Безопасность мобильных платформ

Александр Веселов, *ведущий инженер ЗАО "С-Терра СиЭсПи"*

Мобильные устройства — неотъемлемая часть нашей жизни. Основные черты этого сегмента — повсеместная распространенность и быстрый количественный рост. Злоумышленников привлекает, с одной стороны, прямая связь устройства с реальными деньгами (мобильный банкинг, счет мобильного), которые несложно обналичить, а с другой — различная информация, которая может принести не меньший доход.

На мобильном устройстве могут быть как личные данные владельца (телефонная книга, сообщения, почта, фотографии, видео, сохраненные пароли и т.д.), так и корпоративная информация, предназначенная для служебного пользования. Среднестатистический сотрудник, занятый в сегменте малого и среднего бизнеса, использует для работы настольный компьютер, ноутбук, смартфон и планшетный ПК, каждое из этих устройств представляет собой потенциальную "точку входа" вредоносного ПО в сеть компании.

При личном использовании для защиты информации обычно обходятся ограничением доступа к устройству (пароль, PIN или график для разблокировки) и приложением для поиска устройства в случае потери, реже устанавливают антивирус и шифрование данных флеш-памяти.

В корпоративной среде ситуация несколько иная. Зачастую на мобильном устройстве обрабатывается информация, не только составляющая коммерческую тайну, но и подлежащая обязательной защите в соответствии с законодательством РФ (например, персональные данные). Поэтому обязательным условием использования мобильного устройства для обращения к служебной информации является защищенный удаленный доступ к сети, то есть доступ через VPN-клиент. В зависимости от типа данных шифрование трафика может осуществляться по западным криптоалгоритмам или по отечественному ГОСТу. Активно применяются MDM-решения, осуществляющие контроль приложений, сетевых интерфейсов и многие другие параметры. Сегодня российские вендоры предлагают VPN-клиенты мобильных устройств, работающие под управлением распространенных ОС – iOS, Android и Windows.

iOS

Несмотря на то что доля конкурентов компании Apple на рынке стремительно растет, устройства на платформе iOS не теряют популярности. По данным Gartner, рост продаж компании Apple составляет около 5,2 млн устройств в год. Компания занимает порядка 18% рынка смартфонов и около 40% рынка планшетов.

В марте этого года компания "КриптоПро" объявила о получении сертификата на "КриптоПро CSP" для операционной системы iOS. Криптопровайдер поставляется в составе прикладной программы, как правило, это система документооборота или банк-клиент. Установка осуществляется в составе приложения без взлома устройства.

Компания "Аладдин Р.Д." разработала смарт-карты и ридер для iPad/iPhone. Разработчики приложений для iOS могут использовать внешний (отчуждаемый) сертифицированный криптографический модуль, который применяется в решениях для обеспечения безопасности (VPN, защищенная почта, безопасный доступ к порталам и облачным сервисам, ЭП и др.). Это позволяет использовать усиленную квалифицированную электронную подпись на устройствах Apple.

Компания "ИнфоТеКС" предлагает ViPNet Client для iOS, сертифицированный ФСБ России по классу КС1. Однако в сертификате не указана версия ОС, а правила пользования и тем более формуляр отсутствуют в открытом доступе. Кроме того, производитель предлагает осуществлять установку VPN-клиента с помощью jail-break. Данная возможность не документирована компанией Apple и является, по сути, взломом ОС, приводящим к спорным ситуациям с гарантией производителя. Никто не гарантирует стабильную работу устройства после проведения такого взлома, изменения в устройство пользователь вносит на свой страх и риск. Для некоторых пользователей это может быть приемлемо, но для корпоративного, а тем более финансового сектора этот вопрос требует весьма тщательного изучения и анализа, так как влечет за собой множество дополнительных рисков.

Если пользователь или администратор безопасности все-таки решился на jail-break, не стоит забывать, что ПО, предназначенное для подобного взлома, появляется значительно позже релиза ОС. Пользователи новых моделей Apple будут вынуждены ждать выхода jail-break и, таким образом, будут лишены возможности установить VPN-клиент и защитить трафик между своим устройством и корпоративной сетью.

По той же причине придется отказаться от установки обновлений тем пользователям, на чьих устройствах установлена более старая версия iOS. При этом использование устаревшей прошивки очень часто приносит пользователю массу неудобств.

Таким образом, при кажущемся многообразии средств

защиты для iOS работа с ними остается довольно своеобразной и подразумевает некоторые ограничения: либо использование внешнего дополнительного оборудования, либо применение некорректных способов установки клиента на устройство, либо инсталляцию прикладной программы с дополнительными компонентами третьих производителей для выполнения определенных бизнес-задач.

Android

В настоящее время на рынке предлагаются десятки бюджетных устройств на платформе Android, и в будущем их станет еще больше. Цены на эти устройства продолжают неуклонно снижаться, а фактор цены – один из ключевых, определяющих масштабы внедрений на корпоративном рынке.

Ранее ситуация с ОС Android была во многом аналогична ситуации с iOS, к тому же каждая новая версия требовала внесения изменений в средства защиты. Это происходило потому, что в старых версиях не была обеспечена совместимость драйверов для устройств различных производителей, ядро системы могло претерпевать серьезные изменения в ходе обновлений даже в рамках одной модели и версии ОС. В Android 4.x эту проблему постарались решить. Изменения в ОС позволили разработчикам приложений и средств защиты не привязываться к версии ОС и конкретному устройству, а это, в свою очередь, облегчило распространение программных продуктов и упростило сертификацию.

Сегодня большинство производителей СКЗИ имеют в линейке своих продуктов клиенты безопасности для ОС Android. Причем некоторые из них требуют получения административного доступа для установки (так называемое рутование), что, так же как и jail-break, является взломом ОС. Однако уже появились VPN-клиенты, не требующие прав администратора для установки, например "С-Терра КлиентМ".

Сертифицированного клиента безопасности для ОС Android на данный момент не существует, но в ближайшее время ожидается получение соответствующих сертификатов основными вендорами в данном сегменте: "С-Терра СиЭсПи", "ИнфоТекс", "Код Безопасности".

Таким образом, ситуация с устройствами на платформе Android более благоприятная: на рынке существует ряд специализированных VPN-клиентов, причем есть и такие, установка и использование которых не требуют совершения недокументированных операций и не накладывают ограничений на применение.

Windows

Рассматривая рынок мобильных устройств, нельзя обойти вниманием еще одну ОС, на базе которой в последнее время появляется все больше смартфонов и планшетов. Это давно знакомая и привычная ОС Windows. Ситуация с защитой информации для устройств на платформе Windows 8 хорошо прогнозируема – о технологической совместимости своих продуктов с новой ОС уже заявили "КриптоПро", "С-Терра СиЭсПи", "Инфотекс", "Амикон" и другие. Данные решения пока не сертифицированы, но это вопрос времени, связанный с особенностями порядка сертификации.

Отметим, что использование внешне знакомой ОС, разработанной для хорошо известной x86-архитектуры, будет особенно удобно и приятно системным администраторам и сотрудникам внутренней службы технической поддержки.

Однако необходимо отметить, что между Windows 8 и мобильными версиями Windows существует некоторое различие. Если для Windows 8, как уже было сказано выше, вскоре появятся надежные, сертифицированные решения от известных производителей, то для мобильных версий пока не анонсировалось ни одно решение для защищенного удаленного доступа. Кроме того, далеко не все привычные пользователям приложения портируются на мобильную ОС.

Таким образом, спокойным за безопасность своей информации пользователь может быть только при использовании ОС Windows версии до 7 и в самом скором времени – версии 8. Если же устройство работает на мобильной версии ОС Windows, то варианты VPN-защиты на рынке пока не предлагаются.

Выбор

Подводя итог всему вышесказанному, отметим основные моменты:

1. Выбор мобильного устройства для корпоративного сегмента следует начинать с выбора ОС гаджета.

Компания Apple не торопиться предоставить регулятору исходные коды, а архитектурные ограничения iOS усложняют разработку средств защиты. Набирает обороты ОС Windows, но для мобильных версий этой ОС клиентов безопасности на рынке не предлагают. Скоро появятся новые мобильные ОС, но пока об их широком распространении говорить рано. Android характеризуется более низкой стоимостью устройств, возможностью доступа к исходным кодам и широкими возможностями для разработчиков. Благодаря этому ОС Android более перспективна с точки зрения обеспечения сетевой безопасности.

2. При выборе VPN-клиента для обеспечения безопасного удаленного обмена информацией между мобильным устройством и корпоративной сетью нужно учитывать как простоту инсталляции и использования, так и необходимость совершения недокументированных действий (jail-break, рутование и т.д.). Для безусловного сохранения гарантии на устройство и для более надежной работы следует выбрать VPN-клиент, для установки которого не нужно выполнение подобных операций. ●

Ваше мнение и вопросы присылайте по адресу
infosec@groteck.ru

Другое

В ближайшее время на рынке появятся гаджеты с новыми ОС: Firefox OS от Mozilla и Ubuntu Phone от компании Canonical. До масштабного старта продаж о них можно сделать лишь предварительные выводы, основываясь на информации из пресс-релизов, а также различных выставок и презентаций. Не будем заострять внимание на том, что явная проблема любой новой ОС – недостаток приложений в магазинах. Конкуренция сейчас настолько обостряется, что выпуск каждой новой версии мобильной ОС (той или иной) подстегивает конкурентов. Конечно, чем больше конкурентов – тем лучше, но рынок, как мы видим, довольно медленно и неохотно принимает даже результат творений такого гиганта, как Microsoft. Будем надеяться, что новые ОС будут развиваться динамично и мы сможем применять их в корпоративном секторе.