УДК 004.491
DOI: 10.17726/phillT.2015.9.1.4.491

«АХИЛЛЕСОВА ПЯТА» USB-УСТРОЙСТВ: АТАКА И ЗАЩИТА

Полежаев Петр Николаевич,
преподаватель кафедры компьютерной безопасности и математического обеспечения информационных систем, ФГБОУ ВПО «Оренбургский государственный университет», Оренбург, Россия
newblackpit@mail.ru

Малахов Александр Константинович,
студент, ФГБОУ ВПО «Оренбургский государственный университет», Оренбург, Россия
msan93@mail.ru

Сагитов Артур Маратович,
студент, ФГБОУ ВПО «Оренбургский государственный университет», Оренбург, Россия
sagitov.artur@mail.ru

Аннотация. Статья посвящена уязвимости, которую можно встретить в аппаратно-программных устройствах с интерфейсом USB. Сегодня практически любая компьютерная периферия, включающая в себя устройства хранения информации, начиная от флеш-накопителей и заканчивая сложнейшими медицинскими устройствами, подключается через интерфейс USB, также огромное количество разнообразных устройств используют USB-коннектор для подзарядки встроенных аккумуляторов. В настоящее время универсальность USB-интерфейса является причиной уязвимости компьютеров и устройств, которые его поддерживают. В статье описывается современное использование USB-интерфейса, метод, с помощью которого компьютер различает тип устройства и его предназначение. Выявляются распространенные модели контроллеров среди USB-носителей, подверженных уязвимости. Описываются некоторые виды атак с использованием данной уязвимости с помощью инфекции BadUSB. Приводится способ создания инфицированного USB-устройства. В статье также предлагаются варианты защиты устройств: программные и аппаратные способы защиты от инфекции. Начиная с

простых программ, таких как “USB Security”, заканчивая средствами комплексной защиты информации, такими как “Secret Net”, “Страж NT”, “Dallas Lock”. В плане аппаратной защиты рассмотрено устройство для отключения шины данных или полного отключения USB-порта. Также описаны альтернативные носители данных – зашифрованные и защищенные USB-накопители, в которых встроено аппаратное шифрование.

Ключевые слова: BadUSB, защита USB-устройств, уязвимость USB-устройств, изолированная среда, контроллеры USB.

«THE ACHILLES HEEL» OF USB-DEVICES: ATTACK AND DEFENSE

Polezhaev Petr N.,

Professor, Federal State Educational Government-financed Institution of Higher Professional Education “Orenburg State University”, Orenburg, Russia
newblackpit@mail.ru

Malakhov Aleksandr K.,

student, Federal State Educational Government-financed Institution of Higher Professional Education “Orenburg State University”, Orenburg, Russia
msan93@mail.ru

Sagitov Artur M.,

student, Federal State Educational Government-financed Institution of Higher Professional Education “Orenburg State University”, Orenburg, Russia
sagitov.artur@mail.ru

Abstract. The article is devoted to vulnerability, which can be found in hardware and software devices with USB interface. Today, almost any computer peripherals including storage devices, ranging from flash storage device and ending with the most complex medical devices, is connected via USB, also a huge variety of devices use USB connector to charge the internal battery. Currently, the versatility of the USB interface is the vulnerability of the computers and devices that support it. The article describes the current use of the USB interface, the method by which the computer recognizes the device type and its purpose. Common models of vulnerable controllers among USB

storage devices are identified. Some of the attack types using this vulnerability and BadUSB infections are described. The way to create an infected USB device is provided. Paper also offers security options for devices: hardware and software means of protection from infection, starting with simple programs, such as “USB Security” and finishing with software for complex security, such as «Secret Net», «Guardian NT», «Dallas Lock». We also describe hardware protection with a device, which disables the data bus or disconnects USB. In addition, we also consider alternative storage media - encrypted and secure USB flash drives.

Keywords: BadUSB, USB device security, USB device vulnerability, isolated environment, USB controllers;

Программа или «железо»? При работе над тем или иным проектом мы вряд ли задумываемся над этим вопросом. А ведь ответив на него, можно обезопасить себя, свою разработку, улучшить за счет особенностей реализации. Многие работают с виртуальными машинами на своем компьютере. С помощью специальных программ можно виртуально установить операционную систему на компьютер и работать с полноценной операционной системой (ОС). К какому виду реализации можно ее отнести? Или, например, USB-накопитель. Все пользуются флеш-памятью, но кто задумывался о реализации? На самом деле тут мы сталкиваемся с аппаратно-программной реализацией. А если есть возможность программной реализации, то есть возможность внедрить в данное устройство вредоносный код.

Первая версия шины USB была представлена еще в 1995 году. Изначально в эту технологию закладывалась гибкость, универсальность, простота и удобство использования. Чтобы добиться всего этого, были использованы классы спецификации, которые определяют тип и функциональность нового устройства. В составе ОС находятся драйверы классов, каждый из которых позволяет функционировать соответствующему классу устройств. Таким образом, любое USB-устройство, при наличии USB-разъема, может взаимодействовать с компьютером. С одной стороны, это удобно для пользователей: нет необходимости искать, устанавливать самому драйвера на каждое USB-устройство, будь это клавиатура, мышь или флеш-накопитель. С другой стороны, это ахиллесова пята USB, потому что одни и те же разъемы могут

работать с разными классами устройств, а программно изменив этот класс, можно выдать одно устройство за другое, и ОС ничего не заподозрит. Причем данную операцию владелец устройства, скорее всего, не заметит и также ничего не заподозрит. Необходимо всего лишь перепрограммировать прошивку контроллера USB-устройства, изменив класс спецификации. После этого оно будет выдавать себя за другое устройство [1].

Проблема распознавания «опасного» или вредоносного USB-устройства очень актуальна. Сейчас, взяв флеш-накопитель в руки, нельзя утверждать точно, является ли он опасным или же подверженным угрозе BadUSB. Но рассматривать только флеш-накопители в рамках данной уязвимости – основная ошибка. Любое устройство подвержено угрозе BadUSB, начиная от клавиатуры, заканчивая смартфонами с установленной ОС Android.

Яркий тому пример приведен в 2010 году канадскими компьютерными инженерами. Они сделали USB-клавиатуру с микросхемой, которая копирует файлы, находящиеся на жестком диске, и передает информацию азбукой Морзе встроенным светодиодом. Способ передачи был выбран ради эксперимента, возможно передавать файлы на прописанный злоумышленниками узел.

Опасность угрозы BadUSB высока, потому что все основные чипы контроллеров USB не обладают никакой собственной защитой от их перепрограммирования. По факту основная защита – отсутствие информации в технической литературе и общей документации. Перед нами образец известного принципа «безопасность через неясность» [2].

Каждое USB-устройство имеет свой уникальный идентификатор – VID и PID. VID (vendor identificator) [3] – идентификатор производителя, PID (product identificator) – идентификатор устройства. Они состоят из четырехзначного шестнадцатеричного числа. По их значениям можно определить тип контроллера в USB-накопителе и его производителя, но не всегда это помогает, так как производитель может их указать по своему усмотрению. Для определения типа контроллера и флеш-памяти можно воспользоваться различными утилитами. Наиболее удобной и точной является программа ChipEasy. Она опрашивает контроллер USB-накопителя и получает следующую информацию: идентификатор производителя, идентификатор устройства, серийный номер устройства, производитель флешки и модель, максимальное

потребление тока устройством, файловая система, производитель контроллера устройства, модель контроллера, установленного в USB-устройстве, производитель микросхемы памяти, тип памяти и многое другое. Это позволяет выяснить контроллер, в отличие от технологии «угадывания» модели контроллера по VID\PID [4]. Данная технология была применима до середины 2000-х годов, когда существовало небольшое количество контроллеров и производителей накопителей. Очень часто для прошивки всех контроллеров подходила одна и та же утилита. Сейчас же данный метод устарел, потому что зачастую производители присваивают «не родные» идентификаторы для контроллера. Или для работоспособности утилиты нужно учитывать тип флеш-памяти. Да и немногочисленные базы, в которых хранится информация о контроллерах, могут содержать неверные сведения, благодаря которым можно ошибиться при выборе утилиты.

Любое взаимодействие USB-устройства с компьютером осуществляется с помощью микроконтроллера. Для того чтобы он мог осуществить операции, в его собственной служебной памяти хранится управляющий код. Простой доступ к данной памяти пользователь с помощью каких-либо программных продуктов не имеет, более того, некоторым моделям контроллеров необходимо использование аппаратного программатора. В связи с распространенностью технологии USB многие производители для упрощения выполняют операцию перепрограммирования напрямую через интерфейс. Обычная прошивка – это закрытый код, поэтому принято считать, что его изменение доступно только разработчику. Однако каждое устройство USB включает в себя чип контроллера или, иными словами, собственный управляющий микрокомпьютер, который легко можно перепрограммировать с помощью небольшого физического и программного воздействия. В связи с тем, что оригинальная прошивка чипа занимает меньший объем, чем доступный размер памяти для ее хранения, изменение микрокода прошивки не составит труда.

Компании SRLabs, специализирующейся на исследовании уязвимости информационных систем, аппаратных продуктов, удалось выявить уязвимые контроллеры для таких устройств, как адаптеры SATA, устройства ввода-вывода, веб-камеры, устройства для чтения карт памяти SD Card, USB-разветвители и флеш-накопители. Полный список всех уязвимых устройств до-

статочно большой [5], отметим выявленные уязвимые контроллеры для USB-носителей:

1. ALCOR AU698X.
2. SMI SM325X/SM326X.
3. Skymedi SK62XX SK66XX.
4. Solid State System SSS6677, SSS6690 and SSS6691.
5. Innostor IS903-A2, IS903-A3.

Но данный список тяжело использовать непосредственно по назначению – ради защиты от угрозы BadUSB. До использования USB-накопителя нельзя утверждать со стопроцентной уверенностью, что на данном устройстве установлен тип контроллера, находящийся в этом списке. Можно найти лишь примерную информацию, составленную самими пользователями флеш-накопителей, на каком устройстве какой контроллер уже встречался. Эта информация позволит с некоторой вероятностью избежать использования уязвимого контроллера, но не гарантирует полную безопасность. Можно, конечно, воспользоваться утилитой для определения типа контроллера, но для этого нужно считать с нее прошивку, следовательно, подвергнуть компьютер угрозе.

Приведем три основных примера использования описанной уязвимости.

1. Подключенное BadUSB-устройство (флеш-накопитель) может выдать себя за клавиатуру и начать отдавать команды от имени пользователя, под которым был выполнен вход в ОС. Если был выполнен вход от имени администратора, устройство получает полный доступ ко всем возможностям ОС. Самый простой вариант команды – установка вредоносного ПО или отправка необходимых файлов злоумышленнику. Также существует опасность заражения всех USB-устройств, подключаемых после, потому что нельзя исключить возможность заражения USB-контроллера, находящегося в компьютере.

2. Зараженное устройство способно эмулировать сетевую карту компьютера. Таким образом, диспетчер устройств обнаружит новое сетевое устройство. С помощью специальной прошивки злодей может осуществить подмену стандартных DNS-адресов и перенаправить весь трафик через свой сервер, получив возможность совершать атаку типа «человек посередине».

3. USB-накопитель, который будет использован для переустановки ОС, может уже быть заражен BadUSB-инфекцией и сра-

зу, при установке, прописать в памяти компьютера вредоносные файлы и заразить «чистую» ОС. Администратор может и не узнать об этом, потому что вредоносные файлы будут находиться уже в самой ОС до установки антивирусной программы.

Помимо этого, можно отметить еще несколько сценариев возможных атак через USB-устройства: сокрытие файлов от ОС и файловых менеджеров вместо удаления, изменение файлов при их записывании на флеш-память устройства, таким образом, данные модифицируются «на лету» и антивирусная программа проверяет «чистый» файл до его изменения, после на флеш-накопителе находится уже зараженный файл, возможна эмуляция дисплея с целью получить доступ к скрытой информации и др.

Поскольку данная угроза выполняется на программно-аппаратной реализации микрокодов, опасность и универсальность угрозы BadUSB высока. Она совместима с ОС всех типов. Защита от этой угрозы осложнена. Стандартные манипуляции с переустановкой операционной системы, которые являются универсальным решением на не выводимое другими вариантами вредоносное ПО, не способны «вылечить» компьютер, зараженный инфекцией BadUSB. Потому что USB-накопитель, с которого происходит установка ОС, может содержать вирус благодаря злоумышленнику. Также на компьютере могут быть установлены встроенные устройства, которые подключаются через внутренний USB-порт, например веб-камера, устройство для чтения карт памяти SD Card. Они также могли быть подвержены инфекции или к компьютеру могли быть подключены другие USB-устройства. При возможности эмулирования клавиатуры и скрытого хранения файлов нельзя исключать угрозу подмены системы BIOS. Таким образом, компьютеры или подключенные USB-устройства, которые были заражены инфекцией BadUSB, невозможно вылечить и вернуть к первоначальному состоянию.

Что же необходимо осуществить для этого? Как оказалось, ничего трудного нет, кроме одного момента: получение исходников оригинальной прошивки. Благодаря этому угроза BadUSB не набрала такой популярности, как многие вирусы USB-накопителей. Например, вирус в автозапуске или вирус, скрывающий все данные на устройстве, отображая похожие файлы-вирусы, которые запускал ничего не подозревающий пользователь. Однако это всего лишь вопрос времени…

Чтобы превратить «чистый» флеш-накопитель в BadUSB [6], нужно изменить стандартную прошивку микроконтроллера. Необходимо найти исходники оригинальной прошивки или с помощью реверс-инжиниринга получить исходный код. Затем определиться с типом атаки и написать исполняемый код, это может быть реализовано с помощью Java-скриптов. Далее этот код внедряется в стандартную прошивку микроконтроллера и «зашивается» в него. В свободном доступе находятся программы, используемые, как правило, для восстановления прошивок распространенных флеш-накопителей. Их можно использовать для записи вредоносной прошивки микроконтроллера, для этого нужно перевести накопитель в boot режим. Информацию по данной операции можно изучить в документации к контроллеру, иногда достаточно запуска командной строки, с помощью которой флеш-накопитель переводится в boot-режим командой:

«Путь к скомпилированному приложению для связи с дисками на контроллере /drive= «Буква накопителя» /action=SetBootMode»

Иногда этого может не хватать или в связи с отсутствием приложения для связи с дисками самым надежным вариантом будет физическое воздействие на контроллер, для этого нужно добраться до контроллера флеш-накопителя, разобрав корпус устройства, и замкнуть конкретные пины. Это позволяет осуществить режим перепрограммирования накопителя. В этом режиме необходимо «залить», с помощью стандартной программы восстановления, новую, измененную, прошивку.

После таких манипуляций в руках у нас флеш-накопитель, который при последующем использовании будет выполнять команды, указанные в прошивке. Антивирусам очень тяжело бороться с таким типом атак, потому что невозможно фильтровать USB-трафик и отличить – может устройство самостоятельно подавать такие команды или же это действие выполняет пользователь. Например, в случае подмены USB-клавиатуры, антивирус не в состоянии отличить настоящую клавиатуру от «поддельной» или понять, какое поведение поддельной клавиатуры является вредоносным.

Небольшие методы защиты все-таки существуют. Они не спасут компьютер от заражения, однако могут обезопасить от некоторых разновидностей данной угрозы. Во многих ОС можно ограничить подключение по USB, оставив только доступ для определенного круга устройств. А можно полностью запретить

использование USB-портов. Запрет устанавливается как встроенными средствами операционной системы, так и с помощью дополнительных программ. Рассмотрим каждый вариант.

Среди встроенных средств самым действенным способом является полное отключение USB-портов. В операционной системе Windows для этого необходимо выполнить: «Пуск => Панель управления => Диспетчер устройств => Корневой USB-концентратор => Отключить».

Существенным недостатком данного метода является тот факт, что любой пользователь, имеющий доступ к правам администратора, может включить порты, подвергнув компьютер возможной опасности. Также можно выключить USB-порты в BIOS. И хотя это самый действенный метод защиты, он не применим в большинстве случаев, потому что тогда необходимо будет подключать устройства ввода-вывода через альтернативные порты, например OS/2. Однако далеко не все компьютеры сегодня имеют данный разъем. А отказаться от использования клавиатуры и «мышки» невозможно.

Существует множество простейших программ для управления доступом к USB-портам. Большинство из них бесплатны, некоторые позволяют устанавливать пароли. К сожалению, эти программы запрещают только указанные устройства, тем самым предоставляя неполноценную защиту. Другая часть программ позволяет блокировать только неразрешенные USB-устройства. В белом списке, как правило, находятся клавиатуры, принтеры и мыши, тем самым оставляя лазейку для атаки. Программы обеспечивают защиту от вирусов, которые пытаются проникнуть на компьютер через USB-накопители, а также восстановление скрытых и спрятанных файлов на USB-носителях в результате последствий вирусного воздействия. Примером таких программ являются “USB Security”, “USB Protection & Recovery”, “Antirun” и другие. Наиболее популярной и удобной утилитой, которая не замедляет работу компьютера, является “USB Security”.

Еще один тип платных программ предоставляет средства защиты информации, осуществляющие комплексную защиту информации пользователя. Пример таких программ – отечественные разработки “Secret Net”, “Страж NT”, “Dallas Lock” [7]. В этих программах есть встроенное управление доступом к USB-устройствам с разграничением на различные категории пользова-

телей. Данный тип программ представляет более полную защиту, чем все остальные рассмотренные методы, за исключением отключения USB-портов в BIOS. Например, Dallas Lock позволяет создать изолированную среду. Изолированной системой в данном контексте назовем систему, у которой ограничено использование USB-портов, таким образом не позволяется добавлять новые устройства или полностью запрещено использование интерфейса, в зависимости от настроек. Однако стоит задуматься о рациональности установки продукта Dallas Lock, если вы хотите пользоваться им ради отключения и блокирования USB-устройств. Стоимость лицензии на один компьютер на год составляет 8 000 рублей (при покупке от одной до девяти лицензий). В данную цену включается сам продукт и техническая поддержка на год. Целесообразно использовать Dallas Lock в корпоративной сети для разграничения прав доступа всех пользователей в ней. Программа может разграничить и разрешить доступ определенной группе пользователей к необходимым устройствам. Принимать решение о покупке данной системы стоит в каждом конкретном случае, в зависимости от сети и поставленных задач.

Самый простой и глобальный способ избежать или, по крайне мере, ослабить атаку через BadUSB – это внедрить цифровую подпись изготовителя в прошивку устройства. При каждом подключении к компьютеру проверялась бы сигнатура и пользователю сообщалось бы о безопасности данного устройства. Опции стандарта USB позволяют осуществить данную защиту, но ее плюсы не могут перекрыть минусы, такие как снижение универсальности технологии, удорожание производства устройств и др.

Альтернативой цифровой подписи можно считать шифрование, уже давно существующее и многими использующееся. В данном случае безопасность устройства осуществляется с помощью аппаратного модуля шифрования/дешифрования с физическим вводом пароля и его хранением непосредственно внутри «железа» флеш-накопителя. Это означает, что компьютеру не потребуется какое-либо специальное программное обеспечение при работе с данным накопителем. Многие производители сейчас выпускают такие накопители, среди известных фирм IronKey, Corsair, IStorage, Silicon Power и другие. Некоторые типы таких USB-устройств позволяют аппаратно запрограммировать набор комбинаций для доступа или сброса всей информации. Обычно используется шифро-

вание данных AES-256. Дабы исключить возможность перебора, после десяти неправильных попыток ввода устройство блокируется и удаляет все данные, находящиеся в памяти. А пыле- и водонепроницаемый корпус и эпоксидная смола, которой покрыта память, исключает возможность физического доступа к устройству, т.к. при попытке добраться до флеш-памяти или шины данных смола приводит ее в негодность. Перечислив все положительные моменты, нельзя не отметить и минусы. Это высокая стоимость продукции фирмы IronKey. Например, на американском Ebay цена на данное USB-устройство с 2ГБ флеш-памяти начинается от $85-100 в сравнении с $4-5 простого USB-накопителя. Среди российских разработок можно уделить внимание USB-накопителю Runtex Samurai. Его стоимость составляет около $180 за 8ГБ памяти. Данный накопитель шифрует данные с помощью AES-1024, однако сильно уступает подобным устройствам фирмы IronKey в плане чтения и записи данных: 0,5 Мб/сек против 27 Мб/сек.

Еще один способ – разделить периферию по раздельным классам на разные разъемы USB-портов, чтобы была возможность использовать, например, для накопителей памяти один порт, который не сможет работать с другими классами USB-устройств.

Как вариант можно рассматривать применение специальной программы-экрана, которая позволит осуществить контроль класса устройств и сравнение на соответствие их функций заявленным.

Если мы рассматриваем подключение какого-либо устройства с целью подачи питания, а не передачи данных, можно использовать специальное устройство USB-кондом. Оно устанавливается между USB-устройством, которое необходимо зарядить, и коннектором компьютера. Смысл заключен в отсечении шины данных. Оставляя только контакты массы и +5V для зарядки, исключается возможность передачи данных и соответственно связи с устройством. Стоимость такого устройства начинается с $5.

Возможно, разработчики антивирусных программ будут добавлять дополнительные модули для расширенного контроля над USB-устройствами. Ограничивать доступ к USB-носителям умеют ESET Endpoint Antivirus, Kaspersky Endpoint Security, Dr.Web и другие современные средства. Однако в случае BadUSB таких мер может оказаться недостаточно.

Одним из способов защиты является также осторожность в использовании устройств. Не подключать непроверенные устрой-

ства, не покупать и не использовать бывшие в употреблении, никогда не оставлять компьютер или мобильное устройство без присмотра в незаблокированном состоянии. Даже покупая новое устройство, нельзя быть полностью уверенным в том, что оно не заражено.

С появлением нового стандарта USB Type-C универсального разъема, с помощью которого осуществляется передача информации и зарядка устройства, у злоумышленника появляется возможность получения доступа к системе энергопотребления устройства, что открывает новые возможности нанесения вреда компьютеру пользователя.

В любом случае, все эти меры безопасности меркнут перед самой главной уязвимостью в безопасности – человеческий фактор. Какие бы меры предосторожности ни были применены, человек всегда может посчитать, что устройство безопасно, и разрешить подключение, тем самым открыв прямую дорогу уязвимости.

Изучив подробнее особенности данной угрозы, стоит задуматься о том, кто уже мог реализовать и использовать ее.

Литература:

1. *Васильков А.* Bad USB – как новая атака реализована в разных устройствах [Электронный ресурс]. Режим доступа: http://www.computerra.ru/108106/bad-usb-on-some-devices. (*Vasylkov A.* Bad USB – as a new attack is implemented in different devices [Electronic resource]. Access mode: http://www.computerra.ru/108106/bad-usb-on-some-devices.)
2. *Киви Б.* Чума на ваши USB [Электронный ресурс]. Режим доступа: http://www.3dnews.ru/825348. (*Kiwi B.* A plague on your USB [Electronic resource]. Access mode: http://www.3dnews.ru/825348.)
3. *Jan Axelson*. USB Mass Storage // Lakeview Research. 2006. P. 277-289.
4. *Агуров П.* Интерфейс USB. Практика использования и программирования. СПб.: БХВ-Петербург, 2006. – 624 с. (*Agurov P.* Interface USB. The practice of using and programming. SPb.: BHV-Petersburg, 2006. – 624 p. – P. 146-150.)
5. BadUSB Exposure [Electronic resource]. Access mode: https://opensource.srlabs.de/projects/badusb.
6. Уязвимость BadUSB на практике [Электронный ресурс]. Режим доступа: https://dmyt.ru/forum/viewtopic.php?t=383. (Vulnerability BadUSB in practice [Electronic resource]. Access mode: https://dmyt.ru/forum/viewtopic.php?t=383.)
7. Средства защиты информации и где деготь [Электронный ресурс]. Режим доступа: http://habrahabr.ru/post/134861. (Protection of information and where the tar [Electronic resource]. Access mode: http://habrahabr.ru/post/134861.)