УДК 004.056

СРЕДСТВО ПРОГРАММНОЙ ЗАЩИТЫ ОТ HID-АТАК BADUSB

А.А. Лебедев
УО «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. Рассматривается проблема атак через USB-устройства, эмулирующие клавиатуру, которые не детектируются традиционными антивирусными средствами. Разработан метод активной защиты, основанный на анализе поведения подключаемых устройств в реальном времени. Описана архитектура программного решения, включающая три этапа: мгновенное обнаружение, поведенческий анализ и интеллектуальную блокировку. Приведены результаты экспериментальной проверки эффективности метода.
Ключевые слова: BadUSB; уязвимость; манипуляция; защита информации; поведенческий анализ; USB-устройства; активная блокировка.

SOFTWARE PROTECTION AGAINST BADUSB HID-ATTACKS

A.A. Lebedev
Belarusian state university of informatics and radioelectronics Minsk, Republic of Belarus

Abstract. The problem of attacks via USB devices that emulate a keyboard, which are not detected by traditional antivirus tools, is being considered. A method of active protection based on the analysis of the behavior of connected devices in real time has been developed. The architecture of the software solution is described, which includes three stages: instant detection, behavioral analysis and intelligent blocking. The results of an experimental verification of the effectiveness of the method are presented.
Keywords: BadUSB; vulnerability; data; manimulation; information protection; behavioral analysis; USB devices; active blocking.

Введение

Рост числа кибератак с использованием специализированных USB-устройств, эмулирующих клавиатуру (BadUSB), представляет серьезную угрозу для информационных систем. Устройства, стоимостью от 50 рублей, подключаются к компьютеру и в течение нескольких секунд

выполняют предопределенный скрипт, который может включать кражу паролей, установку вредоносного ПО, модификацию системных настроек или вывод системы из строя. Традиционные антивирусы бессильны против подобных атак, поскольку устройство идентифицируется операционной системой как легитимная клавиатура, а вредоносные действия выполняются на уровне ввода. Существующие методы защиты (ограничение USB-портов, фильтрация типов устройств, аппаратные USB-концентраторы) либо снижают функциональность системы, либо не обеспечивают достаточного уровня защиты от атак, начинающихся сразу после подключения. В данной работе предлагается метод активной защиты, основанный на анализе поведения устройства в реальном времени. Разработанное программное решение USB-Shield позволяет детектировать вредоносную активность на ранней стадии и мгновенно блокировать подозрительное устройство.

Основная часть

BadUSB-устройства (например, Arduino Leonardo, Rubber Ducky) подключаются к USB-порту и эмулируют клавиатуру. Операционная система автоматически инициализирует драйвер HID-клавиатуры, после чего устройство начинает ввод предварительно запрограммированных команд со скоростью, достигающей 1000 символов в секунду. Типичный сценарий атаки занимает 3–5 секунд и может включать: открытие командной строки, загрузку и выполнение вредоносного скрипта, извлечение сохраненных паролей, создание скрытых учетных записей.

Разработанный метод базируется на анализе поведения подключаемого устройства на трех уровнях: физическом, поведенческом и операционном. Реализация выполнена на языке C++ с использованием Windows API, что обеспечивает минимальное потребление ресурсов и высокую скорость реакции.

Этап 1 - Мгновенное обнаружение. Система постоянно мониторит подключение новых USB-устройств. Обнаружение нового устройства инициирует защитный протокол. Время реакции на этом этапе составляет менее 200 мс.

Этап 2 - Поведенческий анализ. После обнаружения устройства запускается анализатор, который проверяет идентификатор устройства на соответствие списку известных вредоносных (например, VID/PID Arduino). После этого измеряет скорость ввода (при превышении определенного количества символов в секунду устройство считается подозрительным). Одновременно с этим распознает последовательности команд, характерные для вредоносных скриптов (более 50 паттернов, включая запуск командных оболочек, изменение реестра, сетевые команды и др.)

Для повышения точности анализа используются как заводские, так и настраиваемые пользователем паттерны через файл конфигурации.

Этап 3 - Блокировка. При выявлении признаков вредоносной активности выполняются следующие действия. Экстренный сброс фокуса ввода на рабочий стол для предотвращения дальнейшего ввода. Блокировка дальнейшего ввода с устройства с помощью низкоуровневого хука клавиатуры. Отключение устройства и удаление его из системы через системные API. Ведение детального журнала событий.

Экспериментальная проверка. Эффективность метода оценивалась на тестовой системе с использованием Arduino Leonardo, настроенного на выполнение типового вредоносного скрипта (открытие командной строки, кража пароля от wifi сети, копирование файлов). Проведено 10 запусков атаки на компьютере под управлением Windows 10 с установленным USB-Shield. Результаты:

Время реакции: в среднем 280 мс (от подключения до блокировки устройства). Эффективность блокировки: 9 из 10 атак были прерваны до выполнения вредоносных команд. Один пропуск связан с особенностью работы драйверов HID при очень высокой скорости ввода, что потребовало дополнительной оптимизации. Ложные срабатывания: зафиксировано 0 ложных срабатываний при использовании легитимных клавиатур, мышей и флеш-накопителей. Для сравнения, те же атаки против стандартных антивирусов прошли успешно в 100 % случаев, поскольку антивирус не обнаружил вредоносных файлов.

Заключение

В работе предложен метод активной защиты от атак BadUSB, основанный на поведенческом анализе. Реализованное программное решение продемонстрировало высокую эффективность в условиях реальных атак, при этом не оказывая заметного влияния на производительность системы. Дальнейшее развитие планируется в направлении расширения базы поведенческих паттернов, интеграции с корпоративными системами управления и поддержки других классов USB-устройств (например, эмуляция сетевых карт).

Сведения об авторе

Лебедев А. А., студент факультета информационной безопасности, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», alexandercorp77@gmail.com.

Information about the author

Lebedev A. A., student, faculty of information security, Educational Institution "Belarusian State University of Informatics and Radioelectronics", alexandercorp77@gmail.com.