Dr.WEB®
с 1992 года

# Обзор вирусной активности для мобильных Android-устройств за 2017 год

# Обзор вирусной активности для мобильных Android-устройств за 2017 год

29 декабря 2017 года

События в сфере информационной безопасности уходящего года показали, что интерес киберпреступников к мобильным устройствам по-прежнему высок. Об этом говорит как появление новых вредоносных Android-программ, так и расширение их функционала. Так, на протяжении последних 12 месяцев владельцам смартфонов и планшетов угрожали троянцы, которые использовали специальные возможности (Accessibility Service) платформы Android. С их помощью они незаметно выполняли вредоносные действия – например, меняли системные настройки, а также скрытно скачивали и устанавливали ПО.

Серьезную опасность вновь представляли банковские троянцы, похищавшие логины, пароли и другую секретную информацию и помогавшие злоумышленникам красть деньги со счетов жертв. Публикация в 2016 году исходных кодов одного из Android-банкеров упростила вирусописателям создание новых вредоносных приложений такого типа.

Актуальной осталась проблема Android-вымогателей – троянцев, которые блокируют мобильные устройства и требуют выкуп за восстановление их работоспособности. В 2017 году среди этих вредоносных программ вновь встречались и энкодеры, шифровавшие файлы.

Нельзя не отметить появление в каталоге Google Play множества новых угроз. Среди них оказались как троянские, так и нежелательные программы.

Кроме того, в 2017 году получили распространение вредоносные приложения, которые открывали веб-сайты для накрутки их популярности, выполняли переходы по ссылкам и нажимали на рекламные баннеры. Были обнаружены и новые троянцы, предназначенные для добычи криптовалют.

# Обзор вирусной активности для мобильных Android-устройств за 2017 год

## Главные тенденции года

- Появление троянцев, использующих специальные возможности ОС Android
- Обнаружение большого числа вредоносных и нежелательных программ в каталоге Google Play
- Появление новых банковских троянцев
- Распространение вредоносных приложений, которые открывали веб-сайты для накрутки счетчика их посещений, нажимали на расположенные на них рекламные баннеры и переходили по ссылкам
- Обнаружение новых троянцев, которые добывали криптовалюты с использованием мощностей зараженных мобильных устройств

## Наиболее интересные события

В 2017 году получили распространение вредоносные программы, которые задействовали специальный режим работы (Accessibiliy Service) ОС Android. Функции этого режима облегчают использование смартфонов и планшетов людьми с ограниченными возможностями. Однако, получив доступ к таким функциям, троянец фактически будет полностью контролировать зараженное устройство и сможет выполнять вредоносные действия без вмешательства владельца аппарата. Например, имитировать нажатие кнопок в диалоговых окнах, открывать и изменять различные настройки, а также автоматически устанавливать другие приложения.

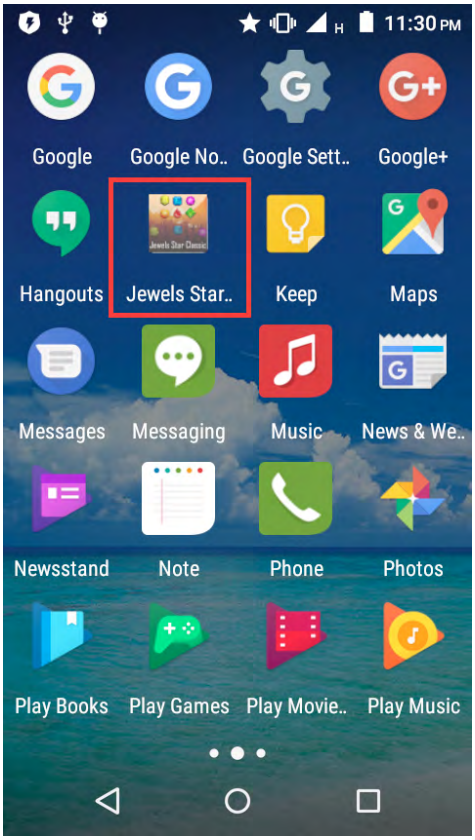
Одним из таких троянцев был Android.BankBot.211.origin. Получив необходимые полномочия, он самостоятельно добавлялся в список администраторов устройства, назначал себя менеджером СМС по умолчанию и мог фиксировать все, что происходило на экране устройства. Android.BankBot.211.origin показывал поддельные формы авторизации при запуске банковских и других программ, делал скриншоты при каждом нажатии клавиатуры, а также передавал злоумышленникам информацию обо всех СМС и телефонных звонках.

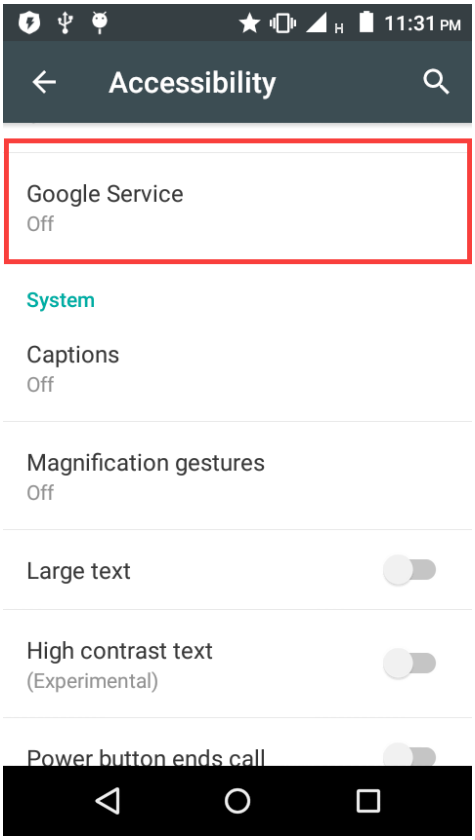

Android.DownLoader.504.origin – еще один троянец, который использовал специальные возможности ОС Android для автоматического выполнения вредоносных действий. Он незаметно скачивал различные приложения, а также других троянцев, после чего самостоятельно устанавливал их.

Кроме того, в прошлом году была выявлена вредоносная программа Android.BankBot.233.origin с аналогичным функционалом. Она извлекала из своих ресурсов и с использованием специальных возможностей незаметно инсталлировала банковского троянца Android.BankBot.234.origin.

# Обзор вирусной активности для мобильных Android-устройств за 2017 год

Он отслеживал запуск Play Маркет и поверх окна приложения показывал фишинговую форму настройки платежного сервиса, в которой запрашивал информацию о банковской карте. Полученные сведения Android.BankBot.234.origin передавал вирусописателям, после чего те могли украсть деньги со счета жертвы.




Киберпреступники используют большинство вредоносных и нежелательных Android-программ для получения прибыли. Наряду с кражей денег с применением банковских троянцев другим популярным источником незаконного заработка злоумышленников является загрузка и установка приложений на мобильные устройства без ведома их владельцев. В 2016 году специалисты «Доктор Веб» отмечали появление и широкое распространение созданных для таких целей троянцев и нежелательных программ. В 2017 году эта тенденция продолжилась. В январе компания «Доктор Веб» рассказывала о троянце Android.Skyfin.1.origin, который внедрялся в процесс программы Play Маркет и скачивал от ее имени приложения из каталога Google Play. Android.Skyfin.1.origin не устанавливал загружаемое ПО, однако полностью имитировал его инсталляцию, подменяя различные параметры при обращении к серверу компании Google и обманывая его. В результате троянец искусственно накручивал счетчик установок и увеличивал популярность программ. Кроме того, он мог самостоятельно оставлять поддельные отзывы, поднимая рейтинг приложений и делая их более привлекательными для пользователей.

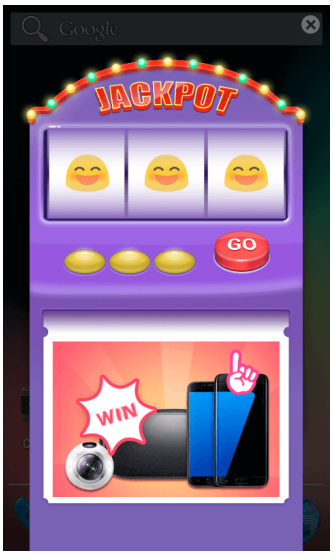
# Обзор вирусной активности для мобильных Android-устройств за 2017 год

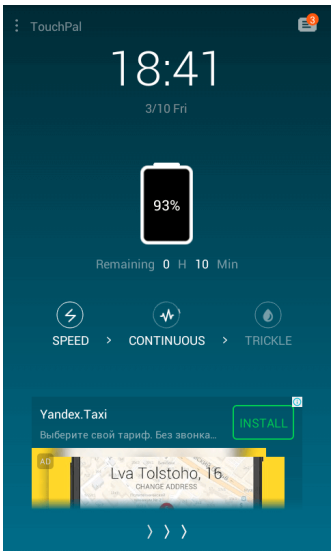
В мае в каталоге Google Play был найден Android.RemoteCode.28, который также загружал другие программы из Интернета. А в июле вирусные аналитики «Доктор Веб» обнаружили троянца Android.Triada.231. Злоумышленники встроили его в одну из системных библиотек ОС Android и поместили в прошивку нескольких моделей мобильных устройств. Android.Triada.231 внедрялся в процессы всех программ и мог незаметно скачивать и запускать дополнительные вредоносные модули.

Другой распространенный метод заработка киберпреступников – загрузка веб-сайтов для накрутки их посещаемости, а также нажатие («клики») на расположенные на них баннеры и другие элементы. Одной из вредоносный программ, которые злоумышленники использовали в 2017 году для этих целей, был распространявшийся через Google Play троянец Android.RemoteCode.106.origin. Он скачивал вспомогательные модули и с их помощью открывал сайты, после чего переходил по имеющимся на них ссылкам и нажимал на объявления.

Схожий функционал был и в обнаруженных в 2017 году новых троянцах семейства Android.Click. Например, Android.Click.132.origin по указанию управляющего сервера незаметно загружал веб-страницы и автоматически нажимал на расположенные на них рекламные объекты. Вредоносные программы Android.Click.268, Android.Click.269 и Android.Click.274 также открывали веб-страницы и нажимали на заданных злоумышленниками областях, накручивая счетчик переходов по рекламным объявлениям. Кроме того, они получали от управляющего центра адреса веб-сайтов, на которые отправляли по 10 миллионов пустых запросов. В результате пользователи, которые установили этих троянцев, невольно становились участниками DDoS-атак.

Показ агрессивной рекламы по-прежнему является популярным источником дохода для вирусописателей и недобросовестных разработчиков ПО. В марте 2017 года компания «Доктор Веб» рассказывала об одном из нежелательных рекламных модулей, получившем имя Adware.Cootek.1.origin. Он был встроен в безобидное приложение-клавиатуру под названием TouchPal и распространялся через каталог Google Play. В общей сложности эту программу загрузили более 50 000 000 пользователей. Adware.Cootek.1.origin показывал надоедливые объявления и даже встраивал баннеры в экран блокировки.



А в апреле в Google Play был найден троянец Android.MobiDash.44, который распространялся под видом руководств к популярным играм. Он показывал навязчивую рекламу, а также мог загружать дополнительные вредоносные модули.

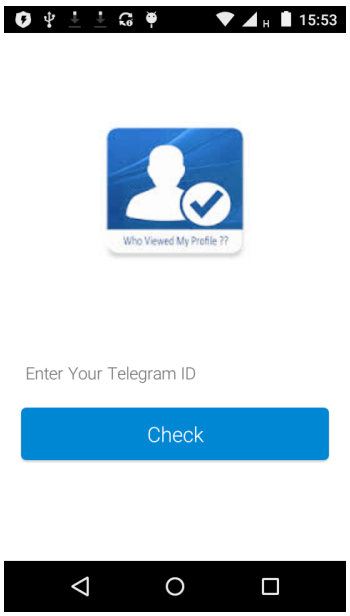
Добычу (майнинг) криптовалют с использованием мобильных устройств нельзя назвать эффективным источником заработка. Тем не менее, этот способ обогащения по-прежнему привлекает киберпреступников. В ноябре 2017 года в каталоге Google Play был обнаружен троянец-майнер Android.CoinMine.3. Эта вредоносная программа незаметно загружала веб-сайт со встроенным в него скриптом, который добывал криптовалюту Monero.

Однако злоумышленники используют вредоносные программы не только для получения прибыли. Некоторые троянцы применяются для слежки и кибершпионажа. Так, в апреле 2017 года появилась информация о вредоносных приложениях Android.Chrysaor.1.origin и Android.Chrysaor.2.origin, задействованных в таргетированных атаках. Они крали переписку из множества программ для общения, таких как Skype, Viber, WhatsApp, Twitter, Facebook, почтовых клиентов и других, перехватывали СМС, осуществляли прослушку через микрофон зараженных смартфонов и планшетов и записывали телефонные звонки. Кроме того, эти троянцы отслеживали местоположение мобильных устройств, похищали историю браузера, передавали злоумышленникам информацию о контактах из телефонной книги и собирали другие конфиденциальные данные.

А уже в июле стало известно о похожем троянце, который получил имя Android.Lipizzan.2. Он также крал переписку из популярных мессенджеров и почтовых клиентов, перехватывал и записывал телефонные разговоры, выполнял прослушку с использованием микрофона, делал скриншоты экрана и отслеживал местоположение зараженных устройств.

Помимо этого, в 2017 году компания «Доктор Веб» обнаружила вредоносную программу Android.Spy.377.origin, которая шпионила за иранскими пользователями. Злоумышленники управляли ей при помощи команд, передаваемых через протокол обмена сообщениями онлайн-мессенджера Telegram. Android.Spy.377.origin отправлял киберпреступникам информацию обо всех доступных на устройстве файлах и мог загружать любой из них на управляющий сервер. Кроме того, по команде вирусописателей троянец рассылал СМС-сообщения, выполнял телефонные звонки, отслеживал координаты зараженного смартфона или планшета, крал все входящие и исходящие СМС, а также другие конфиденциальные сведения.

# Обзор вирусной активности для мобильных Android-устройств за 2017 год




## Вирусная обстановка в сегменте мобильных устройств

Согласно статистике детектирований антивирусными продуктами Dr.Web для Android, в 2017 году на Android-устройствах наиболее часто встречались троянцы, которые без разрешения загружали другие вредоносные программы и скачивали ненужное ПО. Кроме того, существенную долю среди обнаруженных угроз составили рекламные троянцы.

# Обзор вирусной активности для мобильных Android-устройств за 2017 год

- **Android.DownLoader.337.origin**
  Троянец, выполняющий загрузку заданных вирусописателями приложений.
- **Android.HiddenAds**
  Представители семейства троянцев, предназначенных для показа навязчивой рекламы.
- **Android.Triada.63**
  Многофункциональный троянец, выполняющий разнообразные вредоносные действия.
- **Android.Click.171.origin**
  Представитель семейства троянцев, предназначенных для накрутки количества посещений заданных злоумышленниками веб-сайтов.
- **Android.Loki.19.origin**
  Вредоносная программа, предназначенная для загрузки других троянцев.
- **Android.Cooee.1.origin**
  Троянская программа, которая незаметно загружает и устанавливает приложения, а также показывает рекламу.
- **Android.CallPay.1.origin**
  Вредоносная программа, которая предоставляет владельцам Android-устройств доступ к эротическим материалам, но в качестве оплаты этой «услуги» незаметно совершает звонки на премиум-номера.

Что же касается нежелательных и потенциально опасных программ, которые были выявлены на смартфонах и планшетах в 2017 году, то здесь, как и годом ранее, наблюдалась аналогичная картина. За последние 12 месяцев на мобильных Android-устройствах чаще всего встречались нежелательные программные модули, которые показывали рекламу.

**Adware.Jiubang.1**

**Adware.Jiubang.2**

**Adware.Leadbolt.12.origin**

**Adware.Airpush.31.origin**

**Adware.Adpush.7**

**Adware.SalmonAds.1.origin**

**Adware.Avazu.8.origin**

**Adware.Patacore.2**

**Adware.Fly2tech.2**

**Adware.Appsad.3.origin**

Нежелательные модули, которые разработчики ПО и вирусописатели встраивают в приложения для показа агрессивной рекламы.

## Банковские троянцы

Нежелательные модули, которые разработчики ПО и вирусописатели встраивают Банковские троянцы – одни из самых опасных вредоносных приложений, поскольку с их помощью киберпреступники похищают деньги. В течение 2017 года Android-банкеры проникали на мобильные устройства более 1 900 000 раз, что на 9,5% меньше, чем годом ранее. Динамика обнаружения этих вредоносных программ за последние 12 месяцев показана на следующей иллюстрации:

# Обзор вирусной активности для мобильных Android-устройств за 2017 год

Заметным событием уходящего года стало распространение Android-банкеров, созданных на основе опубликованного исходного кода вредоносной программы Android.BankBot.149.origin. Среди них был Android.BankBot.179.origin, обнаруженный в каталоге Google Play в апреле. Этот троянец показывал поддельные формы ввода логина и пароля при запуске более чем 200 банковских приложений. В результате владельцы зараженных смартфонов и планшетов не подозревали, что видят мошенническое окно, и указывали секретную информацию, которая затем передавалась злоумышленникам. Android.BankBot.179.origin перехватывал все поступающие от кредитных организаций СМС с проверочными кодами и автоматически подтверждал перевод денег на счета киберпреступников.

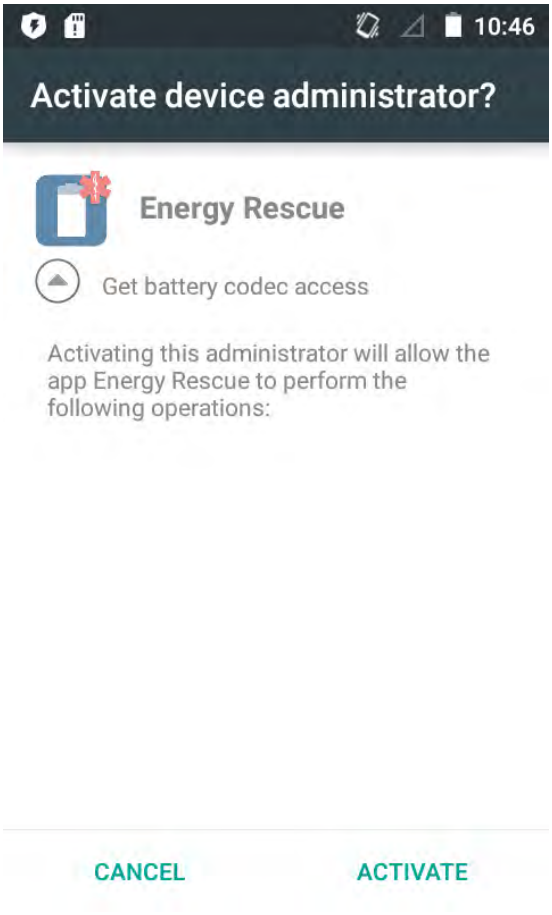
Другие троянцы, созданные на основе опубликованных исходных кодов, получили имена Android.BankBot.160.origin и Android.BankBot.163.origin. Они были встроены в приложения для показа прогноза погоды и также распространялись через каталог Google Play. Эти вредоносные программы отслеживали запуск банковских приложений и демонстрировали поддельные окна авторизации при их открытии.

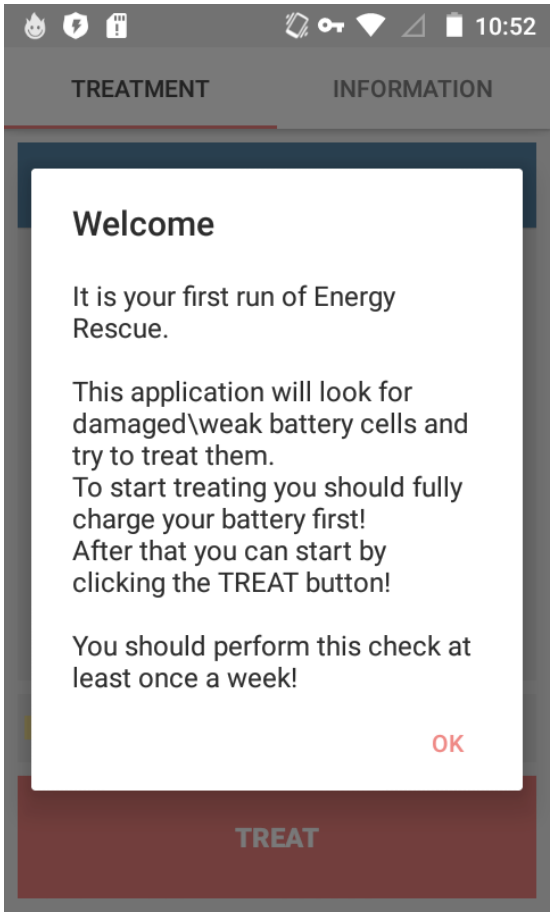
Среди прочих Android-банкеров, которые атаковали пользователей мобильных устройств в 2017 году, был Android.Banker.202.origin. Он скрывался в безобидных программах и распространялся через каталог Google Play. После старта Android.Banker.202.origin извлекал из своих файловых ресурсов и запускал вредоносное приложение Android.Banker.1426. Оно, в свою очередь, скачивало с управляющего сервера один из Android-банкеров семейства Android.BankBot, который крал логины, пароли и другую конфиденциальную информацию.

## Троянцы-вымогатели

Вредоносные программы-вымогатели представляют серьезную опасность. Они блокируют мобильные устройства и даже шифруют файлы на них, после чего требуют выкуп. В 2017 году владельцы Android-смартфонов и планшетов вновь столкнулись с подобными локерами. В течение 12 месяцев антивирусные продукты Dr.Web для Android обнаружили этих троянцев более 177 000 раз. Динамика детектирования Android-вымогателей показана на следующем графике:

Один из таких троянцев был найден в каталоге Google Play в январе и получил имя Android.Locker.387.origin. Он скрывался в приложении под названием Energy Rescue, которое якобы восстанавливало некие поврежденные и слабые ячейки аккумулятора. В действительности же Android.Locker.387.origin не мог выполнить обещанной процедуры и лишь имитировал бурную деятельность. Вместо восстановления батареи он блокировал экран зараженного устройства, для чего запрашивал доступ к функциям администратора и требовал заплатить злоумышленникам.




Уже в июне широкую известность получил вымогатель Android.Encoder.3.origin, который атаковал китайских пользователей и шифровал файлы на карте памяти Android-устройств. Он интересен тем, что его окно с требованием выкупа было оформлено в стиле нашумевшего троянца-шифровальщика WannaCry, заразившего сотни тысяч компьютеров по всему миру в мае 2017 года.

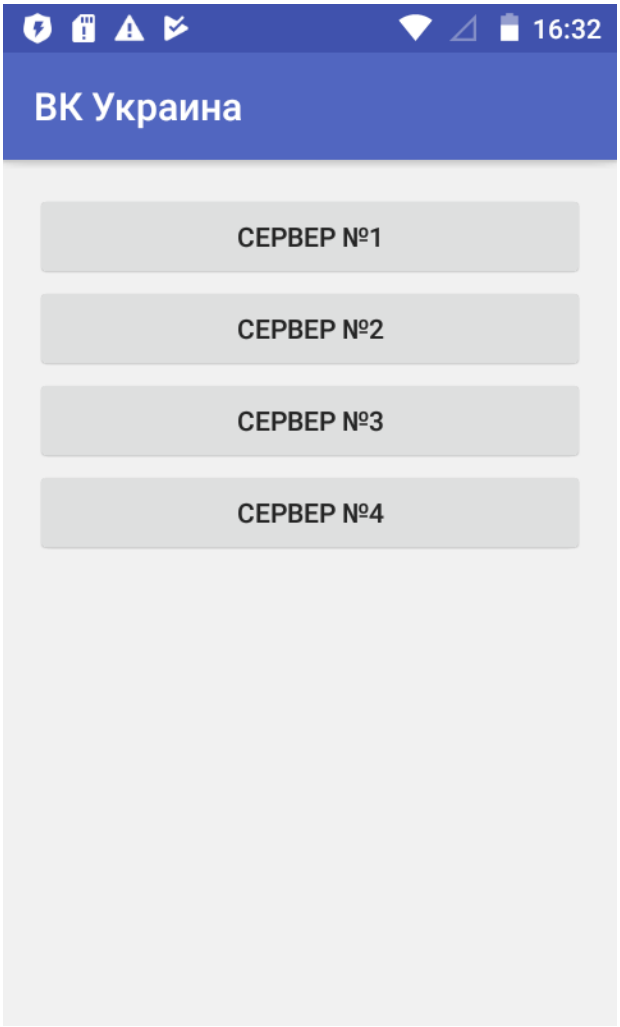

А в конце лета в вирусную базу Dr.Web была добавлена запись для детектирования троянца-вымогателя Android.Banker.184.origin. Он запрашивал доступ к специальным возможностям (Accessibility Service), самостоятельно добавлял себя в список администраторов зараженного устройства, устанавливал собственный пин-код разблокировки экрана, после чего шифровал фотографии, видео, документы и другие файлы.

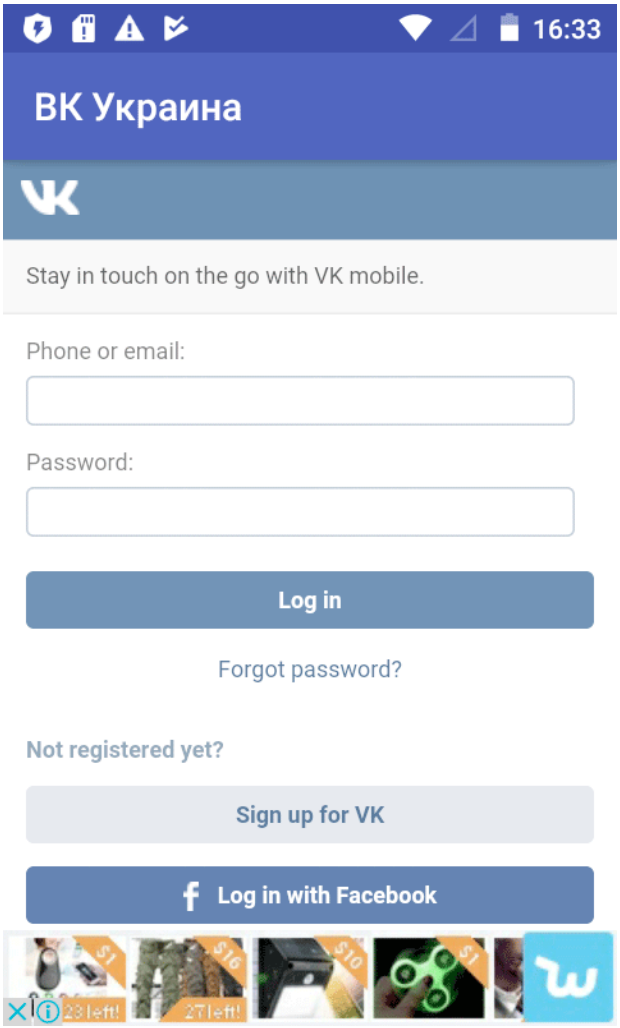
## Угрозы в Google Play

Несмотря на попытки корпорации Google обеспечить безопасность официального каталога приложений Android, в нем по-прежнему встречаются вредоносные и нежелательные программы. В 2017 году в Google Play было выявлено множество различных угроз. В апреле в нем был найден троянец Android.BankBot.180.origin, который скрывался в приложении-фонарике. Он показывал поддельные формы ввода логина и пароля для доступа к банковским учетным записям, а также перехватывал СМС с кодами проверки.

В июне в Google Play был обнаружен троянец Android.Dvmap.1.origin, который с использованием набора эксплойтов пытался получить root-доступ и незаметно устанавливал вредоносный модуль Android.Dvmap.2.origin. Этот модуль соединялся с управляющим сервером и по его команде мог скачивать дополнительные компоненты.

В том же месяце в каталоге Google Play была найдена потенциально опасная программа Program.PWS.1. Она обеспечивала доступ к заблокированным на территории Украины социальным сетям «ВКонтакте» и «Одноклассники». Это приложение использовало сервер-анонимайзер для обхода ограничений, но никак не шифровало передаваемые логин, пароль и другую информацию при работе в соцсетях, что ставило под угрозу конфиденциальность владельцев мобильных устройств.




Позднее в официальном каталоге программ для ОС Android были выявлены СМС-трояны Android.SmsSend.1907.origin и Android.SmsSend.1908.origin, которые отправляли СМС на платные номера и подписывали пользователей на дорогостоящие услуги.

В июле компания «Доктор Веб» рассказала о троянце Android.DownLoader.558.origin. Он был встроен в специализированную программную платформу, применяемую при разработке ПО (SDK, Software Development Kit), которая использовалась для оптимизации и упрощения обновлений приложений. Android.DownLoader.558.origin мог незаметно загружать и запускать дополнительные модули. В этом же месяце в Google Play был найден Android.RemoteCode.85.origin. Этот троянец скачивал и запускал вредоносный плагин, передававший вирусописателям СМС-сообщения пользователя.

В сентябре в Google Play был выявлен троянец Android.SockBot.5, который использовал зараженные устройства в качестве прокси-сервера, реализованного через протокол SOCKS. А уже в ноябре в каталоге был обнаружен Android.DownLoader.658.origin, предлагавший скачать и установить различные приложения.

Кроме того, в течение года в Google Play были найдены новые модификации троянца Android.Spy.308.origin, о котором компания «Доктор Веб» сообщала еще в 2016 году. Как и ранее, вредоносная программа была встроена в безобидное ПО. Основная функция Android.Spy.308.origin – показ навязчивой рекламы, а также загрузка и запуск дополнительных модулей.

## Перспективы и тенденции

Киберпреступники постоянно совершенствуют механизмы распространения вредоносных программ, а также их функциональные возможности. Одну из основных угроз для пользователей мобильных устройств под управлением ОС Android представляют банковские троянцы. В 2016 году специалисты «Доктор Веб» отмечали, что все больше таких вредоносных приложений для кражи конфиденциальной информации отслеживают запуск программ «банк-клиент» и показывают поверх них поддельные формы ввода персональных данных. В 2017 году эта тенденция продолжилась. Можно не сомневаться, что киберпреступники и дальше будут задействовать указанный вектор атаки, а также создавать новых банкеров.

Использование троянцами функций специальных возможностей (Accessibility Service) ОС Android значительно расширило функционал вредоносных программ и сделало их намного более опасными, поскольку благодаря этим полномочиям они фактически получают полный контроль над зараженными устройствами. Угроза для владельцев смартфонов и планшетов настолько серьезна, что компания Google решила значительно ограничить применение таких функций в программах, которые размещаются в каталоге Google Play. Если приложения не предназначены для помощи людям с ограниченными возможностями, они могут быть удалены из официального каталога. Разработчики должны доказать, что их ПО действительно необходимы указанные функции, а также пояснить пользователям, для чего именно они нужны. Тем не менее, с большой уверенностью можно сказать, что вирусописатели найдут способ обхода ограничений и продолжат распространять троянцев с таким функционалом.

Другая вероятная тенденция 2018 года – совершенствование методов противодействия обнаружению и усложнение анализа троянцев. Киберпреступники все чаще используют многоуровневые вредоносные программы, когда основной функционал скрыт в загружаемых модулях или вспомогательных троянских приложениях, расположенных на управляющих серверах. Кроме того, широкое распространение получили всевозможные упаковщики. Наиболее вероятно, что вирусописатели и далее будут применять эти и другие приемы для защиты вредоносных программ.

Также в 2018 году стоит ожидать очередных случаев заражения прошивок мобильных устройств и появления новых троянцев-вымогателей, в том числе шифрующих файлы.

# Обзор вирусной активности для мобильных Android-устройств за 2017 год

## 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
125040, 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