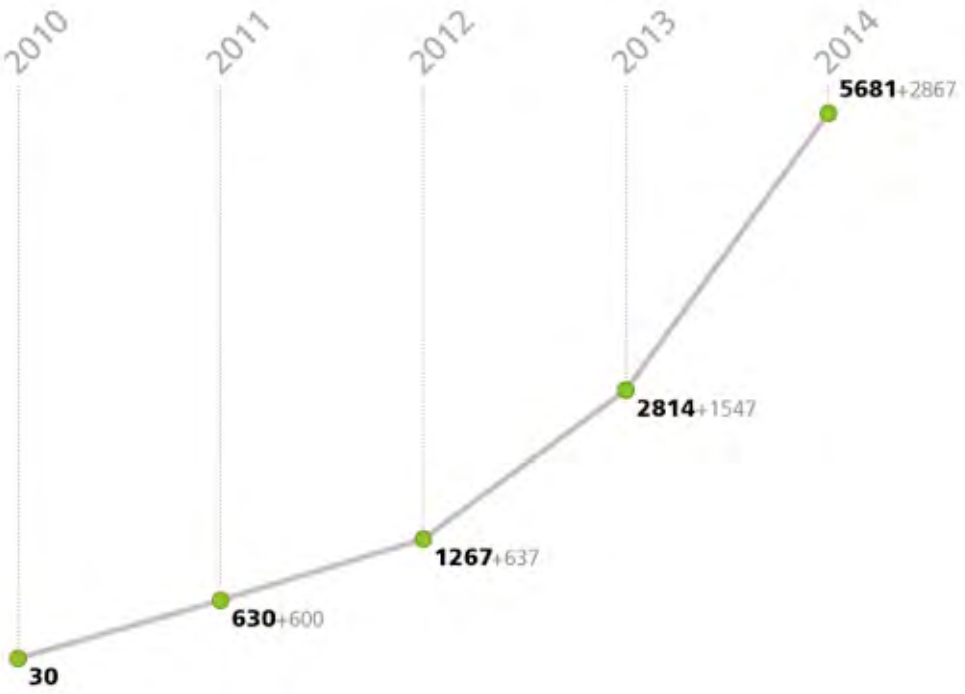
Мобильное воровство

Android — самая популярная среди пользователей операционная система для мобильных устройств и вторая по популярности после Windows для вирусописателей. Первые вредоносные программы для Android появились в 2010 году.

Больше всего вредоносных программ создается для инфицирования мобильных устройств под управлением Android — на это влияет широта распространения данной ОС и открытость ее кода, а также возможность установки приложений, полученных из любого источника.

Этот график показывает рост количества записей вредоносных программ для ОС Android в вирусной базе Dr.Web



Рост количества записей за 2014 год — 102%!

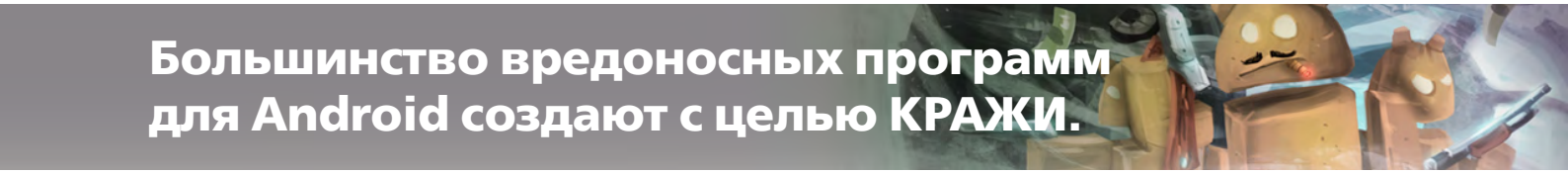
С 2010 года количество записей увеличилось в 189 раз!

На 1 апреля 2015 года количество сигнатур, добавленных в базу Dr.Web для обнаружения вредоносных программ для Android, достигло почти 7 000.

То есть только за три первых месяца 2015 года база увеличилась более чем на 25%!

При этом нужно пронимать, что с помощью одной сигнатуры Dr.Web может определять куда как больше одной вредоносной программы.

Большинство вредоносных программ для Android создают с целью КРАЖИ.



Мобильные устройства обладают богатым функционалом, и создатели Android-троянцев крадут все, что можно украсть:

- Денежные средства — с мобильного счета, систем онлайн-платежей и банковской карты
- Логины и пароли — к системам онлайн-банкинга и электронных платежей, аккаунтам в социальных сетях и т. д.
- СМС-ки
- Звонки
- Сообщения электронной почты
- Фотографии — с их помощью можно шантажировать жертву или нанести ей моральный ущерб, выложив снимки в Интернете
- Записи переговоров владельца мобильного устройства — даже если он сам их не вел, за него это может сделать троянец
- Адреса из книги контактов
- Координаты устройства — т. е. местоположение его владельца и данные о его перемещениях
- Любого рода техническую информацию об устройстве (IMEI/IMSI/SID-идентификаторы, номер мобильного телефона, версию ОС, версию SDK-системы, модель устройства, данные о его производителе)

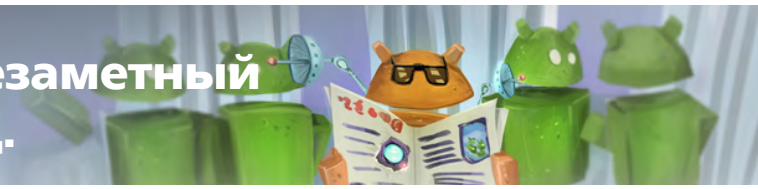
Во многих случаях пользователи сами скачивают и устанавливают на мобильные устройства вредоносные программы!

Так, например, Android.Plankton, способный собирать и передавать информацию о зараженном устройстве, был вручную загружен пользователями 150 000 раз (!) с официального сайта Android Market (прежнее название Google Play), прежде чем был удален администрацией портала.

По статистике Dr.Web для Android, примерно у 50% наших пользователей на устройстве включена опция установки приложений из неизвестных источников (т. е. не из экосистемы Google Play). А это значит, что пользователи могут сами устанавливать вредоносные приложения, скачанные с какого-нибудь сомнительного форума или сайта.

Приемы социальной инженерии позволяют киберпреступникам широкомасштабно распространять троянцев среди пользователей. Например, более 30 тысяч южнокорейских владельцев Android-устройств загрузили банковского троянца Android.SmsBot.75.origin при попытке ознакомиться с судьбой «почтового отправления». Большинство пользователей свято уверены в том, что они заметят действие троянца на мобильном устройстве.

Хороший троянец — это незаметный для пользователя троянец.



Это давно усвоили вирусописатели.

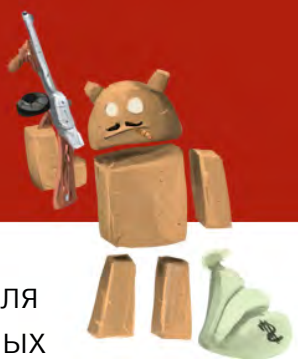
Действие наиболее успешных троянцев, направленных на кражу, в большинстве случаев можно обнаружить только когда все уже украдено.

- Например, троянец-дозвонщик Android.Dialer.7.origin, чтобы уменьшить вероятность обнаружения пользователем своей нежелательной активности, отключает разговорный динамик мобильного устройства на время инициируемого им же «телефонного разговора», а для окончательного сокрытия вредоносной деятельности удаляет из системного журнала, а также из списка совершенных звонков всю компрометирующую его информацию.

- Троянцы, которые крадут средства со счета мобильного телефона путем подписки пользователя на какие-либо платные услуги, также отлично «шифруются» на устройстве жертвы. Обычно платный сервис присылает подтверждающее СМС при успешном завершении операции — вот эти СМС и скрывают троянцы, чтобы пользователь не забил тревогу раньше времени. Некоторые вредоносные программы умеют автоматически отсылать СМС с кодом подтверждения для выполнения авторизации в платных сервисах — такие сообщения тоже нередко перехватываются и скрываются.
- Многие «продвинутые» троянцы распространяются под видом легальных программ, а после запуска удаляют свой значок и в дальнейшем работают незаметно для пользователей.
- Существуют троянцы, которые помещаются злоумышленниками внутрь операционной системы или встраиваются в распространяемые образы прошивок. Такие «партизаны» имеют расширенные полномочия и способны незаметно выполнять самый широкий спектр нежелательных действий.
- Чтобы не попасться антивирусным программам, некоторые троянцы снабжаются функцией противодействия подобному защитному ПО: антивирусы могут блокироваться и даже полностью удаляться ими с устройства.

Троянцы-банкеры

Это семейства Android-троянцев, созданные для кражи средств с банковских карт и из систем онлайн-платежей.



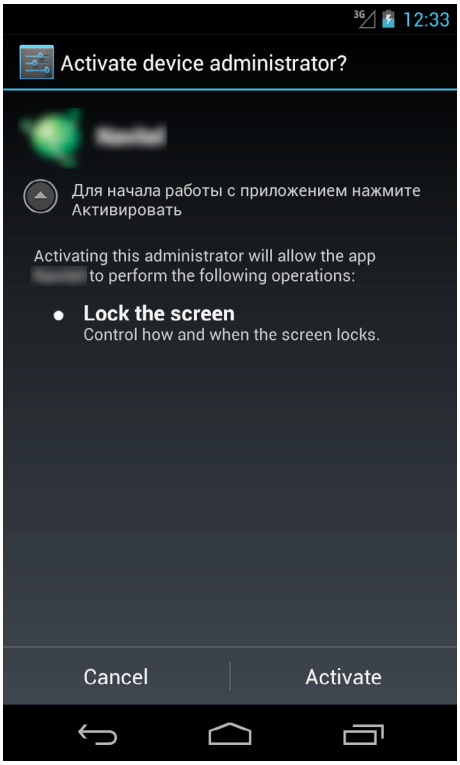
Мобильный банкинг — это действительно удобно. Многие банки предлагают своим пользователям Android-версии приложений для онлайн-банкинга. Их используют не только для проведения личных операций, но и для корпоративных платежей. Как правило, этой возможностью пользуются руководители высшего звена компаний, имеющие доступ к счету.

Кража денежных средств — наиболее важный вектор атак вирусописателей.

Android.BankBot.33.origin

Способен:

- получать информацию о текущем балансе банковского счета и списке подключенных к мобильному телефону пользователя банковских карт;
- похищать аутентификационные данные учетной записи онлайн-банкинга, загружая в браузере зараженного устройства имитирующий внешний вид настоящего интернет-портала банка мошеннический веб-сайт, где жертве будет предложено ввести конфиденциальные сведения для входа;
- выполнять незаконные операции с денежными средствами жертв, выводя их на принадлежащий злоумышленникам счет



Жертва может некоторое время оставаться в неведении о произошедшей краже, потому что Android.BankBot.33.origin способен перехватить и заблокировать СМС-уведомления о совершенных операциях.

Пользователи САМИ устанавливают данного троянца (для этого в настройках операционной системы должна быть разрешена установка программ из сторонних источников)!

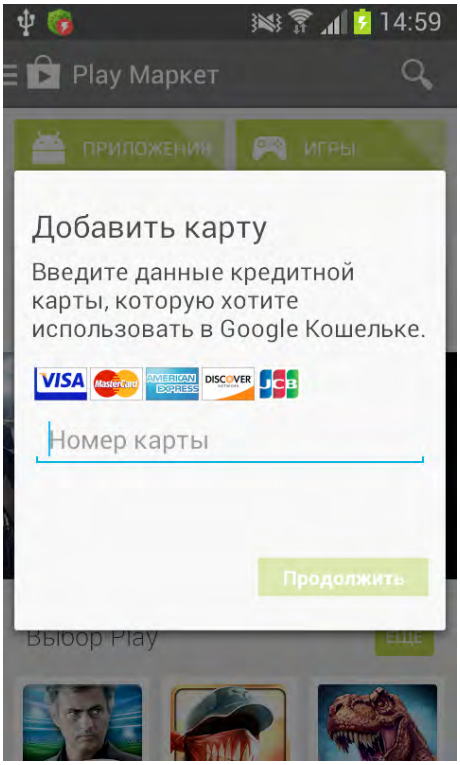
С января по апрель 2015 года данная троянская программа была обнаружена на устройствах пользователей Антивируса Dr.Web для Android 62 840 раз, что составляет 0,37% от общего числа выявленных за этот период угроз.

Android.SpyEye.1

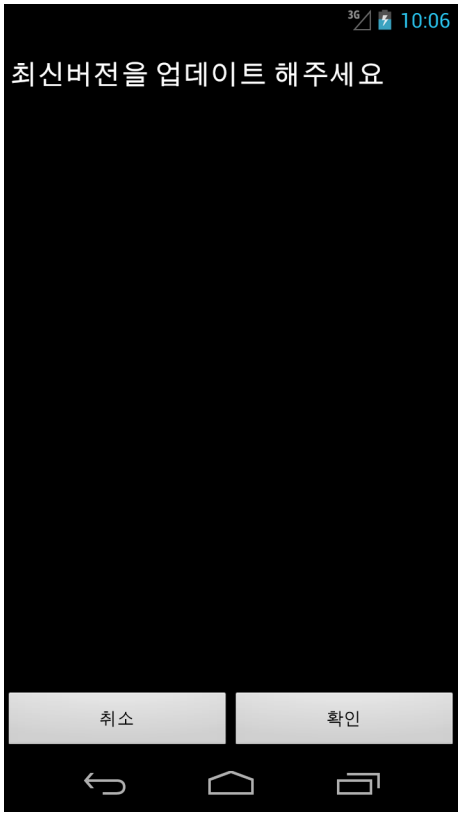
Если пользователь настольного компьютера или ноутбука посещает банковский сайт, адрес которого присутствует в конфигурационном файле заразившего его компьютер банковского троянца, в просматриваемую пользователем веб-страницу осуществляется инъекция постороннего текста или веб-формы для ввода данных доступа к счету. Ничего не подозревающая жертва загружает в браузере 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 обновление к мобильному клиенту, содержащее троянскую программу. Эта программа способна перехватывать и пересылать злоумышленникам направляемые по СМС одноразовые пароли, необходимые для доступа к системе «Банк-Клиент».

Android.BankBot.21.origin

Для того чтобы заполучить платежные реквизиты используемой банковской карты и похитить средства, Android.BankBot.21.origin проверяет, активно ли на мобильном устройстве окно приложения Google Play, и, если это так, имитирует стандартную форму привязки карты к учетной записи пользователя. Введенная жертвой информация передается на принадлежащий злоумышленникам сервер. Дальнейший увод средств — дело техники.



Android.SpyEye.1



Троянец пытается получить права администратора мобильного устройства — он «прячет» от пользователя соответствующий системный запрос за собственным диалоговым окном, в результате чего потенциальная жертва с высокой долей вероятности может предоставить вредоносному приложению необходимые полномочия. Дальнейшая кража денежных средств — дело техники.

Кража входящих СМС

Велика беда, скажете вы, кража СМС-ки. Все зависит от того, с какой целью на ваш телефон было отправлено украденное злоумышленниками СМС.

Какие входящие СМС, потеря которых может привести к финансовому ущербу, крадут троянцы?

- СМС, подтверждающие или спрашивающие разрешения на подключение к мобильным премиум-сервисам и контент-услугам. Их крадут для того, чтобы жертва как можно дольше не узнала о подписке на такие сервисы и не предприняла действий к остановке деятельности троянца.
- СМС с сообщениями от систем «Банк-Клиент», содержащие проверочные mTAN-коды.

Украденные СМС перенаправляются на управляющий троянцем сервер, принадлежащий злоумышленникам. Этот функционал присутствует в троянцах нескольких семейств.

Кража денег путем отправки исходящих СМС

Например, троянцы семейства **Android. SmsSend** списывают деньги с мобильного счета в пользу преступников путем отправки дорогостоящих СМС с телефона жертвы.

Согласно полученной с использованием Dr.Web для Android статистике, число детектирований троянцев семейства Android.SmsSend составило 20 223 854 в 2014 году.

Троянцы семейства Android.SmsBot также могут отправлять, перехватывать и удалять СМС-сообщения.

Согласно полученной с использованием Dr.Web для Android статистике, число детектирований троянцев семейства Android.SmsBot составило 5 985 063 в 2014 году.

Кража денег путем осуществления звонков на премиум-номера

Дозвонщики — семейство Android-троянцев, совершающих втайне от владельца мобильного устройства звонки на премиум-номера. Этот также популярный у вирусописателей способ «заработка».

Согласно полученной с использованием Dr.Web для Android статистике, число детектирований троянцев семейства Android.Dialer составило 177 397 в 2014 году.

Кража адресов контактов

При всей безобидности формулировки — это тоже бизнес. Любой живой контакт можно продать, и на него есть несколько категорий покупателей.

1. Спамеры. Спамерство — это бизнес, который живет и процветает. И это не только спам-рассылки безобидной рекламы.

Массовая отправка содержащих ссылку на загрузку вредоносной программы СМС-сообщений становится все более популярным методом распространения современных Android-угроз.

Например Android.Wormle.1.origin может распространяться при помощи СМС-сообщений среди всех знакомых владельца устройства. На конец ноября 2014 года Android.Wormle.1.origin успел заразить более 15 000 мобильных Android-устройств жителей порядка 30 стран.

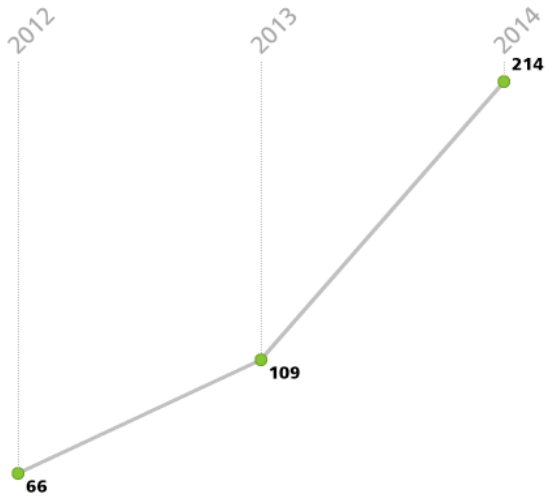
2. Фишеры. Они собирают контакты с целью отправки фишинговых писем со ссылками якобы на сайты банков или платежных систем. Если вы перейдете на такой сайт, фишер сможет выудить у вас аутентификационные данные для входа в систему онлайн-банкинга или данные банковской карты. Причем отдадите вы их собственноручно, введя в предложенную фишером форму нужные данные, думая, что находитесь на сайте банка.

3. Организаторы DDoS-атак — им позарез нужны контакты владельцев мобильных устройств, которые можно заразить и использовать для организаций DDoS-атак, например, на неугодного заказчику конкурента.

4. Шпионы (спецслужбы, конкуренты). Всякий контакт — находка для шпиона или шантажиста. А еще следящие за вами люди могут читать вашу переписку, вести записи ваших разговоров, скачивать на удаленный сервер ваши фотографии.

Например, Android.Spy.130.origin передает злоумышленникам сведения об СМС-переписке, совершенных звонках, текущих GPS-координатах, а также способен незаметно выполнить звонок на заданный номер, превращая зараженный смартфон или планшет в прослушивающее устройство.

График роста количества записей троянцев семейства Android.Spy в вирусной базе Dr.Web



Вы активно используете сервисы

- Google Play
- Google Play Music
- Gmail
- WhatsApp
- Viber
- Instagram
- Skype
- «ВКонтакте»
- «Одноклассники»
- Facebook
- Twitter...?

Злоумышленникам вполне пригодятся данные, которые вы там храните, — с целью продажи или шантажа!

Dr.Web защищает Android-устройства от мобильного воровства

Компоненты защиты

Антивирус
Защитит от троянцев и других вредоносных программ

Антивор
Поможет найти мобильное устройство в случае его утери или кражи и при необходимости удаленно стереть с него конфиденциальную информацию

Антиспам
Оградит от нежелательных звонков и СМС-сообщений

Облачный URL-фильтр
Ограничит доступ к нежелательным интернет-ресурсам вне зависимости от состояния вирусных баз на вашем Dr.Web для Android

Брандмауэр
Проконтролирует сетевую активность приложений

Аудитор безопасности
Произведет диагностику, выявит проблемы безопасности и предложит решения для их устранения

Полезные ссылки

Видео о настройках Dr.Web для Android

О компании «Доктор Веб»

«Доктор Веб» — российский производитель антивирусных средств защиты информации под маркой Dr.Web. Продукты Dr.Web разрабатываются с 1992 года. Компания — ключевой игрок на российском рынке программных средств обеспечения базовой потребности бизнеса — безопасности информации.
«Доктор Веб» — один из немногих антивирусных вендоров в мире, владеющих собственными уникальными технологиями детектирования и лечения вредоносных программ. Компания имеет свою антивирусную лабораторию, глобальную службу вирусного мониторинга и службу технической поддержки.
Стратегической задачей компании, на которую нацелены усилия всех сотрудников, является создание лучших средств антивирусной защиты, отвечающих всем современным требованиям к этому классу программ, а также разработка новых технологических решений, позволяющих пользователям встречать во всеоружии любые виды компьютерных угроз.

Полезные ресурсы
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах