Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2020 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2020 года

9 ноября 2020 года

В октябре антивирусные продукты Dr.Web для Android выявили на защищаемых Android-устройствах на 12.36% больше угроз, чем месяцем ранее. Согласно статистике детектирований, число вредоносных программ увеличилось на 9.08%, нежелательных — на 6%, а потенциально опасных — на 197.24%. Количество обнаруженных рекламных приложений при этом снизилось на 1.51%.

Практически троекратный рост числа потенциально опасных программ в статистике обнаружений обусловлен распространением приложений, защищенных специализированной утилитой Tool.Obfuscapk.1. Она применяется для обфускации исходного кода и может использоваться не только добросовестными разработчиками, но и вирусописателями, которые пытаются защитить троянские программы от обнаружения антивирусами.

В каталоге Google Play были зафиксированы очередные угрозы. Специалисты «Доктор Веб» обнаружили множество новых троянов семейства Android.FakeApp, которые распространялись под видом программ-справочников, якобы предназначенных для помощи в получении налоговых вычетов и социальных компенсаций. На самом деле они загружали мошеннические веб-сайты, с помощью которых злоумышленники могли украсть у пользователей конфиденциальную информацию и деньги.

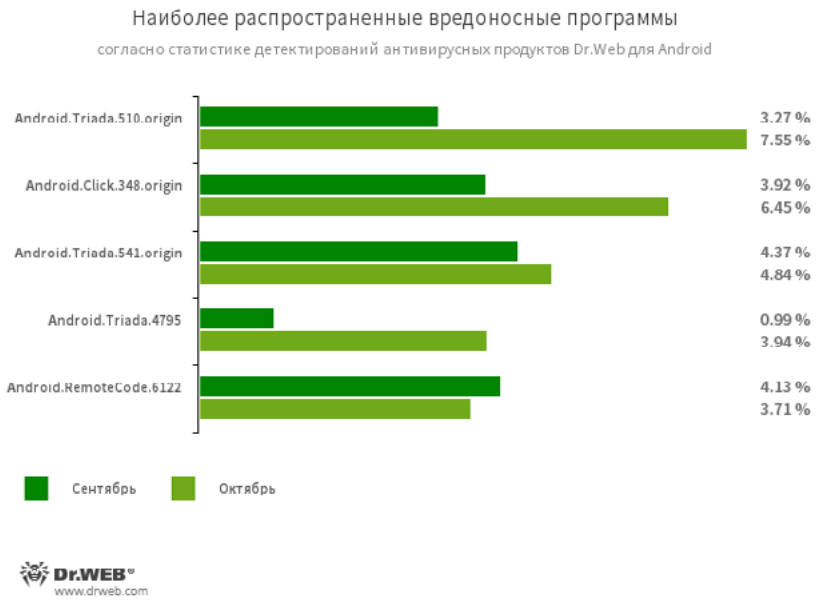
Другая вредоносная программа из Google Play получила имя Android.HiddenAds.2314. Это троян, предназначенный для показа навязчивой рекламы. Он распространялся под видом графического редактора.

ГЛАВНЫЕ ТЕНДЕНЦИИ ОКТЯБРЯ

- Увеличение общего числа угроз, зафиксированных на Android-устройствах
- Значительный рост числа обнаруженных потенциально опасных программ
- Распространение новых угроз в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2020 года

По данным антивирусных продуктов Dr.Web для Android



Android.Triada.510.origin
Android.Triada.541.origin
Android.Triada.4795
Многофункциональные трояны, выполняющие разнообразные вредоносные действия. Относятся к семейству троянских приложений, проникающих в процессы всех работающих программ. Различные представители этого семейства могут встречаться в прошивках Android-устройств, куда злоумышленники внедряют их на этапе производства. Кроме того, некоторые их модификации могут эксплуатировать уязвимости, чтобы получить доступ к защищенным системным файлам и директориям.

Android.Click.348.origin
Вредоносное приложение, которое самостоятельно загружает веб-сайты, нажимает на рекламные баннеры и переходит по ссылкам. Может распространяться под видом безобидных программ, не вызывая подозрений у пользователей.

Android.RemoteCode.6122
Вредоносная программа, которая загружает и выполняет произвольный код. В зависимости от модификации она также может загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2020 года

По данным антивирусных продуктов Dr.Web для Android

Program.FreeAndroidSpy.1.origin

Program.Reptilicus.7.origin

Program.Mrecorder.1.origin

Приложения, которые следят за владельцами Android-устройств и могут использоваться для кибершпионажа. Они способны контролировать местоположение устройств, собирать данные об СМС-переписке, беседах в социальных сетях, копировать документы, фотографии и видео, выполнять прослушивание телефонных звонков и окружения и т. п.

Program.FakeAntiVirus.2.origin

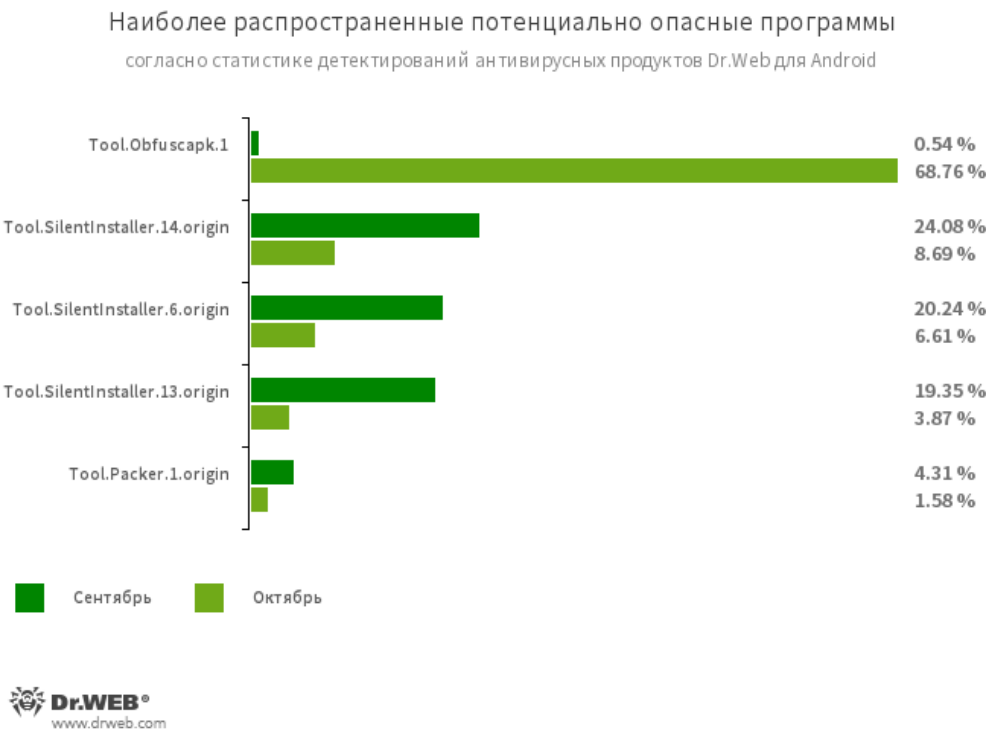
Детектирование рекламных программ, которые имитируют работу антивирусного ПО. Такие программы могут сообщать о несуществующих угрозах и вводить пользователей в заблуждение, требуя оплатить покупку полной версии.

Program.CreditSpy.2

Детектирование программ, предназначенных для присвоения кредитного рейтинга на основании персональных данных пользователей. Такие приложения загружают на удаленный сервер СМС-сообщения, информацию о контактах из телефонной книги, историю вызовов, а также другие сведения.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2020 года

По данным антивирусных продуктов Dr.Web для Android



Tool.Obfuscapk.1

Детектирование приложений, защищенных утилитой-обфускатором Obfuscapk. Эта утилита используется для автоматической модификации и запутывания исходного кода Android-приложений, чтобы усложнить их обратный инжиниринг. Злоумышленники применяют ее для защиты вредоносных и других опасных программ от обнаружения антивирусами.

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.13.origin

Tool.SilentInstaller.14.origin

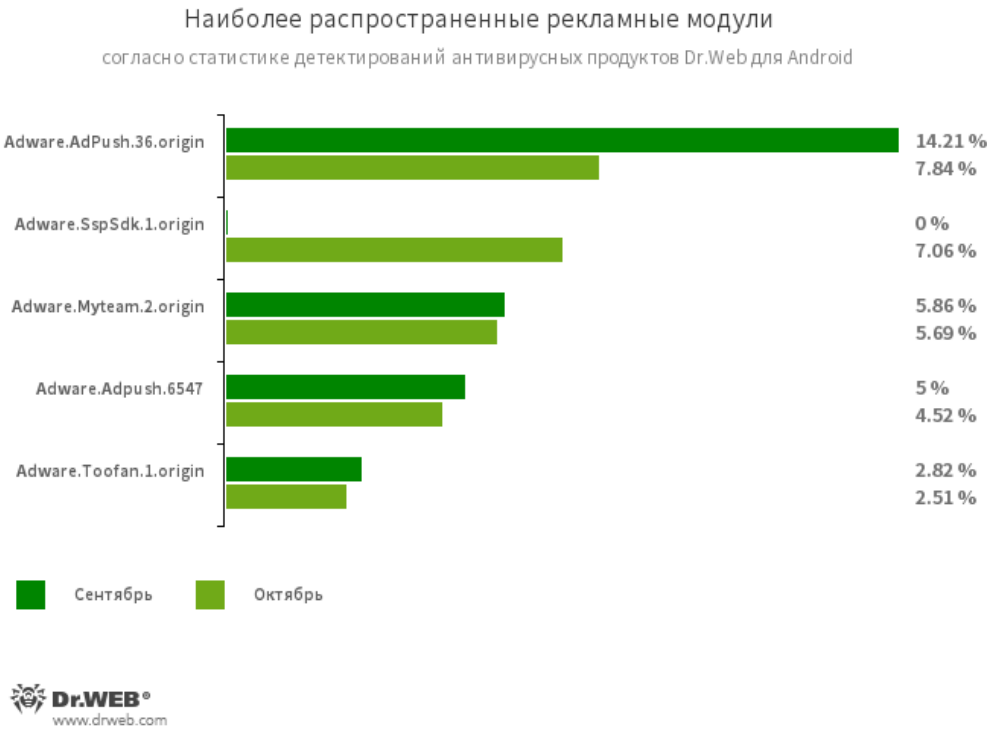
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

Tool.Packer.1.origin

Специализированная утилита-упаковщик, предназначенная для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может быть использована для защиты как безобидных, так и троянских программ.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2020 года

По данным антивирусных продуктов Dr.Web для Android



Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать ярлыки и загружать веб-сайты.

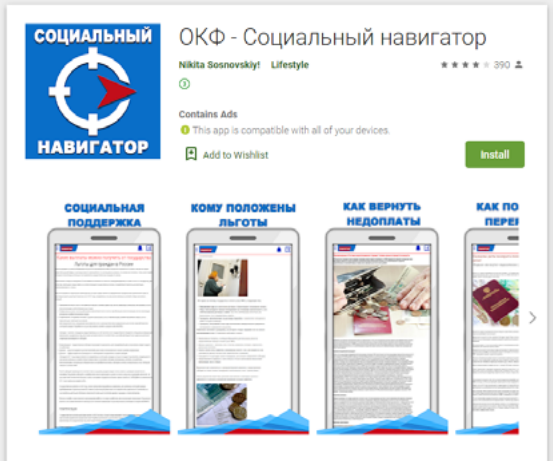
- Adware.Adpush.36.origin
- Adware.SspSdk.1.origin
- Adware.Adpush.6547
- Adware.Myteam.2.origin
- Adware.Toofan.1.origin

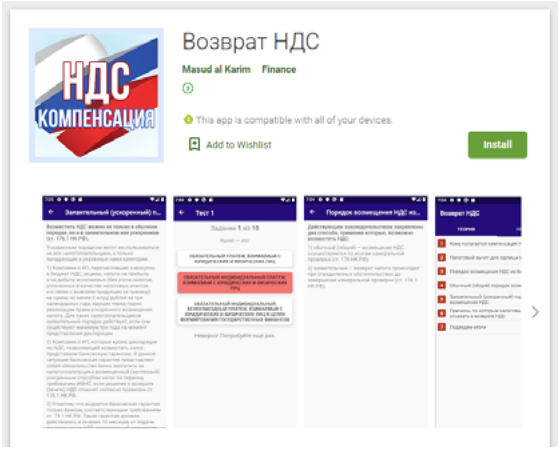
Угрозы в Google Play

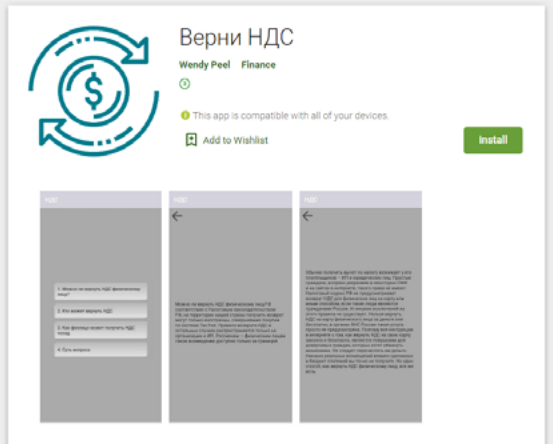
В октябре специалисты «Доктор Веб» выявили в каталоге Google Play 17 новых модификаций троянов семейства Android.FakeApp, которые распространялись под видом безобидных приложений, таких как справочники. Большинство из них злоумышленники вновь выдавали за программы, якобы предназначенные для проверки наличия социальных компенсаций и помощи в получении возврата налогов. По классификации антивируса Dr.Web они получили имена Android.FakeApp.208, Android.FakeApp.209, Android.FakeApp.210, Android.FakeApp.212, Android.FakeApp.213, Android.FakeApp.214, Android.FakeApp.215 и Android.FakeApp.216.

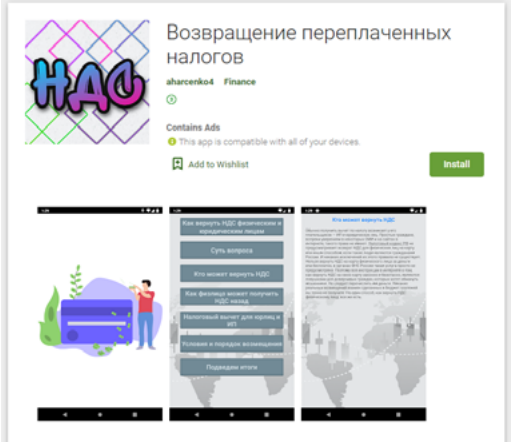
Еще одна модификация представляла собой поддельную программу спортивной тематики и была добавлена в вирусную базу как Android.FakeApp.211.

Однако настоящая и единственная их функция — загрузка мошеннических веб-сайтов. В общей сложности эти трояны скачали свыше 105 000 владельцев Android-устройств.

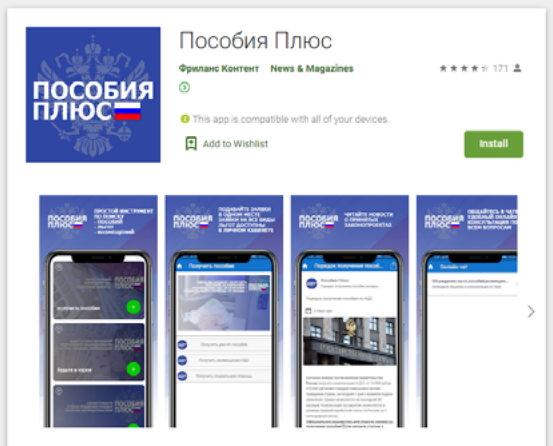


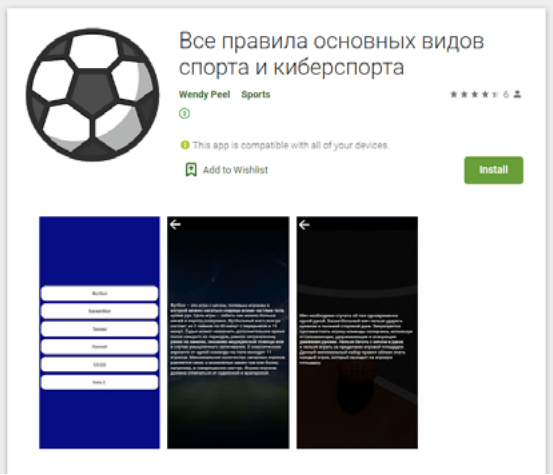






Угрозы в Google Play

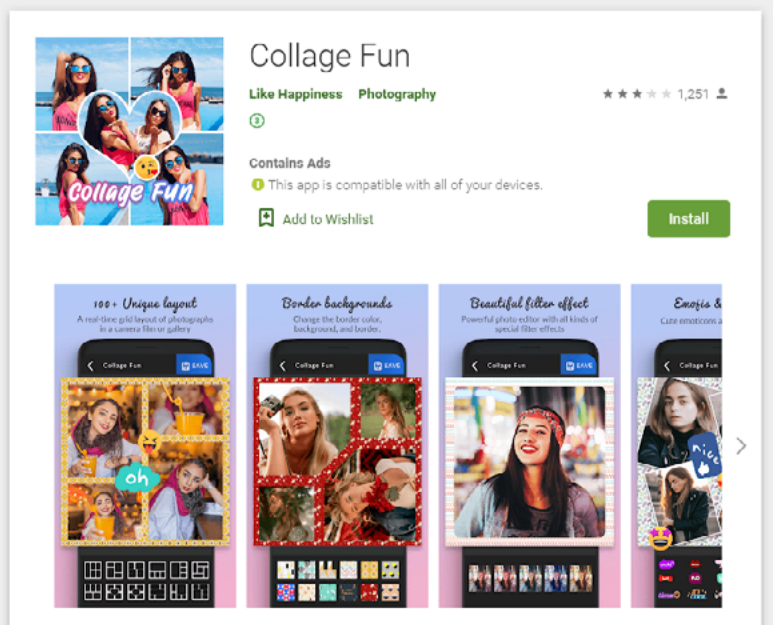




При запуске вредоносные приложения загружают сайты, где потенциальной жертве предлагается указать персональные данные якобы для проверки доступных денежных компенсаций. После того как компенсация «найдена», у пользователя запрашивается дополнительная информация, а затем ему предлагается оплатить налог или пошлину за перевод «возвращаемых» денег. Если владелец устройства соглашается на это, злоумышленники узнают не только его конфиденциальные данные (например, имя, фамилия, номер телефона и адрес электронной почты), но и реквизиты банковской карты с секретным CVV2-кодом. При этом жертва мошенничества не получает никаких обещанных компенсаций.

Другой выявленный троян принадлежал семейству вредоносных приложений Android.HiddenAds и был добавлен в вирусную базу Dr.Web как Android.HiddenAds.2314. Он распространялся под видом программы для редактирования изображений. При запуске троян скрывает свой значок из списка ПО в меню главного экрана, чтобы в дальнейшем его было сложнее обнаружить и удалить с устройства. Затем он начинает показывать рекламу, которая демонстрируется поверх окон других приложений и интерфейса операционной системы, мешая нормальному использованию устройства.

Угрозы в Google Play



Для защиты Android-устройств от вредоносных и нежелательных программ пользователям следует установить антивирусные продукты Dr.Web для Android.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в октябре 2020 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

© ООО «Доктор Веб»,
2003-2020