Уже не шутки

Рынок российских и международных стандартов безопасности, несмотря на благоприятные условия для совершенствования, парадоксальным образом оторван от реальности

текст **Софья Мороз**

1 мая, в День труда, ожидается введение в действие новых версий стандартов СТО БР РФ 1.0/1.2. Скорее всего, при выборе даты никто ничего не подразумевал, но введение нового стандарта безопасности в День труда как бы намекает...
Новая версия стандартов учитывает последние изменения в требованиях по обеспечению защиты персональных данных, в частности Постановления Правительства № 1119 и 21-го приказа ФСТЭК. Учтены требования Положения ЦБ РФ № 382-П от 09.06.2012 о требованиях к обеспечению защиты информации при осуществлении переводов денежных средств. Ожидается, что этот бесспорно на данный момент лучший в России стандарт безопасности будет развиваться и дальше. Но все ли дыры безопасности будут закрыты новыми версиями руководящих документов? Однозначно нет.

Поступательное развитие, постоянное добавление новых методов защиты, четкие формулировки с одной стороны, и неуменьшающееся количество вредоносных программ в сетях компаний и организаций, с другой. Почему компании, прошедшие аттестацию по лучшим стандартам, на практике остаются беззащитными? В рамках одной статьи невозможно назвать все причины, которых на самом деле множество, поэтому рассмотрим только одну угрозу, вызывающую активный интерес СМИ, – заражение вредоносными программами или вирусами.

Действующие редакции СТО БР РФ 1.0/1.2 и Приказа ФСТЭК России № 21 – это действительно достаточно совершенные акты. Что и как они рекомендуют защищать?

Давайте рассмотрим, что подразумевают руководящие документы под защищаемыми объектами. Тщательный анализ требований показывает: от внимания регуляторов ускользнул целый ряд систем и процессов. Отсутствуют рекомендации по защите встраиваемых систем (банкоматов и терминалов), нет требований по защите мобильных платежей, защите информации, передаваемой по беспроводным сетям, защите от мошенничества при бесконтактной передаче данных (в частности, по протоколу NFS; случаи списания средств мошенниками уже известны). И это далеко не полный список.

Может быть, во всех вышеперечисленных случаях угрозы надуманны и существуют только в пресс-релизах разработчиков средств защиты?

Для примера начнем с банкоматов. Встраиваемые устройства работают в особом режиме – они должны функционировать (как и автоматизированные системы управления технологическими процессами) безотказно и непрерывно в режиме 24 часа 7 дней в неделю. Требование непрерывной работы приводит к тому, что устройства не могут перезагружаться в случае прихода того или иного обновления, требующего перезагрузки. А поскольку заранее неизвестно, какое обновление потребует перезагрузки и как оно повлияет на работу удаленного устройства, то зачастую обновления и не устанавливаются. Сейчас много говорят о том, что в связи с прекращением поддержки Windows XP банкоматы на основе этой ОС останутся работать с обнаруженными и незакрытыми уязвимостями. Но, положа руку на сердце, всегда ли на таких банкоматах в ходе регламентов прописывалось применение всех обновлений безопасности?

В результате устройства со всеми найденными от момента создания ОС уязвимостями оказываются идеальной целью для киберпреступников. По сути, хакеров сдерживает только одно – сложность внедрения вредоносных программ. На данный момент, если не считать проникновения из внутренних сетей организации, наиболее часто сети банкоматов заражаются через сменные устройства обслуживающего персонала. Но в этом случае на устройства попадают вредоносные программы общего назначения, не рассчитанные на хищения именно с банкоматов. Максимум, что может произойти при таком заражении, – синий экран или шифрование информации с выводом на экран требования о выкупе. Это неприятно, грозит потерей репутации, распространением фотографий по всему Интернету, но хотя бы не ведет к прямым потерям денежных средств. Целенаправленные атаки тоже возможны, но для них необходим универсальный ключ для вскрытия банкоматов и доступ к конкретным устройствам для их заражения. Возможность заражения путем нештатного использования устройств (например, выхода с них в сеть Интернет) можно не учитывать – это решается организационными методами.

Тем не менее, несмотря на явную сложность процедуры заражения, возможность получения доступа к большому числу финансовых операций невероятно привлекательна для злоумышленников. В связи со вступлением в силу Федерального закона № 161-ФЗ от 27.06.2011 «О национальной платежной системе» финансовые организации все чаще используют фрод-системы, отслеживающие характеристики платежей клиентов. В этих условиях затеряться среди переводов с банкомата или терминала гораздо проще, чем среди прогнозируемых финансовых операций отдельных компаний. Итог предсказуем: менее чем за полмесяца этого года появились два новых троянца для банкоматов.

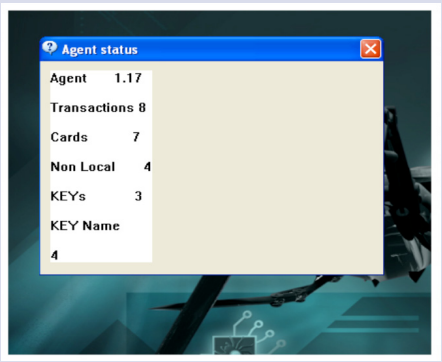

рис. 1. Trojan.Skimer.19

Trojan.Skimer.19 (рис. 1) перехватывает нажатия клавиш EPP (Encrypted Pin Pad) в ожидании специальной комбинации, с использованием которой троянец активируется и может выполнить введенную злоумышленником на клавиатуре команду, например вывести на дисплей банкомата окно со сводной статистикой (количество выполненных транзакций, уникальных карт, перехваченных ключей и т.д.).

Trojan.PWS.OSMP.21 (рис. 2) распространяется в виде динамической библиотеки, которая проникает в терминал с использованием инфицированного флешнакопителя и прописывает себя в отвечающую за автозагрузку ветвь системного реестра Windows под именем Taskbar.

Мало? Рядом с сотнями тысяч ежедневно появляющихся вредоносных программ для десктопов – безусловно. Но по сравнению с количеством обнаруживаемых целевых атак (а это именно целевая атака) два троянца за такой короткий срок – это много. К тому же угрозы нарастают очень быстро: за всю историю противоборства антивирусов и хакеров было обнаружено всего несколько специализированных программ такого рода.

Но вернемся к стандартам. Что они предлагают в качестве мер противодействия? «Реализация антивирусной защиты должна предусматривать <...> применение средств антивирусной защиты».

Основная проблема названных руководящих документов – отсутствие глоссария, дающего определение антивируса и описывающего, что он может и чего не может. Распространено мнение о том, что антивирус должен и обязан обнаруживать все вредоносные программы в момент попытки проникновения. Такое общее преставление выгодно исключительно злоумышленникам.

Дело в том, что наиболее опасные вредоносные программы (и тем более программы для целевых атак) разрабатываются отнюдь не злобными гениями-одиночками, сидящими в темной комнате в окружении взломанных устройств и упаковок от пиццы. Это высокодоходный бизнес, организованный по всем правилам (с разработчиками, руководством, партнерской программой и пр.). При таком подходе новейшие угрозы тестируются на актуальных версиях средств защиты, используемых в атакуемой целевой группе, и не выпускаются в свет, пока обнаруживаются ими. Много ли вредоносных программ можно создать при таком подходе? Группировка, ответственная за Carberp (кстати, тоже нацеленный на хищение денежных средств – только через ДБО), выпускала около ста вредоносных программ в день! И они не обнаруживались в момент проникновения ни одним антивирусом.

Получается, что роль антивируса состоит не только в предотвращении проникновения, но и в обнаружении и удалении ранее неизвестных вредоносных программ. Система антивирусной защиты должна включать не только антивирус, но и как минимум систему ограничения прав и контроля за изменениями. Но только антивирус может лечить активные заражения.

Исчерпываются ли описанными трудностями проблемы защиты банкоматов? К сожалению, нет.

Выше уже говорилось о том, что особенностью работы встраиваемых устройств является невозможность их перезагрузки. Обновления вирусных баз действительно не требуют перезагрузки, но их назначение – опознание пойманного. Для того чтобы опознать, нужно поймать. Для перехвата нужны драйверы. И обновления компонентов, затрагивающих драйверы, вполне могут быть критичными для обнаружения нового типа вредоносных программ.

Получается, что вполне возможна ситуация, когда антивирус мог бы противодействовать новой угрозе, но не сможет сделать это из-за того, что обновления не установлены. Можно ли этому противодействовать? Можно, но необходимо изменить сам подход к защите. Наиболее частым источником заражения становится обслуживающий персонал, в нарушение всех инструкций использующий в собственных целях сменные носители, предназначенные для работы с банкоматами. Поэтому если невозможно обеспечить полную защиту от всех известных угроз на уровне устройства, нужно защитить среду, в которой оно находится, то есть установить (и поддерживать актуальность) средства защиты во внутреннюю сеть компании (если из нее есть доступ в сеть банкоматов), на личные устройства и домашние компьютеры обслуживающего персонала.

При этом, как и в случае защиты самого устройства, желательно не останавливаться только на установке антивируса, нужно использовать средства, ограничи-

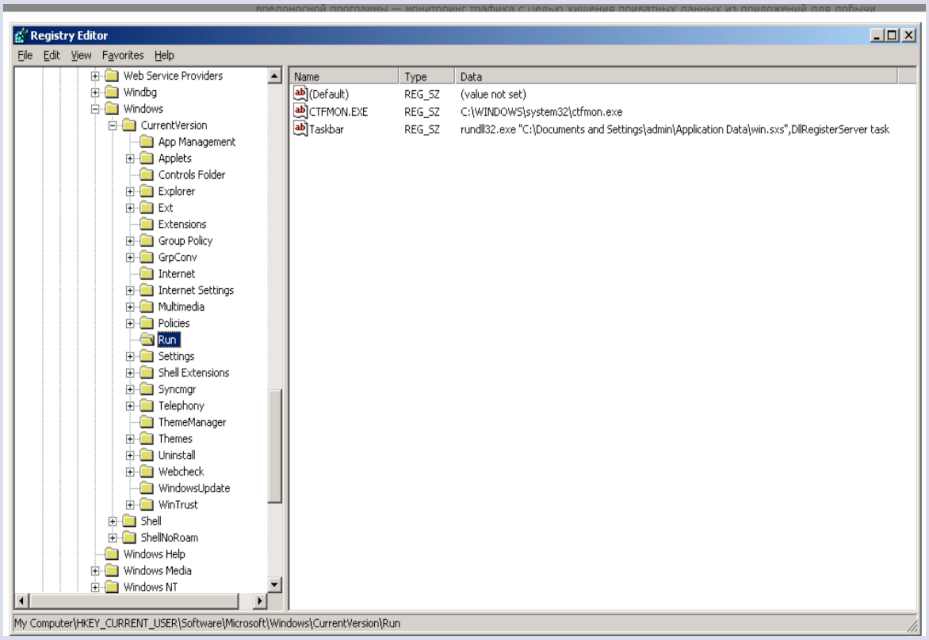

рис. 2. Trojan.PWS.OSMP.21

вающие возможность установки и запуска неизвестных программ, так называемый офисный контроль.

Несмотря на актуальность угрозы, единственным средством защиты встраиваемых устройств на данный момент является Dr.Web ATM Shield.

Почему так получилось? Во-первых, это традиционная для решений компании «Доктор Веб» возможность работы на слабых конфигурациях устройств. Для работы системы защиты вполне достаточно 512 Мб оперативной памяти – именно столько (и не более) сейчас имеют типичные банкоматы. Более того, новая версия Dr.Web ATM Shield специально разработана для защиты слабых компьютеров – работа системы защиты не должна влиять на функционирование используемого на устройстве ПО.

Во вторых, продукты Dr.Web действительно позволяют перекрыть вредоносным программам все пути проникновения. Установка средств защиты возможна не только на банкоматах. Центр управления позволяет контролировать состояние антивирусной защиты любых компьютеров и устройств, в том числе мобильных устройств и домашних компьютеров сотрудников компании. Администраторы компании, использующей Dr.Web ATM Shield, не ограничены в путях установки средств защиты: установка возможна с помощью Active Directory, утилита инсталляции, специально формируемых дистрибутивов – и это еще не весь список.

Dr.Web ATM Shield – это не только антивирус, он включает в себя средства, существенно ограничивающие возможности вольных или невольных злоумышленников. Кроме файлового монитора, обеспечивающего невозможность запуска известных вредоносных программ, и антируткита, обнаруживающего ранее неизвестные угрозы, в состав Dr.Web ATM Shield включены средства офисного контроля. Ограничение возможности работы с локальными каталогами и ресурсами = Интернета не позволяет вредоносной программе передать данные своему хозяину или подключиться к управляющему центру. Запрет использования сменных носителей исключает внедрение с неизвестных сменных устройств. Система контроля интернет-трафика обеспечивает выход в сеть только разрешенных программ и по разрешенным портам. При этом настройки безопасности по умолчанию не могут быть изменены локально – политики безопасности обеспечиваются наличием средств централизованного управления.

Приобретая Dr.Web ATM Shield, клиенты получают не только программный продукт. Поддержка подразумевает консультации по оптимальной настройке системы защиты, тестирование имеющихся конфигураций и многое другое. Напомним, Windows Embedded, который также поддерживается Dr.Web ATM Shield, отличается от обычных десктопных операционных систем тем, что данные ОС могут быть сконфигурированы под конкретные встраиваемые устройства. В связи с этим в них могут отсутствовать те или иные компоненты операционной системы. По сути Dr.Web ATM Shield – это гораздо больше, чем просто программный продукт, это решение для решения проблем. NBJ