УДК 004.056

УГРОЗЫ БЕЗОПАСНОСТИ БАНКОМАТОВ

Мосунов А.А.

Белорусский государственный университет информатики и радиоэлектроники, г. Минск, Республика Беларусь

Научный руководитель: Алефиренко В.М. – канд.техн.наук, доцент

Аннотация. Приведены основные угрозы безопасности банкоматов, методы физического воздействия, аппаратные, программные и психологические методы воздействия на банкоматы. Представлены способы действия злоумышленников для получения конфиденциальной информации и различные виды манипуляции людьми.

Ключевые слова: атака, банкомат, банковская карта, взлом, защита информации, манипуляция, методы воздействия, физическая защита, операционная система, программное обеспечение, система безопасности.

Введение. В последние годы, одновременно с развитием банкоматной сети, выросло и количество случаев банкоматного мошенничества. Злоумышленники используют взлом как средство кражи денежных средств. И несмотря на то, что банкоматы имеют достаточно серьезную защиту, в настоящее время существует множество методов атаки на них.

Основная часть. Взлом и заражение банкомата (АТМ) – желанная цель для кибермошенников, поскольку это позволяет получить доступ к деньгам, хранящимся в нем. При этом злоумышленники могут действовать как удаленно, так и при контакте с банкоматом. Также устройство может стать исходной точкой для взлома всей инфраструктуры банка.

Недостаточная защита периферийных устройств, например, отсутствие аутентификации между периферийным оборудованием и ОС банкомата, позволяет преступнику обращаться к этим устройствам после заражения банкомата вредоносным ПО или напрямую подключать свое оборудование к диспенсеру или картридеру. Это может привести к краже денег или перехвату данных платежных карт.

Все виды атак на банкоматы можно разделить на четыре основные группы.

1. Методы физического воздействия. Самый популярный метод грабежа банкоматов – разбить устройство, взорвать, просверлить. Конечной целью преступника является сейф, в котором хранятся деньги. Однако такие действия очень заметны, и на всю операцию у воров будет лишь 2-3 минуты до того, как приедет наряд полиции.

Физические нападения – взломы, попытки разбить и выгрести содержимое банкоматов – могут быть осуществлены различными способами. Наиболее распространены попытки нанести повреждения с целью проникнуть внутрь устройства и изъять ящик с деньгами путем механического либо термического воздействия на аппарат.

Попытки протаранить, сплющить либо увезти банкомат с места его расположения относятся к категории нападений с применением грубой силы и также имеют целью получение доступа к содержимому денежных ящиков.

В Великобритании такие налеты стали происходить все чаще. С 2003 по 2004 год статистика взломов и попыток кражи банкоматов выросла на 29% – об этом сообщает мобильное подразделение реагирования городской полиции Лондона. Одни лишь потери наличных денег составили при этом примерно шесть миллионов фунтов стерлингов в год. Хотя в США эта статистика заметно ниже, потери все же весьма значительны – подсчеты показывают, что ежегодный урон банковскому бизнесу, наносимый физическими взломами банкоматов, превышает 4,5 миллиона долларов в год. При этом 80% преступлений – в среднем около трех сотен в год – приходятся на факты похищения банкомата с места его установки целиком.

Существует еще одна очень простая атака. Основывается она на последовательности действий, заложенной в банкомат. Так, после получения положительного ответа от банка о

выдаче суммы, банкомат отдаёт команду диспенсеру и начинает отсчитывать необходимое количество банкнот, отдается команда ридеру на возврат карты клиенту. До тех пор, пока клиент её не заберет деньги ожидают в лотке выдачи, а створка лотка будет закрыта. Вот только если мошенник придерживает карточку – она застревает в ридере. А деньги уже находятся в устройстве выдачи, только дверца закрыта. При помощи отвертки или ломика мошенник отжимает створку лотка и достаёт деньги. В это же время банкомат отправляет отчет в банк о неуспешной операции, и списанная сумма возвращаются на счёт. В результате преступник забирает деньги, но карточка тоже у него в руках. А по факту, выдача денег банкоматом не была зафиксирована и списания со счёта не происходило.

2. Аппаратные методы. Для преступника интерес представляют встроенный компьютер, сетевое оборудование, а также основные периферийные устройства – картридер и диспенсер. Атаки на эти компоненты позволяют перехватить карточные данные, вмешаться в процесс обработки транзакции процессинговым центром или отправить команду на выдачу купюр диспенсеру. Для проведения атак злоумышленнику нужно получить физический доступ в сервисную зону банкомата либо подключиться к сети, в которой находится банкомат.

Если не обеспечивается защита данных, передаваемых между банкоматом и процессинговым центром, злоумышленник может вмешаться в процесс подтверждения транзакции. Для этого используется эмулятор процессингового центра, который одобрит любой запрос, поступивший от банкомата, и в ответ отправит команду на выдачу денег.

Некоторые группы злоумышленников начали вести элементарный подсчет времени после вскрытия, а особо «технологичные» стали сверлить отверстия в корпусе технологического отсека банкомата, выламывать рекламные панели или выпиливать части корпуса, таким образом, избегая срабатываний сигнализации вообще. Так появился метод «параллельного подключения своего управляющего оборудования к шине или подмена управляющего оборудования», получивший название *black box.*

Просверлив отверстие в лицевой панели банкомата, злоумышленники могут добраться до кабеля диспенсера. Получив доступ к кабелю, злоумышленник может напрямую подключить диспенсер к своему устройству, запрограммированному для отправки команд на выдачу купюр.

С помощью аппаратных средств такой перехват данный возможен во время передачи данных между ОС банкомата и картридером. В ходе этой атаки между системным блоком банкомата и картридером подключается устройство, которое перехватывает содержимое дорожек магнитной полосы платежных карт. Подобные атаки возможны из-за отсутствия аутентификации и шифрования данных при взаимодействии с картридером и передачи данных карты в открытом виде. Эти недостатки были обнаружены во всех исследуемых банкоматах.

Долгое время преступники использовали физические накладки на картридер – скиммеры, которые считывали информацию непосредственно с магнитной полосы.

Так называемый шиммер устанавливается в устройство для чтения карт, причем злоумышленник может проделать эту операцию за считанные минуты, делая вид, например, что производит легитимное изъятие денежных средств. Шиммеры записывают в процессе всю необходимую атакующему информацию. Позже эта информация извлекается злоумышленником и используется для создания поддельной копии карты.

Половина случаев мошенничества приходится на кэш-трэппинг. *Cash-trapping* можно перевести как «захват денег». Из названия понятна суть этого метода. Существует множество видов кэш-трэппинга, но принцип у всех один – нарушить работу шаттера (механизм, выдающий наличность). Мошенники с помощью специальных приспособлений нарушают работу шаттера и ждут, когда кто-то воспользуется банкоматом для снятия денег. Терминал не может выдать наличность, так как она застревает, тогда операция отменяется. Злоумышленнику остается только достать купюры из аппарата.

3. Программные методы. Появление специального вредоносного программного обеспечения (ПО) для банкоматов предоставило преступникам более изящную и неприметную альтернативу физическому взлому. Ранее их методы ограничивались либо традиционным взломом сейфового замка с помощью лома или болгарки, либо эффектным подрывом банкомата с применением горючей газовой смеси. Разумеется, ни один из этих способов нельзя назвать тихим и незаметным.

В схеме кражи денег из банкоматов с помощью вредоносных программ можно выделить четыре принципиальных этапа:

– злоумышленник получает доступ к машине, локальный или удаленный;

– производится инжектирование вредоносного кода в систему банкомата;

– как правило, за заражением следует перезагрузка банкомата – система перезагружается, казалось бы, в штатный режим, но в то же время оказывается под контролем вредоносной программы, т.е. злоумышленников;

– заключительный этап, т.е. цель всего действа, – хищение денег.

Существует несколько различных вариантов вредоносных программ для банкоматов.

Утилиты прямой выдачи наличных обладают функционалом, именуемым *jackpotting*, позволяющим злоумышленникам осуществить несанкционированную выдачу денег из банкомата без необходимости авторизации транзакции на стороне банка. Данный подход требует серьезной подготовки и реализуется, как правило, организованными преступными группировками.

Программные методы взлома банкоматов осуществляются путем удаленного внедрения вредоносного ПО, предполагающее предварительную компрометацию внутренней корпоративной сети банка, получение административных привилегий и дальнейшее распространение вредоносного кода на сеть банкоматов от легитимного с точки зрения самих конечных устройств источника.

Для проведения атак на сетевом уровне злоумышленнику прежде всего необходим доступ к сети, к которой подключен банкомат. Если злоумышленник – сотрудник банка или провайдера, то у него есть возможность получить доступ удаленно.

В других случаях требуется физическое присутствие, чтобы открыть сервисную зону, отключить *Ethernet*-кабель от банкомата и подсоединить свое устройство до модема или вместо него. Затем злоумышленник сможет подключиться к этому устройству и проводить атаки на доступные сетевые службы или атаки типа «человек посередине». Иногда модем расположен снаружи банкомата, и для того, чтобы подключиться к сетевому кабелю, не нужно даже иметь доступ к сервисной зоне.

Обойти установленные средства защиты и получить контроль над диспенсером возможно при подключении к жесткому диску банкомата.

Самый простой способ – напрямую подключиться к жесткому диску. Если содержимое диска не зашифровано, злоумышленник может записать на него вредоносную программу, содержащую команды для взаимодействия с диспенсером. Затем эту программу необходимо добавить в белый список приложения *Application Control* – для этого достаточно внести изменения в конфигурационные файлы. Далее при загрузке банкомата в рабочем («защищенном») режиме защитное ПО запустится и будет функционировать, но нарушитель сможет выполнить произвольный код с использованием вредоносного ПО. Злоумышленник может и вовсе отключить средства защиты, например, удалить файлы с диска.

4. Психологические методы. Многие схемы мошенничества, связанные с банковскими картами, основаны на технологии социальной инженерии. Они предполагают вытягивание из клиента конфиденциальной информации с использованием различных каналов коммуникаций (например, просят сообщить по телефону реквизиты банковской карты, одноразовые пароли) либо убеждение в совершении тех или иных действий под различными предлогами.

Иногда мошенники в процессе звонка просят установить на телефон специальное приложение якобы для лучшей защиты – им оказывается программа удаленного доступа и

управления, с помощью которой можно зайти в личный кабинет онлайн-банка жертвы и перевести оттуда деньги на свой счет.

Программы удаленного доступа помогают не только украсть все имеющиеся деньги, но и оформить в мобильном приложении предодобренный кредит, если такой продукт предлагается клиенту, а затем вывести и заемные средства.

В последнее время стали появляться более сложные схемы: к звонкам от «банковских работников» добавились звонки от «правоохранительных органов», которые «подтверждают», что кто-то пытается украсть деньги клиента, поэтому их надо спасти путем перевода на «безопасный» счет.

Во время пандемии и перехода многих процессов в онлайн-формат киберпреступники также активизировались в интернете. По данным экспертов, за первое полугодие 2020 года мошенникам удалось украсть в интернете свыше 2 миллиарда рублей, то есть более 50% из общего объема похищенных за этот период средств. Зафиксирован значительный, почти в семь раз, рост количества сайтов в категории мошеннических: лже-опросы, лже-компенсации, лже-выигрыши и так далее.

Также мошенники создают поддельные сайты банков, чтобы узнать данные для входа в личный кабинет.

Кроме того, на руку мошенникам переход по ссылкам из непроверенных источников, скачивание сомнительных приложений, игнорирование установки антивируса и его предупреждений. Все это позволяет злоумышленниками получить логины и пароли от личного кабинета или первичные данные по банковской карте.

Заключение. Таким образом, были рассмотрены все возможные способы взлома банкоматов и получения данных банковских карт злоумышленниками. На основные этого был проведен анализ безопасности банкоматов. Необходимо отметить, что несмотря на то, что современные банкоматы обладают достаточно серьезными функциями защиты, этого недостаточно, чтобы полностью предотвратить их взломы. Злоумышленники придумывают все более изощренные методы атаки. Поэтому необходимо постоянно быть бдительными, обращать внимание на подозрительное окружение, и, в случае необходимости, незамедлительно обращаться в ваш банк. Банки в свою очередь должны постоянно совершенствовать и модернизировать банкоматы, тем самым обеспечив им физическую защиту.

Список литературы

1. *Берлин А.Н., – Терминалы и основные технологии обмена информацией. – М.: Бином, 2014.*
2. *Anti-Malware – Способы атак на банкоматы и их последствия [Электронный ресурс]. – Электронные данные. – Режим доступа: https://www.anti-malware.ru/analytics/Threats_Analysis/atm-attacks*
3. *Искусство управления информационной безопасностью – Как воруют деньги с наших пластиковых карт [Электронный ресурс]. – Электронные данные. – Режим доступа: http://www.iso27000.ru/chitalnyi-zai/bezopasnost-elektronnyh-platezhei/kak-voruyut-dengi-s-nashih-plastikovyh-kart*
4. *Областной центр социальной защиты населения – Безопасное использование банковских карт [Электронный ресурс]. – Электронные данные. – Режим доступа: https://xn-jtbeshedqe3c.xn--p1ai/fingram/bankkart.php*

UDC 004.056

ATM SECURITY THREATS

Mosunov A.A.

Belarusian State University of Informatics and Radioelectronics, Minsk, Republic of Belarus

Alefirenko V.M. – PhD, associate professor

Annotation. The main threats to the security of ATMs, methods of physical influence, hardware, software and psychological methods of influence on ATMs are given. Methods of attackers' actions to obtain confidential information and various types of human manipulation are presented.

Keywords: attack, ATM, bank card, hacking, information protection, manipulation, methods of influence, physical protection, operating system, software, security system.