В статье подробно описаны реально существующие векторы атак на банкоматы российских банков, а также различные уязвимости машин для выдачи наличных денег. Какие конструктивные особенности банкоматов используются для атак того или иного типа? На какие уязвимые места АТМ следует обратить особое внимание банку? Действительно ли атаки типа Black Box больше не актуальны? Где злоумышленник может неожиданно для специалистов по ИБ найти информацию, необходимую ему для совершения атак?

Как злоумышленники используют уязвимости АТМ

Алексей АНТОНОВ,
Digital Security, директор по работе с ключевыми клиентами

Несмотря на то что возможности для хакерских атак на системы ДБО, внутренние системы банков и клиентов все расширяются, атаки на банкоматы до сих пор «пользуются спросом» у злоумышленников. Устройства АТМ «удобны» для них, в частности, тем, что имеют лишь пассивную защиту (системы видео-/аудионаблюдения и средства обеспечения безопасности самих устройств), а современные технические средства и специальные навыки позволяют в некоторых случаях провести атаку за три-четыре минуты.

Итак, поговорим подробнее о том, что злоумышленник может сделать с банкоматом.

Типовые атаки на АТМ

Как известно, банкомат можно разделить на две зоны: сервисную и сейфовую. Сервисная зона содержит все внешние и внутренние устройства для взаимодействия пользователя с банкоматом, а также хост (системный блок). Сейфовая зона соответственно содержит сейфы диспансера и купюроприемника. Все внутренние и периферийные устройства соединены шинами данных с хостом.

В среде информационной безопасности есть такое понятие, как модель нарушителя (злоумышленника). Эта модель описывает атакующего для понимания его возможностей. В случае с банкоматами может быть два типа атакующих:

Алексей АНТОНОВ

— удаленный атакующий — это тот, кто атакует банкоматы программным способом через банк, проводя атаку предварительно на сам банк, а уже потом на банкомат;

— локальный атакующий — это тот, кто имеет физический доступ к банкомату и совершает атаку, находясь около него.

В данной статье мы рассматриваем только локального атакующего.

Для того чтобы получить доступ к денежным средствам, хранящимся внутри АТМ, злоумышленник использует различные уязвимости:

— уязвимости проектирования — это не совсем правильные архитектурные решения, которые позволяют получить доступ к «проводам» внутри банкомата или подключиться напрямую к определенному устройству;

— уязвимости конфигурирования — это в большей степени программные уязвимости, ошибки в прошивке и драйверах устройств;

— уязвимости реализации — это слабости, которые появились в ходе эксплуатации банкомата. Сюда входят некорректно настроенные параметры, принудительно или случайно отключенные компоненты, программы и т.д.

Для того чтобы получить доступ к денежным средствам, хранящимся внутри АТМ, злоумышленник использует различные уязвимости: проектирования, конфигурирования, реализации.

Обычно злоумышленники используют следующие типы атак:

— Black Box — подключение к шине диспенсера с целью отправки на него неавторизованных команд, направленных на вывод наличных средств;

— Deposit Forgery — подделка валюты, номинала и количества купюр, внесенных злоумышленником через купюроприемник, за счет перехвата и модификации сообщений. Эксплуатация возможна в режиме Man in the Middle (MitM) шины данных купюроприемника;

— ATM Malware Jackpotting — атака на хостовую часть банкомата с помощью вредоносного программного обеспечения (ВПО). Данное ВПО может быть использовано как в локальных атаках, так и в дистанционных атаках, то есть со стороны сетевой инфраструктуры банка. Векторами для выполнения атаки при локальном доступе могут быть:

✓ Malformed-устройство — физический или виртуальный поддельный девайс, который эмулирует поведение реального периферийного с целью эксплуатации уязвимостей в ПО (библиотеках или драйверах) производителя;

✓ User Input Emulation — эмуляция пользовательских носителей информации и устройств ввода, например клавиатуры, мыши, CD-привода, флеш-накопителя и т.п., с целью доставки ВПО на хост.

Как злоумышленники используют уязвимости АТМ

При реализации атак злоумышленник учитывает фактор действия определенных средств защиты, в том числе срабатывания сигнализации и приезда наряда полиции. Поэтому ко всем типам атак он предъявляет одно важнейшее требование: они должны быть реализованы не более чем за 4–7 минут. Конечно, время условное, поскольку в практике нередки случаи полного игнорирования охранными организациями факта взлома в течение нескольких часов, благодаря чему злоумышленникам удавалось атаковать сразу несколько расположенных рядом банкоматов.

Конструктивные особенности АТМ

Поскольку мы рассматриваем модель локального злоумышленника, для проведения атаки ему необходимо получить доступ к интересующим его шинам данных или компонентам устройства. Для этого он должен определить так называемые конструктивные особенности банкомата. Иными словами, изучить корпус АТМ и понять, как и где применить средства механического воздействия, которые позволяют провести процедуры сверления, разрезания, выпиливания или выжигания, с целью дальнейшего получения неавторизованного доступа к критическим шинам данных, главным распределительным модулям и узлам банкомата. А в некоторых случаях — получения доступа и к системному блоку.

Такими критическими шинами данных, как было сказано ранее, являются шины от периферийных устройств банкомата до системного блока, шина данных диспенсера, шина данных купюроприемника.

Злоумышленник может получить информацию о конструктивных особенностях либо от доверенного лица из банка (инсайдера), либо купив аналогичную модель банкомата на просторах интернета. Как показывает практика, поскольку лицевая панель банкомата выполнена в основном из пластика, получить доступ к шинам данных не составляет никакого труда.

Например, у банкоматов корпорации NCR самой уязвимой точкой в конструкции является пластиковая рекламная панель — единственная преграда между системным блоком и атакующим. То же можно сказать и о банкоматах Diebold. Банкоматы OKI и вовсе целиком выполнены из пластика, что только облегчает процесс деструктивного воздействия.

Как показывает практика, в среднем удается определить от трех до пяти уникальных мест в конструкции банкомата, на которые злоумышленник может деструктивно воздействовать с целью доступа либо к шинам данных, либо к самому системному блоку (рис. 1).

Алексей АНТОНОВ

Рисунок 1

Уязвимые места банкомата

В зависимости от того, к какому типу шины данных был получен доступ, становится возможной реализация одного или нескольких типов атак.

Далее подробно рассмотрим каждый из типов атак.

Атака методом прямого диспенса (Black Box/Robbery/DrillBox)

Последнее время многие говорят, что атаки типа Black Box уже неактуальны, их невозможно эксплуатировать и т.д. Но, как показывает наша исследовательская практика, такие атаки «живы» и постоянно находятся новые уязвимости, которые позволяют проводить их все новыми и новыми способами.

Тенденцию развития такого типа атак видим не только мы, но и сами производители данных устройств. Это видно из рис. 2: статистика показывает количество зарегистрированных инцидентов (незарегистрированных может быть гораздо больше) атак типа Black Box.

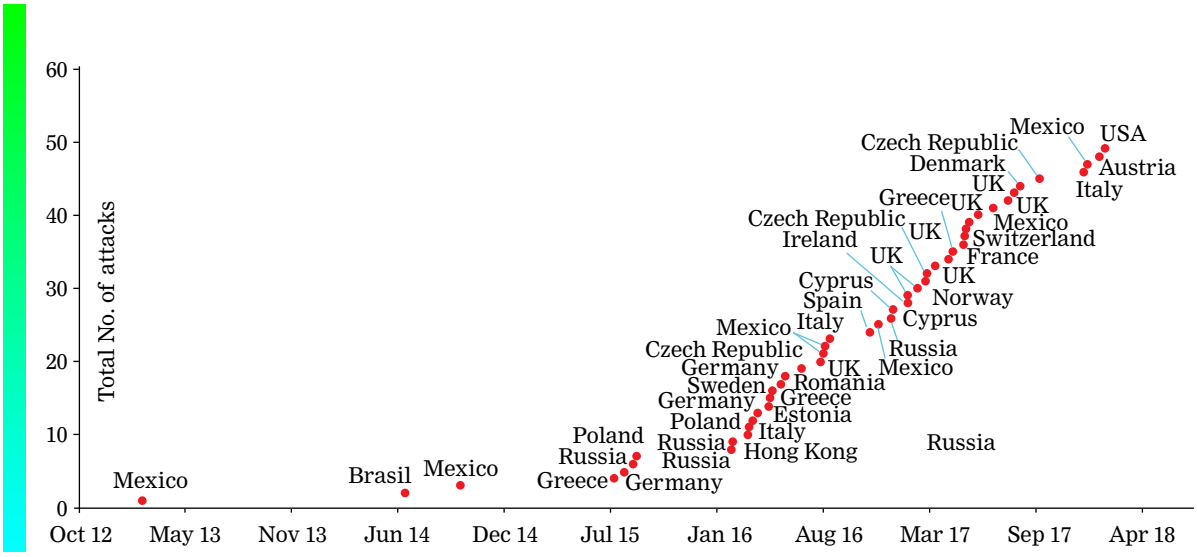
Теперь давайте поговорим подробнее о самих атаках. Злоумышленник может провести атаку типа Black Box, если есть возможность подключения к шине диспенсера.

В большинстве случаев производители банкоматов выносят системный блок в сервисную зону ATM, то есть в его верхнюю часть. И все, что отделяет злоумышленника от системного блока, — это пластиковая панель, на которой обычно располагается реклама либо логотип банка.

Как злоумышленники используют уязвимости АТМ

Рисунок 2

Статистика атак типа Black Box



Вырезав отверстие в такой панели дрелью с биметаллической буровой коронкой, злоумышленник получает доступ к системному блоку, к которому подключена шина данных диспенсера. Она-то атакующему и нужна.

Многие говорят о том, что атаки типа Black Box уже давно неактуальны, поскольку между хостом и диспенсером используется шифрование с применением стойких криптографических алгоритмов. Но, как показывает практика, это не всегда так.

Например, в одном из самых распространенных банкоматов в России, произведенном NCR, действительно используется шифрование шины данных — AES-128. Но при этом в самом встраиваемом программном обеспечении (прошивке) диспенсера присутствует логическая уязвимость, которая заключается в отсутствии аутентификации хоста. Ее эксплуатация приводит к возможности сброса текущих ключей шифрования и установке произвольных. После этого злоумышленник имеет возможность отправлять диспенсеру любые команды, в том числе и на выдачу наличных средств.

Стоит также отметить, что некоторые производители, включая Wincor, в некоторых моделях выносят системный блок в сейф. Казалось бы, таким образом они защищают свои банкоматы от атак типа Black Box. Но при этом сам кабель от диспенсера вынесен в сервис-

Алексей АНТОНОВ

ную зону и подключен к общему USB-концентратору, доступ к которому атакующий также может с легкостью получить.

В ряде случаев даже при наличии возможности использовать шифрование канала имеют место уязвимости класса конфигурирования (как программные, так и программно-аппаратные), связанные с принудительным отключением шифрования. В этих случаях злоумышленнику ничего не мешает выполнить атаку типа Black Box.

Уязвимости конфигурирования обычно возникают из-за того, что сервисные инженеры невнимательно подходят к настройке как самого банкомата, так и программного обеспечения производителя либо служба безопасности банка при разработке модели угроз и анализе рисков не учитывает все варианты действий злоумышленника.

На форумах, где обсуждаются проблемы эксплуатации банкоматов и пути их решения, злоумышленник может найти массу полезной для него (и недоступной в иных местах) информации: например, о том, как проблематично сервисным инженерам работать с защитными функциями банкомата и как средства защиты в ходе эксплуатации просто отключаются, сталкиваясь с различными проблемами. Конфигурацию могут не проверять годами, а значит, понять, что у каких-то банкоматов просто-напросто не работают встроенные средства защиты, специалистам банка не всегда возможно. Злоумышленник может попробовать вычислить тот банк и даже тот банкомат, про который говорят на специализированных форумах, и далее с легкостью провести на него атаку, зная, что именно в этом банкомате не работают средства защиты.

В ряде случаев даже при наличии возможности использовать шифрование канала имеют место уязвимости класса конфигурирования (как программные, так и программно-аппаратные), связанные с принудительным отключением шифрования.

Атака типа Deposit Forgery

При наличии возможности подключения к шине купюроприемника злоумышленник может провести атаку типа Deposit Forgery, которая позволяет выполнить подделку валюты, номинала и количества внесенных купюр.

Для анализа возможности реализации данной атаки, как и в случае с атакой типа Black Box, он проводит исследование встраиваемого программного обеспечения купюроприемника и программного обеспечения на хостовой части с целью изучения протокола взаимодействия.

Здесь, чтобы осуществить задуманное, злоумышленнику необходимо, используя специальное техническое программно-аппаратное средство, встать в разрыв между хостовой частью и купюроприемником (осуществить атаку типа Man in the Middle) и в момент зачис-

ления наличных подделать значения определенных полей в передаваемых сообщениях, указывающих на валюту, номинал и количество вносимых купюр.

Внесенные таким образом наличные средства позже могут быть выведены абсолютно легально.

Атаки типа ATM Malware Jackpotting

Атаки с использованием Malformed-устройств

Программное обеспечение производителей банкоматов имеет обширный пласт драйверов и библиотек, которые применяются для подключения и работы с разнообразными периферийными устройствами, включая пинпад, кардридер, сканер штрихкодов, различные USB-модемы, VPN-ключи, цифровые камеры и пр.

Наличие уязвимостей в таком программном обеспечении дает возможность атакующему применять вектор с использованием Malformed-устройства, которое он подключает к шинам данных одного из периферийных девайсов с учетом конструктивных особенностей. Malformed-устройство — это специально сконструированный девайс, который эмулирует работу реального, но в подходящий момент отправляет специальным образом сформированные данные, приводящие к эксплуатации ранее найденной уязвимости. В результате атакующий получает возможность выполнить произвольный код и получить наличные деньги.

Здесь необходимо отметить зачастую крайне низкое качество кода программного обеспечения периферийных устройств, многие компоненты которого были написаны лет десять назад и более. Отсутствуют встроенные механизмы защиты (/GS — stack cookies, /DYNAMICBASE для модулей), бывают отключены и системные механизмы защиты (DEP).

Успешное использование таких уязвимостей чаще всего приводит к исполнению произвольного кода с высокими привилегиями, поскольку эти компоненты расположены в системных сервисах и ядре ОС.

Атаки методом User Input Emulation

Обладая физическим доступом к компьютеру внутри банкомата, злоумышленнику нетрудно добиться запуска своих программ или изменить поведение установленных программ нужным образом. Если сервисные инженеры банка об этом не позаботятся, ему может оказаться достаточно присоединить свой носитель информации и два раза кликнуть. При желании ему недорого обойдется автомати-

Алексей АНТОНОВ

зация ввода нужных команд, манипуляций окнами, в конечном счете — запуск вредоносной полезной нагрузки.

Здесь могут возникнуть трудности с окном интерфейса банка, которое закрывает все остальные элементы управления ОС (kiosk-mode), но существует множество тривиальных способов получить фокус для ввода, переключиться, вызвать какой-нибудь системный компонент (вроде «режима залипания клавиш»).

Троянские программы

Получив возможность запуска произвольного кода на хостовой части в банкомате, атакующий уже близок к цели. Чтобы выполнить управление диспенсером с хостовой части — запросить выдачу наличных, существует и успешно применяется ряд инструментов. Есть как простейшие троянские программы (Alice), так и «замороченные» с функциями для контроля снятия наличных дропами (Tyupkin). Доступность и простота этих средств могут недооцениваться. Подробные технические описания и семплы есть в блогах антивирусных компаний и публичных «песочницах». Все это злоумышленник может повторить или использовать.

Чем более строгие политики запретов и меры контроля применяются, тем труднее пользоваться защищаемой системой: больше ложных срабатываний, конфликтов, потребления весьма ограниченных ресурсов системы.

В качестве примера назовем один из последних продаваемых продуктов такого рода — троянскую программу Cutlet Maker. На ее официальном сайте есть детальное описание с картинками и видео уязвимых мест банкомата Wincor, подробная инструкция по использованию и прототип устройства для автоматизации атаки с использованием вектора User Input Emulation.

Тем не менее, здесь перед атакующим могут возникнуть последние препятствия: во-первых, специальные средства защиты банкоматов, во-вторых, возможно, недостаточность имеющихся привилегий учетной записи в системе.

Обход средств защиты (Application Control)

В случае использования злоумышленником посторонних инструментов в системе, таких как названные выше троянские программы, банку способны помочь разграничения и запреты, вносимые средствами защиты информации (СЗИ).

Помимо обычных функций выявления известных семейств троянских программ, широко используемой практикой является запрет запуска любых посторонних, то есть не добавленных заранее в «белый» список, программ и прочих компонентов, например в таких продуктах, как McAfee Solidcore, Kaspersky Embedded Systems Security, Safe'n'Soft TPSecure. Иногда детектирование вредоносных программ

производится только статически, без поведенческого анализа, что не создаст препятствий для полиморфного кода. Что касается защиты типа «белых» списков программ, то такие системы защиты распространяют свой контроль не на все объекты, которые можно использовать для запуска своего кода. Кроме того, СЗИ усложняют эксплуатацию устройств и поэтому бывают отключены сервисными инженерами.

Бывает также, что защитные продукты вносят собственные слабости в систему. Пример: уязвимость, найденная Дмитрием Турченковым из компании Embedi, — обход «белых» списков и повышение привилегий.

Как и в случае с банковскими троянскими программами, злоумышленник может найти в открытых источниках описания предлагаемых защит, скачать дистрибутивы для исследования, почитать форумы инженеров, работающих с банкоматами, где специалисты делятся опытом решения проблем использования СЗИ совместно с другим ПО. Из доступной информации можно сделать выводы, какие продукты сейчас используются в нашей стране крупными банками и как работает защита. В обсуждениях можно найти конкретные версии ПО и модели банкоматов. Полезную для поиска простых обходов СЗИ информацию можно обнаружить, проанализировав его конфигурацию. При наличии дистрибутива СЗИ можно выявить слабые места его архитектуры.

Таким образом, сколько существуют средства защиты, столько же совершенствуются методы их обхода. Чем более строгие политики запретов и меры контроля применяются, тем труднее пользоваться защищаемой системой: больше ложных срабатываний, конфликтов, потребления весьма ограниченных ресурсов системы. Ввиду этого зачастую реально осложняющие жизнь злоумышленнику механизмы бывают отключены, а разработчики СЗИ весьма ограничены в том, какие изменения они могут вносить в систему.

Повышение привилегий

В случае если для обращения к устройству окажется недостаточно привилегий — например, при запуске «проводником» процесс наследует токен обычного пользователя, а устройство захвачено сервисным процессом — перед атакующим стоит необходимость повышения своих привилегий в системе. Однако есть отдельный класс эксплойтов, решающих эту задачу, с учетом того, что на машинах типа банкоматов чаще всего используется устаревшее, но стабильное ПО.

Алексей АНТОНОВ

Для повышения привилегий часто используются уязвимости:
— операционной системы;
— стороннего программного обеспечения;
— программного обеспечения производителя банкомата.

Кроме того, злоумышленники обнаруживают интересные для себя «фичи» в средствах защиты, устаревших драйверах устройств, неправильно настроенных атрибутах прав доступа.

Что поможет обеспечить безопасность?

Чтобы обладать полной информацией о проблемах с защитой АТМ, банкам, конечно же, необходимо регулярно проводить комплексный анализ ПО и «железа» для выявления наиболее удобных подходов к его взлому. Но из общих рекомендаций, которые универсальны для всех, можно выделить необходимость применять базовые правила информационной безопасности при установке и поддержке технических средств.

К таким базовым правилам можно отнести те процессы, которые используются при поддержке пользовательских рабочих станций, например: только разрешенная конфигурация и настройки, обновленный софт, установленные средства защиты. Такие меры не помогут от всех атак, поскольку панацеи не существует, но позволят устранить большое количество известных уязвимостей, которые эксплуатируются злоумышленниками. Ну и, наверное, самое важное — делать это постоянно. Безопасность нельзя обеспечить разовыми мерами — это постоянный процесс, который надо налаживать, улучшать, «докручивать».

На SAS 2017, главной конференции года по кибербезопасности, специалисты «Лаборатории Касперского» Сергей Голованов и Игорь Суменков рассказали о нескольких кейсах, связанных с интересными для злоумышленников способами взлома банкомата: удаленно, почти удаленно и с помощью дрели.

ATMitch — вредоносное ПО с удаленным управлением

Осмотрев опустошенный злоумышленниками банкомат, служба безопасности банка не нашла ни вредоносных программ, ни странных отпечатков пальцев, ни следов физического взлома или подключения сторонних устройств, способных взять банкомат под контроль.

Однако сотрудники банка обнаружили текстовый файл kl.txt. Они предположили, что буквы kl могут быть как-то связаны с KL, то есть с «Лабораторией Касперского», и обратились туда.

Получив данные из файла log.txt, специалисты смогли сформулировать правило для YARA — инструмента исследования вредоносных программ — и задали поисковый запрос для базы вредоносных файлов. Спустя день поиски принесли плоды: был обнаружен файл tv.dll, который успел «всплыть» дважды: в России и Казахстане. Этой ниточки хватило, чтобы распутать весь узел.

После тщательного исследования dll-файла стало понятно, как проводилась атака. Специалисты воспроизвели ее на специальном банкомате, установленном в лаборатории, и в результате тестируемый банкомат «послушно» выдал загруженные в него банкноты.

ATMitch в деле

Атака начинается с того, что преступники проникают на сервер банка, используя незакрытую уязвимость. Открытый код и общедоступные программы позволяют инфицировать банковские компьютеры. При этом зловред хранит свои данные в оперативной памяти системы, а не на жестком диске, что позволяет ему оставаться незаметным для защитных решений. Более того, после перезагрузки исчезают какие-либо следы заражения.

Взяв под контроль компьютеры в банке, зловред подключается к командному серверу и позволяет мошенникам удаленно загрузить вредоносное ПО прямо в систему банкоматов.

Так ATMitch добирается собственно до банкомата. Благодаря настроенному туннелю от командного сервера в банк это все выглядит как вполне легитимное обновление ПО, так что ни одно средство защиты не поднимает тревогу. Попав внутрь, ATMitch отправляется на поиски файла по имени command.txt. В нем содержатся односимвольные команды, которые используются для управления банкоматом. Например, O означает «Открыть лоток для выдачи наличных».

Обнаружив файл, ATMitch первым делом интересуется, сколько денег есть в банкомате, а затем просит машину выдать определенное количество купюр. К этому моменту возле банкомата оказывается сообщник преступников, который забирает наличные.

Преступники постарались замести все следы, поэтому специалисты банка не нашли никаких сторонних исполняемых файлов на жестком диске ограбленного банкомата. После извлечения денег ATMitch стер даже файл command.txt.

ATMitch потенциально способен заразить любой банкомат, поддерживающий библиотеку XFS, а это умеют практически все современные банковские машины.

Bl@ckb0x_m@g1k: простой, но очень эффективный трюк

Второй кейс начался с классической тупиковой ситуации: пустые логи, никаких подозрительных файлов на жестком диске. Более того, мошенник даже заклеил объектив камеры наблюдения.

Банкомат демонтировали. Разобрав его в своем офисе, специалисты обнаружили подключенный к USB-хабу банкомата Bluetooth-адаптер, а на жестком диске нашлись драйверы для Bluetooth-клавиатуры.

Этого хватило, чтобы реконструировать всю схему. Итак, мошенник сначала подключил Bluetooth-адаптер к банкомату, а потом подождал три месяца, чтобы логи очистились (они хранятся как раз три месяца). Затем преступник вернулся, заклеил камеру наблюдения, достал Bluetooth-клавиатуру, подключил ее и перезагрузил устройство в режим обслуживания. Так он смог запустить сервисную команду по опустошению кассет с деньгами.

Дрель, самая настоящая электродрель

Злоумышленник взломал банкомат с помощью электродрели, оставив после себя идеально круглое отверстие диаметром около 4 см прямо рядом с клавиатурой, с которой вводят PIN. Затем последовало несколько похожих происшествий в России и Европе, разве что отверстия были не такими круглыми. В конце концов полиция поймала подозреваемого, вооруженного ноутбуком и набором проводов.

Специалисты разобрали банкомат, установленный в тестовой лаборатории, чтобы понять, что же искал преступник рядом с клавиатурой. Там нашелся 10-контактный коннектор, подключенный к шине, которая связывала между собой практически все компоненты банкомата: от компьютера до кассет с купюрами. Кроме того, в банкомате использовалось очень слабое шифрование, которое можно было без особого труда взломать.

Итак, шифрования практически нет, так что в командах разобраться не проблема; подключившись к любой части банкомата, можно управлять всеми его компонентами, между которыми нет никакой системы авторизации, так что любую часть можно заменить незаметно для всех остальных.

Как злоумышленники используют уязвимости АТМ

Потратив $15 и определенное количество времени, специалисты сделали простую микросхему, с помощью которой можно было управлять банкоматом. Подключив ее к последовательной шине, они заставили тестируемый банкомат выдать фальшивые деньги, которые использовались в тестовых целях. Похоже, преступник произвел те же действия, только банкомат был заряжен настоящими деньгами, а вместо микросхемы использовался ноутбук.

К сожалению, банкоматы нельзя обновить удаленно, чтобы избавиться от описанной уязвимости. Нужно менять «железо», то есть технический специалист должен уделить время каждому банкомату.