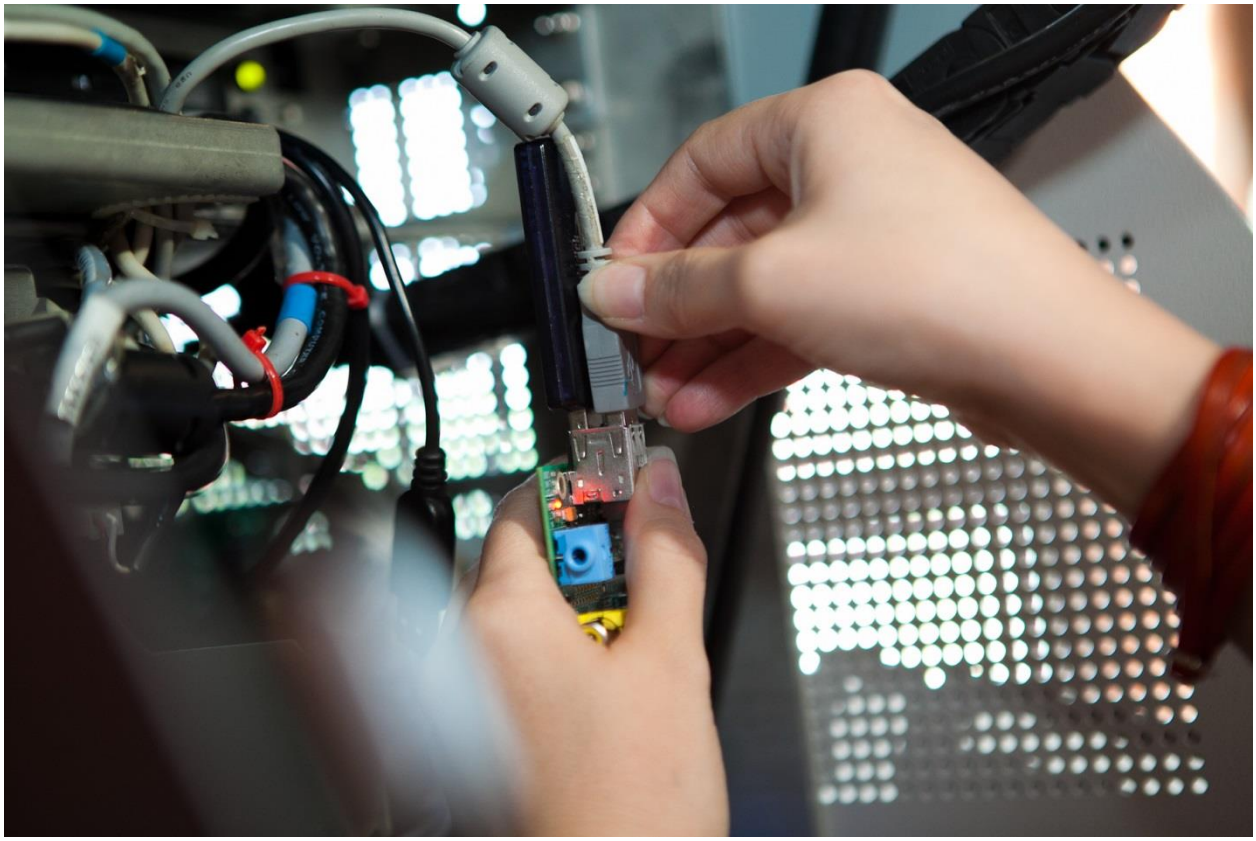
POSITIVE TECHNOLOGIES

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061 / МОСКВА / ПРЕОБРАЖЕНСКАЯ ПЛОЩАДЬ / Д.8
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

Атака на банкомат с помощью Raspberry Pi

Что только не делают с банкоматами: их выдирают из стены, привязав тросом к автомобилю, сверлят, взрывают и режут (иной раз в здании Госдумы). По статистике EAST, преступники стали реже использовать скимминг, предпочитая траппинг и физические диверсии. Немало хлопот специалистам по безопасности доставляет и еще один новый тренд — вирусные атаки на банкоматы. Тут и Trojan.Skimer, и Backdoor.Ploutus, и совсем свежий зловред Tyupkin, и другие «приложения», известные и не очень. Малварь загружается в компьютер банкомата, как правило с внешних носителей, и используется для несанкционированной выдачи денег или перехвата карточных данных. Еще один способ атаки описали эксперты Positive Technologies Ольга Кочетова и Алексей Осипов на конференции по компьютерной безопасности Black Hat Europe 2014, проходившей в октябре в Амстердаме.



Для проверки защищенности тестового банкомата, пережившего три форума Positive Hack Days, был выбран популярный миниатюрный контроллер Raspberry Pi. Устройство легко прячется внутри корпуса и не привлекает внимания технического персонала, который, к примеру, меняет бумагу во встроенных принтерах и потому имеет ключи от сервисной зоны.

Найти документацию с описанием интерфейсов банкоматов не так сложно, и об этом еще пять лет назад писал Алексей Лукацкий в своих «Мифах информационной безопасности». Оборудование

ATM и платежных терминалов, независимо от производителя, имеет общий API для доступа и управления различными модулями и работает на платформе Windows в соответствии с единым стандартом «расширений для финансовых услуг» (XFS).

Зная API, можно получить контроль над хост-компьютером банкомата и напрямую управлять различными периферийными устройствами, установленными внутри шкафа ATM, — картридером, клавиатурой для набора PIN-кода, сенсорным дисплеем, диспенсером банкнот и т. п. Не стоит забывать также об уязвимостях операционной системы банкомата, а их у Windows на много лет вперед припасено.

Слабое место

Прежде чем установить Raspberry Pi и подключить устройство к портам Ethernet, USB или RS-232, банкомат необходимо вскрыть. В верхней части ATM находится сервисная зона. Именно здесь расположен компьютер, управляющий устройствами банкомата, сетевое оборудование (в том числе плохо защищенные GSM/GPRS-модемы). Сервисная зона практически не контролируется, так как используется обслуживающим персоналом для различных работ. Получить к ней доступ значительно проще, чем к сейфу с деньгами, расположенному внизу. Ее можно открыть несложными в изготовлении ключами или совсем простыми подручными средствами.

Но просто открыть мало — надо сделать это быстро и незаметно.

На конференции Black Hat исследователи Positive Technologies продемонстрировали, сколько времени потребуется злоумышленникам, чтобы установить микрокомпьютер в сервисную зону ATM для использования его в роли сниффера — перехватчика PIN-кода и номера кредитной карты — или аппаратного скиммера, который не оставляет следов на внешнем виде банкомата. Понадобилось две минуты, чтобы разблокировать корпус банкомата, интегрировать микрокомпьютер, замаскировать и подключить его к интернету.

В процессе подготовки к выступлению Raspberry Pi был запрограммирован для управления периферийными модулями АТМ. К микрокомпьютеру подключался Wi-Fi-адаптер, к которому можно было подключиться с любого устройства, со смартфона например. Команды на выдачу денег в диспенсер отправлялись посредством специально реализованного веб-интерфейса. В качестве примера была показана выдача нескольких банкнот, а после некоторой доработки отправляемого кода банкомат сразу же расставался со всеми заложенными купюрами. К слову, в каждой кассете типичного АТМ помещается от двух до трех тысяч купюр, и таких кассет обычно четыре — для нескольких номиналов.

Надо ли говорить, что в ходе эксперимента банкомат выдавал купюры, не оставляя никаких записей в своем компьютере, а встроенная видеокамера банкомата хоть и работала, но, как и другие устройства внутри захваченного АТМ, контролировалась с помощью Raspberry Pi.

Можно ли защититься

Обеспечить безопасность банкоматов нелегко. Многое зависит от сценария атаки. К примеру, НИЦ «Охрана» МВД рекомендует производителям использовать дымогенератор, ультразвуковой барьер и ксеноновый стробоскоп, а специалисты британской LINK — запретить стандартные замки для доступа в сервисную зону и активнее применять веб-камеры.

Однако основная проблема, по мнению наших исследователей, — это возможность инсталлировать в банкомат любые устройства или программы (вплоть до Angry Birds), что вызвано обилием критических уязвимостей в операционных системах. Ситуацию могла бы изменить совместная работа производителей банковского оборудования над новой открытой спецификацией, которая бы обеспечила безопасное взаимодействие и эффективную проверку подлинности компонентов АТМ: чтобы любой желающий, раздобыв ключ от сервисной зоны, не смог так просто подключить к системе все что угодно.

О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована ФСТЭК и ФСБ, продукция сертифицирована ФСТЭК, «Газпромом» и Минобороны РФ. Более 1000 организаций в 30 странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, выполнения требований регуляторов и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня по вопросам защиты SCADA- и ERP-систем, крупнейших банков и телекомов. Согласно исследованиям IDC, в 2013 году компания заняла третье место на российском рынке ПО для безопасности, а также стала лидером по темпам роста на международном рынке систем управления уязвимостями. Подробнее о компании — на сайте ptsecurity.ru.