ATM под прицелом

взлом с системным подходом или привет из реального мира

Алексей Антонов / директор по работе
с ключевыми клиентами Digital Security

Digital Security

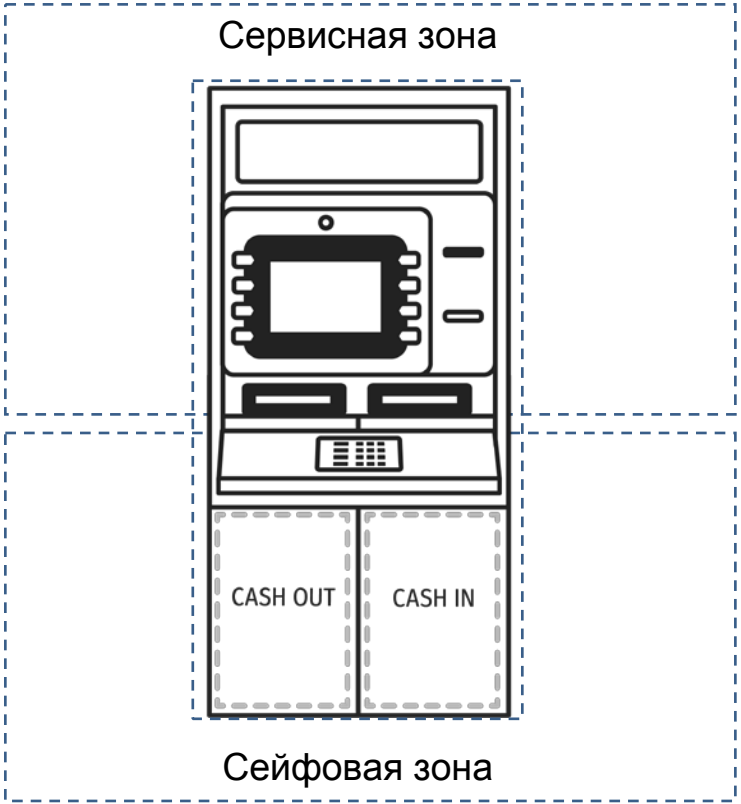
Введение

Почему именно банкоматы ?

Новые виды вредоносного ПО

Конструкция банкомата

Периферия



Шины данных

Модель нарушителя

И классы уязвимостей

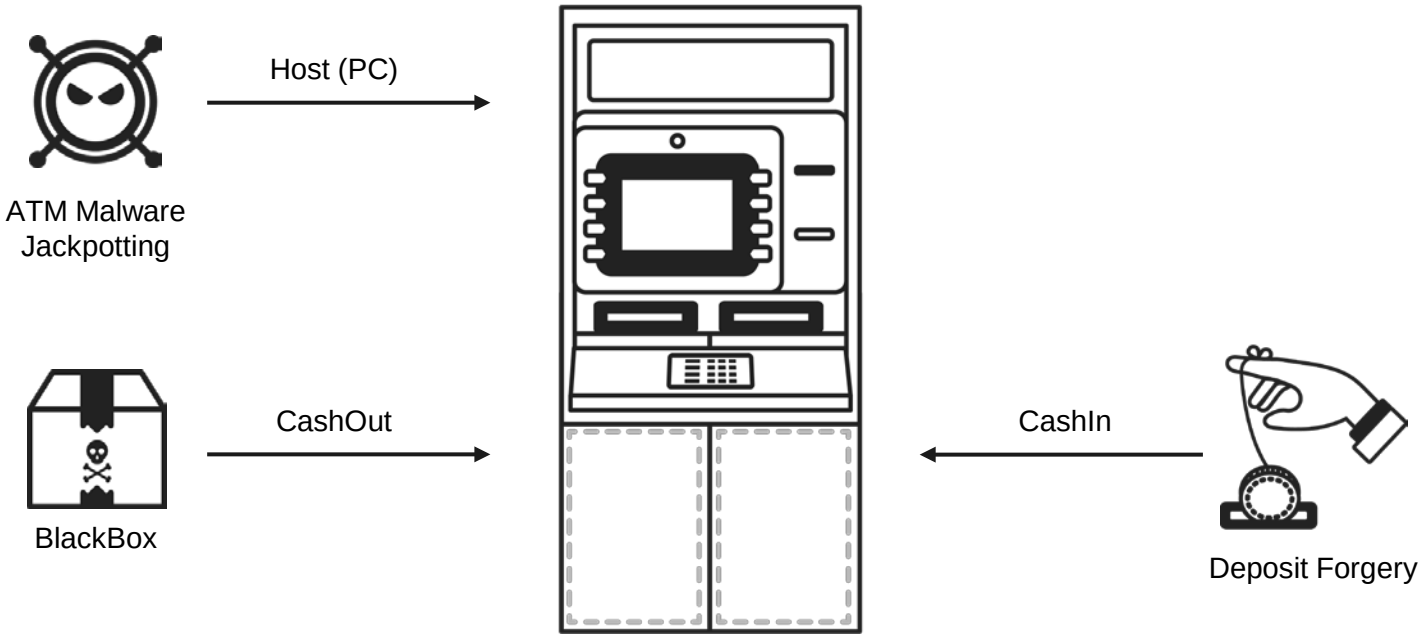
Уязвимости:

- Проектирования
- Реализации
- Конфигурации

Local

Remote

Типовые атаки



Digital Security

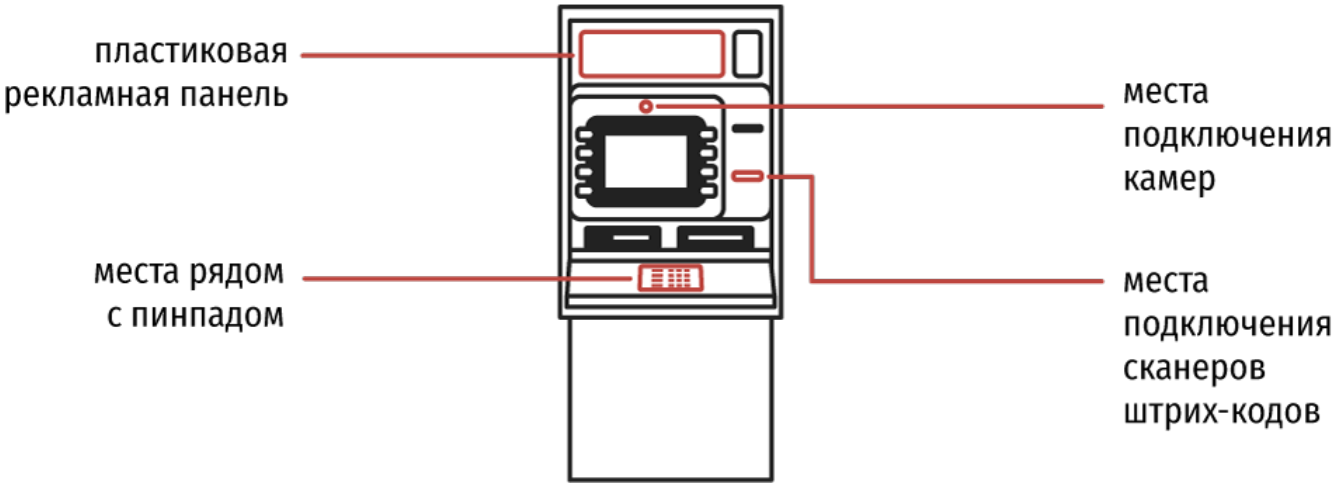
Конструктивные особенности

Точки подключения

Конструктивные особенности

Примеры

3-5 уязвимых мест



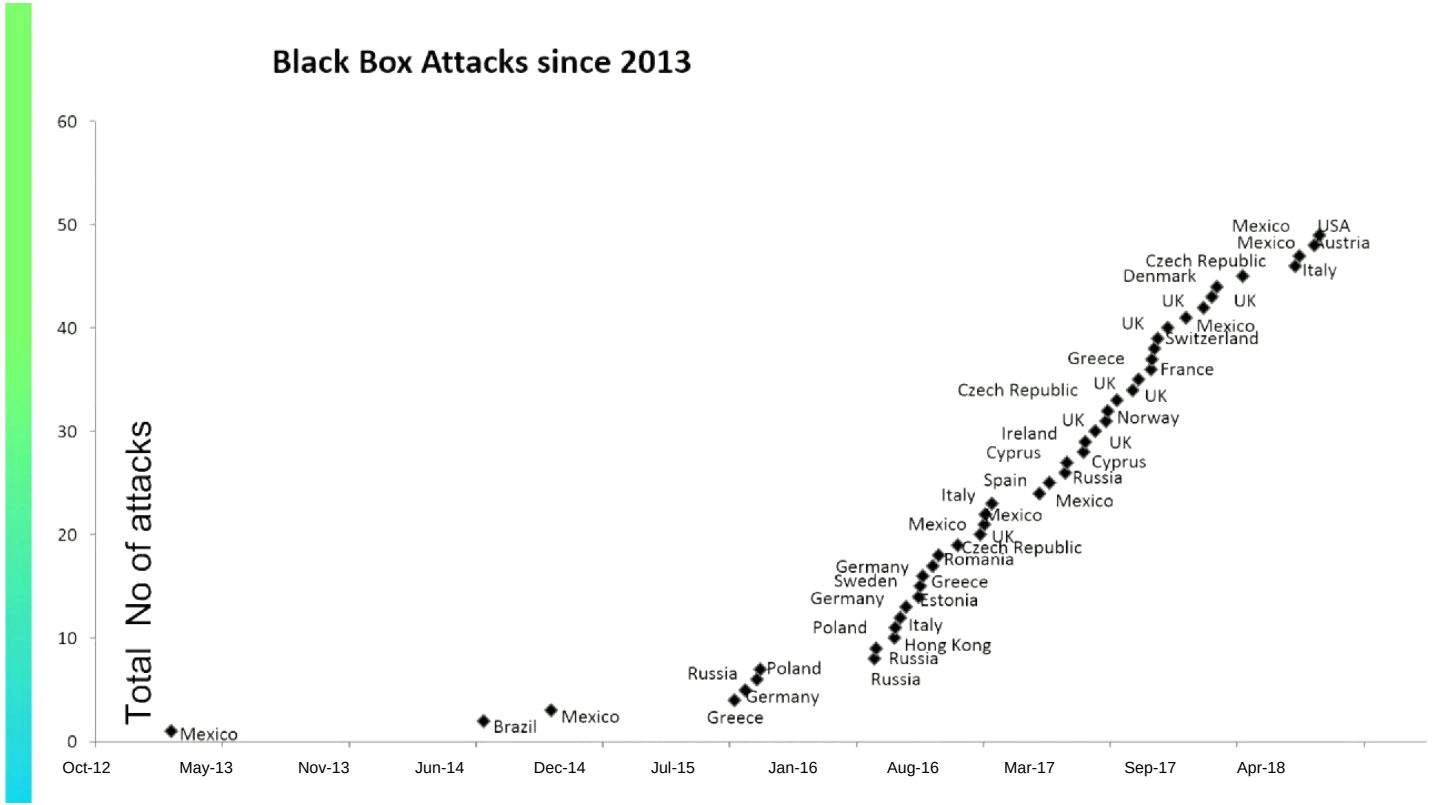
Digital Security

BlackBox

Атака на диспенсер

BlackBox

Статистика от NCR



BlackBox

Суть атаки

Злоумышленнику необходимо знать:

Протоколы взаимодействия

Текущую конфигурацию

Уязвимости

BlackBox

Шаг 1

BlackBox

Шаг 2

BlackBox

Шаг 3

BlackBox

Шаг 4

Шифрование

NCR - Прошивка диспенсера - уязвимость - смена ключей шифрования

Практика - принудительное отключение - переключение перемычки на контроллере

Вообщем с этим шифрованием геморой еще тот 🤦

Re: Dispenser не проходит проверку подлинности.

БЫСТРАЯ ЦИТАТА

Проверил еще на одном банкомате. Тот же эффект. Стоял патч (в софте) и новый драйвер. Заменил рабочую миску с другого рабочего банкомата. И все стало. Перестановка патча и нового драйвера, переключение с Phisycal на USB и обратно - все не помогло.

Аппаратные средства

ATM Keeper

CerberLock

- Работают хорошо, если настроены правильно
- Часто бывают проблемы

Это очередной гемор… Поставили этот Cerber SDC-Lock v.2. Прошел день… У провайдера случились проблемы с каналом связи и ВПН-рестартер таки взял банкомат и перезагрузил… Имеем отвалившийся диспенсер.

Digital Security

DepositForgery

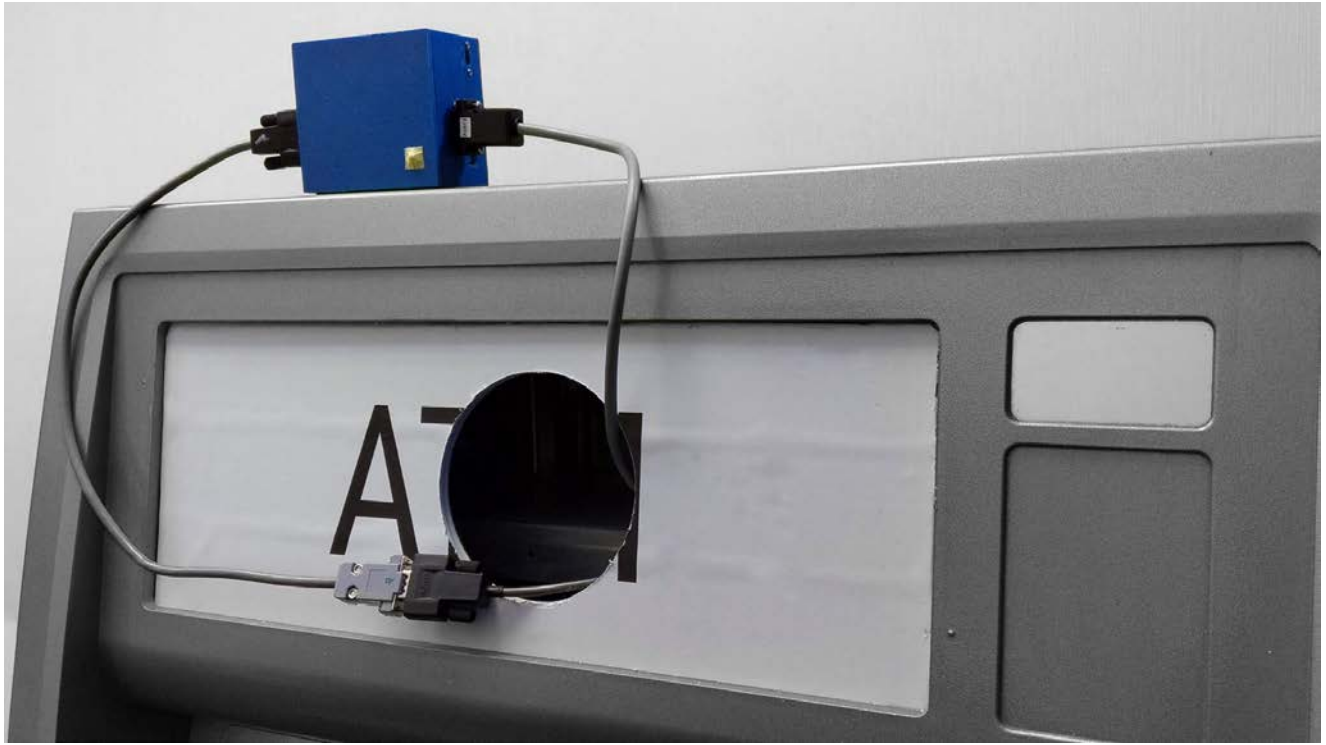
Атака на купюроприемник

Deposit Forgery

Суть атаки

DepositForgery

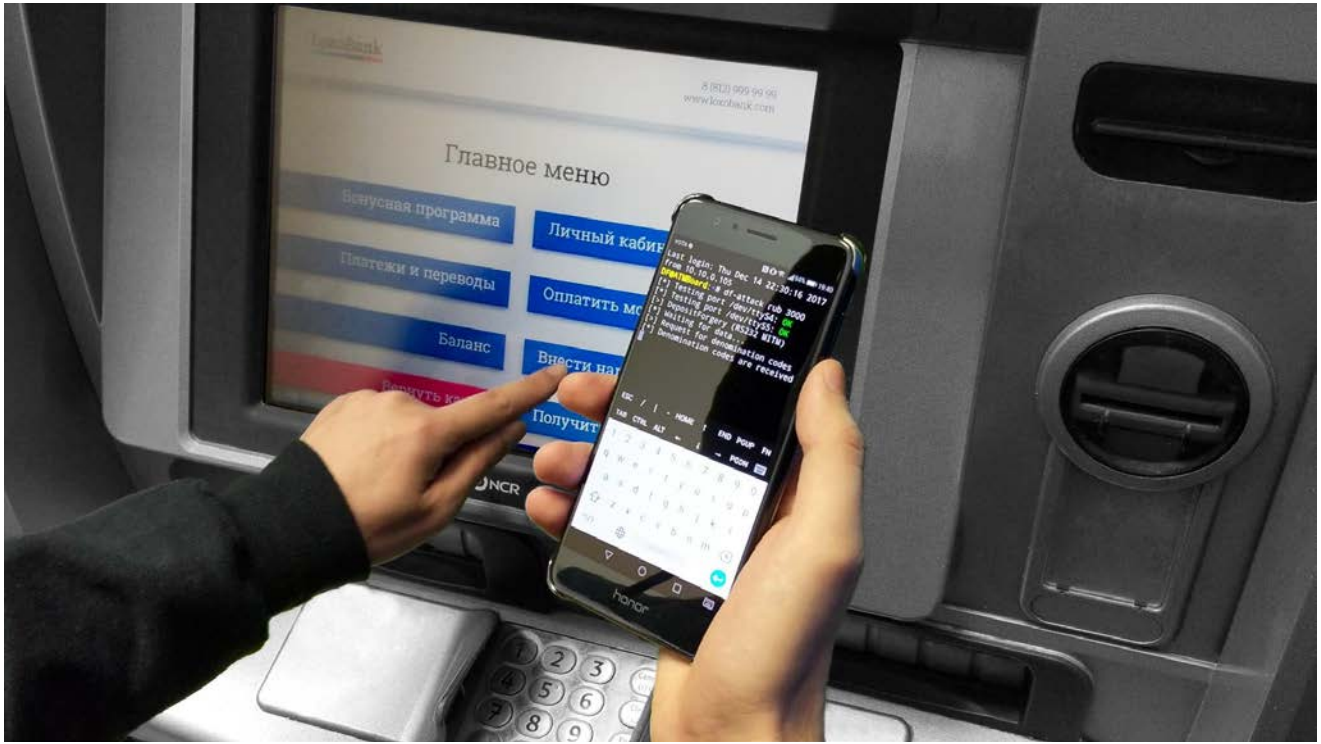
Шаг 1



Digital Security

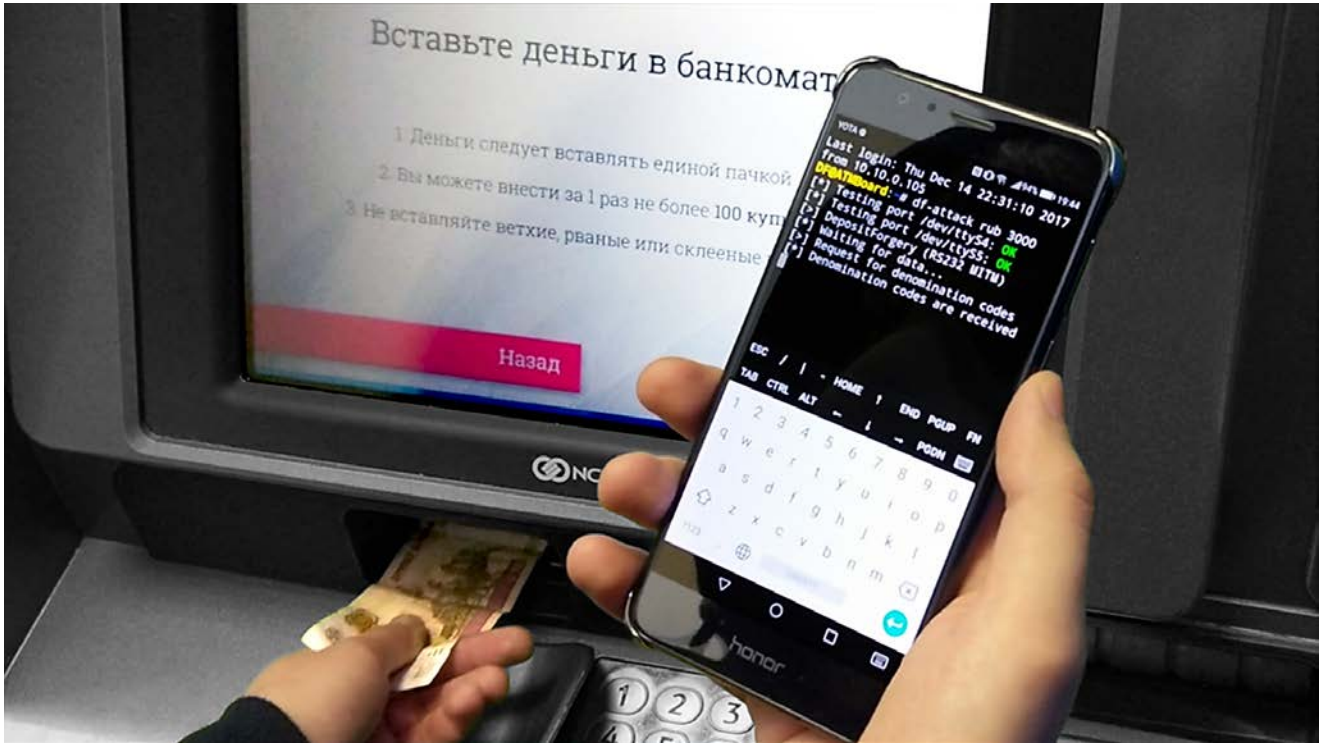
DepositForgery

Шаг 2



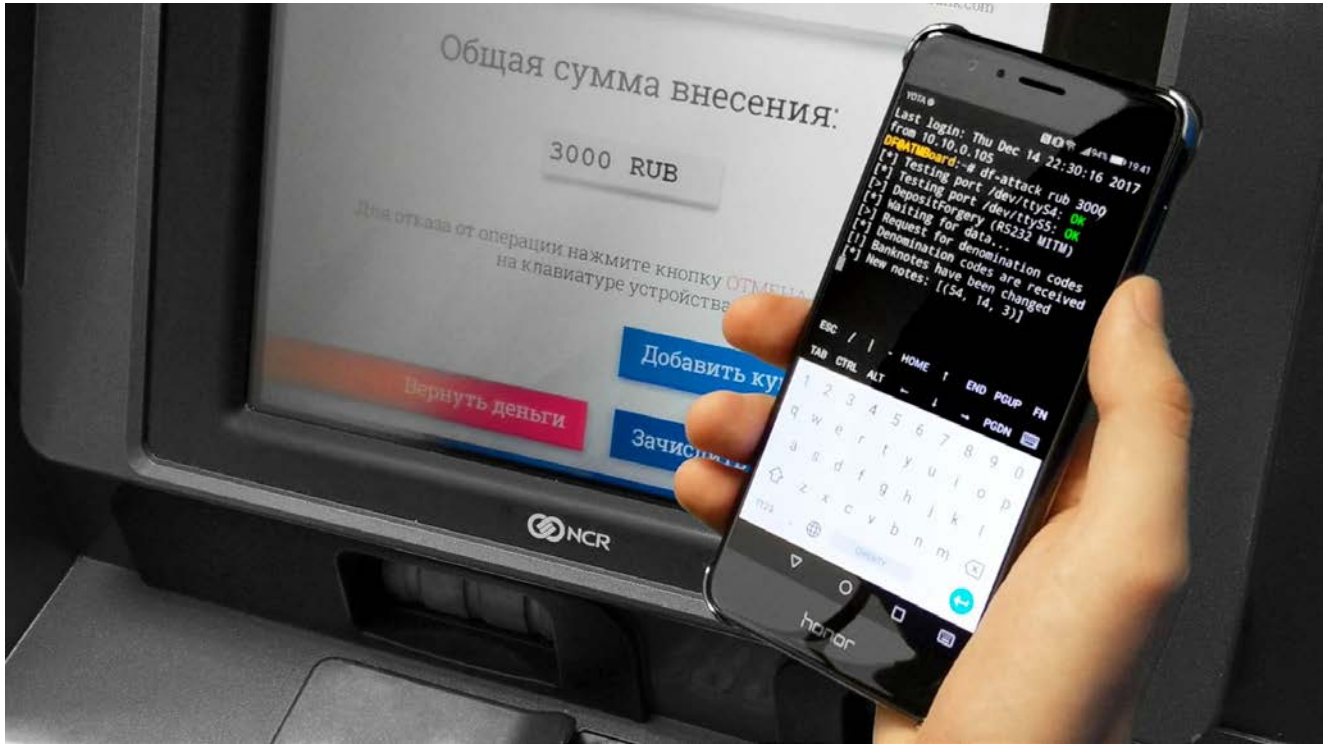
DepositForgery

Шаг 3



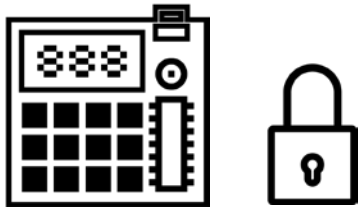
DepositForgery

Шаг 4



DepositForgery

Шаг 5



Диспенсер - защищен

Купюроприемник - нет

Анти-фрод

Не создавать аномалий для фрод-мониторинга

Digital Security

ATM Malware Jackpotting

Атака на хост

ATM Malware Jackpotting

Malformed устройство

User Input Emulation

Digital Security

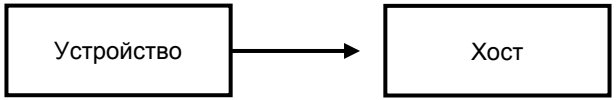
ATM Malware Jackpotting

Malformed устройство. Эксплуатация уязвимостей на хосте.

Malformed Device

Суть атаки

В нормальном режиме работы



В режиме атаки

Digital Security

ATM Malware Jackpotting

Malformed-устройство / Шаг 1

ATM Malware Jackpotting

Malformed-устройство / Шаг 2

ATM Malware Jackpotting

Привилегии

Можно повысить

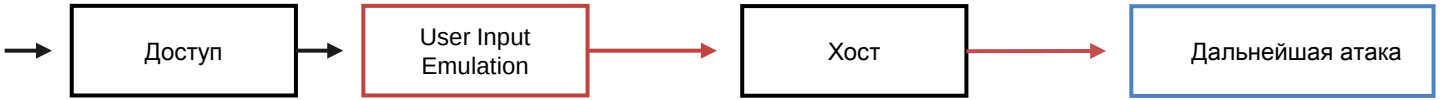
Digital Security

ATM Malware Jackpotting

Эмуляция пользовательского ввода

User Input Emulation

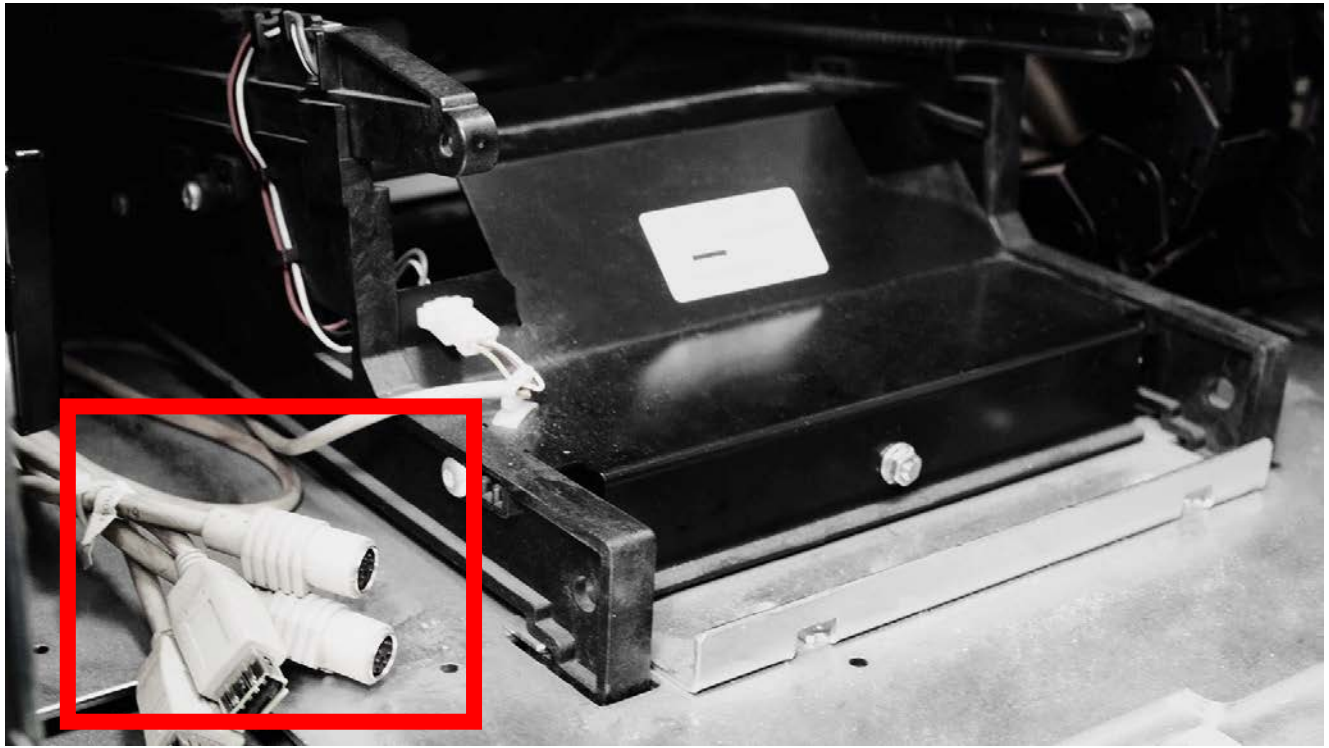
Суть атаки



Хост управляется ОС общего назначения, поэтому возможно подключение множества периферийных устройств.

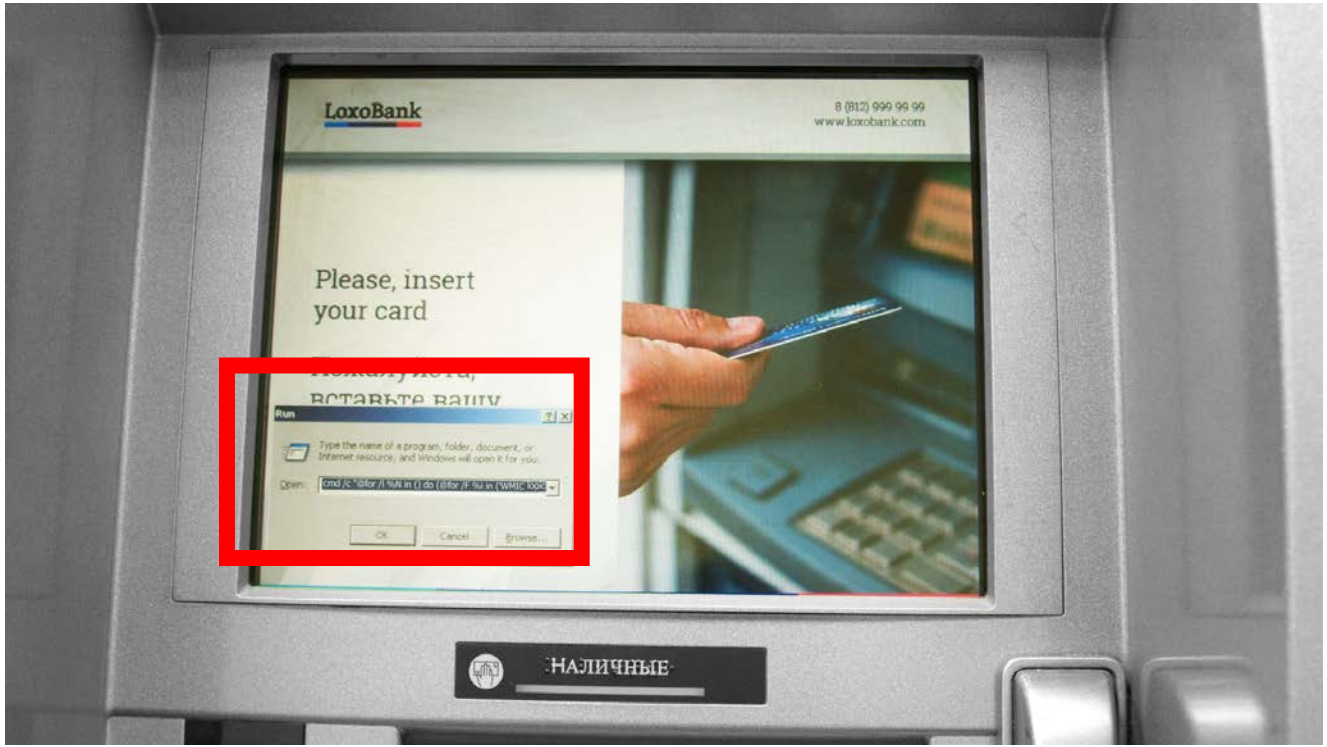
ATM Malware Jackpotting

User Input Emulation / Шаг 1



ATM Malware Jackpotting

User Input Emulation / Шаг 2



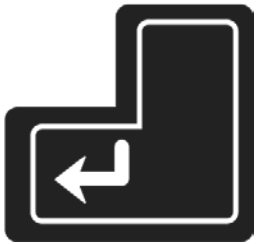
Digital Security

ATM Malware Jackpotting

User Input Emulation / Шаг 3

Киоск поверх окон

Альт коды



Клавиатурные сокращения

Скриптовые перечисления

Специальные СЗИ

Запрет запуска постороннего кода (белые списки)

Задействовать встроенные средства позволяющие запускать произвольный код:

Powershell

VBA

Отладчики

СЗИ пропускают
запуск DLL библиотек

Неправильное использование СЗИ

народе "Носорог", хотя как его только не крестили. При совместной работе с FPSU ip-клиентом этот гаденыш валит соединение клиента. Каким образом - остается загадкой. По крайней мере, лично перекопал все логи самого носорога - никакой активности не отражено. Без антивиря все работает прекрасно. Где копать??? Мы, простите за французский, за%%%%сь ездить по банкоматам

Есть проблема с 2-мя новыми банкоматами. Постоянное зависание. В мониторинге вижу ошибку Card reader operation suspended и Чековый принтер: аппаратная ошибка. Проблема уходит при удалении антивируса SafenSoft Syswatch, при повторной установке его, проблема возвращается.

Есть такая проблема. Удаляли носорога вчистую.

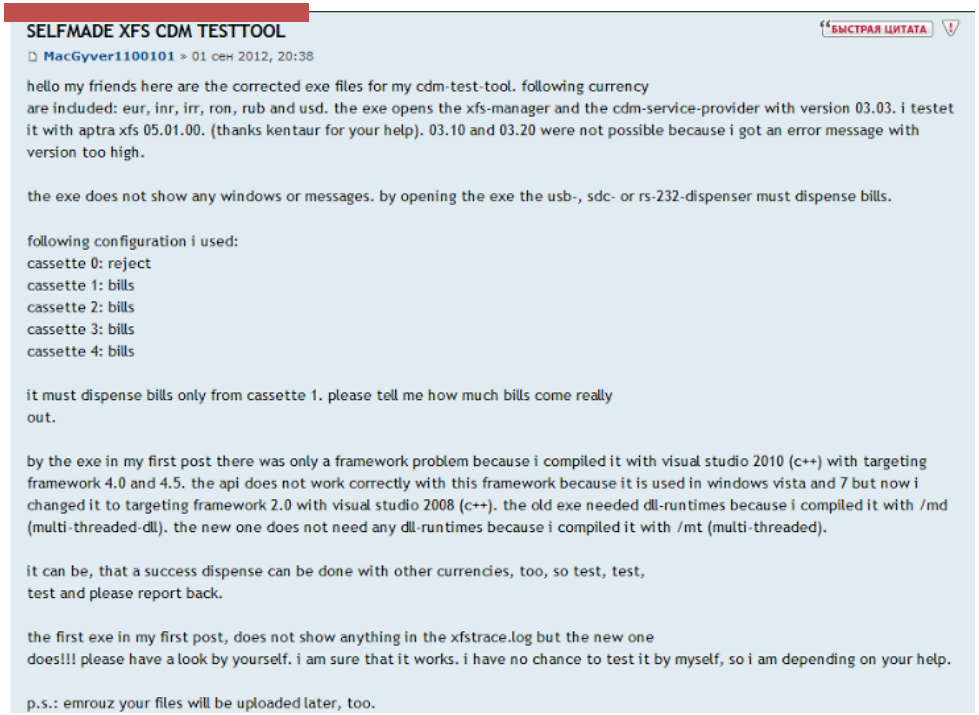
Поддерживаю! Носорог - убийца банкоматов.
В пятницу было: NCR 6622, 4-5-6 - все кресты. После удаления носорога всё заработало.

Re: Wincor 4040 (Ошибка Secure Channel)

Попробуй отключить защиту, антивирусы и т.п. После этого попробуй еще раз.

ATM Malware Jackpotting

Полезная нагрузка



SELFMADE XFS CDM TESTTOOL

БЫСТРАЯ ЦИТАТА

MacGyver1100101 » 01 сен 2012, 20:38

hello my friends here are the corrected exe files for my cdm-test-tool. following currency
are included: eur, inr, irr, ron, rub and usd. the exe opens the xfs-manager and the cdm-service-provider with version 03.03. i testet it with aptra xfs 05.01.00. (thanks kentaur for your help). 03.10 and 03.20 were not possible because i got an error message with version too high.

the exe does not show any windows or messages. by opening the exe the usb-, sdc- or rs-232-dispenser must dispense bills.

following configuration i used:
cassette 0: reject
cassette 1: bills
cassette 2: bills
cassette 3: bills
cassette 4: bills

it must dispense bills only from cassette 1. please tell me how much bills come really
out.

by the exe in my first post there was only a framework problem because i compiled it with visual studio 2010 (c++) with targeting framework 4.0 and 4.5. the api does not work correctly with this framework because it is used in windows vista and 7 but now i changed it to targeting framework 2.0 with visual studio 2008 (c++). the old exe needed dll-runtimes because i compiled it with /md (multi-threaded-dll). the new one does not need any dll-runtimes because i compiled it with /mt (multi-threaded).

it can be, that a success dispense can be done with other currencies, too, so test, test,
test and please report back.

the first exe in my first post, does not show anything in the xfstrace.log but the new one
does!!! please have a look by yourself. i am sure that it works. i have no chance to test it by myself, so i am depending on your help.

p.s.: emrouz your files will be uploaded later, too.

bankomatchik.ru

Digital Security

Спасибо за внимание

Без иронии, хотелось бы поблагодарить и передать привет юзерам форума «банкоматчик.ру» за множество полезных материалов