Dr.WEB®
Антивирус

Информационный бюллетень

Мобильные устройства как угроза безопасности сетей компаний и домашних компьютеров пользователей

Дата составления **15.05.12**

Текущий уровень опасности **Высокий**

Наиболее актуальные угрозы безопасности компаний*	Дополнительная информация
Вредоносные программы, создаваемые для кражи финансовых средств, в том числе с банковских карт и систем дистанционного банковского обслуживания, используемых компаниями	http://news.drweb.com https://blogs.drweb.com Информационный бюллетень от 2.04.12
Вредоносные программы, создаваемые для мобильных устройств	Тема выпуска
Проникновение вредоносных программ с личных компьютеров и устройств пользователей	

* Актуальность угроз определяется не только количеством вредоносных программ различных типов, но и уровнем защиты от них, используемой в компаниях и организациях различного типа.

125124, Россия, Москва, 3-я улица Ямского поля, вл.2, корп. 12а
Телефон: +7 (495) 789-45-87 (многоканальный)
Факс: +7 (495) 789-45-97

www.drweb.com | www.freedrweb.com | www.av-desk.com

Тема выпуска: Мобильные устройства как угроза безопасности сетей компаний и домашних компьютеров пользователей

Типичные представители вредоносных программ

К категории наиболее опасных можно отнести:

1) **для ОС Android:** Android.SmsSend, Android.Gongfu, Android.Plankton, Android.GoldDream, Android.Crusewind, Android.SpyEye, Android.DreamExploid, Android.Wukong;
2) **для ОС iOS:** iPhoneOS.HLLW.Ikee, коммерческие программы-шпионы.

Кроме специализированных под конкретные ОС вредоносных программ, существуют троянцы, способные работать на любой мобильной платформе с поддержкой Java (например, Symbian и большинство сотовых телефонов).

Причина актуальности угрозы

На данный момент недостаточная защищенность мобильных устройств представляет серьезную угрозу как для их владельцев, так и для компаний, сотрудники которых так или иначе используют мобильные устройства.

В отличие от персональных компьютеров мобильные устройства дают злоумышленникам гораздо больше возможностей. Заразив персональный компьютер, злоумышленники могут:

- блокировать зараженное устройство;
- получить доступ к почтовой переписке, паролям используемых программ, системам работы с денежными средствами;
- получить доступ к конфиденциальным данным, сохраненным в виде файлов, фотографиям.

Все это актуально и для мобильных устройств, но наряду с этими, уже привычными угрозами, внедренная в мобильное устройство вредоносная программа может:

- отправлять СМС и звонить на платные номера;
- включать микрофон без ведома жертвы — и тем самым получать информацию «из первых уст»;
- получать данные от GPS-навигатора о местонахождении жертвы — ее присутствии или отсутствии в определенных местах;
- получать доступ к конфиденциальным данным, сохраненным в виде фотографий и звуковых записей, а также СМС-переписке и истории совершенных звонков.

Владелец зараженного устройства отказывается под полным круглосуточным контролем!

Для компаний заражение мобильных устройств сотрудников представляет особо опасную угрозу их безопасности:

- большинство сотрудников работают с корпоративной почтой и конфиденциальными данными на своих устройствах. Более семидесяти процентов для работы используют только личные устройства;
- зараженные устройства, даже не подключенные к сети, могут быть использованы для атаки на нее — через беспроводные сети.

Отсутствие защиты не просто снижает эффективность работы — это создает возможность утечки, подмены или компрометации важных для компании материалов.

Нельзя забывать и о том, что до семидесяти процентов заражений локальной сети происходят с помощью личных устройств и сменных носителей сотрудников компании.

При этом, согласно статистике, до шестидесяти процентов устройств, находящихся в пределах ее территории, ей не принадлежат и не контролируются с точки зрения информационной безопасности. Более того, сотрудники работают не только на своем рабочем месте, но и дома, в дороге, на отдыхе — распространение мобильных устройств и доступность Интернета в любой момент и в любом месте дают эту возможность — отсутствует гарантия получения только безопасного контента, вне офиса люди никак не защищены от атак хакеров.

Не ограничиваемые корпоративной политикой безопасности пользователи устройств самостоятельно скачивают и устанавливают приложения (приложения для работы с документами, приложения для работы в социальных сетях и сети Интернет...). При этом эти приложения могут как иметь уязвимости, так и содержать в своем составе специально разработанные вредоносные программы-троянцы. По статистике, каждая пятая программа имеет уязвимости, что позволяет проводить атаки на целевые группы.

Дополнительно усугубляет проблему формирование профессиональных хакерских группировок — вредоносные программы перед выпуском тестируются на актуальных антивирусах и некоторое время после релиза не обнаруживаются ими. В тоже время — как и в случае с обычными компьютерами — для снятия денег криминальной структурой, имеющей четкую организацию, требуется от одной до трех минут.

Причина роста количества угроз для Android — открытость основных исходных кодов этой операционной системы. Любые обнаруженные в ней уязвимости мгновенно становятся достоянием широкой общественности.

ОС Android доступна большому числу производителей, выпускающих смартфоны с различными техническими характеристиками и версиями операционной системы. Несмотря на попытки Google оперативно выпускать обновления системы, закрывающие обнаруживаемые уязвимости, фрагментация платформы часто мешает пользователям своевременно получать эти обновления, так как каждый производитель имеет свою стратегию по их выпуску. Случается и так, что производитель вообще отказывается от дальнейших обновлений некоторых моделей по причине их устаревания, экономическим или техническим соображениям или же по каким-либо другим причинам, и пользователи становятся беззащитными перед угрозой троянцев, использующих root-эксплойты.

Доступный исходный код Android также может применяться различными энтузиастами, создающими свои сборки операционной системы. Вирусописатели освоили и эту нишу. Они могут распространять троянские программы (**Android.SmsHider**), имеющие цифровую подпись одного из образов такой сборки.

Благодаря этому методу приложение получает недоступные в обычных условиях права суперпользователя в системе, которой принадлежит использованный для подписи сертификат безопасности. А некоторые злоумышленники могут и вовсе встраивать троянские программы в подобные сторонние прошивки.

Пути и методы проникновения

Распространение вредоносных программ происходит следующими путями:

1. Использование известных уязвимостей, эксплуатирующихся для повышения привилегий вредоносного приложения в системе (**Android.Gongfu, Android.DreamExploid, Android.Wukong**).
2. Использование методов социальной инженерии. Наиболее часто используются следующие методы:
    1) предложение установить обновления (в том числе с «официального веб-сайта Opera Mini») (**Android.Crusewind, Java.SMSSend, Android.SmsSend**);
    2) предложение открыть уровни популярной игры;
    3) предложение в демонстрируемой рекламе срочной проверки мобильного устройства на вирусы. Нажав на рекламное сообщение, пользователь попадает на сайт, якобы сканирующий мобильное устройство. При этом сайт может заимствовать внешний вид известных антивирусных ресурсов и программ, например, внешнее оформление Dr.Web Security Space версии 7.0 (**Android.SmsSend**).

При этом зачастую вредоносная программа даже не использует для установки никаких уязвимостей — ее установка возлагается на жертву. Иногда в комплекте с инфицированным приложением жертве предлагается специальная пошаговая инструкция, позволяющая запустить ОС с полномочиями администратора. В инструкции утверждается, что это необходимо для корректной работы запускаемой программы или ее обновления (**Android.Gongfu**).

3. Оптимизация поисковых запросов. В ключевых словах, которые разработчики добавляют в описания программ, помещаются популярные словосочетания, не относящиеся к данному продукту, например, названия популярных игр. В результате ссылки на подобные программы часто демонстрируются в первых строках результатов поиска по каталогу программ.
4. Использование методов фишинга. Далеко не все пользователи Android в курсе, что ресурса под названием Android Market больше не существует. Пользователи обращаются с соответствующими запросами к поисковым системам и получают в выдаче ссылки на веб-сайты, подражающие своим оформлением оригинальному порталу Android Market. Как вариант в сети Интернет могут размещаться статьи, написанные «известными экспертами», рекомендующими «скачивать только с официального сайта Android Market», — и содержащие ссылки на фишинговый сайт. Существуют специально разработанные партнерские программы, позволяющие создавать сайты-подделки, с которых посетителям раздаются различные вредоносные приложения, в том числе троянцы семейства Android.SmsSend.
5. Размещение вредоносных программ в официальном каталоге приложений (Google Play, ранее известный как Android Market) (**Android.SmsSend, Android.DreamExploid, Android.DDLight**).
6. Распространение в составе легитимных программ на популярных сайтах-сборниках приложений (**Android.Spy, Android.Gongfu, Android.GoldDream, Android.Anzhu**), в том числе в составе приложений, целью которых является деятельность, связанная с отправкой СМС, поиском в Интернете, слежкой за пользователем, установкой других приложений и т. д.
7. Маскировка под обычные приложения (в том числе приложения, позволяющие изменять фоновый рисунок Рабочего стола Android, программы составления гороскопов, диет, программа-фонарик, чат-бот (программа I-Gir) и т. д.).
8. Взлом веб-ресурсов (в том числе автоматический с использованием специализированного ПО). При открытии веб-страниц происходит автоматическое перенаправление пользователя на интернет-ресурс, имитирующий оформление взломанного сайта, или начинается непосредственно загрузка троянца.
9. Использование ботнетов, предоставляющих возможность внедрения программ на зараженные компьютеры.

Особенностью методик заражения мобильных устройств является учет возможности использования жертвами различных платформ. Так, в зависимости от типа клиентской ОС жертвы могут получать либо приложения для Android (.apk), либо кросс-платформенные файлы типа .jar.

Цель проникновения

1. Рассылка СМС. Зараженные устройства могут использоваться для рассылки спама или иных тестовых сообщений (**Android.NoWay**), политических (**Android.Arspam**) и религиозных сообщений. Список рассылки может задаваться извне или браться из списка абонентов адресной книги. При этом вредоносная программа старается скрыть следы своей деятельности, удаляя из памяти смартфона отосланные ею сообщения и входящие СМС с информацией о приеме платежа оператором (**Android.SmsSend**). Отправка платного СМС может производиться уже на этапе установки вредоносной программы – при запуске пользователю демонстрируется текст о том, что владелец мобильного устройства соглашается с некими условиями, причем само соглашение с перечнем этих условий, как правило, отсутствует. В случае если соглашение присутствует, оно может быть скрыто от пользователя или иметь нейтральный, незаметный вид. Например, последнее слово в тексте может представлять собой гиперссылку на страницу с лицензионным соглашением и никак не выделяться на фоне окружающих слов. При подтверждении согласия нажатием на соответствующую кнопку приложение немедленно попытается отправить платное СМС-сообщение. Также возможен вариант, когда после запуска на экране устройства появляется вступительный текст и две кнопки: подтверждение согласия с условиями лицензии, и вторая, при нажатии на которую должен открываться текст соглашения, при этом соглашение располагается на стороннем веб-сайте, который в данный момент не функционирует, поэтому ознакомиться с предлагаемыми условиями пользователь не может.
2. Осуществление звонков на платные номера (**Android.Fakevoice**), кража денег со счетов владельцев мобильных телефонов путем подписки их на различные платные сервисы.
3. Добавление сайтов, указанных в конфигурационном файле вредоносной программы, в закладки браузера (**Android.Anzhu** не просто устанавливает закладки из переданного вирусописателями списка, но также меняет их атрибуты, помечая как посещенные, что придает таким закладкам больший вес в глазах пользователя).
4. Кража конфиденциальной информации (**Android.Gongfu, Android.SpyEye, Android.DreamExploid, Android.Gone**). Так, **Android.Gone.1** за 60 секунд «угоняет» всю хранящуюся на работающем под управлением Android мобильном телефоне информацию, включая идентификационную информацию о зараженном устройстве (в том числе версию операционной системы, модель телефона, наименование мобильного оператора, номер IMEI и телефонный номер пользователя), контакты, сообщения, последние звонки, историю браузера и т. д. Украденные данные загружаются на специально созданный вирусописателями сайт. Данные могут быть проданы для использования в спам-рассылках, целевом вымогательстве, осуществляемом с учетом знания данных жертвы. К числу платных шпионских программ относятся **Flexispy, Mobile Spy, Mobistealth**.
5. Вымогательство денег за похищенную информацию (**Android.Gone**).
6. Запуск и удаление различных программ на инфицированном устройстве, загрузка других вредоносных приложений (**Android.Gongfu, Android.Anzhu**).
7. Выполнение на инфицированном устройстве получаемых от управляющего центра команд (функции бэкдора имеют **Android.Plankton, Android.Gongfu, Android.GoldDream, Android.Anzhu**). Расширяемая архитектура вредоносных программ дает возможность владельцам криминальной сети загружать специальные дополнения (плагины) для выполнения дополнительных деструктивных действий – в том числе для проведения атаки на целевую компанию.
8. Блокировка окна браузера баннером, требующим отправить на короткий номер платное СМС-сообщение. Баннер выводится на экран не какой-либо троянской программой, а встроенным в просматриваемую пользователем веб-страницу сценарием, написанным на языке JavaScript. Данная угроза особо опасна для пользователей, устанавливающих антивирусное ПО в минимальной конфигурации, включающей только файловый монитор, – в этом случае антивирус не имеет возможности среагировать на угрозу.
9. Кража паролей доступа к различным программам, например паролям доступа к ftp-ресурсам компании.
10. Кража денежных средств компании через системы ДБО (**Android.SpyEye**). При обращении к различным банковским сайтам, адреса которых присутствуют в конфигурационном файле троянца, в просматриваемую пользователем веб-страницу осуществляется инъекция постороннего содержимого, которое может включать различный текст или веб-формы. Таким образом, ничего не подозревающая жертва загружает в браузере настольного компьютера или ноутбука веб-страницу банка, в котором у нее открыт счет, и обнаруживает сообщение о том, что банком введены в действие новые меры безопасности, без соблюдения которых пользователь не сможет получить доступ к системе «Банк-Клиент», а также предложение загрузить на мобильный телефон специальное приложение, содержащее троянскую программу.
11. Включение зараженных машин в управляемые ботнеты, координируемые из одного (или нескольких) командных центров.

Методы перехвата информации

1. Контроль за всеми СМС-сообщениями, а также входящими и исходящими телефонными звонками, запись сведений об этих событиях (в том числе телефонных номеров, с которых или на которые выполнялся звонок или отправлялось сообщение), сохранение содержания звонка и содержимого СМС (**Android.GoldDream**).
2. Запись нажатий пользователем клавиш – в том числе на виртуальной клавиатуре (**Android.AntaresSpy.1**).
3. Перехват информации, вводимой пользователем в браузере (в том числе во время работы с банком).
4. Подмена страниц банковских сайтов – в просматриваемую пользователем веб-страницу осуществляется инъекция постороннего содержимого, которое может включать различный текст или веб-формы. Таким образом, ничего не подозревающая жертва загружает в браузере настольного компьютера или ноутбука веб-страницу банка, в котором у нее открыт счет, и обнаруживает сообщение о том, что банком введены в действие новые меры безопасности, без соблюдения которых пользователь не сможет получить доступ к системе «Банк-Клиент», а также предложение загрузить на мобильный телефон специальное приложение, содержащее троянскую программу (**Android.SpyEye.1**).
5. Анализатор трафика и вклинивание в интернет-трафик в поисках учетных данных и передаваемых значений.
6. Перехват функций, которые могут участвовать в передаче данных.

Методы маскировки от средств контроля и наблюдения

1. Повышение прав до привилегий root и загрузка другого вредоносного приложения в качестве фонового сервиса, запускаемого в дальнейшем автоматически без участия пользователя.
2. Внедрение в другие работающие приложения – без использования собственного процесса.
3. Шифрование вирусными упаковщиками.
4. Деактивация используемых антивирусов.
5. Подмена цифровых сертификатов, файлов cookies.
6. Подмена домашней страницы в браузерах.
7. Блокировка доступа к различным ресурсам сети Интернет – в том числе серверам обновлений систем безопасности.

Обязательные средства защиты

Средство защиты	Необходимость применения
Система проверки ссылок	Система Cloud Checker позволяет исключить возможность перехода на зараженные и мошеннические ресурсы.
Проверка всех поступающих на устройство файлов (через GPRS/Infrared/Bluetooth/Wi-Fi/USB-соединения или во время синхронизации с ПК)	Позволяет уменьшить риск внедрения вредоносных программ из недоверенных источников, а также избежать скрытой загрузки незапрошенных компонентов приложений, содержащих вредоносный функционал.
Формирование списка разрешенных приложений	Позволяет уменьшить риск запуска неизвестных приложений без их предварительной проверки на безопасность.
Система ограничения доступа	Позволяет ограничить количество посещаемых ресурсов до необходимого минимума, что минимизирует риск заражения с сайтов, содержащих вредоносные объекты.
Антивирусный монитор	Позволяет исключить заражение с помощью вредоносных объектов, проникших на машину пользователя без проверки – в том числе в запароленных архивах или с помощью специальных протоколов передачи данных.
Антивирусный сканер	Периодическая глубокая проверка дает возможность обнаружения ранее неизвестных вирусов, находящихся в неактивированном виде.

Кроме установки и настройки программных средств защиты, рекомендуется:

1) ограничить права пользователей и запретить для них вход с правами администратора;
2) разрешить выход в Интернет только с отдельных компьютеров сети, не содержащих конфиденциальной информации;
3) своевременно устанавливать все обновления системы безопасности и использовать стойкие пароли.

Внимание! Перечисленные меры защиты должны быть предприняты на всех компьютерах, на которых производится работа с финансовыми средствами – в том числе в обязательном порядке на компьютерах и мобильных устройствах, вне зависимости от используемой операционной системы.

Рекомендуемые средства защиты

Средство защиты	Необходимость применения
Загрузка приложений только из известных и проверенных источников	Разработчики вредоносных программ зачастую предлагают загрузить известную программу «удобно и бесплатно». Однако в большинстве случаев сайты разработчиков этих программ позволяют сделать то же самое!*
Использование системы удаленного управления мобильным устройством в случае его утери или кражи	Система Антивор позволяет исключить риск утечки конфиденциальной информации путем кражи устройства.
Система централизованного управления	▪ Позволяет исключить возможность отключения пользователями систем защиты. ▪ Позволяет устанавливать единые для всей компании или групп пользователей правила информационной безопасности. ▪ Позволяет в случае возникновения той или иной угрозы мгновенно менять настройки системы безопасности.
Система сбора и анализа статистики	Дает возможность контролировать уровень защищенности компании в режиме реального времени, определять источники заражения.
Система сбора информации для служб технической поддержки	Позволяет минимизировать время решения тех или иных проблем.

* Для компаний, использующих решения Dr.Web для защиты рабочих станций, предоставляется бесплатная лицензия на Dr.Web Mobile Security Suite на тот же срок и на такое же количество защищаемых объектов, что и купленная лицензия.

Скомпрометированные средства защиты

Средство защиты	Методы обхода системы защиты
Установка приложений только с официального сайта Google Play* (ранее Android Market)	Схема работы Google Play позволяет загружать на него вредоносные программы, тем более что в момент загрузки на Google Play они могут не детектироваться ни одним антивирусом.
Использование программ, работающих в защищенном окружении (в том числе Java)	Подмена программных компонентов

* Плюсом использования Google Play является возможность централизованного удаления установленных приложений. Компания Google, как и Apple, может задействовать эту функцию, например, в случае если то или иное приложение представляет угрозу для пользователей.

Пример настройки средств защиты

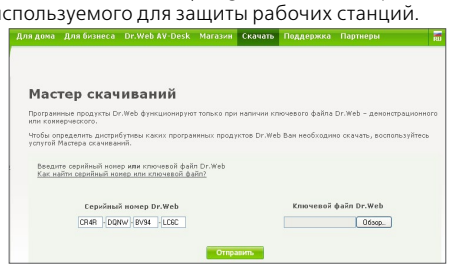
В качестве примера рассмотрим настройку системы защиты для операционной системы Android.

Установку версии антивируса Dr.Web, поддерживающей возможность централизованного управления, можно осуществить путем запуска установочного файла на мобильном устройстве или с помощью программы синхронизации с ПК. Версию без централизованного управления можно установить также с **Google Play** – для этого нужно только найти в списке приложений Dr.Web для Android и нажать **Install** (**Установить**).

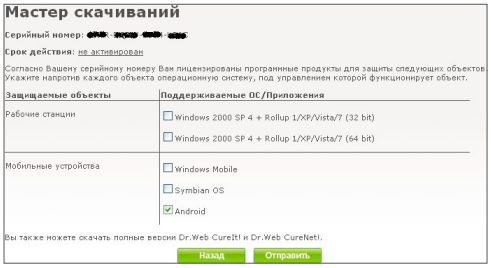
Чтобы установить приложение без использования Google Play, необходимо разрешить такой вид установки. Для этого откройте экран **Настройки** –> **Приложения** и установите флажок **Неизвестные источники**.

Для установки версии с возможностью использования в корпоративной сети необходимо:

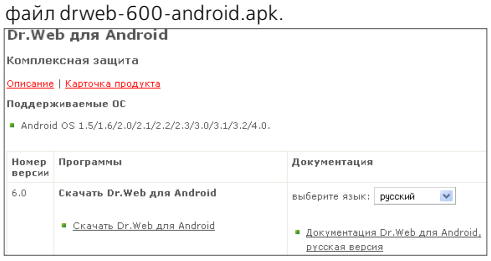
✓ Скачать файл установки Dr.Web для Android. Для этого на странице https://download.drweb.com/?lng=ru вводим серийный номер продукта, используемого для защиты рабочих станций.



Нажимаем **Отправить** и на странице **Мастера скачивания** выбираем, что мы хотим защищать.



Скачиваем файл drweb-600-android.apk.



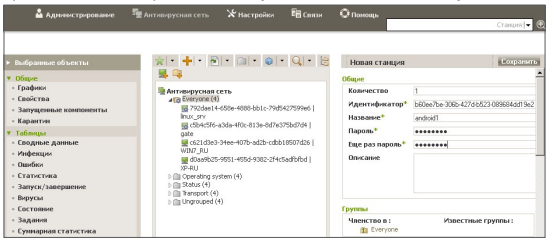
✓ Подключаем мобильное устройство к компьютеру при помощи USB-соединения и выбираем опцию распознавания мобильного устройства как диска.

✓ Копируем на SD-карту файл drweb-600-android.apk.

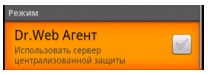
✓ Запускаем на мобильном устройстве любой файловый менеджер (например, ASTRO из Android Market), открываем папку /sdcard и запускаем drweb-600-android.apk.

✓ Антивирус Dr.Web установлен, однако для дальнейшей работы с приложением необходимо либо зарегистрировать лицензию и скопировать полученный ключевой файл на защищаемое устройство, либо подключить его к системе централизованного управления.

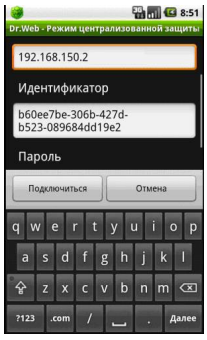
Для включения устройства в состав системы безопасности открываем Центр Управления Enterprise Security Suite и создаем новую станцию.



Зайдя в меню Dr.Web для Андроид, переходим в раздел **Инструменты** или нажимаем кнопку **Меню** и выбираем пункт **Настройки**. В разделе **Режим** отмечаем флажок **Dr.Web Агент**.



В открывшемся окне указываем IP-адрес сервера централизованной антивирусной защиты и через двоеточие после IP-адреса порт, использующийся для подключения к серверу, идентификатор, присвоенный вашему мобильному устройству при создании станции, и пароль.



Нажимаем **Подключиться**.

В режиме централизованной защиты блокируется возможность ручного запуска и настройки обновлений. Системный администратор может определять параметры постоянной защиты, определять список приложений, доступных пользователям антивирусной сети на их устройствах, и проводить проверку системы по требованию.

О компании «Доктор Веб»

Компания «Доктор Веб» – российский разработчик средств информационной безопасности и лидер российского рынка интернет-сервисов безопасности. Антивирусные продукты Dr.Web разрабатываются с 1992 года и имеют сертификаты ФСТЭК России, ФСБ России и Министерства обороны РФ.

Наличие в нашем штате экспертов по различным вопросам, связанным с информационной безопасностью, позволяет нам максимально учитывать особенности работы компаний самого разного размера и профиля деятельности. Мы предлагаем нашим клиентам оптимальный выбор продуктов, имеющих минимальную совокупную стоимость, и, как разработчик этих продуктов, гарантируем их высокое качество.

Проверить качество работы наших решений вы можете как с помощью бесплатных лечащих утилит Dr.Web CureNet! и Dr.Web CureIt!, так и с помощью сервиса тестирования наших решений – Dr.Web LiveDemo.