KASPERSKY lab

БЕЗОПАСНОСТЬ БАНКОМАТОВ И POS-СИСТЕМ

Как обеспечить безопасность критически важных платежных устройств

www.kaspersky.ru

ПРОБЛЕМЫ

Встроенные системы, например банкоматы, имеют ряд специфических уязвимостей. Как правило, они распределены по большой территории, их сложно контролировать, и они редко обновляются. Банкоматы и кассы, через которые «проходят» наличные деньги и данные кредитных карт, крайне привлекательны для киберпреступников. Таким устройствам требуется направленная интеллектуальная защита высочайшего уровня.

Проблема медленных циклов обновления и старых операционных систем существует во многих высокотехнологичных сферах — например, в промышленном секторе. Многие космические спутники также используют программы и устройства, которые устарели уже десятки лет назад. Эта проблема затрагивает и такие динамично развивающиеся отрасли, как финансовые организации и ритейл.

В банковском секторе эти проблемы распространяются не только на конечные устройства: внутренние автоматизированные системы банков тоже зачастую не обновляются годами. Что же касается банкоматов, то около 80% банков предпочитают дожидаться конца жизненного цикла устройств (то есть 5–10 лет, а то и дольше) и только тогда покупать новые машины со свежими программами, вместо того чтобы регулярно обновлять существующие.

Самой популярной операционной системой для банкоматов и POS-систем до сих пор является семейство Windows® XP. Прекращение поддержки этой ОС ударило по многим компаниям и государственным органам. Особенно от этого пострадали финансовые организации, ведь на операционной системе Windows XP Professional for Embedded Systems до сих пор работает множество банкоматов. Microsoft® перестала поддерживать эту версию системы наряду с домашними версиями еще в апреле 2014 года.

Замена банкоматов и POS-систем — это дорогой, долгий и болезненный процесс. Кроме того, при обновлении программ часто приходится заменять устаревшее, но все еще работающее аппаратное оборудование.

УГРОЗЫ

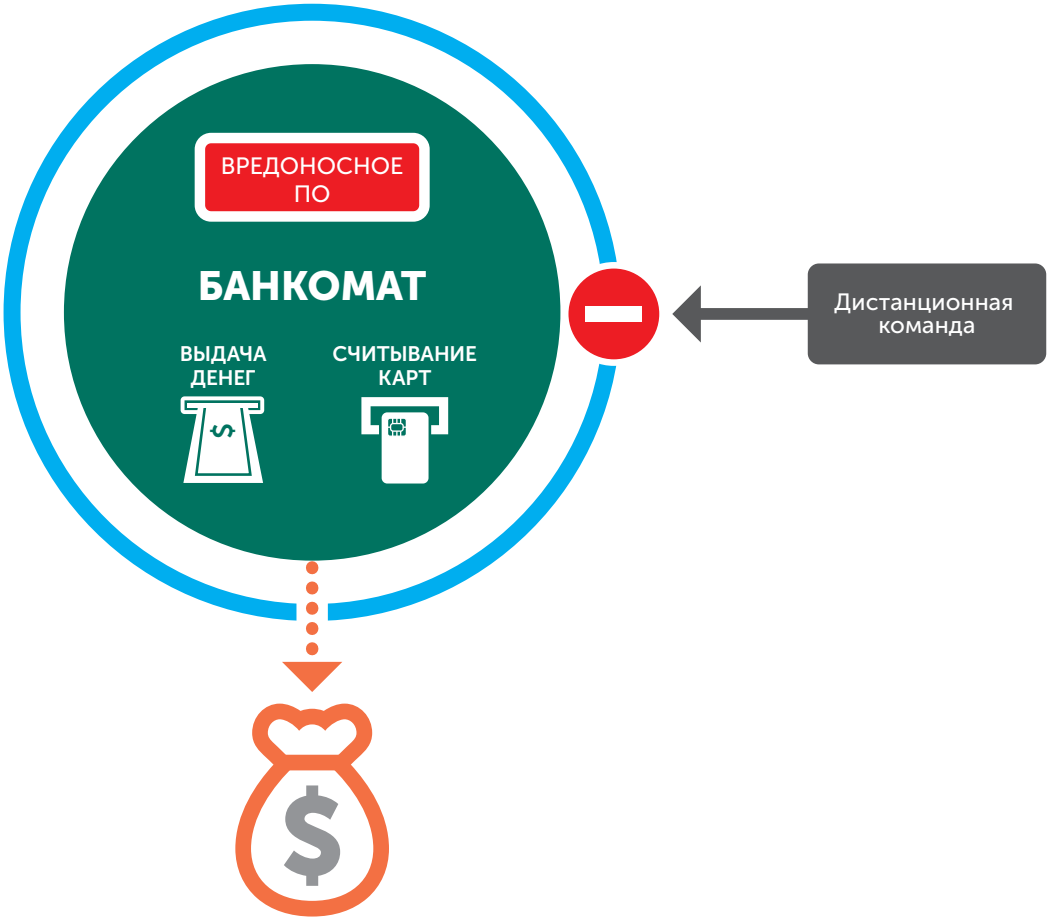
Банкоматы охраняются куда менее тщательно, чем банки, хотя в них хранятся наличные деньги. А в POS-системах содержится личная информация и данные о кредитных картах. И те и другие — желанные цели киберпреступников.

В 2009 году киберпреступники провели первую серьезную атаку на банкоматы при помощи вредоносной программы Skimer. С тех пор кибератак проводится все больше, и они становятся все изощреннее. В 2015 году киберпреступники побили новые рекорды. Появились такие программы, как Ploutus, Tyupkin, Carbanak, CardStealer, vSkimmer, Chewbacca, POSeydon и FindPOS.

Обычные антивирусы не могут защитить банкоматы от новых угроз. К тому же их сложно установить на устаревшие банкоматы с несовременным ПО и медленным соединением. В результате вирусы по-прежнему ежедневно попадают в системы банкоматов и касс крупнейших банков и магазинов.

Профессиональные хакеры все чаще пишут программы для взлома конкретной сети банкоматов или POS-систем. Причина понятна: кибератака на банкомат — это простой и быстрый способ заработать. Но она также может быть частью более масштабной диверсии. Такие целевые атаки, как Carbanak, могут привести к потере миллиардов долларов США.

СХЕМА НАПАДЕНИЯ НА БАНКОМАТ



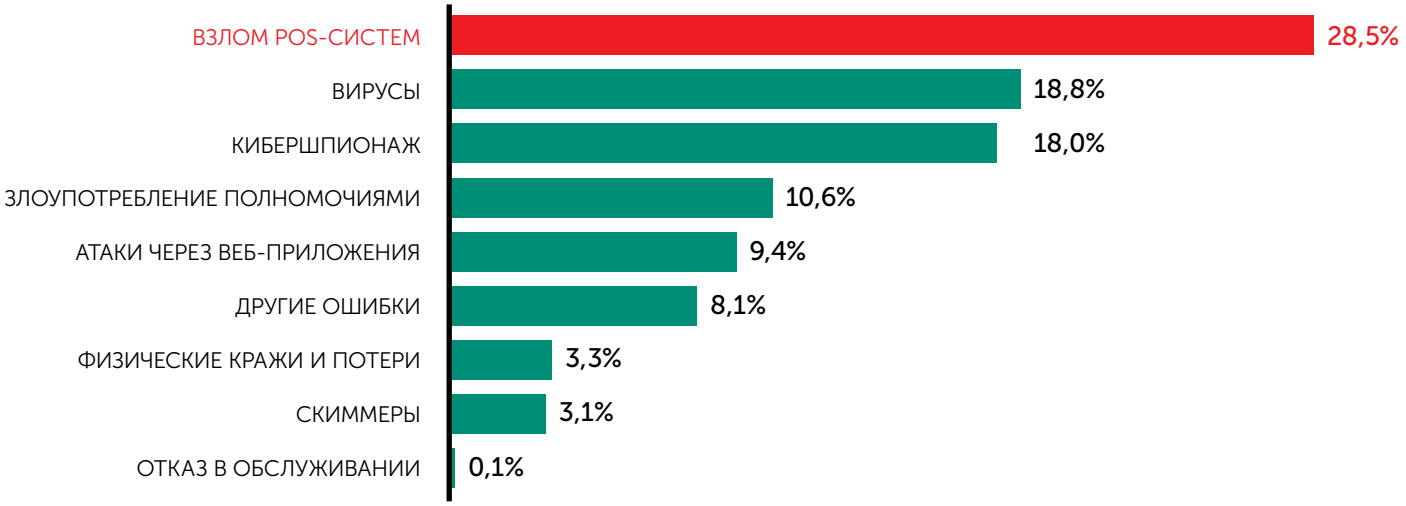
Банкоматы, распределенные по широкой территории, — идеальная цель для направленной кибератаки через вредоносную программу. USB-порт и клавиатура расположены в закрытом на простой замок шкафчике с передней или боковой стороны банкомата, что очень удобно для преступников.

Но замок, возможно, даже не придется взламывать. Инженеры техобслуживания нередко выводят USB-кабель за пределы шкафчика, чтобы им не приходилось каждый раз искать ключи. К сожалению, просто отключить USB-порты и CD-дисководы нельзя: они действительно нужны инженерам для регулярного обслуживания.

После того как вирус проник в сеть через один из банкоматов, он может на какое-то время «затаиться», собирая информацию и готовясь к нападению. В определенный момент — например, при вводе конкретной карты или PIN-кода — вирус запустит процесс изменения системы, и зараженные банкоматы отдадут преступникам все хранящиеся в них деньги.

УГРОЗЫ, НАПРАВЛЕННЫЕ НА POS-СИСТЕМЫ

Статистика нарушений безопасности в IT

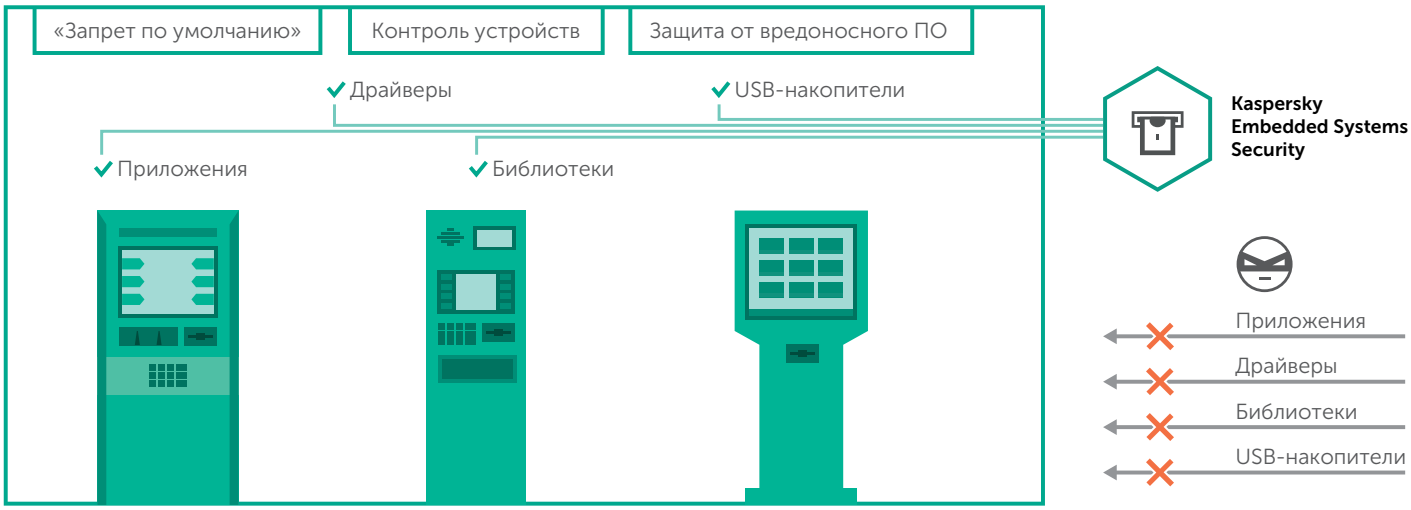


ОТЧЕТ О РАССЛЕДОВАНИЯХ ВЗЛОМОВ, VERISON, 2015

Одна из главных уязвимостей POS-систем – это межплатформенные программы. Как правило, они создаются небольшими сторонними компаниями или внутренними IT-отделами. Часто в таких программах функциональности уделяется больше внимания, чем безопасности. Как и в случае с банкоматами, легкий доступ к USB-портам и CD-дисководам может считаться удобством, а не уязвимостью.

Большинство касс работает с кредитными и дебетовыми картами, поэтому, как и банкоматы, они должны соответствовать стандартам PCI DSS. Все они без исключения работают с личной информацией клиента – и владелец POS обязан ее защищать. Наконец, все они подключены к внутренней сети, а значит, легко уязвимы для целенаправленных атак.

KASPERSKY EMBEDDED SYSTEMS SECURITY



«Лаборатория Касперского» создала решение для защиты банкоматов, кассовых систем и киосков самообслуживания. Оно создано с учетом актуальных угроз, функционала устройств, особенностей операционных систем, соединений и архитектуры. Решение полностью совместимо с семейством Windows XP.

Решение Kaspersky Embedded Systems Security позволяет снизить риски, присущие всем встроенным системам и разработано специально для банкоматов и POS-систем. Оно защищает специфические для этих архитектур уязвимости и учитывает особенности работы программ и устройств. Одна консоль с интуитивно понятным управлением позволит управлять многоуровневой системой безопасности на всех системах и во всей IT-инфраструктуре.

Режим «Запрет по умолчанию» для приложений, драйверов и библиотек в сочетании с функцией контроля устройств – надежный способ обеспечить безопасность эксплуатации технически устаревших систем.

Решение Kaspersky Embedded Systems Security устанавливает режим «Запрет по умолчанию» и не позволяет пользователю из него выйти. Благодаря минимальным системным требованиям, решение отлично подходит для устаревших систем на базе Windows XP. Проверка по требованию осуществляется через дополнительный антивирусный модуль Kaspersky Security Network. При необходимости можно воспользоваться также системой управления установкой исправлений.

Таким образом, одно решение избавляет сразу от трех проблем:
- Обеспечивает безопасность сложных для контроля систем
- Обеспечивает совместимость с пунктами 5.1, 5.1.1, 5.2, 5.3 и 6.2 стандарта PCI DSS
- Позволяет заменить устаревшие программы и устройства тогда, когда это удобно.

Режим «Запрет по умолчанию»

Большинство традиционных антивирусных решений не обеспечивает полной защиты от целенаправленных атак. Режим «Запрет по умолчанию» – это новый, более радикальный подход. Он не позволяет запускать без одобрения администратора никаких исполняемых файлов, драйверов и библиотек, помимо базового ПО и средств защиты ПО, на любых банкоматах или в POS-системах.

Контроль устройств

Функция «Контроль устройств» отслеживает попытки физического подключения USB-устройств к системе и не позволяет подключить неавторизованные устройства к банкомату или терминалу. Таким образом блокируется одна из главных уязвимостей, которую киберпреступники регулярно используют как точку входа в систему.

Поддержка всех версий Windows: от Windows XP до Windows 10

Официальная поддержка Windows XP Embedded была прекращена 12 января 2016 года. Windows Embedded for Point of Service не поддерживается с 12 апреля 2016 года. Для семейства Windows XP больше недоступны обновления безопасности и техническое сопровождение. Решение Kaspersky Embedded Systems Security полностью поддерживает работу с семейством Windows XP.

Архитектура, рассчитанная на работу со встроенными системами

Решение Kaspersky Embedded Systems Security обеспечивает полноценную защиту на низкопроизводительных аппаратных платформах, которыми оборудованы большинство банкоматов и касс. Системные требования программы минимальны – от 256 МБ оперативной памяти и 50 МБ места на диске. В режиме «по требованию» антивирусный модуль устанавливается отдельно и запускается только во время ручных или плановых проверок.

Интеграция с Kaspersky Security Network

Согласно требованиям PCI DSS, все системы, через которые принимаются кредитные и дебетовые карты, должны быть снабжены регулярно обновляемой антивирусной программой. Kaspersky Embedded Systems эффективно защищает от вредоносного ПО, а также обеспечивает регулярное обновление – автоматически или вручную – базы вредоносных сигнатур. Поскольку свыше половины всего вредоносного ПО, обнаруженного в системах банкоматов и POS, было запущено посредством эксплойтов «нулевого дня», «Лаборатория Касперского» рекомендует также пользоваться для защиты аналитическими данными облачной сети Kaspersky Security Network: это позволит предотвратить атаки на основе эксплойтов, снизить возможный вред и минимизировать время реагирования.

ПОДДЕРЖКА СТАНДАРТА PCI DSS

Функционал Kaspersky Security for Embedded Systems выполняет и даже превосходит все требования стандарта PCI DSS 3.1:

5.1: Развернуть антивирусное ПО на всех системах, обычно подверженных воздействию вредоносного ПО (особенно на персональных компьютерах и серверах).

5.1.1: Убедиться, что антивирусное ПО способно обнаруживать и устранять все известные типы вредоносного ПО, а также обеспечивать защиту от них.

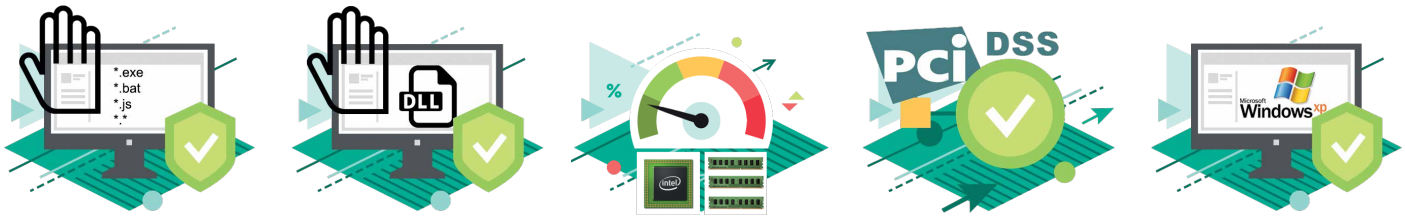
5.2: Гарантировать, что все антивирусные механизмы поддерживаются в актуальном состоянии, выполняют периодическое сканирование, создают журналы регистрации событий, которые хранятся согласно требованию 10.7 стандарта PCI DSS.

5.3: Убедиться, что антивирусные механизмы постоянно запущены, и пользователи не могут их ни отключить, ни изменить без явного разрешения, которое выдается руководством на каждый конкретный случай и на ограниченный период времени.

6.2: Гарантировать, что все системные компоненты и ПО защищены от известных уязвимостей путем установки применимых обновлений безопасности, которые выпускает производитель. Устанавливать критичные обновления безопасности в течение одного месяца с момента их выпуска.

БОЛЬШЕ, ЧЕМ АНТИВИРУС

Стандарт безопасности данных индустрии платежных карт (PCI DSS) регулирует большое число технических требований и параметров для систем, принимающих платежные карты. Однако требования к безопасности банкоматов и POS-систем направлены лишь на борьбу с вирусами. Многочисленные атаки последнего времени показали, что обычного антивируса с ограниченным функционалом может не хватить для защиты от угроз для банкоматов и POS-систем. Требуется новый подход: для критически важных встроенных систем нужно применять технологии контроля устройств и запрета по умолчанию, которые уже подтвердили свою эффективность в других защитных решениях.



Решения для защиты крупного бизнеса: kaspersky.ru/enterprise