие как блокировка системных интерпретаторов, фильтрация HID-отчётов и ограничение доступа для неподтверждённых устройств. Обосновывается эффективность гибридной модели защиты, не требующей использования специализированного оборудования.

Ключевые слова. кибербезопасность, BadUSB, USB-устройство, USB, атака, программное обеспечение, защита, пользователь.

В мире кибербезопасности существует множество угроз, и некоторые из них используют маскировку под безобидные устройства. Одной из таких угроз является BadUSB – атака, при которой вредоносное программное обеспечение загружается на USB-устройство, заставляя его вести себя как другое, более опасное устройство. Чаще всего это эмуляция клавиатуры (HID – Human Interface Device), которая может выполнять команды, вводить текст или даже запускать вредоносные скрипты без ведома пользователя.

Суть атаки BadUSB заключается в том, что злоумышленник перезаписывает прошивку USB-контроллера устройства. Это означает, что устройство перестает быть просто «флешкой» или «мышкой» и может имитировать любое другое HID-устройство. Наиболее распространенные сценарии включают:

Эмуляция клавиатуры, при котором устройство может "печатать" команды, которые запускают вредоносные программы, скачивают файлы, изменяют настройки системы или даже удаляют данные. Это происходит настолько быстро, что пользователь может даже не заметить, что что-то происходит.

Эмуляция сетевой карты, при котором устройство может создавать виртуальную сетевую карту, через которую злоумышленник может перехватывать трафик или получать доступ к сети.

Эмуляция USB-модема, при котором устройство позволяет злоумышленнику получить доступ к интернету через зараженное устройство.

Главная опасность BadUSB заключается в его невидимости. Антивирусное программное обеспечение часто не может обнаружить вредоносную прошивку, так как она находится на аппаратном уровне, а не в файловой системе.

Защита от BadUSB требует комплексного подхода, сочетающего пассивные и активные меры.

Пассивная защита направлена на минимизацию вероятности заражения устройства BadUSB. Одним из методов является ограничение использования неизвестных USB-устройств. Политика «не подключать ничего, кроме доверенных устройств» – это самый простой, но эффективный метод. USB-порты могут быть физически заблокированы или отключены на уровне BIOS. Создание списка разрешённых USB-устройств позволяет блокировать любое устройство, не входящее в данный перечень. Использование специализированного оборудования включает применение USB-data-блокеров, которые физически блокируют передачу данных через USB-порт, допуская только зарядку подключённых устройств. USB-фильтры – это некоторые аппаратные решения могут фильтровать USB-трафик, блокируя подозрительные команды или типы устройств. Регулярное обновление прошивок и программного обеспечения является необходимым условием защиты, для чего важно поддерживать в актуальном состоянии операционную систему и драйверы. Это требуется для обнаружения и нейтрализации некоторых видов вредоносного ПО, которое может быть установлено после успешной эмуляции HID [1].

В основе подхода минимизация поверхности атаки через блокировку системных интерпретаторов, в основании которого лежит принцип минимизации привилегий и ограничения доступа к критическим системным интерпретаторам.

Поскольку атаки на базе эмуляции HID-устройств опираются на автоматизированный ввод последовательности символов для вызова командных оболочек, блокировка исполняемых файлов powershell.exe и cmd.exe через системный реестр или групповые политики нивелирует вектор атаки. При подключении вредоносного устройства и попытке инициализации командного сценария операционная система блокирует запуск целевого процесса, руководствуясь установленными правилами ограничения программного обеспечения. Таким образом, даже при успешной эмуляции клавиатуры и воспроизведении полезной нагрузки, выполнение деструктивного кода становится

невозможным из-за отсутствия доступного интерпретатора в пользовательской сессии, что представлено на рисунке 1. Данный метод демонстрирует эффективность превентивных мер, направленных на сужение поверхности атаки без использования специализированных аппаратных средств защиты.

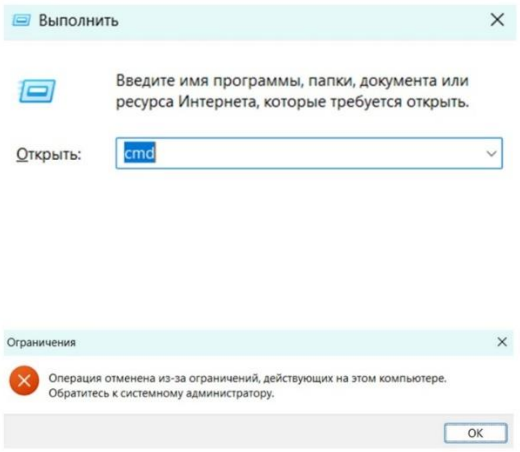

Рисунок 1 – Результат блокировки интерпретаторов

Активная защита – это обнаружение и реагирование на вредоносные воздействия. Активная защита направлена на выявление и нейтрализацию уже активных атак BadUSB. Мониторинг поведения USB-устройств – это анализ HID-событий. Системы мониторинга могут отслеживать события, генерируемые HID-устройствами [2].

Специализированное программное обеспечение может анализировать последовательность и тип генерируемых HID-событий, сравнивая их с типичным поведением доверенных устройств. Для обнаружения аномалий нужны системы обнаружения вторжений и системы управления информацией и событиями безопасности, которые могут быть настроены на выявление аномального поведения USB-устройств. Использование специализированного программного обеспечения для обнаружения BadUSB. Это сканирование прошивки USB-контроллеров. Существуют инструменты, которые пытаются обнаружить модифицированную прошивку на USB-контроллерах. Эмуляция «ловушек» – это создание виртуальных USB-устройств или портов, которые при подключении к ним подозрительного устройства будут генерировать предупреждения, не позволяя выявить атакующего, не подвергая реальные системы риску. Контроль целостности прошивки – это цифровые подписи прошивок. USB-устройства должны иметь прошивки с цифровыми подписями от доверенных производителей. Системы могут проверять эти подписи перед разрешением устройству работать в полном режиме. Однако, это требует поддержки со стороны производителей и не является широко распространенной практикой для всех типов USB-устройств. [3].

Важные серверы и рабочие станции должны быть максимально изолированы от внешних USB-устройств. Разделение сети на более мелкие сегменты может ограничить распространение вредоносного ПО, если атака BadUSB все же произойдет.

Атаки BadUSB представляют собой серьезную угрозу, поскольку они используют доверие к обычным устройствам и действуют на аппаратном уровне, что затрудняет их обнаружение. Комплексный подход, сочетающий пассивные меры предотвращения и активные методы обнаружения и реагирования, является ключом к эффективной защите. Внедрение строгих политик использования USB-устройств, использование специализированного оборудования и программного обеспечения, а также постоянное обучение пользователей помогут минимизировать риски и обеспечить безопасность цифровой среды от этой невидимой угрозы.

Список использованных источников:

1. Полежаев П.Н., Малахов А.К., Сагитов А.М. «Ахиллесова пята» USB-устройств: атака и защита // Философские проблемы информационных технологий и киберпространства. 2015. № 1(9). С. 106–117.

2. Агуров П.В. Интерфейс USB. Практика использования и программирования. СПб. : БХВ-Петербург, 2004. 576 с.

3. Петин В.А. Проекты с использованием контроллера Arduino. СПб. : БХВПетербург, 2015. 448 с.