Кибербезопасность банкоматов: что противопоставить «прямому диспенсу»?

Традиционный подход с навесными средствами программной защиты не обеспечивает требуемые темпы распространения обновления банкоматного ПО в защищенном режиме

Светозар Яхонтов,
директор по развитию бизнеса ООО «Протекшен Технолоджи»

Банальным будет повторять традиционные для отрасли безопасности «страшилки» про то, как хакеры атакуют сети банкоматов. Как известно, волки из сказок не страшны, пока не покусают.

Приведем статистику. Исходя из нашей практики более 40% реализованных нашей компанией проектов по защите ПО устройств банковского самообслуживания – постинцидентные. За 2014–2016 гг. на территории Российской Федерации произошло более сотни инцидентов атак типа «прямой диспенс» на банкоматы в двух десятках банков. Ряд банков подвергся повторяющейся серии атак, поскольку у них не хватило ресурса оперативно реализовать контрмеры на территориально распределенной сети устройств.

Часто факт инцидента выявлялся спустя неделю и более после самой атаки службой экономической безопасности как недостаток купюр в кассетах по итогам очередной инкассации. За такой срок проведение мероприятий по горячим следам имеет низкую вероятность успеха. В подавляющем большинстве случаев потерпевшие не разглашали информацию об инцидентах, репутационный риск наступает не после инцидента, а после огласки.

Продемонстрированная низкая степень готовности банков реагировать на инциденты повлияла на ощущение безнаказанности у организаторов атак. Полученные преступниками средства эффективно инвестируются в подготовку новых акций, с соответствующим ресурсным и методическим обеспечением.

Подобная ситуация стала возможной вследствие следующих моментов:

- Безучастность служб, ответственных за меры технической защиты и реакции на инциденты в вопросах эксплуатации сети устройств самообслуживания. Во многих, чаще крупных, банках инфраструктура дистанционных каналов обслуживания не входит в область контроля служб информационной безопасности. Так сложилось исторически в период активной экспансии каналов дистанционного обслуживания.
- Не поддерживаемые и не обновляемые версии операционных систем и прикладного ПО, что делает программную среду банкомата уязвимой.

В то же время многие (преимущественно крупные) банки имели возможность уделить внимание вопросам защищенности программного обеспечения банкоматов. Есть примеры отдельных банков, которые можно считать «лучшей практикой» по мировым меркам.

Однако среди банков, которые в разное время начинали внедрение специализированных средств программной защиты, есть и примеры незавершенных проектов. Несмотря на достаточное финансирование проектов и доступность ресурсов для

развертывания и администрирования, эти банки не смогли преодолеть весьма распространенные стоп-факторы. Дьявол, как известно, кроется в деталях.

Ни для кого не секрет, что специализированные средства программной защиты для банкоматов реализованы на технологиях «белых списков». Этот подход наиболее оптимален, потому что зловреды для атаки на банкоматы пишут на заказ, к антивирусным аналитикам они по понятным причинам не попадают, в результате средства защиты на основе сигнатур для защиты ПО банкоматов неэффективны.

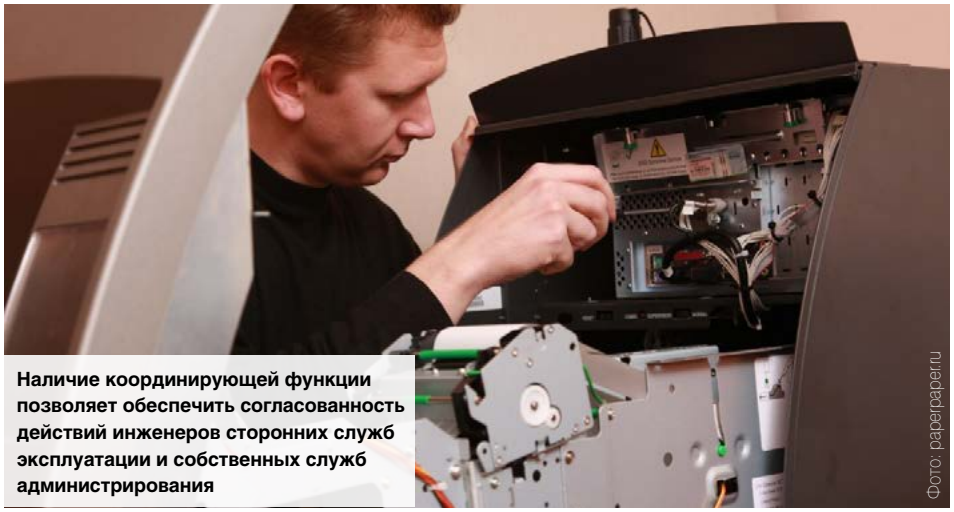

Фото: paperpaper.ru

Наличие координирующей функции позволяет обеспечить согласованность действий инженеров сторонних служб эксплуатации и собственных служб администрирования

При использовании технологий «белых списков» в программной среде устройства разрешен старт только тех процессов, которые соответствуют определенным жестким правилам:

- Соответствие контрольной суммы процесса заданному в правилах значению. Старт процесса, чья контрольная сумма отличается от заданной в правилах, блокируется.
- Расположение процессов в определенных директориях.
- Цифровые сертификаты процесса заданы в правилах.

Ситуационное внесение изменений в настройки средства защиты требует контроля за действиями инженеров «в полях»

В результате при разработке специализированных средств защиты для банкоматов (как для любых средств защиты от таргетированных атак) заложен запрет на внесение любых несанкционированных изменений в программную среду устройства. Т. е. обеспечивается некое статичное состояние защищенности, сохранение системы в последнем заведомо исправном состоянии при любых попытках деструктивного воздействия.

Однако представим себе реальную ситуацию эксплуатации ПО на банкомате.

Инженер сторонней службы эксплуатации приехал по наряду установить на банкомат обновление платежного приложения или ПО, добавляющее функционал нового банковского продукта. С собой этот инженер привез флешку с дистрибутивом или утилитой, обладающей функционалом для внесения необходимых изменений в конфигурацию ПО на банкомате.

Если инженер попытается запустить новое ПО на банкомате с функционирующей защитой, то результаты предсказуемо будут следующими:

- Старт инсталлятора будет заблокирован, т. к. его контрольной суммы нет в правилах;
- Либо после внесения изменений будут блокированы последующие попытки старта измененных исполняемых файлов.

Оба варианта нежелательны для службы эксплуатации.

В результате инженер вынужден отключить защиту на устройстве. Он вносит изменение в ПО и… оставляет банкомат. Свою работу инженер выполнил, а вопросы защищенности ПО на банкомате находятся не в его зоне ответственности.

Ожидаемо, что в этом случае внести изменения в правила контроля и включить защиту должен специалист службы эксплуатации банка, ответственный за обслуживание ПО на банкоматах. Однако практика ситуационного внесения изменений в настройки средства защиты требует высокой квалификации специалиста и контроля за действиями инженеров «в полях», что весьма ресурсоемко и трудноосуществимо.

Поэтому уже спустя квартал существенная часть банкоматов сети остается либо с отключенной защитой, либо после включения защиты неработоспособной. Учесть внесенные изменения спустя столь долгий срок не представляется возможным. Аварийное восстановление работоспособности банкомата – мероприятие весьма затратное. И после повторения ситуации один-два раза принимается решение по прекращению эксплуатации средства защиты вовсе: доступность сети устройств с точки зрения бизнеса приоритетней.

Итак, что мы имеем в итоге? Формально средства защиты развернуты. Фактически – защиты нет. Поскольку обеспечение мер защиты для службы эксплуатации банкоматов не является определяющим KPI, то сложившаяся ситуация остается таковой долгое время. Пока практика применения средства защиты вовсе не утратится.

Практика банков, реализовавших режим безопасной эксплуатации ПО на сети банкоматов, отличается наличием координирующей функции, позволяющей обеспечить согласованность действий инженеров сторонних служб эксплуатации и собственных служб администрирования. Это достигается наличием внедренных практик управления нарядами на проведе-

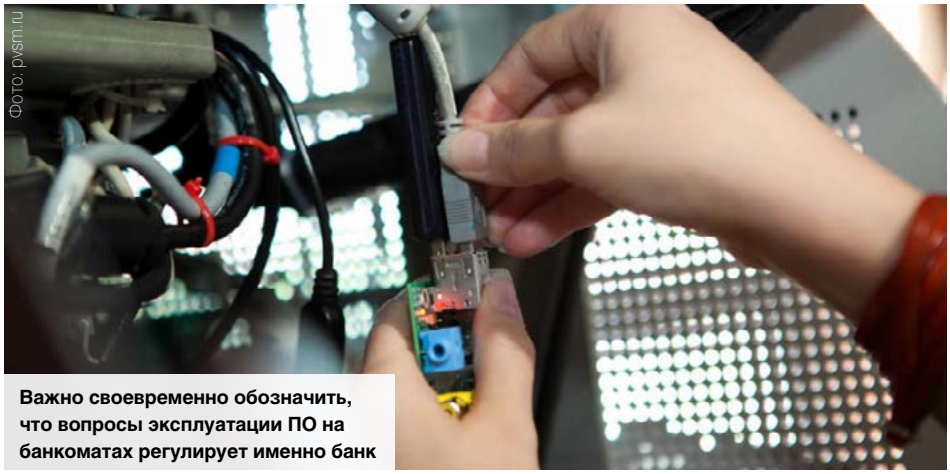
Фото: pysm.ru

Важно своевременно обозначить, что вопросы эксплуатации ПО на банкоматах регулирует именно банк

ние работ со сквозной информатизацией. В России таких банков нет. Автору статьи приходилось наблюдать подобную практику лишь в двух банках в Восточной Европе.

Задачу можно решить и другим способом – путем применения функционала контроля использования доверенных инсталляторов в сети банкоматов. При этом осуществляются следующие шаги:

- Дистрибутив перед передачей сторонней службе эксплуатации проходит внутреннюю проверку на совместимость с программной средой сети устройств.
- Проводится проверка корректности работы нового требуемого и старого актуального функционала.
- Проводится проверка дистрибутива на наличие известных вирусов, критичных уязвимостей компонент ПО, а также соответствия предполагаемой технологии развертывания политикам безопасности.
- После проведения всех проверок дистрибутив либо подписывается сертификатом банка, либо, при наличии такового, сертификат доверенного издателя дистрибутива заносится в «белый список». Правило распространяется групповыми политиками на клиентские модули средств защиты на устройствах
- Проверенный дистрибутив передается службе эксплуатации для развертывания на устройствах.

Теперь при запуске такого инсталлятора внесенные изменения автоматически будут добавлены в правила контроля. Это обеспечивает возможность внесения только санкционированных изменений в ПО устройств самообслуживания без необходимости отключения защиты.

На этом моменте стоит остановиться подробнее. Приведем обратный пример: при создании «золотого образа» (системный образ эталонного устройства) инженеры банка внесли в состав ПО дистрибутив плеера для проигрывания рекламного контента на устройствах самообслуживания. Дистрибутив был скачан из недоваренного источника и содержал набор файловых вирусов и бекдоров. Обнаружить заражение удалось спустя несколько месяцев после развертывания «золотого образа» на территориально распределенной сети устройств.

По нашей статистике, около 80% банков в России использует в качестве средства удаленного администрирования на устройствах решение RAdmin. Сам функционал и доступные привилегии данного средства администрирования являются брешью в защите без реализации дополнительных мер контроля (ограничения системных привилегий обеспечивающих процессов, ограничение сценариев запуска, ограничение сетевой активности процессов и т. д.). При этом клиентская часть данного средства администрирования распространяется с использованием скриптов, содержащих в открытом виде пароль и порты, и не удаляется из файловой системы после развертывания.

Подобное стало возможным вследствие отсутствия внутреннего контроля за использованием ПО на устройствах самообслуживания.

По нашему опыту, внедрение вышеописанной практики контроля за внесением изменений в ПО устройств осуществляется достаточно легко. Уже через несколько недель количество ситуаций, когда инженер сторонней службы эксплуатации не смог выполнить работы по наряду вследствие отсутствия согласованной банком версии дистрибутива, сводится к нулю. Важно своевременно обозначить, что вопросы эксплуатации ПО на банкоматах регулирует именно банк.

Наиболее продвинутые практики реализации режима безопасной эксплуатации ПО на устройствах самообслуживания мы наблюдаем у отдельных операторов крупных сетей устройств в странах Юго-Восточной Азии. Высокие темпы проникновения как традиционных, так и новых банковских услуг в регионе, высокая степень детерминации услуг для разных категорий клиентов требуют весьма оперативно и регулярно вносить обновления и новое ПО, обеспечивающее функционал новых банковских продуктов. Использование традиционного подхода с навесными средствами программной защиты не обеспечивает требуемые темпы распространения обновления в защищенном режиме. Технические меры защиты реализуются в функционале самих платежных приложений:

- Самозащита собственных компонент платежных приложений от попыток несанкционированной модификации.
- Механизмы безопасного внесения изменений в ПО.
- Средства мониторинга активности процессов.

В своей совокупности эти подходы позволяют выводить новые банковские продукты оперативно, реализовывать мощную выталкивающую модель предложения, не ограничиваемую излишними процедурами контроля.