Защита устройства под управлением Android

С появлением первого вымогателя-шифровальщика Simplocker для Android актуальность вопроса защиты устройства под управлением этой ОС от вредоносного кода вышла на новый уровень. Сам Android является наиболее популярной для вредоносных программ платформой. Эти вредоносные программы пользуются некоторыми преимуществами «открытости» Android, по сравнению с другими мобильными ОС, такими как MS Windows Phone 8 или Apple iOS. Одно из наиболее очевидных преимуществ заключается в отсутствии жесткого ограничения на установку программ из одного источника – официального центра цифровой дистрибуции Google Play.

В наших годовых отчетах, посвященных мобильным угрозам для Android, мы указывали на экспоненциальное увеличение количества вредоносных программ для этой платформы. При этом появляются не только новые варианты уже известных семейств вредоносного ПО, но также новые семейства и новые разновидности такого ПО. Со временем Android становится похож на некое подобие Windows для смартфонов. Это касается типов и количества вредоносного ПО, которое уже существует для этой мобильной ОС.

В этом документе мы хотим предоставить рекомендации пользователям по защите от вредоносных программ для Android.

Устанавливайте приложения только из официального центра цифровой дистрибуции Google, который называется Google Play, или же из других надежных источников

Под другими надежными источниками подразумеваются крупные «доверенные» компании, которые специализируются на предоставлении контента Android пользователям, например, Amazon. Как уже неоднократно подчеркивалось, устанавливая приложения из других источников (центры цифровой дистрибуции, магазины приложений), вы серьезно рискуете, поскольку они могут не выдвигать требований к проверке безопасности таких приложений или намеренно размещать там вредоносный контент.

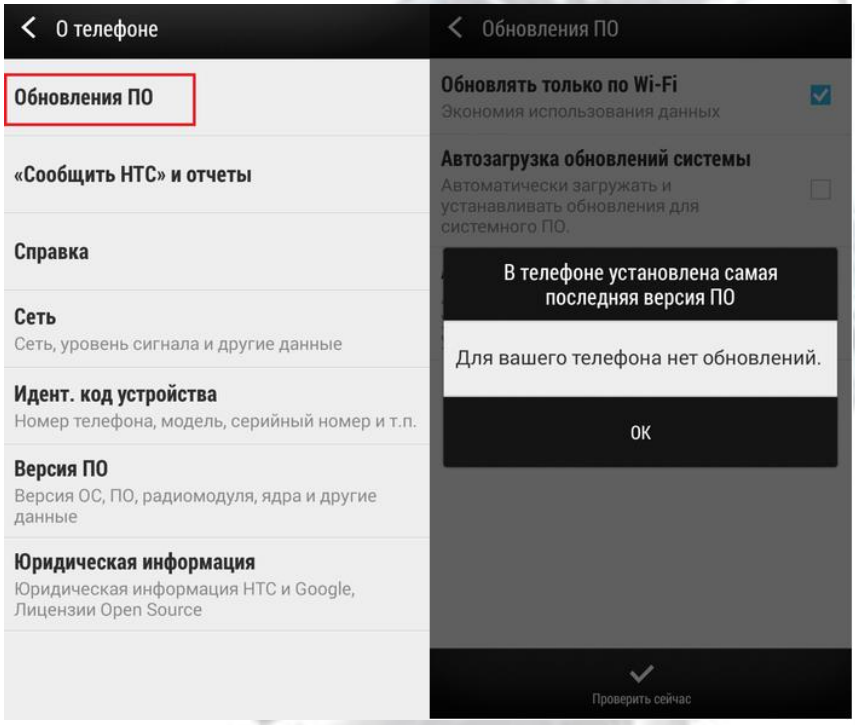
Не доверяйте фишинговым сообщениям

Злоумышленники используют методы социальной инженерии и фишинговые сообщения для заражения устройства пользователя вредоносным ПО. Суть одного из таких сообщений может заключаться в предложении скачать по ссылке якобы необходимое приложение для мобильного устройства. Такое сообщение со ссылкой может распространяться как через SMS, так и посредством электронной почты.

Своевременно обновляйте прошивку устройства и установленные приложения

С выходом новой версии Android, производители мобильных устройств выпускают адаптированные версии ОС для производимого ими устройства (прошивка). Новые версии ОС содержат улучшенные возможности безопасности, а также исправленные уязвимости. Своевременное обновление устройства существенно повысит его иммунитет к различного рода вредоносным программам, в том числе и тем, которые распространяются через уязвимости в ОС.

Для проверки версии вашей ОС перейдите в «Настройки» — «О телефоне» — «Обновления ПО».



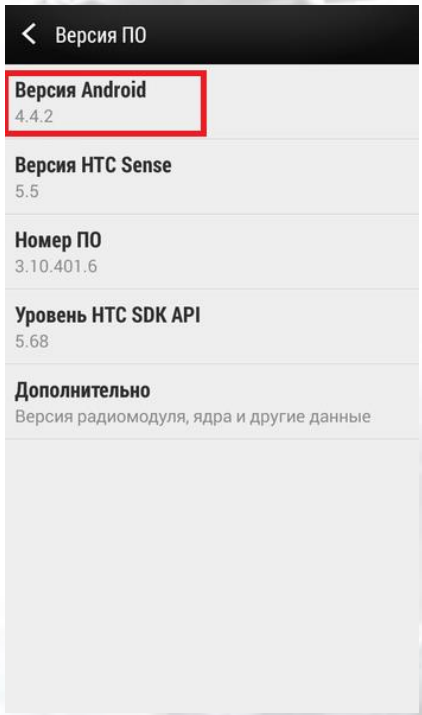


Рис. Меню проверки версии Android (на скриншоте последняя версия Android для HTC One Mini).

Используйте функцию блокировки вашего устройства

Используйте PIN-код для блокировки вашего устройства. Если оно попадет в руки злоумышленников, это значительно усложнит задачу получения конфиденциальных данных из вашего устройства.

Регулярно выполняйте операцию резервного копирования

Регулярно выполняемая процедура резервного копирования поможет своевременно восстановить актуальные версии файлов в том случае, если к ним будет потерян доступ на

устройстве. Резервные копии лучше всего хранить на компьютере или в облаке (т. е. на удаленном сервере). Для этого могут быть использованы как стандартные возможности ПО производителя устройства, так и установленные из магазина приложений Google Play. Резервное копирование может происходить автоматически при подключении вашего устройства к компьютеру (зависит от модели и производителя устройства).

Не используйте операции типа rooting или jealbreak

Операционная система Android использует свои внутренние возможности разграничения прав доступа для приложений. Обычное приложение не может получить доступ к системным файлам или другим критически важным настройкам системы, что значительно повышает иммунитет Android к вредоносному ПО, которое может вывести устройство из строя. Операция типа rooting (jealbreak) приводит к снятию подобных ограничений, т. е. после ее применения запускаемое приложение может получить неограниченный доступ к устройству, его файлам и настройкам. Подобным «преимуществом» могут воспользоваться вредоносные программы.

Стоит также отметить, что многие производители смартфонов официально не поддерживают операции rooting. Это говорит о том, что устройство после такой операции лишается гарантии производителя.

Перед установкой приложения проверяйте запрашиваемые им права

Перед установкой приложения ОС выводит список запрашиваемых им прав доступа или «разрешений» (permissions). Такие запрашиваемые права как «Полный доступ к сети» (Full network access) или возможность отправки SMS-сообщений должны заставить вас дважды подумать об установке этого приложения. В то же время, этот признак не является абсолютным сигналом того, что приложение точно является вредоносным. Скорее это работает в том случае, когда приложение запрашивает права, не свойственные заявленным функциональным возможностям. В таком случае, это может служить сигналом к тому, что это приложение содержит скрытные возможности.

Используйте мобильный антивирус

Вредоносные программы для Android специализируются не только на том, чтобы подписывать пользователя на платные услуги или заниматься рассылкой платных SMS-сообщений. На сегодняшний день количество различных разновидностей вредоносного ПО под Android приближается к тому, что мы видим в мире Windows. Очередным доказательством этому послужило появление вымогателя-шифровальщика Simplocker, который шифрует файлы пользователя на устройстве (аналогичен Cryptolocker для Windows). Чтобы поддерживать свое устройство в безопасности, мы рекомендуем установить на него мобильный антивирус ESET Mobile Security для Android. Эта мера существенно повысит иммунитет Android к заражению вредоносными программами.

Не платите злоумышленникам

Если ваше устройство стало жертвой мобильного вымогателя-шифровальщика, например, Android/Simplocker, ни в коем случае не выполняйте требования злоумышленников, которые просят перевести денежные средства на их счет для восстановления доступа к вашим файлам. Никто не может гарантировать, что доступ к файлам будет восстановлен, или же что в дальнейшем они снова не затребуют выкуп.