Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2018 года

Обзор вирусной активности для мобильных устройств в августе 2018 года

31 августа 2018 года

В августе 2018 года специалисты компании «Доктор Веб» обнаружили троянца для ОС Android, способного подменять номера электронных кошельков в буфере обмера. Кроме того, вирусные аналитики выявили в каталоге Google Play множество троянцев, которых злоумышленники использовали в различных мошеннических схемах незаконного заработка. Также в течение месяца в официальном каталоге программ для ОС Android было зафиксировано несколько новых Android-банкеров и троянцев-загрузчиков, скачивавших на мобильные устройства другое вредоносное ПО. Помимо этого, в августе специалисты по информационной безопасности обнаружили опасного троянца-шпиона, которого вирусописатели могли встраивать в безобидные программы и распространять таким образом под видом оригинальных приложений.

Главные тенденции августа

- Обнаружение Android-троянца, подменяющего номера электронных кошельков в буфере обмена
- Распространение банковских троянцев
- Обнаружение в каталоге Google Play множества вредоносных программ
- Выявление опасного троянца-шпиона, которого злоумышленники могли встраивать в любые приложения

Обзор вирусной активности для мобильных устройств в августе 2018 года

Мобильная угроза месяца

В начале уходящего месяца вирусные аналитики компании «Доктор Веб» обнаружили троянца Android.Clipper.1.origin, который отслеживает буфер обмена и подменяет копируемые в него номера электронных кошельков популярных платежных систем и криптовалют. Вредоносную программу «интересуют» номера кошельков Qiwi, Webmoney, «Яндекс.Деньги», Bitcoin, Monero, zCash, DOGE, DASH, Etherium, Blackcoin и Litecoin. Когда пользователь копирует один из них в буфер обмена, троянец перехватывает его и передает на управляющий сервер. В ответ Android.Clipper.1.origin получает информацию о номере кошелька злоумышленников, на который заменяет номер жертвы. В результате владелец зараженного устройства рискует перевести деньги на счет вирусописателей. Подробнее об этом троянце рассказано в новостной публикации, размещенной на нашем сайте.

Обзор вирусной активности для мобильных устройств в августе 2018 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.HiddenAds

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

Обзор вирусной активности для мобильных устройств в августе 2018 года

По данным антивирусных продуктов Dr.Web для Android

Adware.Zeus.1

Adware.Adpush.2514

Adware.SalmonAds.3.origin

Adware.Jiubang.2

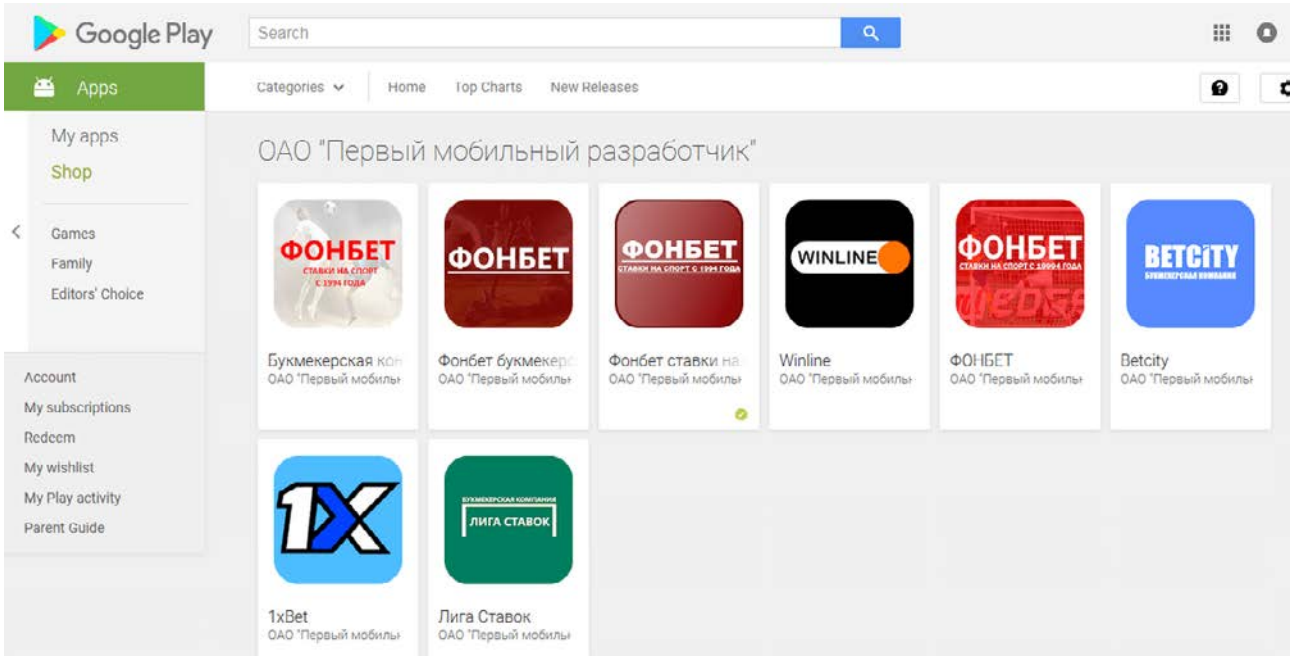
Adware.Patacore.1.origin

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

Обзор вирусной активности для мобильных устройств в августе 2018 года

Троянцы в Google Play

В августе в каталоге Google Play было выявлено множество вредоносных программ. На протяжении всего месяца вирусные аналитики компании «Доктор Веб» отслеживали распространение в нем троянцев семейства Android.Click. Наши специалисты обнаружили 127 таких вредоносных приложений, которые злоумышленники выдавали за официальные программы букмекерских контор.



При запуске эти троянцы показывают пользователю заданный управляющим сервером веб-сайт. На момент обнаружения все выявленные представители семейства Android.Click открывали интернет-порталы букмекерских фирм. Однако в любой момент они способны получить команду на загрузку произвольного сайта, который может распространять другое вредоносное ПО или использоваться в фишинг-атаках.

Еще одним троянцем-кликером, обнаруженным в августе в Google Play, стал Android.Click.265.origin. Злоумышленники использовали его для подписки пользователей на дорогостоящие мобильные услуги. Вирусописатели распространяли эту вредоносную программу под видом официального приложения для работы с интернет-магазином «Эльдорадо».

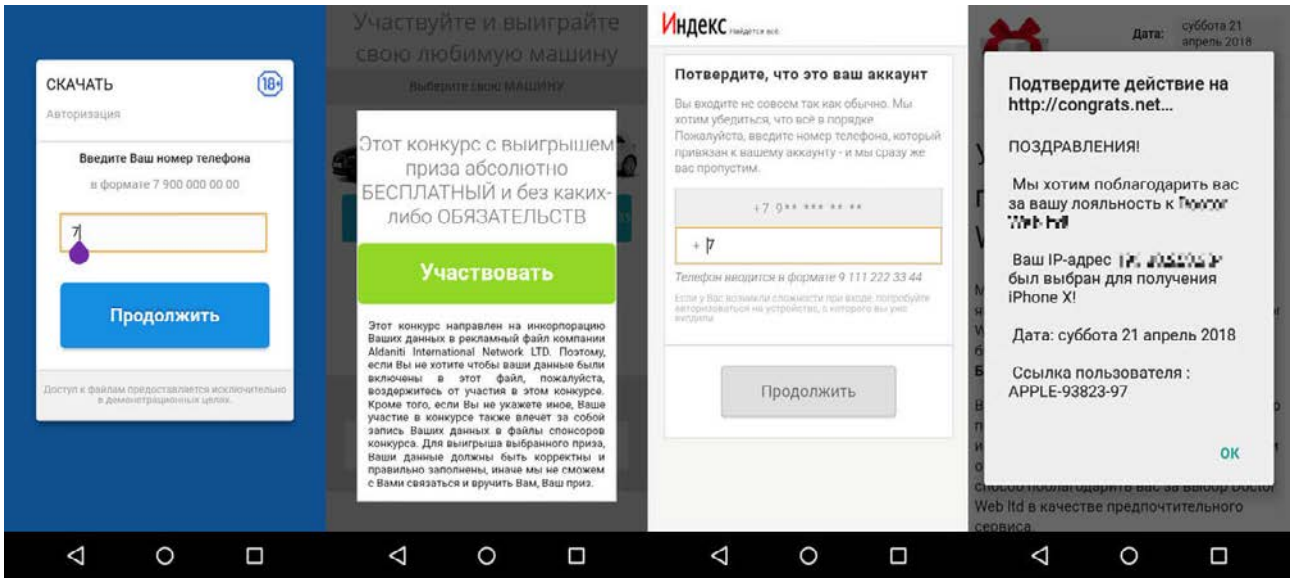
Обзор вирусной активности для мобильных устройств в августе 2018 года

Троянцы в Google Play

Троянец Android.Click.248.origin, известный вирусным аналитикам «Доктор Веб» с апреля, в августе вновь появился в каталоге Google Play. Как и ранее, он распространялся под видом известного ПО. Android.Click.248.origin загружает мошеннические сайты, на которых предлагается скачать различные программы или сообщается о некоем выигрыше. Для получения приза или скачивания приложения у потенциальной жертвы запрашивается номер мобильного телефона, на который приходит код подтверждения. После ввода этого кода владелец мобильного устройства подписывается на дорогостоящую услугу.

Трояны в Google Play

При этом, если Android-смартфон или планшет подключен к Интернету через мобильное соединение, подписка на платный сервис выполняется автоматически сразу после того, как киберпреступники получают номер.

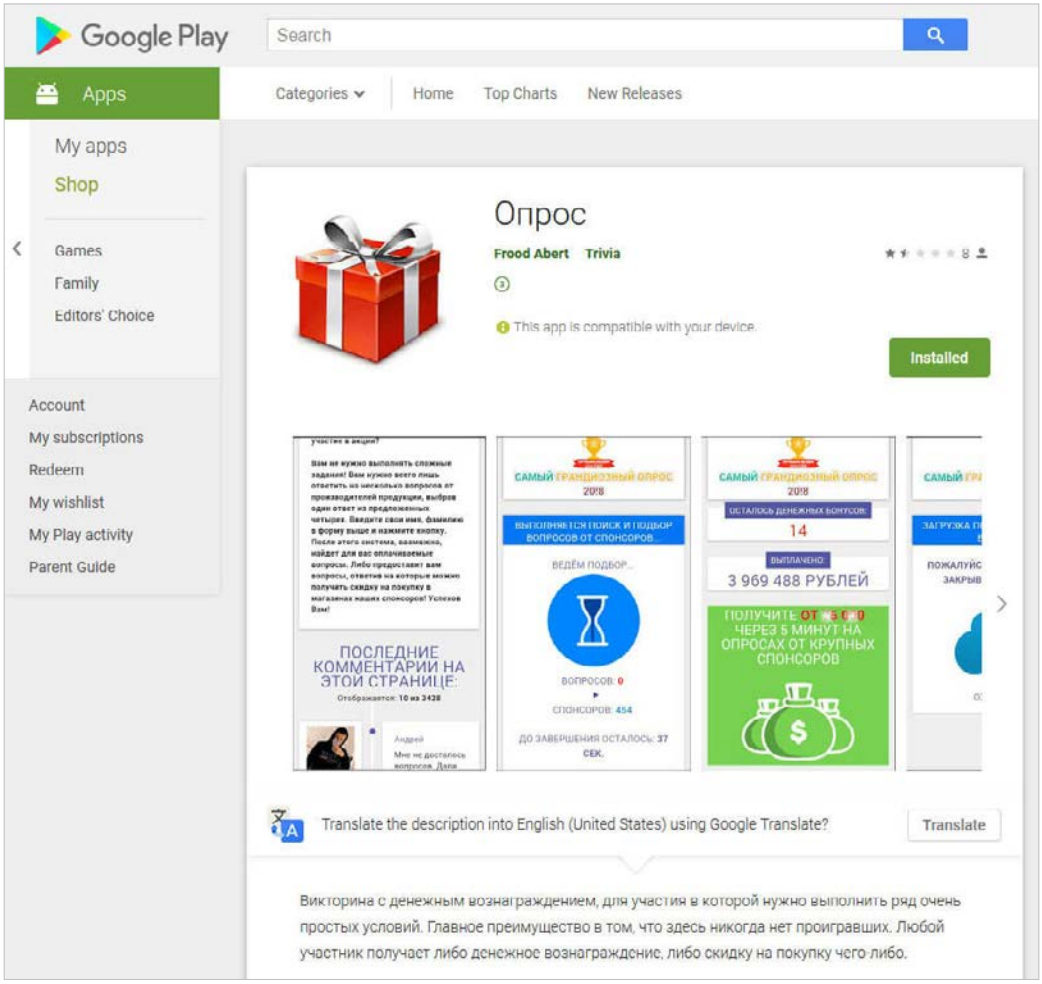


Более подробную информацию об этих троянцах-кликерах можно получить, прочитав соответствующую новостную публикацию на нашем сайте.

В конце августа вирусные аналитики «Доктор Веб» обнаружили в Google Play трояна Android.FakeApp.110, которого сетевые жулики использовали для незаконного заработка. Эта вредоносная программа загружала мошеннический сайт, на котором потенциальной жертве предлагалось за вознаграждение пройти опрос. После ответа на все вопросы требовалось выполнить некий идентификационный платеж в размере 100-200 рублей. Однако после перевода денег мошенникам никакой оплаты пользователь не получал.

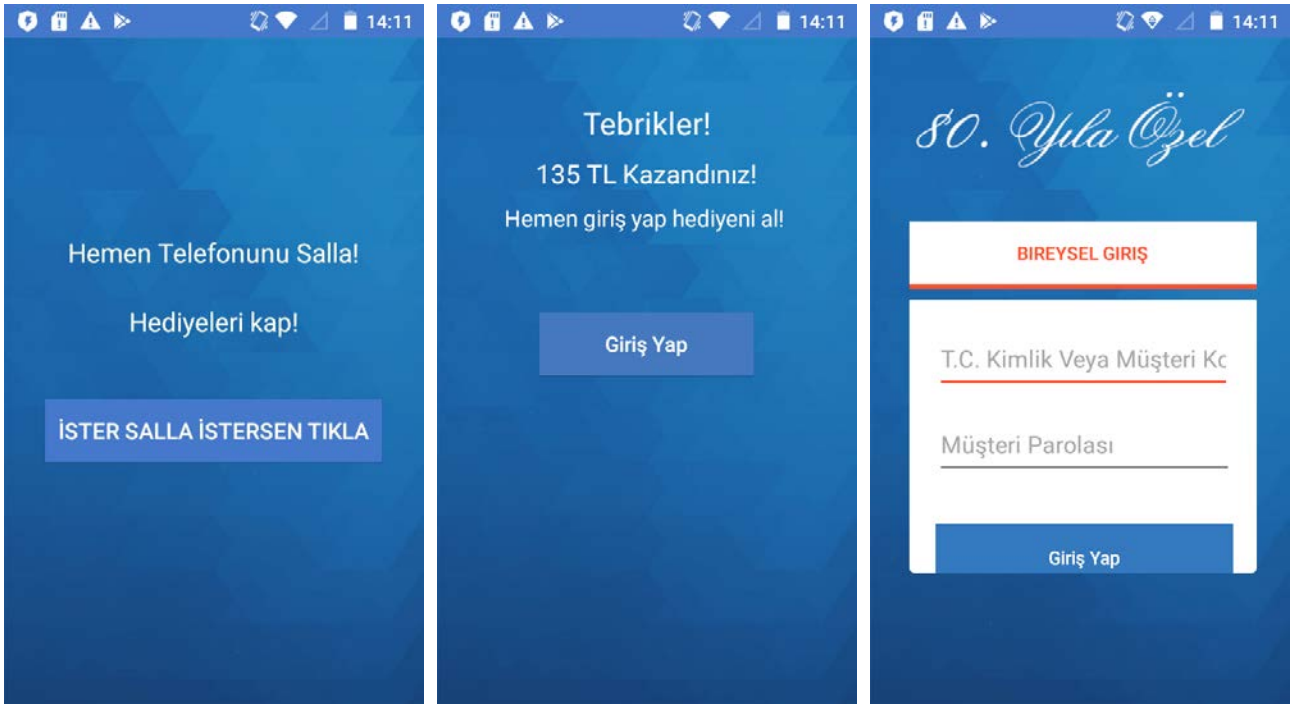
Обзор вирусной активности для мобильных устройств в августе 2018 года

Трояны в Google Play



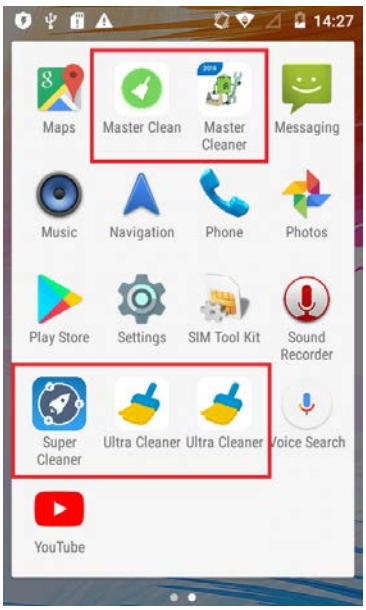
Среди вредоносных программ, обнаруженных в каталоге Google Play в августе, оказались очередные Android-банкеры. Один из них получил имя Android.Banker.**2843**. Он распространялся под видом официального приложения одной из турецких кредитных организаций. Android.Banker.**2843** крал логины и пароли для доступа к банковской учетной записи пользователя и передавал их злоумышленникам.

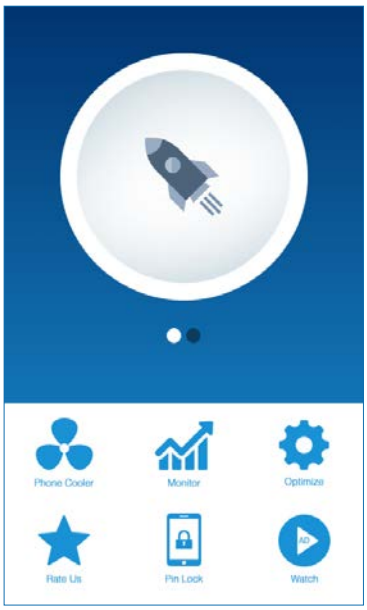
Троянцы в Google Play



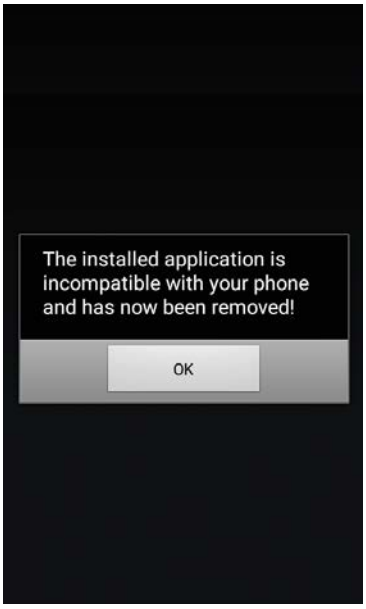
Другой банковский троянец, добавленный в вирусную базу Dr.Web как Android.Banker.2855, вирусописатели распространяли под видом различных сервисных утилит. Эта вредоносная программа извлекала из своих файловых ресурсов и запускала троянца Android.Banker.279.origin, который похищал банковские аутентификационные данные пользователей.

Троянцы в Google Play



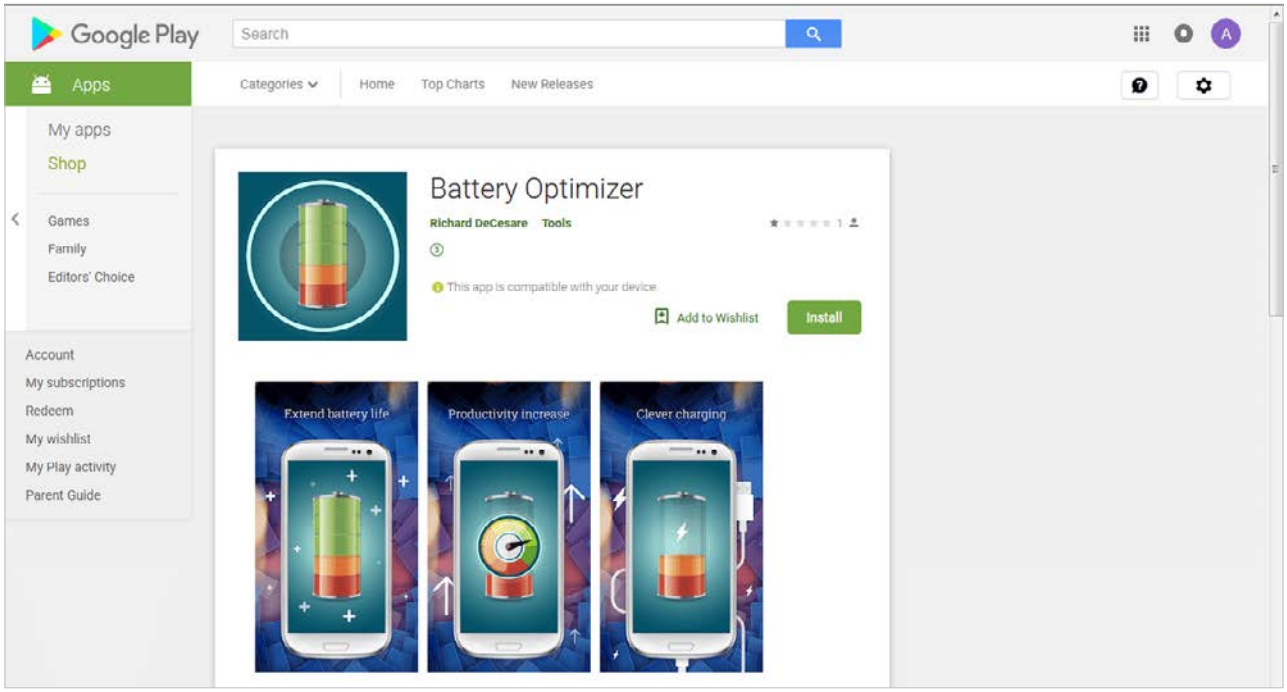


Некоторые модификации Android.Banker.**2855** пытались скрыть свое присутствие на мобильном устройстве, показывая после запуска поддельное сообщение об ошибке и удаляя свой значок из списка приложений на главном экране.



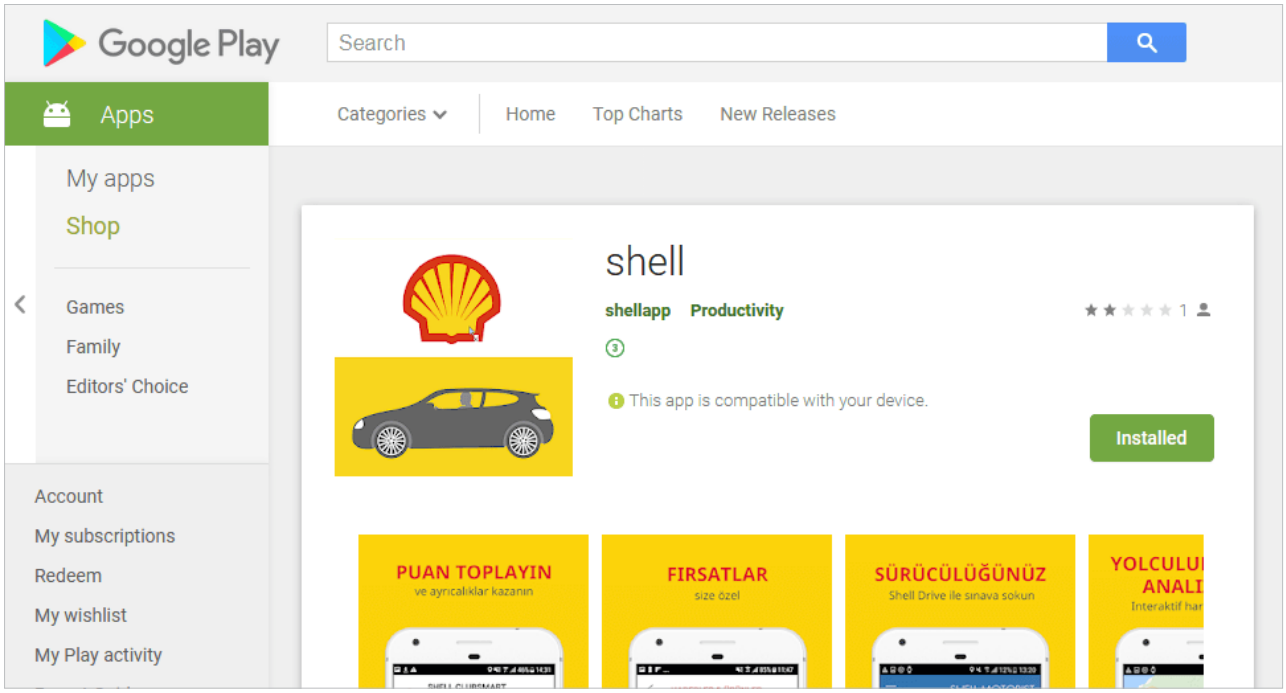
Троянцы в Google Play

Другой Android-банкер, получивший имя Android.BankBot.325.origin, скачивался на зараженные смартфоны и планшеты троянцем Android.DownLoader.772.origin. Злоумышленники распространяли эту вредоносную программу-загрузчик через каталог Google Play под видом полезных приложений – например, оптимизатора работы аккумулятора.



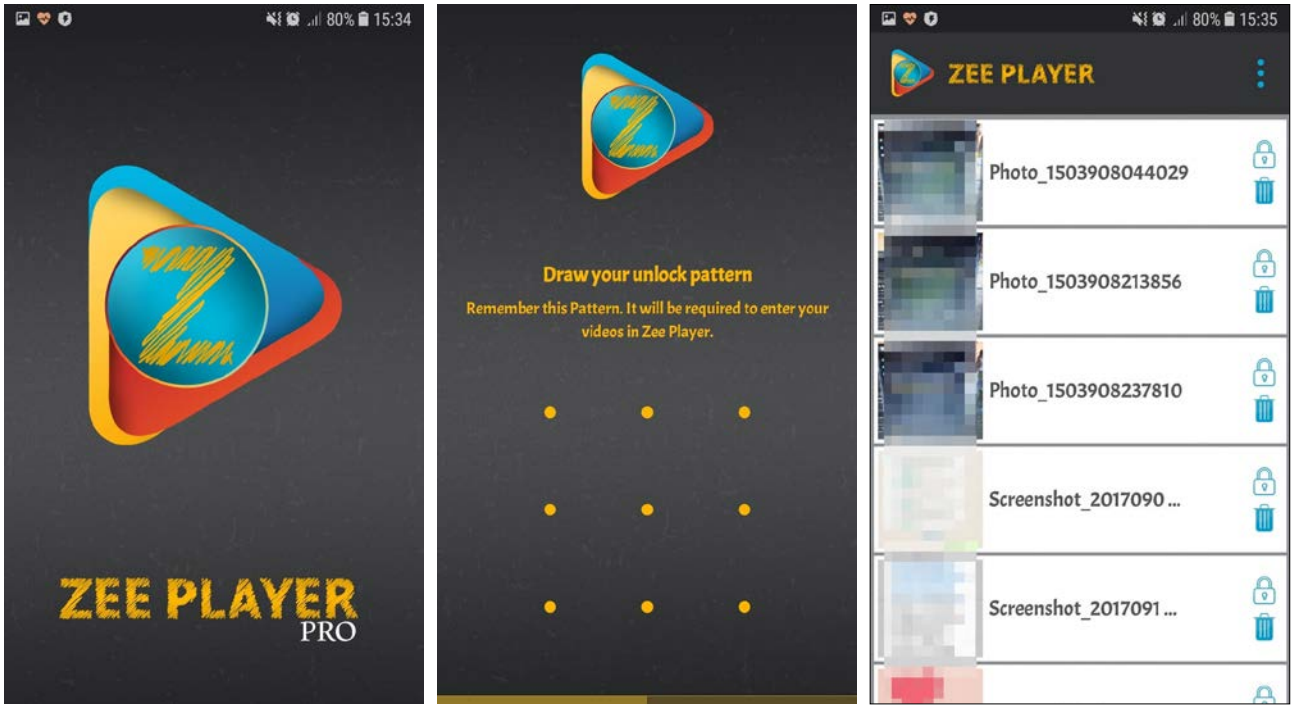
Кроме того, вирусные аналитики «Доктор Веб» выявили в Google Play загрузчика Android.DownLoader.768.origin, распространявшегося под видом приложения от корпорации Shell. Android.DownLoader.768.origin скачивал на мобильные устройства различных банковских троянцев.

Трояны в Google Play



Также в августе в Google Play был найден троянец-загрузчик, добавленный в вирусную базу Dr.Web как Android.DownLoader.784.origin. Он был встроен в приложение под названием Zee Player, позволявшее скрывать хранящиеся в памяти мобильных устройств фотографии и видео.

Трояны в Google Play



Android.DownLoader.784.origin загружал трояна Android.Spy.409.origin, которого злоумышленники могли использовать для кибершпионажа.

Android-шпион

В августе вирусная база Dr.Web пополнилась записью для детектирования троянца Android.Spy.490.origin, предназначенного для кибершпионажа. Злоумышленники могут встраивать его в любые безобидные приложения и распространять их модифицированные копии под видом оригинального ПО, не вызывая подозрений у пользователей. Android.Spy.490.origin способен отслеживать СМС-переписку и местоположение зараженного смартфона или планшета, перехватывать и записывать телефонные разговоры, передавать на удаленный сервер информацию обо всех совершенных звонках, а также снятые владельцем мобильного устройства фотографии и видео.

Каталог приложений Google Play является самым безопасным источником программ для устройств под управлением ОС Android. Однако злоумышленникам по-прежнему удается распространять через него различные вредоносные программы. Для защиты Android-смартфонов и планшетов пользователям следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в августе 2018 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