

Обзор вирусной активности для мобильных Android-устройств в мае 2017 года



Обзор вирусной активности для мобильных Android-устройств в мае 2017 года

31 мая 2017 года

Компания «Доктор Веб» представляет майский обзор вирусной обстановки для смартфонов и планшетов на Android. В прошедшем месяце в каталоге Google Play было обнаружено несколько Android-троянцев. Один из них загружал приложения из Интернета и похищал конфиденциальную информацию. Другой мог скачивать и запускать дополнительные программные модули и показывал навязчивую рекламу. Кроме того, в мае злоумышленники распространяли банковского троянца, который крал деньги со счетов пользователей.

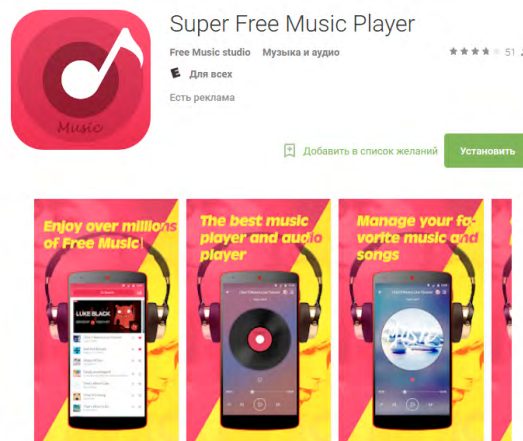
Главные тенденции мая

- Обнаружение троянцев в каталоге Google Play
- Распространение Android-банкера

Обзор вирусной активности для мобильных Android-устройств в мае 2017 года

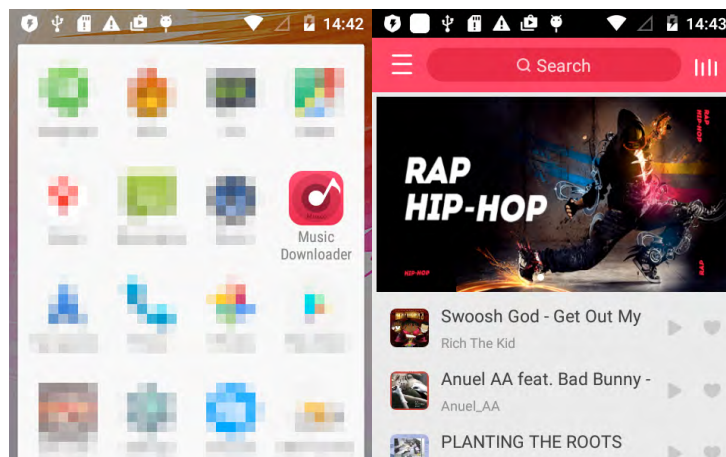
«Мобильная» угроза месяца

В начале мая в каталоге Google Play был обнаружен троянец [Android.RemoteCode.28](#), который был встроен в приложение-аудиоплеер. Он скачивал из Интернета другие программы и передавал на управляющий сервер информацию о зараженном устройстве, а также сведения об установленном на нем ПО.



Особенности [Android.RemoteCode.28](#):

- основной вредоносный функционал троянца находится во вспомогательном программном модуле, который зашифрован;
- [Android.RemoteCode.28](#) начинает вредоносную активность только через 8 часов после своего запуска;
- троянец проверяет наличие эмулятора и средств отладки и при их обнаружении прекращает работу.



Узнайте больше

Лаборатория-live | Вирусные обзоры | Горячая лента угроз | Вирусная библиотека

Обзор вирусной активности для мобильных Android-устройств в мае 2017 года

По данным антивирусных продуктов Dr.Web для Android



- **Android.HiddenAds.83.origin**
- **Android.HiddenAds.76.origin**
- **Android.HiddenAds.68.origin**

Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.

- **Android.Sprovider.9**

Троянская программа, предназначенная для показа навязчивой рекламы в панели уведомлений ОС Android, а также загрузки и запуска других приложений, в том числе вредоносных.

- **Android.Triada.264.origin**

Представитель многофункциональных троянцев, выполняющих разнообразные вредоносные действия.



- **Adware.Jiubang.1**
- **Adware.Batmobi.2.origin**
- **Adware.Leadbolt.12.origin**
- **Adware.Airpush.31.origin**
- **Adware.Appsad.1**

Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

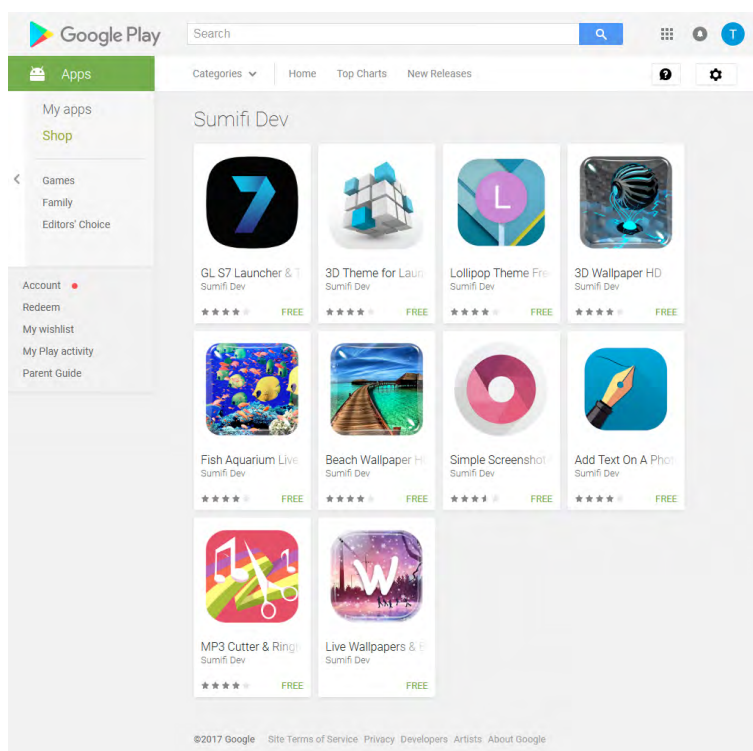
Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

Обзор вирусной активности для мобильных Android-устройств в мае 2017 года

Троянец в Google Play

В середине прошлого месяца в каталоге Google Play были выявлены приложения со встроенным в них троянцем [Android.Spy.308.origin](#). В частности, они распространялись разработчиком Sumifi Dev. Это не первый случай, когда указанная вредоносная программа проникает в официальный каталог ПО для Android. Об одном из таких инцидентов компания «Доктор Веб» [сообщила](#) в июле 2016 года. После обнаружения [Android.Spy.308.origin](#) разработчик обновил зараженные приложения, удалив троянский компонент, и теперь они не представляют опасности.

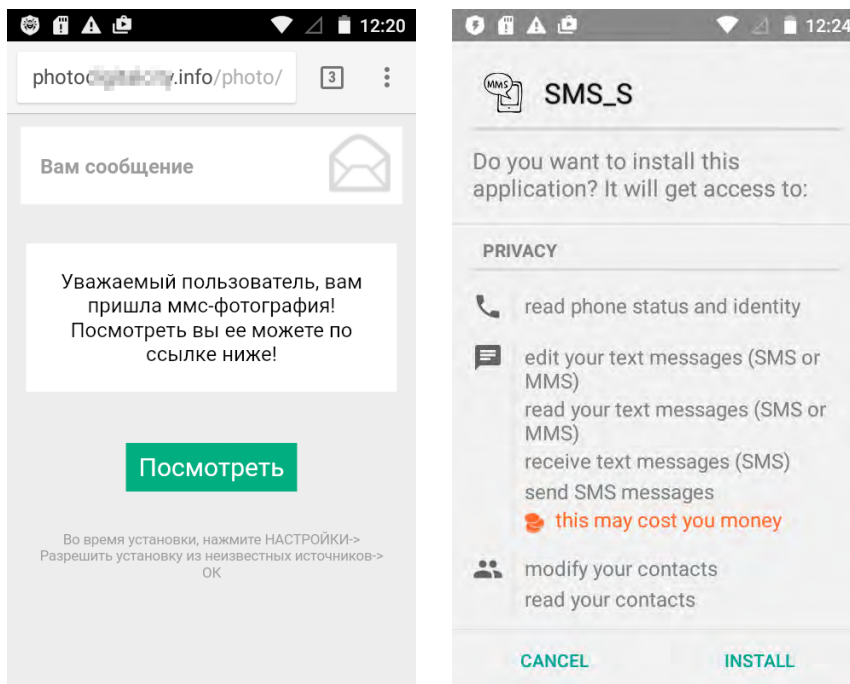


инцидентов компания «Доктор Веб» сообщила в июле 2016 года. После обнаружения [Android.Spy.308.origin](#) разработчик обновил зараженные приложения, удалив троянский компонент, и теперь они не представляют опасности.

Обзор вирусной активности для мобильных Android-устройств в мае 2017 года

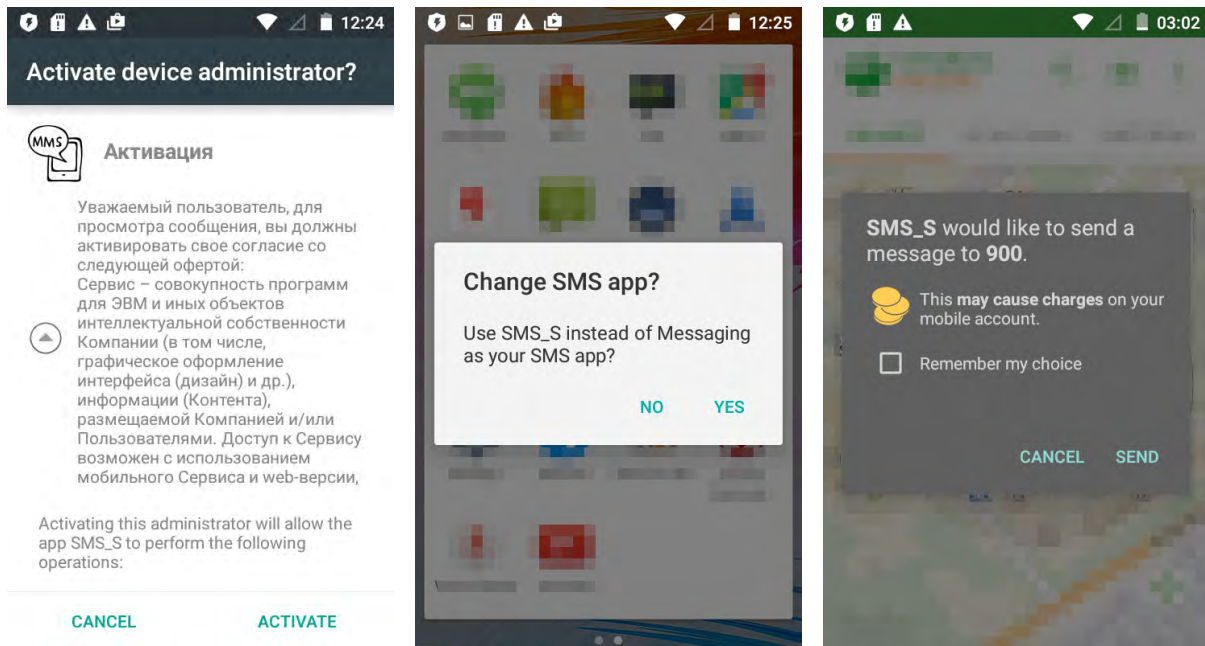
Банковские троянцы

В мае под видом ММС-сообщений киберпреступники распространяли банковского троянца [Android.BankBot.186.origin](#). Пользователям приходили СМС со ссылкой, при переходе по которой в веб-браузере открывался мошеннический сайт. С него на мобильное устройство загружался арк-файл вредоносного приложения.



[Android.BankBot.186.origin](#) запрашивает доступ к функциям администратора мобильного устройства, чтобы усложнить свое удаление. Кроме того, он пытается подменить собой стандартное приложение для работы с СМС. Это необходимо для обхода системы безопасности новых версий ОС Android и получения возможности отправлять и перехватывать сообщения. После этого троянец проверяет баланс доступных банковских счетов пользователя и незаметно переводит деньги киберпреступникам.

Обзор вирусной активности для мобильных Android-устройств в мае 2017 года



Вредоносные программы для мобильных Android-устройств по-прежнему представляют опасность. Троянцы могут распространяться как с использованием мошеннических веб-сайтов, так и через официальный каталог приложений Google Play. Для защиты от опасного и нежелательного ПО владельцам смартфонов и планшетов под управлением ОС Android необходимо установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в мае 2017 года

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

[ВебЮметр](#) | [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](#)



© ООО «Доктор Веб»,
2003-2016

Узнайте больше

[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)