Мошенничество с использованием банковских карт
и способы борьбы с ним

Алексей Гребенюк

Старший консультант по безопасности FortConsult A/S

Максим Тигулев

Руководитель направления дизайна и внедрения решений Radian-QS

Во всем мире наметилась устойчивая тенденция к росту карточных хищений. По данным Cards Business Review, список стран с высоким уровнем пластиковой преступности возглавляет Украина - 19% всех случаев мошенничества, далее следуют Индонезия - 18,3%, Югославия - 17,8%, Турция - 9% и Малайзия - 5,9%. В Соединенных Штатах, где карточный оборот очень велик, совершается лишь 1,7% всех преступлений. Целью любого киберкриминалитета являются деньги. Для их отъема придумываются и используются многочисленные методы и технологии - пишутся вредоносные программы, взламываются серверы предприятий, крадутся персональные данные и т.п. Сегодня ясно, что киберпреступность - это большой бизнес, оборот денег которого зачастую больше, чем в торговле наркотиками, а риски быть пойманным и наказанным при этом существенно меньше.

В случае с картами для преступников существует два наиболее очевидных пути: получить доступ к банкомату, либо приобрести по украденной или поддельной карте товары, с целью их последующей продажи.

Объект атаки - банкомат

Банкомат (Automatic Teller Machine - ATM) считается одним из наиболее важных технологических изобретений XX века, так как он способен обеспечивать наличными миллионы держателей банковских карт двадцать четыре часа в сутки, семь дней в неделю.

Банкоматы упростили финансовые операции и стали важной точкой соприкосновения между клиентами и банками. Согласно последним исследованиям розничных банковских сетей, сегодня в мире более 2 миллионов ATM, а к 2015 году их будет уже 3 миллиона.

Популярность среди потребителей, простота использования и прямой доступ к наличным деньгам делают банкоматы объектом номер один в списке мошенников. Этот факт в сочетании с высоким уровнем посткризисной безработицы привел к увеличению числа преступлений, так или иначе связанных с этим оборудованием. Все более изощренными становятся копирование информации с магнитной полосы карточки (скимминг), установка ловушек для купюр в банкомат, хакерские атаки. Все эти факторы привели к значительным потерям наличности за последние годы.

Публичность и доступность ATM и есть основная причина того, что они являются предметом массовых внешних фродов для банков.

Атаки на банкоматы делятся на физические нападения и на ATM - мошенничества. Физические нападения, как правило, совершаются с целью получения доступа к наличности или другим ценным активам, находящимся в сейфах банкоматов. Некоторые из наиболее распространенных методов включают увоз банкомата, взрыв (с применением газа или без него), вскрытие (с использованием роторной пилы, паяльной лампы, термобурения или алмазной резки). Успех физического нападения определяется количеством украденного и скоростью, с которой совершается атака.

Что касается ATM-мошенничества, то здесь есть много различных категорий. Говоря обобщенно, мы можем подвести под эту категорию любую сознательно реализуемую "криминальную" технику, которая позволяет преступнику извлечь "выгоду" из банкомата. Наиболее распространенными видами ATM-мошенничества являются:

- кража карточки (так называемая "ливанская петля");
- кража ПИН (так называемый "заплечный серфинг");
- скимминг (копирование информации с магнитной полосы карточки);
- установка ловушек для купюр в банкомат (так называемая "ловушка для налички");
- "отмена операции";
- киберскимминг;
- мошенничество при депозитных операциях.

Новостью стало появление "подложных" банкоматов (Киев, ТРЦ "Караван"), когда был установлен внешне полностью легитимный банкомат с надписью, призывающей снять наличные без комиссий держателям карт четырех крупных банков Украины. И только бдительность сотрудников служб безопасности одного из крупных игроков украинского карточного бизнеса позволила вскрыть эту мошенническую схему.

Банкомат (Automatic Teller Machine - ATM) считается одним из наиболее важных технологических изобретений XX века, так как он способен обеспечивать наличными миллионы держателей банковских карт двадцать четыре часа в сутки, семь дней в неделю

Эксперты по вопросам безопасности банкоматов считают скимминг одним из наиболее распространенных видов ATM-мошенничества. Скимминг предполагает создание копии информации, закодированной на магнитной полосе карты. Скиммер (устройство для скимминга) может быть присоединено к ATM-слоту извне или может поджидать вашу карточку непосредственно внутри банкомата. Устройства для скимминга имеют различные формы и размеры, а также различаются по сложности и конфигурации. При наиболее изощренной установке они не прерывают нормальную работу банкомата, карта держателя принимается ридером и возвращается к владельцу, однако с магнитной полосы копируется нужная мошеннику информация. Одно из наиболее эффективных устройств для скимминга известно как "софий-

ский вариант". Приспособления опытных скиммеров очень сложно обнаружить невооруженным глазом.

Но, какими бы сложными ни были мошеннические приспособления, многие банки и международные компании успешно ведут борьбу со скимингом с помощью технологических инноваций. В настоящее время в Европе более 20 млн. операций ежедневно проводятся под защитой технологии CPK+ от компании TMD Security - лидера в области создания инструментов по борьбе со скимингом. Этот успех объясняется применением инновационной защиты устройств изнутри. Технология CPK+ совместима со всеми типами банкоматов и терминалов самообслуживания, ее базовые устройства легко устанавливаются, при этом программное обеспечение терминала не нуждается в дополнительной настройке.

В начале "эпохи скимминга" банки массово столкнулись со считывающими накладками, устанавливаемыми мошенниками на банкоматы. Несмотря на эффективность данного устройства с точки зрения преступников, реализация данного вида мошенничества весьма сложна и затратна (всегда должно присутствовать подставное лицо - дроп, которое устанавливает и снимает накладку). Видимо, тогда впервые и возникла мысль о программном скимминге. Ведь драйвер картридера полностью считывает магнитную полосу платежной карты.

Банкоматы и платежные терминалы быстро переходят на системы с элементной базой Intel, операционные системы на базе Microsoft Windows и используют протоколы TCP/IP. Все это серьезно увеличивает риски атак на данные устройства, и такие прецеденты уже были.

Чтобы достичь успеха на этом направлении, киберпреступники начали разрабатывать индивидуальные или, как принято говорить, целевые (таргетированные, от англ. targeted) атаки.

Хорошим примером целевой атаки явился взлом платежной системы RBS WorldPay в ноябре 2009 года, когда в банкоматах 280 городов мира за 15 минут была украдена сумма, приблизительно равная 9 млн. долл. США.

И все же киберпреступникам нужна большая анонимность. Поэтому в последнее время мошенники все чаще пытаются получить доступ к наличным деньгам с помощью разнообразных компьютерных программ. Вредоносное ПО вводится в банкомат посредством сетевых атак, инсайдеров или дропов с помощью других зараженных устройств. После проникновения в ПО банкомата, вредоносное программное обеспечение будет собирать информацию о транзакциях. Взломанный банкомат физически ни чем не отличается от нормального, и пользователи по внешним признакам никак не могут получить информацию об опасности.

Первый троян для банкоматов, разработанный под платформу DieBold Agilis, как раз и реализует принципы программного скимминга. При этом заложенные авторами возможности очень широки, что говорит, как минимум, об их хороших знаниях программной "начинки" конкретного АТМ. Данное зловредное ПО представляет собой комплекс для считывания и хранения магнитной полосы и перехвата ПИН-кода. Технически в нем даже заложена функциональность инкассации.

Перехваченные программой данные сохраняются в памяти и могут выдаваться при предъявлении мастер-карт разного уровня доступа. При этом информация может распечатываться на принтере банкомата, записываться на специальную карту или показываться на экране.

Негативный опыт Diebold не должен создавать впечатление, что уязвимы банкоматы какого-то конкретного бренда. Технология уже отработана, значит, до появления новых семейств, "заточенных" под продукцию других вендоров, осталось не так много времени. Специалистам по безопасности надо готовиться к новым целевым атакам…

Какие же существуют варианты защиты программного комплекса АТМ и денег держателей платежных карт? Первый и основной - установка средств безопасности на АТМ. Это сигнализация на дверцы сервисной зоны и программы обеспечения информационной безопасности (межсетевой экран и средства борьбы с вредоносным кодом). При этом следует очень внимательно следить за рекомендациями вендора, чтобы средства информационной безопасности из друга не превратились во врага. Ведь, по сути, сканирующий модуль антивируса по принципу работы ничем не отличается от действий троянской программы при выполнении операции чтения карты.

Поэтому выходом в данном случае может быть применение средств информационной безопасности, построенных на иных принципах, нежели простой сигнатурный анализ. Например, таких, как программы, предоставляемые NCR - одним из ведущих поставщиков АТМ. Продукты, подобные Solidcore для Aptra компании NCR останавливают введение несанкционированного кода в банкомат, защищая систему от программного скимминга.

Вместо того чтобы реагировать на разнообразные атаки по мере их появления, Solidcore для Aptra действует проактивно, позволяя банкомату выполнять исключительно авторизированные команды. В частности, Solidcore для Apt-

ra создает и обновляет учетную запись "хороших" кодов и позволяет загружаться только тем кодам, которые проиндексированы в учетной записи, или "белом списке". Естественно, авторизированный код не может быть модифицирован, удален или подменен вредоносным ПО.

Несмотря на вышеописанные угрозы, каждый день в мире безопасно проводятся миллионы АТМ-операций. По сравнению с огромным количеством успешных транзакций в более чем 2 миллионах банкоматов по всему миру, только очень небольшой процент оказывается связанным с криминалом.

Угрозы, связанные с повседневной эксплуатацией АТМ, известны как производителям, так и специализированным организациям, которые профессионально занимаются вопросами обеспечения безопасных платежей, например, ATMIA или European ATM Security Team (EAST, https://www.european-atm-security.eu/), члены которой профессионально противодействуют атакам на АТМ.

Многие компании, среди которых и FortConsult A/S, сотрудничают с обеими организациями. Так, например, недавно FortConsult A/S вступил в EAST для более качественного взаимодействия, поскольку только участники этой организации имеют доступ к внутренним отчетам и могут реально оценивать уровень угроз и рисков, свойственных каждой стране, в частности, России и Украине.

Объект атаки - POS

Торговые точки или POS (Point of sale) также являются объектом атаки для карточных мошенников.

В самом начале становления карточного бизнеса, в том числе и в России, считалось, что присутствие в торговой точке кассира, обученного тщательно проверять карту и следить за поведением клиента, поможет снизить риски мошенничества. Теория того времени, например, говорила, что преступник должен покупать все товары подряд, невзирая на цену, и складывать их в корзину трясущимися руками.

Однако на практике существенную роль играет человеческий фактор: во-первых, не каждый кассир - психолог, во-вторых, у него много другой ответственной работы, в-третьих, настоящего профессионального мошенника выявить невозможно - он прилично одет и спокойно покупает дорогой товар.

Современный бизнес, особенно розничный, предъявляет жесткие требования по скорости обслуживания клиентов - от этого зависит проходимость магазина и, соответственно, выручка. В последние пару лет мы наблюдаем, как POS-терминалы поворачиваются буквально "лицом к клиенту" (сети "Макдональдс", "Старбакс", гипермаркеты "Ашан"), то есть операцию оплаты по карте клиент совершает сам, не давая карту в руки кассиру. При этом по части операций на небольшие суммы подпись клиента не запрашивается, карта не проверяется, кассовый чек не выдается.

Торговые точки или POS (Point of sale) также являются объектом атаки для карточных мошенников.

Это очень удобно для торговца, но порождает новые риски для банков и их держателей карт - как показывает статистика, в такие точки теперь устремились любители легкой наживы, причем не очень высокой квалификации. В терминалы самообслуживания уже пытались предъявить к оплате даже "белый пластик" - карты с записанной на них краденной магнитной полосой, также были зафиксированы случаи сговора преступников с кассирами.

В целом, можно сказать, что на данный момент фрод в банкоматах даже более контролируем, чем в торговых точках, так как мошенники только пробуют подходы к новым системам, и основная волна мошенничеств в новых условиях еще не подошла.

Но специалисты по информационной безопасности, а также компании-интеграторы уже готовятся к ней, заранее планируя меры противодействия. Для тех же крупных торговых сетей разработаны и внедрены системы проактивного мониторинга операций, которые позволяют защитить держателя карты и предотвратить совершение операции, если она является подозрительной.

Таким образом, жизнь не стоит на месте, война "щита и меча" продолжается по всем фронтам. Поэтому при проектировании информационных систем необходимо обращаться к специалистам по интеграции и безопасности, чтобы учесть в проектах не только требования стандартов, но и самые последние угрозы, а также новые методы работы киберпреступников.