УДК 004.056

СПОСОБЫ ПРОТИВОДЕЙСТВИЯ АТАКАМ ТИПА BADUSB

А.А. Лебедев
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. В последнее время число подключаемых в компьютер устройств возросло. Вместе с ними возрос риск, что в одном из USB устройств будет вшит вредоносный код. Атака BadUSB представляет собой серьезную угрозу для информационной безопасности. Данный тип атаки может быть использован как для кражи, так и для уничтожения информации и получения неавторизованного доступа к системе. BadUSB часто используется теми, кто уже имеет физический доступ к системе, однако нередко это происходит и по неосторожности самих сотрудников компании. В этой статье приведены угрозы что может представлять атака BadUSB, концепция данной атаки, а также возможные защитные решения.
Ключевые слова: BadUSB; уязвимость; манипуляция, микроконтроллер, Arduino.

METHODS TO COUNTER BADUSB ATTACKS

A.A. Lebedev
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. Recently, the number of devices connected to a computer has increased. Along with them, the risk has increased that malicious code will be embedded in one of the USB devices. The BadUSB attack poses a serious threat to information security. This type of attack can be used to steal or destroy information and gain unauthorized access to the system. BadUSB is often used by those who already have physical access to the system, but this often happens due to the negligence of the company's employees themselves. This article describes the threats that a BadUSB attack can pose, the concept of this attack, as well as possible defensive solutions.
Keywords: BadUSB; vulnerability; data theft; manipulation, microcontroller, Arduino.

Введение

BadUSB – это обобщенное название класса атак, основанных на эксплуатации уязвимостей USB-протоколов и архитектуры USB-устройств [1]. Атака связана с изменением прошивки устройства таким образом, чтобы оно имитировало другое устройство (например, клавиатуру), выполняло вредоносные команды или вмешивалось в работу компьютера (рис. 1). Успех атаки достигается путем скрытного проникновения на объект, атаки на внимательность жертвы либо ее отвлечения. С развитием технологий и увеличением числа подключаемых периферийных устройств эта угроза становится все более актуальной.

Основная часть

Основная проблема BadUSB заключается в том, что большинство современных операционных систем доверяют устройствам, подключаемым через USB-порт, предоставляя им высокий уровень привилегий. Отсюда следуют риски:

1. Потеря контроля над системой. После подключения BadUSB злоумышленник может удаленно управлять компьютером, запускать произвольные программы, изменять настройки системы или устанавливать вредоносное ПО.

2. Кража данных. Устройство может перехватывать нажатия клавиш, пароли, файлы или другие конфиденциальные данные, передавая их на сервер атакующего.

3. Распространение инфекции. При наличии NAND памяти, зараженное BadUSB-устройство способно распространять вредоносное ПО на другие компьютеры и сети, превращаясь в вектор распространения угроз.

4. Скрытность. Традиционные антивирусы не способны выявить такие устройства, поскольку они действуют на уровне аппаратного взаимодействия между устройством и операционной системой.

На практике, подготовить USB устройство для реализации атаки такого типа (рис. 1) довольно легко.

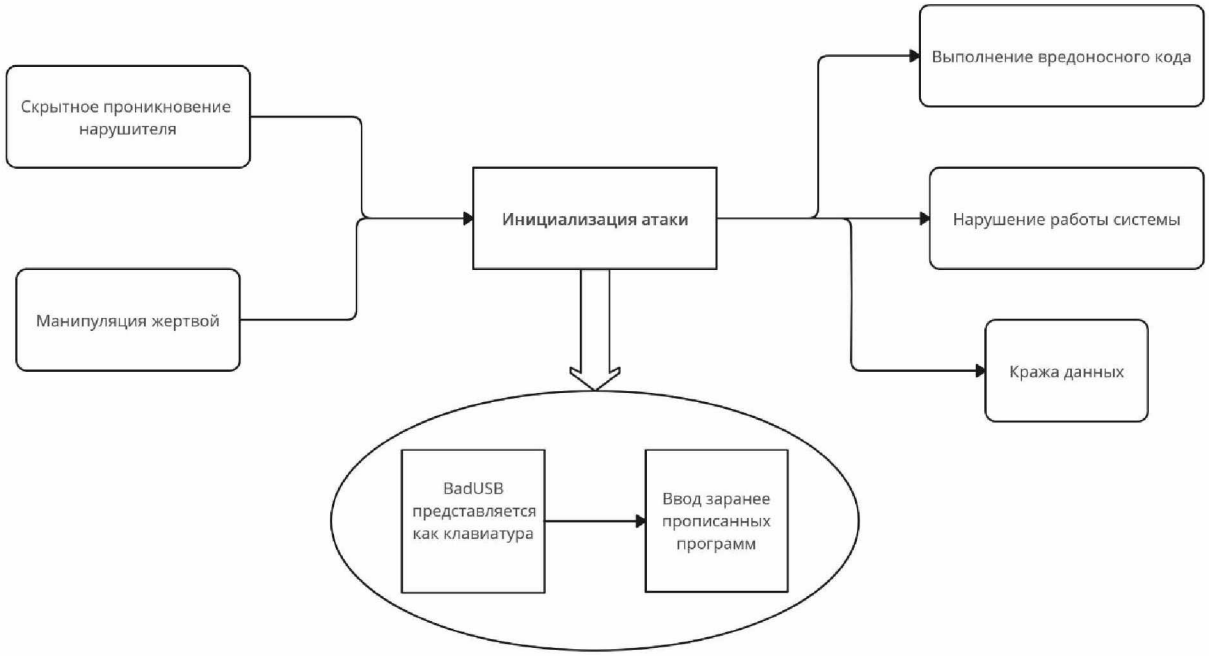

Рис. 1. Принцип атаки BadUSB
Fig. 1. The principle of the BadUSB attack

Все, что потребуется, это плата с микропроцессором (например, Arduino Leonardo в корпусе, замаскированным под USB носитель), среда для прошивки микроконтроллера (Arduino IDE), знание языка программирования данной среды, командной строки/powershell на целевой машине, и базовое понимание работы операционных систем, исполняемых ими файлов и системных процессов. Ввиду доступности всех вышеизложенных компонентов в сети Интернет, сделать себе подобное устройство сможет немало людей. Это пример простой атаки, однако даже такой подход сможет причинить большой вред системе, если команды, которые будет воспроизводить микроконтроллер, будут составлены грамотно.

Однако для защиты от такого типа атаки есть решение, представленное на рис.2. Суть заключается в запуске фонового процесса, который, в момент обнаружения подключения нового USB устройства, запускает сканер аномальной активности. В программе прописаны сценарии, что чаще всего выполняются при подключении BadUSb, такие как нажатие комбинации клавиш Win+R, ввод строки «cmd», и другие. При обнаружении демаскирующих признаков, программа сбрасывает фокус с активного окна, чтобы не дать дописать опасную команду, и, по возможности, извлекает это устройство. А поскольку данный тип BadUSB фактически имитирует клавиатуру, то работает, как и клавиатура, только в активном окне.

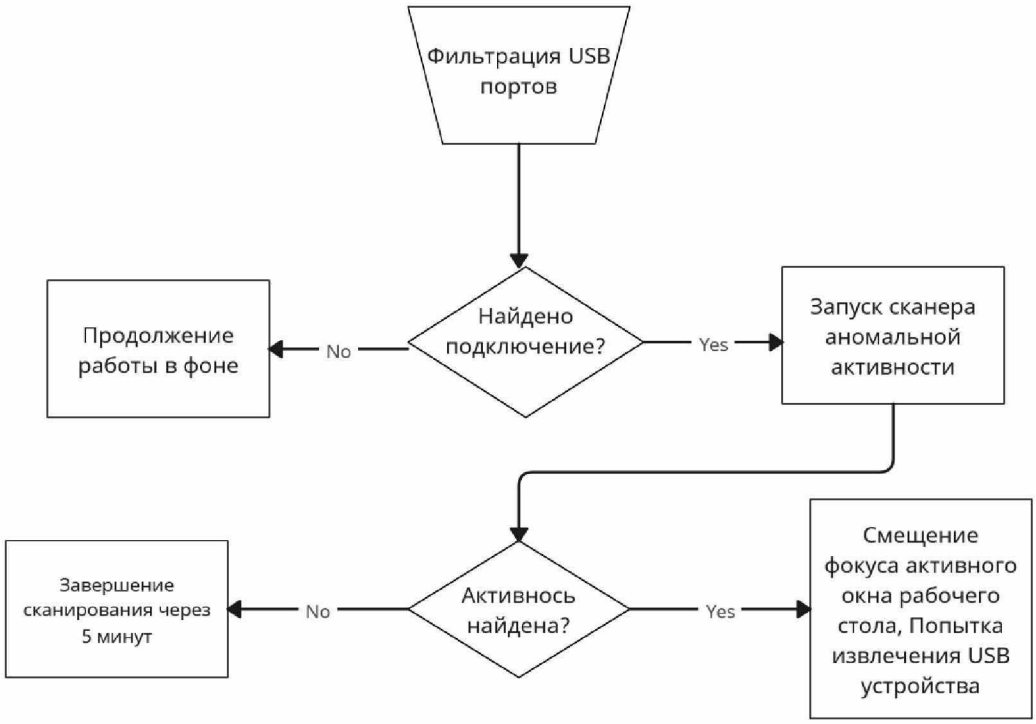

Рис. 2. Логическая схема работы защитного ПО
Fig. 2. The logical scheme of the security software operation

Таким образом, даже простое подключение зараженного USB-накопителя может привести к серьезным последствиям для безопасности информационной системы. Для минимизации рисков успешных атак BadUSB других типов, таких как, например, перепрошитые сетевые карты, можно также использовать и другие решения:

1. Контроль доступа к портам USB. Один из способов – ограничить возможность подключения неизвестных устройств через USB-порты. Это можно сделать на уровне BIOS/UEFI или с помощью специализированных программных решений, которые требуют подтверждения подключения от пользователя.

2. Фильтрация типов устройств. Современные операционные системы могут фильтровать типы подключаемых устройств, блокируя доступ таким потенциально опасным категориям, как клавиатуры или сетевые карты.

3. Мониторинг активности. Специализированные программы могут отслеживать аномальную активность USB-устройств, выявляя попытки эмуляции клавиатурных команд или несанкционированного доступа к сети.

4. Аппаратные решения. Разработка USB-концентраторов с функцией проверки подлинности устройств и предоставления им доступа к системе также является перспективным направлением. Такие концентраторы могут проверять цифровые подписи или идентификаторы устройств, обеспечивая дополнительный уровень защиты [2].

5. Ограничение прав на выполнение команд. Ограничение прав пользователя на компьютере минимизирует ущерб, который может нанести BadUSB, так как немало атак требуют повышенных привилегий. Даже если устройство успешно инициализировано в системе, ограничение прав может предотвратить выполнение критически важных действий, что актуально для Unix-систем.