Dr.WEB®
с 1992 года

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в январе 2019 года

# Обзор вирусной активности для мобильных устройств в январе 2019 года

## 1 февраля 2019 года

В уходящем месяце владельцам Android-устройств угрожало множество вредоносных программ. В начале января вирусные аналитики «Доктор Веб» исследовали троянца Android.Spy.525.origin, предназначенного для кибершпионажа. Позднее были обнаружены очередные рекламные троянцы, которые получили имена Android.HiddenAds.361.origin и Android.HiddenAds.356.origin. В течение месяца наши специалисты обнаружили несколько новых кликеров семейства Android.Click, которых вирусописатели выдавали за официальные приложения букмекерских контор. Кроме того, киберпреступники распространяли троянцев-загрузчиков семейства Android.DownLoader, скачивавших на смартфоны и планшеты Android-банкеров.

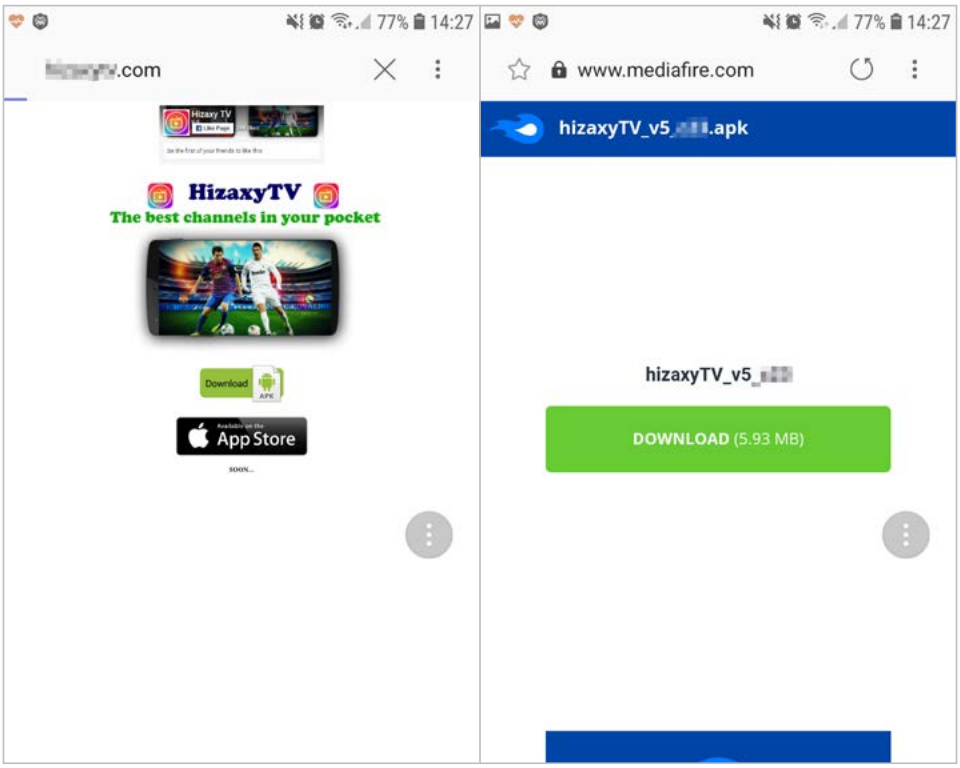
## Главные тенденции января

- Обнаружение вредоносных программ в каталоге Google Play
- Распространение Android-троянца, предназначенного для кибершпионажа

# Обзор вирусной активности для мобильных устройств в январе 2019 года

## Мобильная угроза месяца

В начале января в вирусную базу Dr.Web была добавлена запись для детектирования троянца-шпиона Android.Spy.525.origin. Он распространялся через каталог Google Play под видом полезных приложений, а также с использованием принадлежащего злоумышленникам вредоносного сайта, при посещении которого потенциальные жертвы перенаправлялись на популярный файлообменный ресурс MediaFire, где хранилась копия троянца.




По команде управляющего сервера Android.Spy.525.origin мог отслеживать местоположение зараженного смартфона или планшета, красть СМС-переписку, информацию о телефонных звонках, данные из телефонной книги, хранящиеся на устройстве файлы, а также показывать фишинговые окна.

# Обзор вирусной активности для мобильных устройств в январе 2019 года

## По данным антивирусных продуктов Dr.Web для Android


Android.Backdoor.682.origin

Троянская программа, которая выполняет команды злоумышленников и позволяет им контролировать зараженные мобильные устройства.

Android.RemoteCode.197.origin

Вредоносное приложение, предназначенное для загрузки и выполнения произвольного кода.

Android.HiddenAds.261.origin

Android.HiddenAds.659

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.Mobifun.4

Троянец, который загружает различные приложения.

# Обзор вирусной активности для мобильных устройств в январе 2019 года

## По данным антивирусных продуктов Dr.Web для Android


Adware.Zeus.1

Adware.AdPush.29.origin

Adware.Patacore.1.origin

Adware.Patacore.168

Adware.Jiubang.2

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

## Угрозы в Google Play

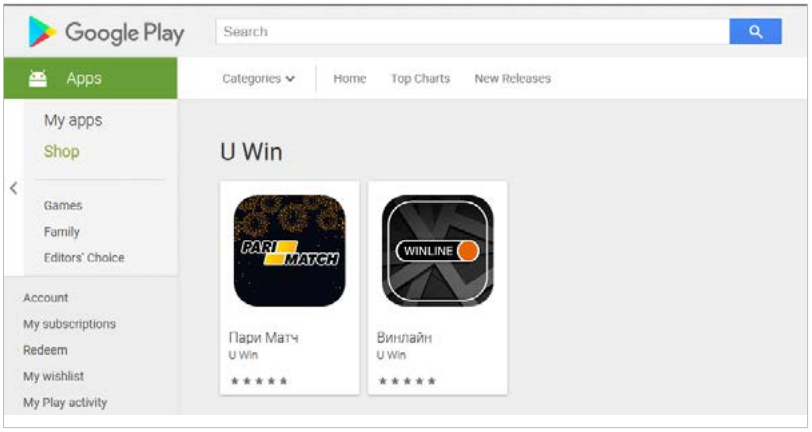
Помимо Android.Spy.525.origin, в январе в Google Play были обнаружены и другие угрозы. В начале месяца вирусная база Dr.Web пополнилась записями для детектирования троянцев Android.HiddenAds.361.origin и Android.HiddenAds.356.origin. Эти вредоносные программы представляли собой модификации Android.HiddenAds.343.origin, о котором наша компания сообщала в декабрьском обзоре 2018 года. Android.HiddenAds.361.origin и Android.HiddenAds.356.origin распространялись под видом полезных программ. После запуска они скрывали свои значки и начинали показывать рекламу.

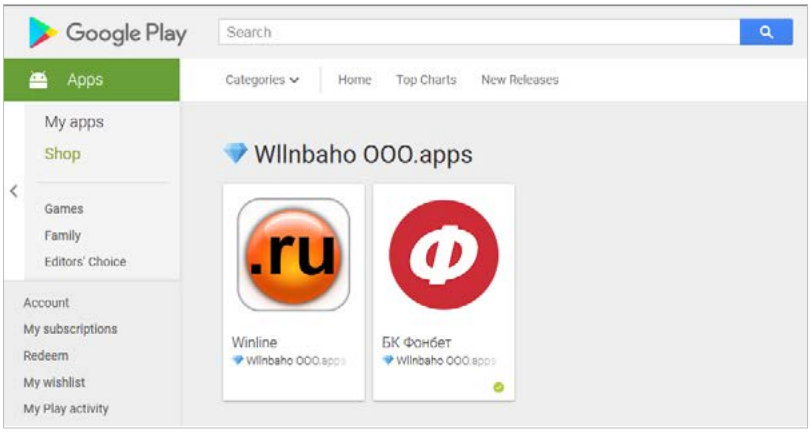
Кроме того, вирусные аналитики исследовали множество загрузчиков. Киберпреступники выдавали их за полезные программы, такие как конвертеры валют, официальные банковские приложения и другое ПО. Эти троянцы получили имена Android.DownLoader.4063, Android.DownLoader.855.origin, Android.DownLoader.857.origin, Android.DownLoader.4102 и Android.DownLoader.4107. Они скачивали и пытались установить на мобильные устройства Android-банкеров, предназначенных для кражи конфиденциальной информации и денег со счетов клиентов кредитных учреждений.

Одним из загружаемых банковских троянцев был Android.BankBot.509.origin, являвшийся модификацией Android.BankBot.495.origin. О нем наша компания сообщала в декабре прошлого года. Этот банкер использовал специальные возможности (Accessibility Service), с помощью которых самостоятельно управлял установленными приложениями, нажимая на кнопки и элементы меню. Другой троянец, получивший имя Android.BankBot.508.origin, показывал фишинговые окна и пытался украсть логины, пароли и другую персональную информацию. Кроме того, он перехватывал СМС-сообщения с кодами подтверждения финансовых операций.

В конце января специалисты «Доктор Веб» обнаружили очередных троянцев-кликеров семейства Android.Click. Среди них — Android.Click.651, Android.Click.664, Android.Click.665 и Android.Click.670. Злоумышленники распространяли их под видом официальных программ букмекерских контор. Эти вредоносные приложения могли по команде управляющего сервера загружать любые веб-сайты, что представляет серьезную опасность.

## Угрозы в Google Play




Специалисты компании «Доктор Веб» продолжают отслеживать «мобильную» вирусную обстановку и оперативно добавлять в вирусную базу Dr.Web записи для детектирования и удаления вредоносных и нежелательных программ. Благодаря этому смартфоны и планшеты с установленными на них продуктами Dr.Web для Android находятся под надежной защитой.

# Обзор вирусной активности для мобильных устройств в январе 2019 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
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 | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах