Защита корпоративных мобильных устройств

Владимир Безмалый

Сегодня наличием мобильного устройства сложно кого-то удивить. Наша жизнь немыслима без смартфонов и планшетов, а с недавних пор и без других подключаемых устройств вроде финтес-трекеров и умных часов со встроенными плеерами.

А задумываемся ли мы о том, какие угрозы влечет за собой использование подобных устройств? Да, их удобство несомненно, но ваша информационная безопасность теперь постоянно находится под угрозой. Что привносит в нашу жизнь использование мобильных устройств, только ли благо? Надеюсь, что, ознакомившись с этой статьей, вы задумаетесь над проблемой надлежащей защиты новомодных приспособлений. Итак, приступим.

Сегодня смартфоны и планшеты имеют такое же высокое быстродействие и большой объем памяти, как настольные персональные компьютеры несколько лет назад. Многие мобильные устройства значительно повышают производительность труда, облегчая сотрудникам доступ к информации. Однако необходимо понимать, что их использование влечет за собой и новые риски для организаций, поскольку в случае утраты устройства конфиденциальные, корпоративные и просто персональные данные могут попасть в руки злоумышленников. Кроме того, в геометрической прогрессии растут новые типы вредоносного программного обеспечения, спама и программ для взлома мобильных устройств.

Мобильные устройства сегодня объединяют функции телефона с возможностью полноценной обработки данных, ранее присущей только компьютерам. Помимо совершения обычных телефонных звонков и отправки SMS-сообщений, пользователи могут запускать приложения, сохранять данные и обмениваться ими в корпоративных сетях и в Интернете. Карты памяти уже обеспечивают вполне приемлемый объем для хранения большого размера файлов и приложений. Не стоит забывать, что сегодня разработчики программ могут писать приложения для мобильных платформ, применяя все больше программных инструментов. А развитие беспроводных технологий способствовало ускоренному повсеместному внедрению таких устройств в бизнес-среде.

Увеличение пользовательской базы, развитие мобильных платежей и интернет-банкинга не могло не привлечь внимание киберпреступников. Вслед за этим

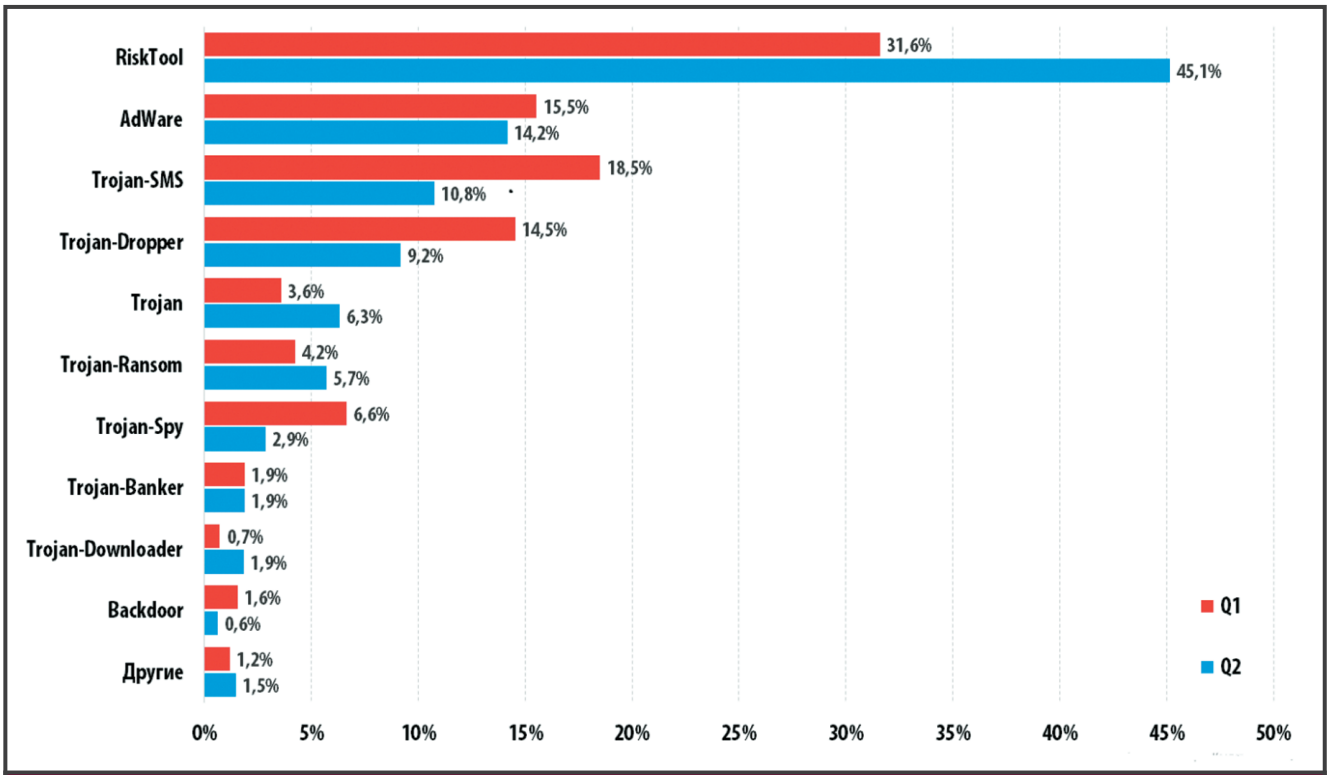

Рисунок 1. Распределение новых детектируемых мобильных программ по типам (Q1 2016 и Q2 2016)

и руководство компаний уже приходит к выводу, что обеспечение безопасности и контроль мобильных устройств сотрудников так же важны, как и обеспечение безопасности рабочих станций и серверов.

Бесконтрольное использование смартфонов в офисе угрожает вашему бизнесу, и беда в том, что вы даже не подозреваете, как. Сегодня мобильные телефоны используются для переговоров и коммуникаций не чаще, чем для хранения информации и обмена важными корпоративными данными. И вот почему.

- ***Бизнес становится более мобильным.*** Сотрудники, руководители или эксперты могут отвечать на письма и бизнес-запросы в любое время из практически любого места. Снижается время реакции, возрастает продуктивность работы компании. Это позволяет вести бизнес более эффективно и быстрее реагировать на изменения рынка, что особенно важно в условиях кризиса при работе на развивающихся рынках.
- ***Возрастает мобильность сотрудников.*** Несмотря на всю очевидность такого утверждения, взять с собой в поездку планшет гораздо проще, чем везде таскать по определению более тяжелый ноутбук.
- ***Гораздо удобнее для обеих сторон.*** Сотрудник работает на устройстве, которое, вероятнее всего, он сам выбирал, с удобным ему интерфейсом, а работодатель получает мгновенный отклик и удовлетворенность сотрудников. К тому же заполнять форму в специальном приложении на планшете в комфортном месте и в подходящее время удобнее, чем вписывать данные в бланки документов вручную.
- ***Просто дешевле.*** Многие компании, понимая преимущества мобильности своих сотрудников, либо выдают устройства, либо, чаще, принимают политику BYOD (Bring Your Own Device) и подключают личные устройства пользователей к корпоративной сети и службам.

Вместе с тем существует и ряд недостатков, присущих мобильным системам.

1. Вредоносные программы, кибератаки на мобильные устройства.
2. Риски применения в корпоративной сети «взломанных» самим сотрудником устройств с измененным кодом встроенной операционной системы и правами администратора (Jailbreak и Root).
3. Риск утраты (потери, хищения) устройства.

В этой статье речь пойдет о защите мобильных устройств. Что мы понимаем под защитой мобильных устройств? В первую очередь антивирусную защиту. Во многих ситуациях ее бывает достаточно. Антивирус спасет от вирусов, а чтобы вместе с телефоном при пожаре не потерялись важные контакты, заметки и фотографии любимого пуделя, достаточно настроить синхронизацию с «облаком»: iCloud, Google Drive и т. д.

Однако в данной статье мы будем говорить о защите корпоративных мобильных устройств, которые либо принадлежат компании, либо обрабатывают данные, принадлежащие ей. Причем таких устройств много, а вот администраторов, которые за них отвечают, — значительно меньше. Но и современные технологии для защиты от вредоносных программ обезопасят

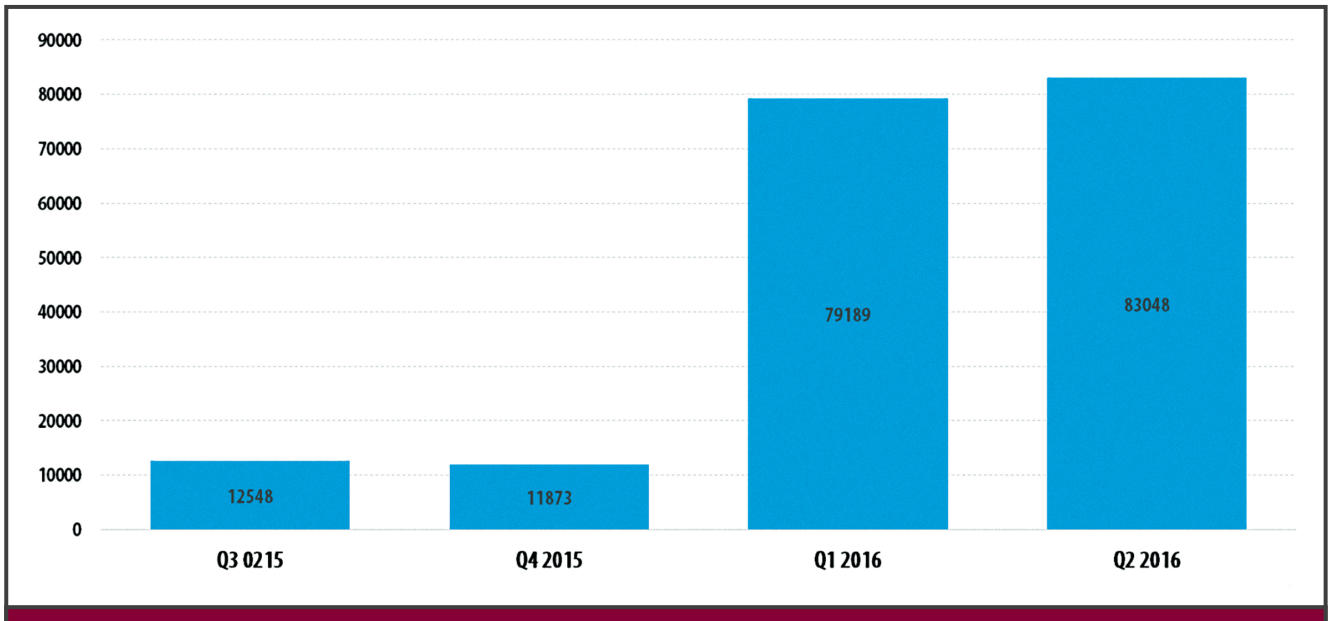

Рисунок 2. Рост числа троянцев-вымогателей

устройство не только от вирусов, но и от более широкого спектра угроз, включая троянцы, фишинговые ссылки и т. д.

Вредоносные программы

По данным «Лаборатории Касперского», распределение новых детектируемых мобильных программ по типам (I квартал 2016 и II квартал 2016) выглядит так, как на графике, представленном на рисунке 1.

При этом растет количество мобильных троянцев-вымогателей (см. рисунок 2).

Продуктами «Лаборатории Касперского» для защиты мобильных устройств было обнаружено:

- 3 626 458 вредоносных установочных пакетов;
- 27 403 установочных пакетов мобильных банковских троянцев;
- 83 048 установочных пакетов мобильных троянцев-вымогателей.

Уже из этих цифр понятно, что проблему антивирусной защиты нельзя назвать надуманной. Что же делать? Рассмотрим, как организована защита от атак вредоносных программ в продукте Kaspersky Security для мобильных устройств.

Защита от угроз вредоносных программ

Данный компонент входит только в состав решения для мобильной операционной системы Android. Он состоит из двух служб.

- ***Постоянная защита.*** По умолчанию проверяет только новые приложения при первом запуске. Это сделано для того, чтобы уменьшить влияние службы на производительность устройства.

Если аппаратное обеспечение вашего устройства позволяет, настройки постоянной защиты можно сделать более строгими — перевести ее в «Расширенный режим защиты». В этом случае проверяются все файлы, причем не только при первом запуске, но и при каждом открытии, сохранении, копировании, перемещении, редактировании, установке и запуске.

Все настройки постоянной защиты находятся в разделе «Защита». Расширенный режим включается флагом «Расширенный режим защиты».

Можно упростить расширенный режим — оставить проверку только исполняемых файлов: EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF. Для этого дополнительно требуется отметить опцию «Проверять только исполняемые файлы».

При обнаружении угрозы Kaspersky Security для мобильных устройств попытается ее устранить. Если файл вылечить нельзя, то по умолчанию он будет помещен на карантин.

Карантин всегда локальный, в хранилище сервера администрирования информация об обнаруженном вредоносном объекте отправлена не будет. Администратор только получит информацию о детектировании угрозы.

- ***Поиск вирусов и вредоносных программ*** — более ресурсоемкая задача, запускаемая пользователем вручную или по расписанию (по умолчанию каждый день в 9 утра).

Расписание запуска поиска вирусов задается политикой Kaspersky Security для мобильных устройств, и запустить вручную его можно только из локального интерфейса. Все настройки поиска вирусов собраны в разделе «Проверка».

По умолчанию сканируется вся доступная память устройства, включая архивы (ZIP, JAR, JAD, SIS, SISX, CAB, APK). Но проверяются только исполняемые файлы (EXE, DLL, MDL, APP, APK, RDL, PRT, PXT, LDD, PDD, CLASS, SO, ELF).

Можно усилить поиск вирусов — проверять все файлы: снять флаг «Проверять только исполняемые файлы».

Можно ослабить — не проверять архивы: снять флаг «Проверять архивы с распаковкой».

При запуске поиска вирусов по расписанию проверяется вся доступная память, как описано выше.
При запуске вручную пользователь сможет выбрать один из трех вариантов:

1. Быстрая проверка — сканировать только установленные приложения.
2. Полная проверка — сканировать все устройство.
3. Проверка папки — сканировать только заданную папку (на устройстве или карте памяти).

Измененная операционная система и права администратора

Почему администратору важно знать о наличии измененной встроенной операционной системы и прав администратора устройства?

- На устройстве с операционной системой iOS пользователь вправе установить программу не из App Store, а такое программное обеспечение может оказаться вредоносным.
- На устройстве с операционной системой Android пользователь может удалить решения для обеспечения защиты, а так же, как и в случае с продуктами Apple, существует риск установки подозрительных приложений из сторонних репозиториев программ.

Измененная операционная система

Корпорация Apple тщательно следит за отсутствием опасных и потенциально вредоносных программ в App Store, но, увы, не всегда решает эту задачу и, главное, это не защитит вас от главной угрозы — невнимательности или пренебрежения требованиями безопасности со стороны самого пользователя.
В Интернете достаточно много сайтов с подробными инструкциями, как взломать операционную систему iOS любой версии. В большинстве случаев пользователю просто нужно загрузить на компьютер специальную утилиту, подключить через программу iTunes свой смартфон и воспользоваться соответствующим мастером. После этого у него появится доступ к файловой системе, и он сможет устанавливать приложения из альтернативных источников. А в них отсутствия вредоносных программ никто не гарантирует.
Kaspersky Security для мобильных устройств не может пресечь взлом. Но его модуль Safe Browser способен зафиксировать изменения во встроенной операционной системе и уведомить администратора.
Защитное решение для iOS является комплексным при использовании профилей для устройств iOS в решениях для управления мобильными устройствами MDM и профилей модуля SafeBrowser for iOS.
С помощью профиля решения MDM можно:

- применять политики, регламентирующие строгость и формат паролей, настройки подключения к Microsoft Exchange, соединения VPN, возможность использования камеры и другие настройки;
- заблокировать устройство, сбросить пароль на нем, а также очистить устройство;
- установить или удалить приложение, как стороннее так и из App Store и т. д.

С помощью профиля SafeBrowser for iOS можно:

- осуществлять и настраивать веб-фильтрацию трафика в самом браузере;
- обнаруживать изменения во встроенной операционной системе и информировать об этом администратора;
- выполнять поиск географического положения утерянного устройства.

Сумма этих возможностей позволяет администратору управлять устройствами iOS наравне с устройствами Android, где подобные возможности также имеются.

Получение прав администрирования в операционной системе Android (Rooting)

Операционная система Android не запрещает доступ к файловой системе. Сотрудник может использовать свой планшет как флешку, но с некоторыми ограничениями. Все приложения Android запускаются в собственной изолированной среде, а системные файлы доступны только для чтения. Это нельзя назвать полноценной защитой от вирусов, но такие ограничения служат дополнительными барьером. Например, вредоносное приложение не сможет без участия пользователя украсть данные другого приложения.
Однако пользователь может взломать операционную систему — получить неограниченные права администратора. В том числе на модификацию системных файлов и получение доступа к данным всех установленных приложений.
Kaspersky Security для мобильных устройств не может запретить выполнение операций по получению прав администрирования в операционной системе. Но в состоянии это обнаружить и выполнить следующие действия:

1. Уведомить администратора.
2. Применить настроенное администратором действие, например заблокировать устройство или автоматически удалить корпоративные данные.

Как настроить оповещение о взломе? За детектирование взлома на iOS отвечает Safe Browser. Поэтому и для iOS, и для Android все настраивается в Kaspersky Security для мобильных устройств.

Действия администратора при получении уведомления о взломе

Если устройство корпоративное, необходимо заблокировать или очистить его, если принадлежит пользователю, то удалить корпоративные данные.
По умолчанию функция удаления всех бизнес-данных на Android отключена. Администратор должен ее включить. Соответствующий флаг расположен в разделе «Анти-Вор». Настройка будет применена при следующей синхронизации, и только после этого администратор сможет удаленно очистить устройство. Это можно сделать,

отправив соответствующую команду из узла «Управление мобильными устройствами»/«Мобильные устройства».

Вместе с тем можно настроить автоматическое действие на рутинг Android, подкорректировав политику Kaspersky Security для мобильных устройств в разделе «Контроль соответствия».

- Условие: операционная система взломана.
- Временное ограничение: немедленно.
- Действие: удалить корпоративные данные или удалить все данные.

Контроль соответствия необходимо сделать обязательным, установив соответствующее действие в политике.

Защита от фишинга

В режиме веб-защиты проверка веб-трафика работает по умолчанию: блокирует сайты, содержащие фишинговые и вредоносные ссылки. Стоит отметить, что веб-защита в Kaspersky Security для мобильных устройств работает с браузерами, поэтому для безопасного доступа в Интернет на iOS и Windows Phone пользователь должен применять Safe Browser, а в операционной системе Android — родной браузер или Google Chrome.

Для корпоративных устройств с iOS и Android веб-защиту можно настроить так, что:

- будут блокироваться все сайты, кроме заданного администратором набора URL (белые списки);
- будут блокироваться сайты, отнесенные «облачным» сервисом Kaspersky Security Network к небезопасным (черные списки).

По умолчанию блокируются только фишинговые сайты и сайты с вредоносным содержимым. Однако администратор может задать больше категорий для блокировки, например запретить социальные сети и игры.

Все настройки этого режима находятся в разделе «Веб-фильтр». Наполнение категорий проходит автоматически через сеть KSN, следовательно, мобильное устройство должно иметь доступ к KSN. Для корпоративных устройств, кроме того, возможно блокирование заданного списка URL.

Использование личных устройств

Как правило, пользователи приносят в корпоративную сеть личные смартфоны и планшеты. Иногда руководство компании не хочет централизованно закупать мобильные устройства и разрешает сотрудникам использовать личные, в первую очередь для доступа к корпоративной почте. В таком случае сотрудники могут работать вне офиса, а компания не будет нести дополнительные расходы. Такая политика называется «принеси свое устройство», Bring Your Own Device (BYOD). Как и в любой политике, здесь есть свои плюсы и минусы.

Плюс: отсутствие необходимости решения технических проблем (сотрудники будут сами напрямую обращаться в сервисные центры производителей) и затрат на обновление парка (сотрудники сами покупают новые телефоны).

Минус: отсутствие контроля установленных программ и всего устройства в целом. Пользователь остается владельцем смартфона и имеет право делать с ним все, что захочет, — подарить или продать, играть в игры, потерять, и никому не рассказать об этом.

Таким образом, при принятии компанией политики использования личных устройств сотрудников задача ответственного за безопасность администратора сводится к защите корпоративных данных. Что будет происходить при этом с самим устройством — личное дело владельца.

В идеальном случае корпоративные данные должны храниться внутри организации и не покидать ее. Но сегодня компаниям выгоднее дать сотрудникам возможность работать с ними из дома, во время отпуска, на больничном, в командировке и т. д. Но как контролировать эти данные, если нет права контроля устройств? Контролировать доступ к корпоративным данным.

Это можно сделать, выделив корпоративные приложения и разрешив доступ к корпоративным ресурсам только из конкретных приложений. При этом необходимо:

1. Запретить доступ к корпоративным данным всем остальным приложениям, установленным на устройстве.
2. Сделать так, чтобы запуск корпоративных приложений требовал дополнительной аутентификации.
3. Все корпоративные данные, поступающие на устройство и хранящиеся на нем, должны автоматически шифроваться.

Для управления сохранностью данных при использовании личных устройств в Kaspersky Security для мобильных устройств применяется контейнеризация. При этом корпоративные данные хранятся в контейнерах, которые могут быть удалены в случае утраты (или хищения) устройства или когда сотрудник увольняется. При этом корпоративные данные изолированы от личной информации пользователя, и их удаление никак не скажется на сохранности личных данных на телефоне сотрудника.

При этом следует:

1. Запретить обмен данными между корпоративными программами и всеми остальными, установленными на устройстве.
2. Ввести дополнительную аутентификацию пользователя при запуске корпоративных приложений.
3. При сохранении на диск все данные, полученные по корпоративным каналам, автоматически шифровать.

В одной статье весьма сложно описать все функции, реализованные в таком продукте, как Kaspersky Security для мобильных устройств. Однако, надеюсь, она поможет вам составить свое мнение о продукте.

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