Решение по защите банкоматов от атак типа Black box и прямой Cash dispense

КОМСЕТ
сервис

Метод хищения денежных средств из банкомата - «Прямой диспенс» или «Black box»

Атака основана на перехвате управления контроллером диспенсера банкомата с использованием подключения к шине данных специализированного оборудования, имитирующего функции управляющего системного блока банкомата (Black Box). Отличительной особенностью описываемого вида атаки является то, что ее вектор направлен на слабозащищенный физический интерфейс передачи данных между системным блоком и модулем выдачи банкнот (диспенсером).

При совершении атаки, злоумышленники получают доступ к открытому участку общей шины и подключают «Black Box» устройство к линии связи, после чего отправляют команду контроллеру диспенсера на выдачу наличных. Проникновение в технологический отсек осуществляется с помощью технологического ключа, который у многих моделей банкомата одинаковый, физическим взломом замка технологического отсека, удалением рекламных панелей банкомата или сверлением отверстий в корпусе технологического отсека.

Рис. 1 Сверление отверстия для получения доступа к шине данных между системным блоком и диспенсером. Видны два ряда ровных отверстий, для получения доступа к шине данных RS 485.

Результатом атаки является потеря наличности, находящейся в банкомате, менее чем за 10 минут.

СМИ о хищении денежных средств из банкоматов:
https://meduza.io/feature/2017/04/04/prosto-prosverli-dyrku
https://ria.ru/incidents/20161019/1479560109.html

Принцип действия защитного устройства “ЗУБ-Р”

Внешний вид устройства

Техническое решение на базе изделия разработки и производства ЗАО «КОМСЕТ-сервис» «Защитное устройство банкомата - размыкатель» ЗУБ-Р предназначено для для защиты банкоматов от несанкционированного проникновения в технологический отсек и попыток подключения несанкционированных устройств к диспенсеру банкомата (атака «Прямой cash dispense» и «Black box»).

Устройство «ЗУБ-Р» устанавливается внутри сейфа банкомата в разрыв шины данных. Для этого стандартный разъем диспенсера, подключается к «ЗУБ-Р», а дополнительным защищенным кабелем осуществляется сопряжение «ЗУБ-Р» с системным блоком в технологическом отсеке банкомата.

Порт Ethernet «ЗУБ-Р» подключается к имеющемуся в банкомате коммутатору для организации защищённого канала передачи данных (используются протоколы стека TCP/IP) с центральным сервером системы.

Устройство считывания ключей размещается внутри технологического отсека банкомата.

При включении электропитания банкомата, как первичном, так и после проведения технического обслуживания, информационный канал обмена через шину данных системного блока банкомата и диспенсера по умолчанию разорван (состояние «по умолчанию» настраивается в конфигурации «ЗУБ-Р»). Для его восстановления необходима команда администратора центрального сервера системы, либо идентификация ключа специалиста, обслуживающего банкомат.

При открывании технологического отсека банкомата происходит срабатывание концевых выключателей, в результате которого «ЗУБ-Р» переходит в режим фиксации. В этом режиме в течение 30 секунд (интервал времени настраивается в конфигурации «ЗУБ-Р») необходимо приложить носитель идентификационного ключа к считывателю. Если этого не произошло, происходит разрыв информационного канала. Дальнейшее его восстановление возможно только по команде оператора центрального сервера системы. Если носитель приложен и ключ идентифицирован, канал не разрывается. При обратном закрытии технологического отсека происходит фиксация факта в журнале событий.

Кроме контроля срабатывания концевых выключателей «ЗУБ-Р» контролирует разрыв кабеля между системным блоком банкомата и самим устройством для исключения возможности подключения к кабелю, ведущему к диспенсеру, иного устройства в обход концевых выключателей (например, путем сверления отверстия в технологическом отсеке банкомате).

Все события, как то: открывание/закрытие технологического отсека, прикладывание носителя к считывателю, результат идентификации ключа, изменение состояния реле блокировки информационного канала, разрыв кабеля фиксируются в журнале событий с привязкой к точному времени и передаются на централизованный сервер управления.

Централизованное управление защитой

Централизованный сервер управления поставляется в виде виртуального образа (Virtual Appliances), а также может быть инсталлирован на физическом оборудовании Заказчика специалистами ЗАО «КОМСЕТ-сервис».

Функции централизованного сервера управления включают в себя:

- Мониторинг состояния устройств
- Управление состоянием устройств (разрыв/восстановление соединения цепи)
- Заведение новых устройств и их разделение по группам
- Управление ключами на устройствах
- Централизованный сбор журналов регистрации событий с устройств

Для выполнения указанных функций на сервере управления создаются учетные записи, которым присваивается одна из основных ролей доступа. В стандартной поставке в системе присутствуют 2 роли — «оператор» с правом просмотра событий и мониторинга устройств и «администратор» с правом управлять устройствами и ключами доступа. Количество ролей по желанию Заказчика может быть увеличено.

Все события выполняемые пользователями фиксируются во внутреннем журнале регистрации событий сервера, который также как и журналы событий с устройств может быть отправлен системой на централизованный лог-сервер Заказчика или SIEM решение (например, HP Arcsight).

Сетевое взаимодействие между устройствами и сервером реализовано на базе протоколов стека TCP/IP с двухсторонним взаимодействием и применением шифрования согласно протоколу TLS.

Преимущества

1 Архитектура

Решение «ЗУБ-Р» полностью автономное и самодостаточное. Не требует установки дополнительных программных агентов на банкомат, что исключает:

- архитектурную уязвимость аналогичных решений в виде возможной атаки на управляющий агент средства защиты, размещённый на физически доступном для злоумышленника системном блоке банкомата.
- дополнительную нагрузку на системные ресурсы банкомата.

2 Опыт

ЗАО «КОМСЕТ-сервис» производит высокоточное оборудование, построенное на базе собственных аппаратных платформ и программного обеспечения, начиная с 2003 года, что позволяет нам производить продукцию высокого качества.

3 Журналирование событий

Развитая система журналирования событий и интеграция с SIEM решениями различных производителей.

4 Произведено в России

5 Соответствие требованиям

Разработано с учётом требований международных платёжных систем по безопасности. Не требует применения дополнительных средств защиты для обеспечения собственной безопасности.

6 Совместимость и универсальность

Поддержка любых интефейсов диспенсеров и малые габариты позволяют применять наше решение на любой модели банкомата

7 Поддержка и доработка

Работая с нами – Вы работаете с непосредственным разработчиком решения, который готов обеспечить быструю доработку программного и аппаратного обеспечения под требования Заказчика, а также реализовать любой дополнительный функционал.

8 Централизованное управление

Возможность управления всеми устройствами из одной консоли с гибким разделением полномочий.

ЗАО «КОМСЕТ-сервис»

Закрытое акционерное общество «КОМСЕТ-сервис», сокращённое название ЗАО «КОМСЕТ-сервис», зарегистрировано 13 марта 2003 года в городе Москва.

Юридический адрес ЗАО «КОМСЕТ-сервис»: 115054, г. Москва, ул. Дубининская, д.57, стр. 1.

Адрес месторасположения структурных подразделений и почтовый адрес: 105037, г. Москва, ул. 1-я Парковая, д.7.

email: info@komset.ru | ssv@komset.ru
тел.: +7 (495) 921 29 16

www.komset.ru

Основные виды деятельности ЗАО «КОМСЕТ-сервис»:

- Разработка, серийное изготовление, поставки и поддержка эксплуатации электронного оборудования, необходимого для построения систем единого точного времени и тактовой синхронизации, использующего глобальные навигационные спутниковые системы ГЛОНАСС и GPS
- Контрактная разработка электронных изделий передачи данных, систем мониторинга технологических процессов, безопасности и т.п.
- Расчёт, проектирование, построение, аудит и техническая поддержка сетей тактовой сетевой синхронизации для операторов связи
- Организация семинаров и курсов повышения квалификации в области новых технологий