Обратная сторона Android

Подходит ли эта операционная система для BYOD?

Владимир Безмалый

Массовость мобильных платформ и безопасность — понятия несовместимые. Увы, вопросам безопасности производители смартфонов внимания почти не уделяют. Почему? Безопасность требует от пользователя самоограничения, а ему нужно здесь и сейчас, поэтому если думать о безопасности, то разработка станет долгой и непозволительно дорогой.

Положительные качества операционной системы Android — массовость и низкая цена, но есть и оборотная сторона — невнимание производителей к безопасности. Убедиться в этом можно, взглянув на ленту новостей: каждый день поступают сообщения о том или ином изъяне в безопасности этой операционной системы, установленной на миллионы устройств. Специалисты компании Pentest опубликовали отчет (http://ilenta.com/news/ios-android-wp/news_11960.html), посвященный дополнительным функциям популярного приложения Flash Keyboard под Android, загруженного 50 млн раз с Google Play. Данное приложение открывало всем желающим сведения о производителе и модели устройства, идентификатор IMEI, MAC-адрес, адрес электронной почты владельца, версию операционной системы, координаты с точностью до 1–3 метров и подробности о любых прокси-серверах, используемых устройством. Приложение было удалено из Google Store, но вскоре появилось вновь. Согласно данным Mobile Threat Intelligence Report Q1 2016, хакеры находят все больше и больше вариантов заражения устройств на базе Android: создать и распространить вредоносную программу для этой операционной системы намного проще, чем для iOS. Фактически все вредоносные программы для Android имеют 76% уникальных вариантов, а для iOS их 22%. Вероятно, iOS более устойчива к вредоносным программам.

Возможно, об этом и не стоило бы беспокоиться, однако оказывается, что такой угрозе подвергаются и корпоративные устройства, например количество телефонов, в которых зловредные программы получили права суперпользователя, составляет для Android 0,71% против 0,02% для устройств под iOS. Это и неудивительно: одно из пяти (19,3%) корпоративных устройств под управлением Android разрешает установку программного обеспечения из сторонних хранилищ.

Исследователи из Check Point обнаружили новые версии печально известных вредоносных программ для мобильных устройств Triada и Horde, способных обходить механизмы защиты Google и заражать приложения в Google Play (Viking Jump, Parrot Copter, Memory Booster, Simple 2048 и WiFi Plus). Новая версия Horde способна мониторить текущие процессы в Android Lollipop и Marshmallow. Для предотвращения подобной активности Google заблокировала для приложений возможность вызывать команду getRunningTasks (), однако Horde обходит

это ограничение. Примечательно, что подобная техника ранее не встречалась, и в скором времени данная функция появится и у других образцов вредоносных программ.

Недавно специалисты McAfee обнаружили в магазине Google Play Store десятки инфицированных приложений, ставших жертвами троянца Android/Clicker.G, причем мишенью были исключительно устройства российских пользователей. У наиболее популярного из пострадавших приложений число загрузок обычно не превышало 5 тыс., при этом программы обладали работающим интерфейсом и имели положительные отзывы, но, попав на устройства Android, через шесть часов начинали проявлять активность, интенсивно работая с рекламой.

Вредоносы регулярно обходят механизмы защиты магазина Google; например, в докладе о безопасности Google Android 2015 (Android Security Annual report) говорится, что 0,15% приложений магазина содержали вредоносный код. В конце апреля 2016 года компания PhishLabs обнаружила в магазине Play Store 11 охотящихся за финансовой информацией пользователей приложений, а чуть ранее специалисты компании «Доктор Веб» нашли 104 программы типа spyware с Android. Spy.277, а затем обнаружили в каталоге Google Play нового троянца Android.PWS.Vk.3, который похищал у пользователей имена и пароли от учетных записей в социальной сети «ВКонтакте». Этот троянец представляет собой полноценный аудиоплеер, который позволяет прослушивать музыку, размещенную в данной социальной сети. Чтобы получить доступ к заявленной функциональности, пользователям необходимо войти в свою учетную запись, введя имя и пароль. Однако здесь владельцев мобильных устройств ждет сюрприз: вредоносное приложение отправляет введенные данные на управляющий сервер, и злоумышленники фактически получают полный доступ к учетным записям жертв.

Сегодня все чаще при использовании Android неожиданно в совершенно случайных местах начинает вылезать реклама. Почему? Приложение подождало N дней и передало учетные данные на свой сервер, и сразу понять, кто показывает рекламу, сложно, а зачастую и невозможно, учитывая, что разрешение на доступ в Интернет требуют обычно все приложения. Только за первый квартал 2016 года системы «Лаборатории Касперского» для защиты мобильных устройств обнаружили более 2 млн вредоносных установочных пакетов, что в 11 раз больше, чем в предыдущем квартале, 4 тыс. мобильных банковских троянцев и 3 тыс. мобильных троянцев-вымогателей.

Как ни прискорбно, надежного решения пока нет и рабочие данные на корпоративных смартфонах и планшетах нельзя применять в принципе, что ставит под сомнение жизнеспособность концепции использования в компании личных устройств сотрудников (BYOD).

На сегодня платформа Android работает на 10 тыс. моделей смартфонов и планшетов, из-за чего сложилась угрожающая ситуация на рынке обновлений программного обеспечения — темпы распространения обновлений остаются низкими.

На сегодня лидерами по разработке обновлений остаются смартфоны от Google (Nexus) и Samsung. По мнению Гэла Бениамини, признанного эксперта в области компьютерной безопасности, введенного компанией Qualcomm в свой «Зал славы по безопасности продуктов», пользователям, которые заботятся о безопасности своих данных, стоит приобретать только аппараты линейки Google Nexus или Samsung. Nexus первыми получают от Google обновления «по воздуху», и, значит, любая обнаруженная на них уязвимость будет убрана в первую очередь. Samsung не отстает от Google в обновлении прошивок своих аппаратов. Все остальные разработчики выпускают обновления редко и нерегулярно, а некоторые не делают этого совсем (см. таблицу 1).

Доля устройств под управлением новой версии Android 6.0 составляет чуть более 18%, а ведь с момента ее выхода прошел уже год. Что касается iOS, то здесь картина немного другая (см. таблицу 2).

С момента выхода iOS 10 ситуация изменилась. На следующий день после выпуска iOS 10 была установлена на 14,5% устройств, а чуть менее чем через неделю, после выхода iPhone 7 и iPhone 7 Плюс, эта операционная система была установлена на 34% устройств.

Для того чтобы успокоить потребителей и указать, что все не так страшно, специалисты Google в своем отчете объединили все подкатегории вредоносных программ (spyware, backdoor, call_fraud, sms_fraud, phishing, DDoS, ransomware и даже generic_malware) в менее страшную категорию — «потенциально» вредоносных приложений. Однако в отчете указывается, что существует еще много устройств на базе Android, не получающих ежемесячные обновления: 70,8% всех активных устройств на базе Android выполняется под управлением современных версий Android. Но это означает, что оставшиеся устройства обновить нельзя, новых прошивок, выпущенных разработчиками, просто нет, а это почти 400 млн устройств. Безусловно, мне могут возразить, что есть другие прошивки, созданные независимыми разработчиками. Но будут ли ими заниматься пользователи? Да и кто может быть уверен в их корректной работе и отсутствии уже «зашитого» вредоносного программного обеспечения. Мне приходилось иметь дело со смартфонами, в которых вредоносная программа была уже в прошивке.

Почему так происходит? Компания Google заявила о том, что обновления будут выпускаться не дольше чем два года с момента появления версии, а ведущий производитель смартфонов под управлением Android, Samsung, назвала еще более короткий срок — 1,5 года. Если ранее в выигрышном положении были покупатели Android Nexus, то сегодня Google уже заявила об окончании поддержки этих устройств, которое произойдет максимум через год.

Почему разработчики не выпускают прошивки? Ведь Google производит

их довольно регулярно. Проблема в том, что практически каждый из разработчиков устройств стремится «доделать» операционную систему под конкретный аппарат, и Android для Nexus и Android для безымянного китайского производителя будут отличаться. Понятия единого стандарта, увы, не существует.

Что делать? Самым правильным будет совет не использовать устройства на базе Android для решения важных задач, связанных с обработкой персональной, банковской и коммерческой тайны, а также для любых корпоративных применений. Но если вы все же решитесь это делать, то запомните несколько правил.

- Используйте надежные пароли для любых мобильных приложений. Ни один пароль не должен быть удобным для запоминания. Ваш PIN-код обязан быть сложным, это первая линия защиты, и чем он сложнее, тем труднее добраться до конфиденциальных данных.
- Не устанавливайте root-доступ. Любой зловред, который может быть запущен на вашем устройстве, автоматически получит ваши права.
- Используйте антивирус, которому доверяете.
- Применяйте двухфакторную аутентификацию на всех службах. Привыкайте к тому, что если служба предлагает использовать на смартфоне двухфакторную аутентификацию, то делать это обязательно. Более того, если есть выбор, какой из служб пользоваться, выбирайте ту, у которой реализована двухфакторная аутентификация, значительно затрудняющая взлом учетной записи.
- Шифруйте устройство. Безусловно, производительность устройства снизится на 15–20%, но, если на нем хранятся важные данные, оно того стоит. Чтобы узнать, зашифровано ли ваше устройство, перейдите в раздел «Настройки», «Безопасность» и найдите раздел «Шифрование». Если устройство помечено как «Зашифрованное», то ваша безопасность заметно усилена. Если вы приобрели новое устройство на базе Android Marshmallow, то ваше устройство зашифровано по умолчанию.
- Используйте менеджер паролей. Не разрешайте приложениям сохранять ваши пароли, если только это не специальный менеджер паролей. Ведь если вы потеряете свое устройство, то злоумышленник сможет использовать все пароли.
- Регулярно обновляйте операционную систему и приложения.
- Не используйте открытые беспроводные сети. Если все же это вам очень нужно, применяйте VPN.
- Не устанавливайте приложения из неизвестных источников. Никто не может поручиться за безопасность такого продукта.

Таблица 1. Перечень версий Android по состоянию на 6 сентября 2016 г.

Версия	Наименование	API	Доля устройств
2.2	Froyo	8	0,1%
2.3.3–2.3.7	Gingerbread	10	1,5%
4.0.3–4.0.4	Ice Cream Sandwich	15	1,4%
4.1.x	Jelly Bean	16	5,6%
4.2.x		17	7,7%
4.3		18	2,3%
4.4	KitKat	19	27,7%
5.0	Lollipop	21	13,1%
5.1		22	21,9%
6.0	Marshmallow	23	18,7%

Таблица 2. Перечень версий iOS

Версия iOS	Доля устройств, %
9.x	92,78
8.x	6,32
7.x	0,77
6.x	0,13

Конечно, для управления корпоративными смартфонами и планшетами применяются системы класса Mobile Device Management (MDM), но они сами по себе несут новые угрозы, особенно для персональных данных. Данный класс программного обеспечения может применяться для сбора различной информации, например регистрировать местоположение устройств, собирать данные об установленных приложениях и посещаемых вебсайтах. Эксперименты с несколькими системами MDM, проведенные в компании Bitglass, показали возможность перехвата сообщений, посланных через Gmail, Messenger и другие приложения, а также паролей к страницам в социальных сетях и к банковским счетам. Разумеется, для этого необходимо иметь доступ к административным функциям системы. Кроме всего прочего, инструментарий MDM обладает возможностями удаления с устройства приложений и данных, вплоть до полной очистки памяти смартфона. Многие инструменты позволяют также ограничивать доступ к другим функциям смартфона, например к резервному копированию данных в «облако» iCLoud. Все это, как подчеркивается в докладе Bitglass, повышает риск потери личных данных.

Несмотря на то что кто-то сочтет это преимуществом, а не недостатком, все же, с точки зрения пользователя, нежелательно терять свои личные данные в случае, если ты увольняешься из компании. Лучшим выходом в такой ситуации будет четкое разделение информации на личную и корпоративную. И MDM должен иметь доступ только к корпоративному контейнеру. И не более.

Владимир Безмалый (vladb@windowslive.com) — специалист по обеспечению безопасности, Kaspersky Lab Certified Consultant, Kaspersky Lab Certified Trainer, имеет звания MVP Consumer Security, Microsoft Security Trusted Advisor