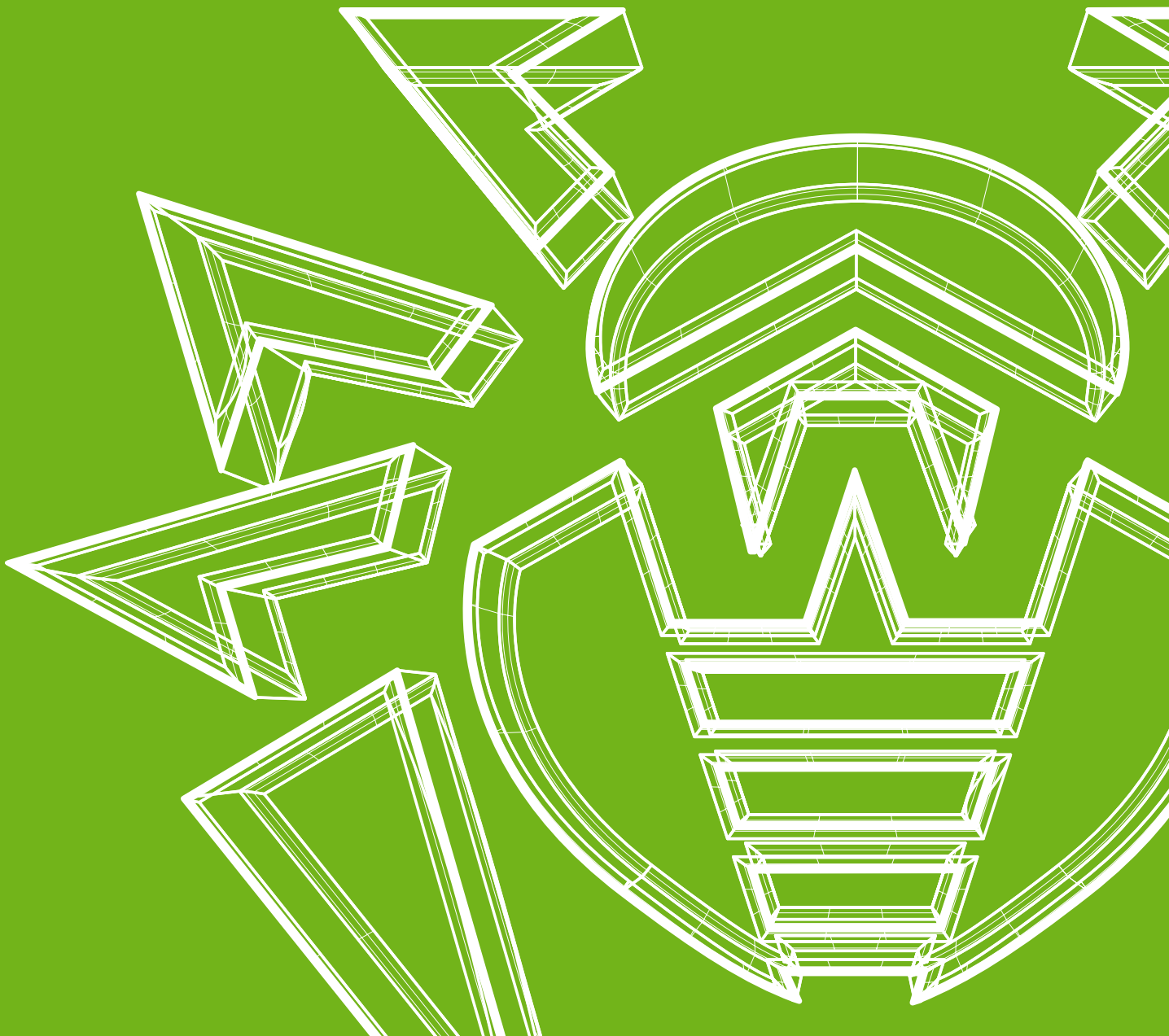
Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 года



«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 года

14 июня 2022 года

В мае активность трояна Android.Spy.4498, похищающего информацию из уведомлений от других приложений, снизилась на 13,48%. Тем не менее эта вредоносная программа по-прежнему является наиболее распространенной Android-угрозой. Среди лидеров по числу детектирований на устройствах пользователей также остаются рекламные трояны Android.HiddenAds. Их активность по сравнению с апрелем выросла на 13,57%.

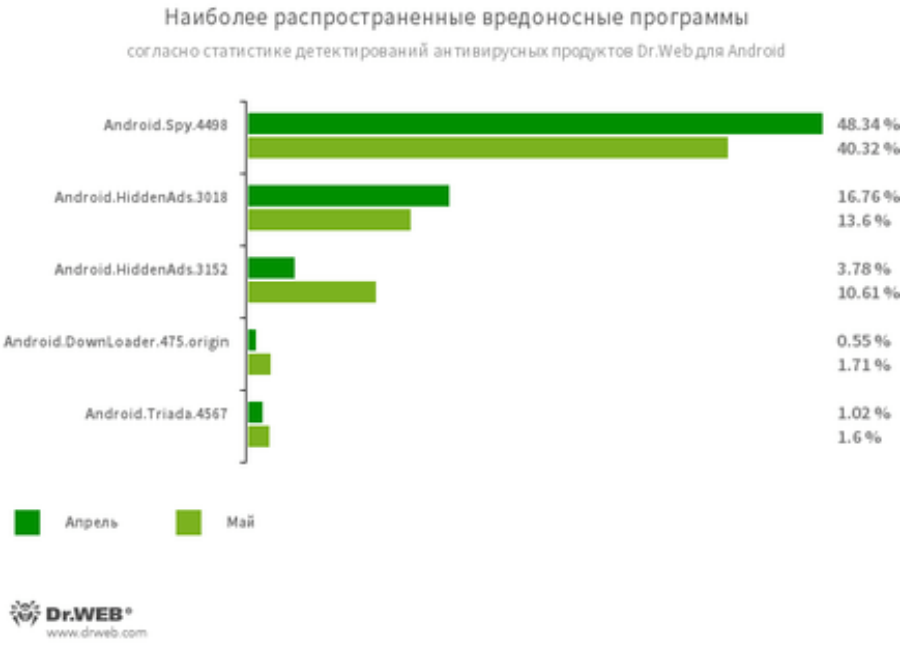
В течение месяца вирусная лаборатория компании «Доктор Веб» зафиксировала распространение новых вредоносных приложений в каталоге Google Play. Среди них — трояны семейства Android.Subscription, подписывающие пользователей на платные услуги, мошеннические программы Android.FakeApp, трояны-похитители паролей из семейства Android.PWS.Facebook, помогающие киберпреступникам взламывать учетные записи социальной сети Facebook, а также рекламные трояны Android.HiddenAds.

ГЛАВНЫЕ ТЕНДЕНЦИИ МАЯ

- Снижение активности трояна Android.Spy.4498
- Рост активности рекламных троянов
- Появление новых вредоносных программ в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 года

По данным антивирусных продуктов Dr.Web для Android



Android.Spy.4498

Троян, крадущий содержимое уведомлений от других приложений. Кроме того, он загружает и предлагает пользователям установить другие программы, а также может демонстрировать различные диалоговые окна.

Android.HiddenAds.3018

Android.HiddenAds.3152

Трояны, предназначенные для показа навязчивой рекламы. Представители этого семейства часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другими вредоносными программами. Попадая на Android-устройства, такие рекламные трояны обычно скрывают от пользователя свое присутствие в системе — например, «прячут» значок приложения из меню главного экрана.

Android.DownLoader.475.origin

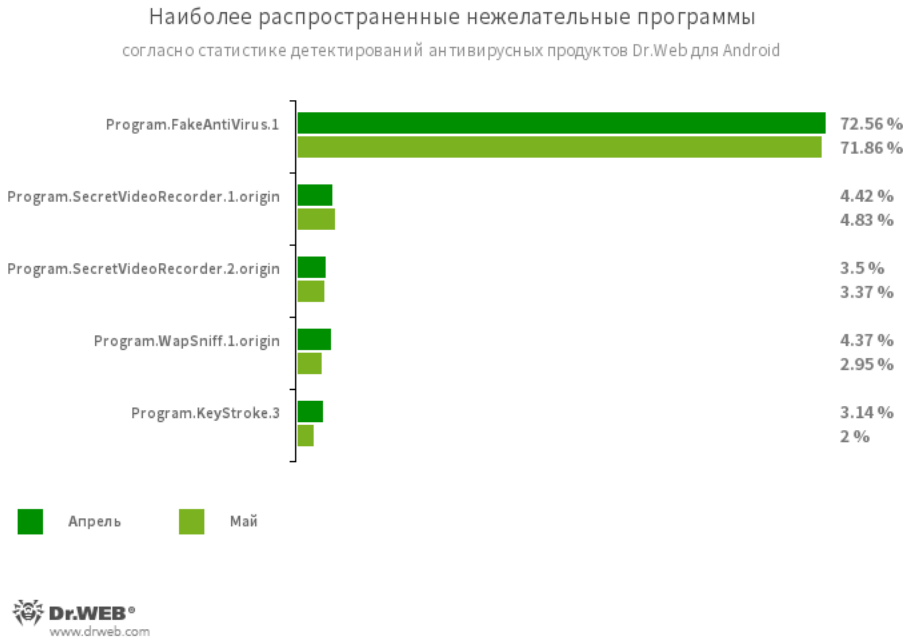
Троян, загружающий другие вредоносные программы и ненужное ПО. Он может скрываться во внешне безобидных приложениях, которые распространяются через каталог Google Play или вредоносные сайты.

Android.Triada.4567.origin

Многофункциональный троян, выполняющий разнообразные вредоносные действия. Относится 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.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 года

По данным антивирусных продуктов Dr.Web для Android



Program.FakeAntiVirus.1

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.SecretVideoRecorder.1.origin

Program.SecretVideoRecorder.2.origin

Детектирование различных версий приложения, предназначенного для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Эта программа может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает ее потенциально опасной.

Program.WapSniff.1.origin

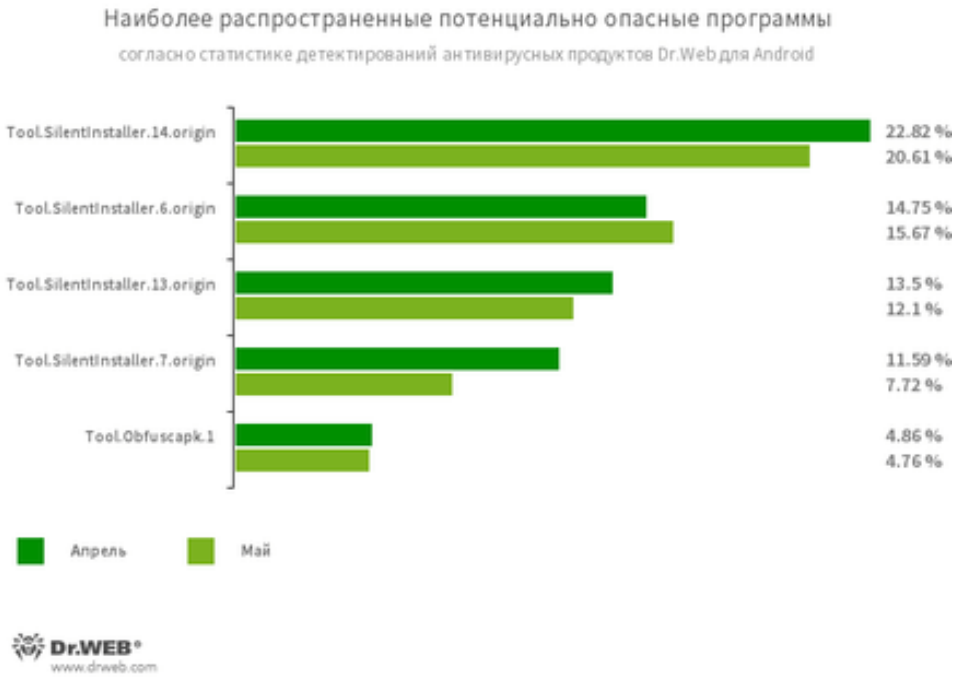
Программа для перехвата сообщений в мессенджере WhatsApp.

Program.KeyStroke.3

Android-программа, способная перехватывать вводимую на клавиатуре информацию. Некоторые ее модификации также позволяют отслеживать входящие СМС-сообщения, контролировать историю телефонных звонков и выполнять запись разговоров.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 года

По данным антивирусных продуктов Dr.Web для Android



Tool.SilentInstaller.14.origin

Tool.SilentInstaller.6.origin

Tool.SilentInstaller.13.origin

Tool.SilentInstaller.7.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.Obfuscapk.1.origin

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.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 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.SspSdk.1.origin

Adware.AdPush.36.origin

Adware.Adpush.6547

Adware.Adpush.2146

Adware.Myteam.2.origin

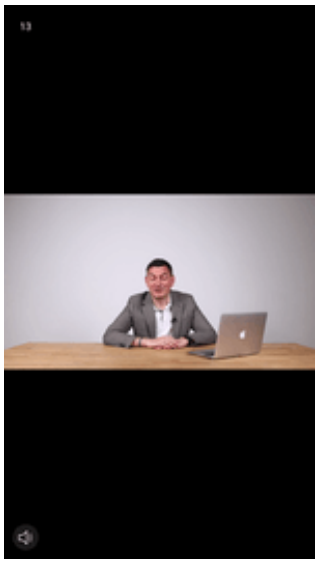
Угрозы в Google Play

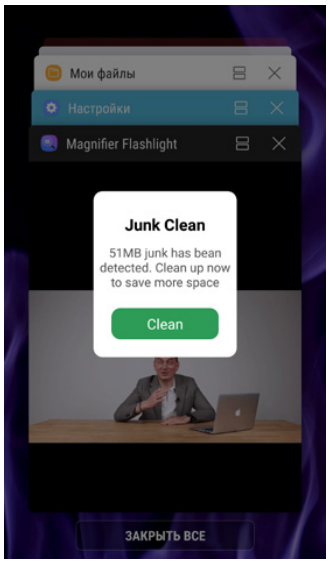
В мае специалисты компании «Доктор Веб» обнаружили в каталоге Google Play множество новых угроз. Среди них — рекламные трояны Android.HiddenAds.3158 и Android.HiddenAds.3161.

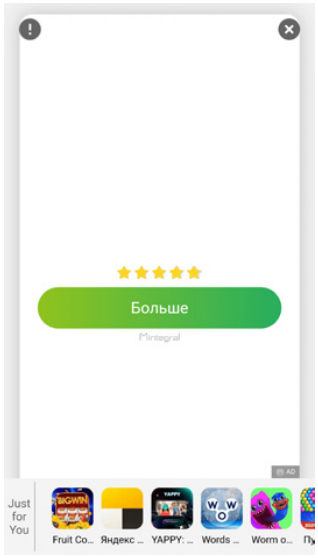
Первый представлял собой сборник изображений Wild & Exotic Animal Wallpaper. Он пытался скрыться от пользователя, заменяя значок приложения в меню главного экрана менее заметным, а также изменяя имя на «SIM Tool Kit». Кроме того, программа запрашивала разрешение отключить для нее функцию экономии заряда аккумулятора, чтобы постоянно работать в фоновом режиме. Это позволяло трояну показывать рекламу даже тогда, когда владелец устройства долго не использовал приложение.

Угрозы в Google Play

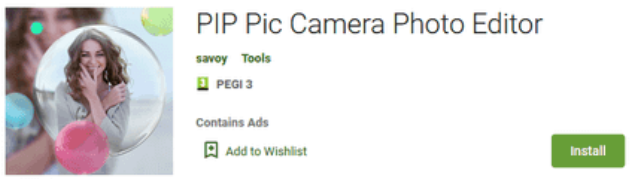
Второй троян распространялся под видом программы-фонарика Magnifier Flashlight. Он скрывал свой значок из списка программ в меню главного экрана, после чего периодически демонстрировал рекламные видеоролики и баннеры. Примеры такой рекламы:



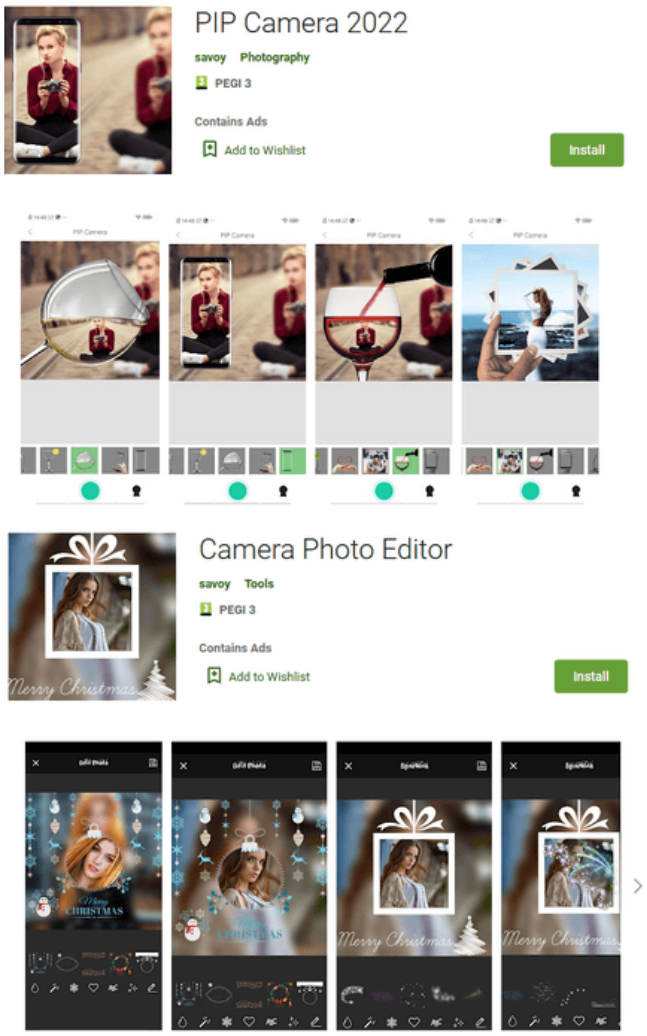




Были выявлены очередные троянские программы, которые крадут необходимые для взлома учетных записей Facebook данные (деятельность социальной сети Facebook запрещена на территории России). Они распространялись под видом редакторов изображений PIP Pic Camera Photo Editor (Android.PWS.Facebook.142), PIP Camera 2022 (Android.PWS.Facebook.143), Camera Photo Editor (Android.PWS.Facebook.144) и Light Exposure Photo Editor (Android.PWS.Facebook.145), а также астрологической программы ZodiHoroscope - Fortune Finder (Android.PWS.Facebook.141).

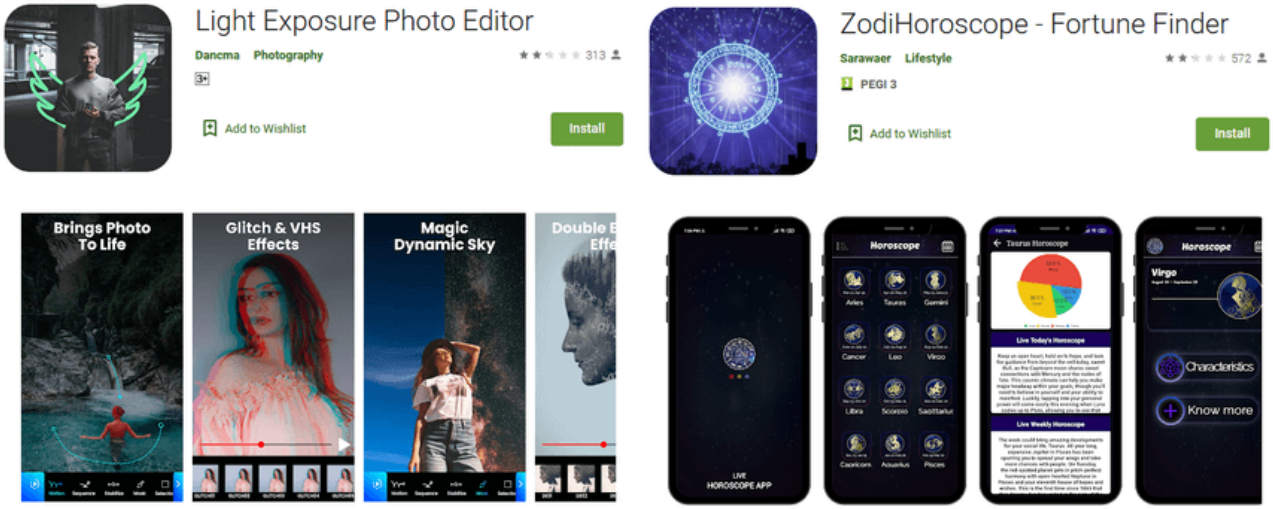


Угрозы в Google Play

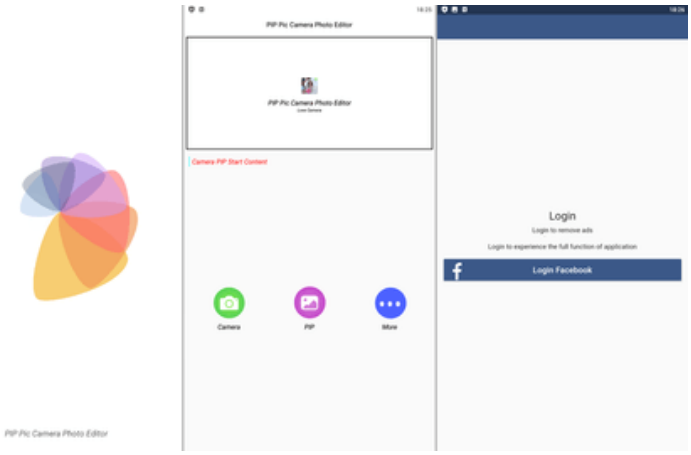


«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 года

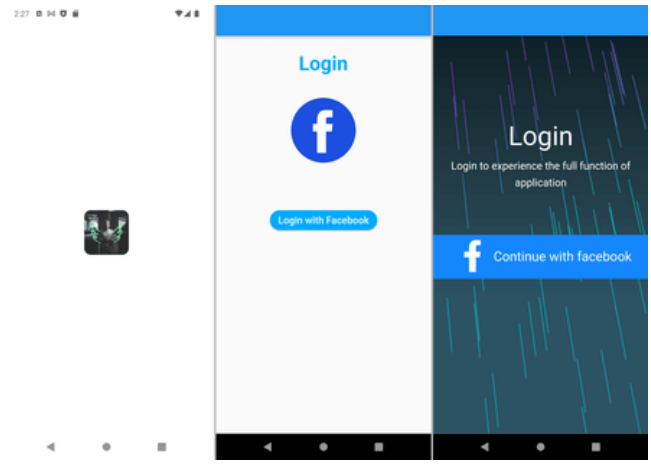
Угрозы в Google Play

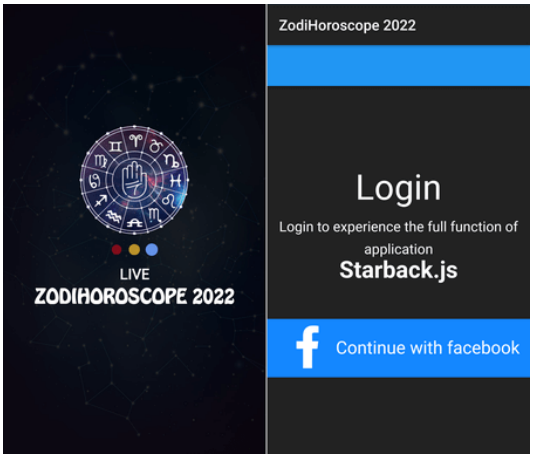


Эти трояны под различными предлогами (например, якобы для доступа ко всем функциям приложений или отключения рекламы) предлагают потенциальным жертвам войти в учетную запись Facebook, после чего перехватывают и передают киберпреступникам вводимые логины, пароли и другие данные авторизации.

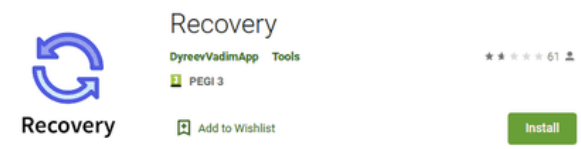


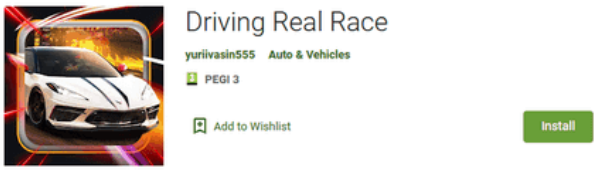
Угрозы в Google Play

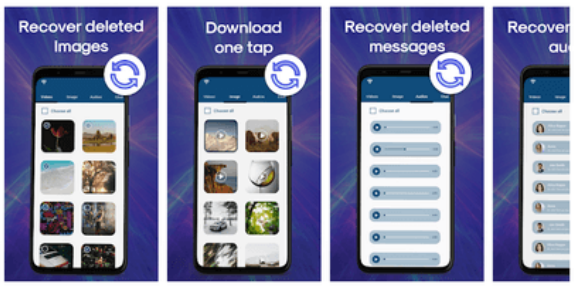




Среди найденных вредоносных программ также были новые представители семейства троянов Android.Subscription, предназначенных для подписки пользователей на платные услуги. Один из них, добавленный в вирусную базу Dr.Web как Android.Subscription.9, распространялся под видом программы Recovery для восстановления данных. Другой — под видом игры Driving Real Race: он получил имя Android.Subscription.10. Эти вредоносные приложения загружали сайты партнерских сервисов, через которые выполнялась подписка.

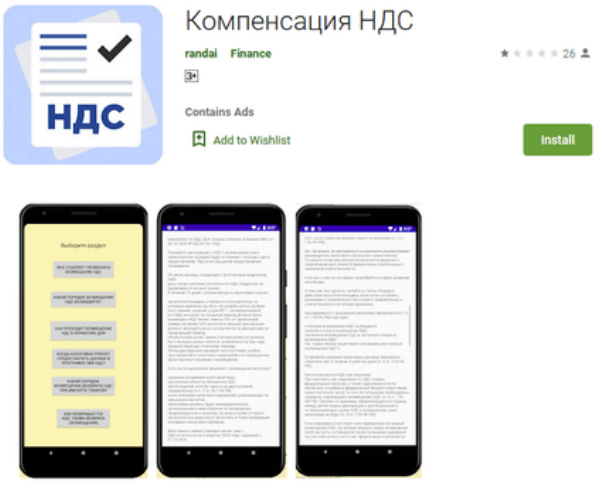




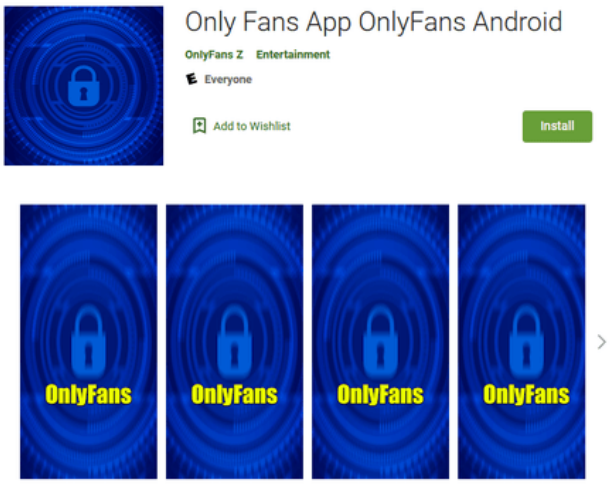


Угрозы в Google Play

Кроме того, злоумышленники вновь распространяли программы-подделки. Среди них — приложение «Компенсация НДС» (Android.FakeApp.949), якобы предназначенное для поиска и получения пособий и выплат российскими пользователями. На самом деле оно загружало мошеннические сайты, при помощи которых киберпреступники пытались похитить у жертв конфиденциальную информацию и деньги.



Другую подделку злоумышленники выдавали за приложение Only Fans App OnlyFans Android, которое якобы позволяло получить бесплатный доступ к закрытым профилям и платному контенту сервиса OnlyFans.

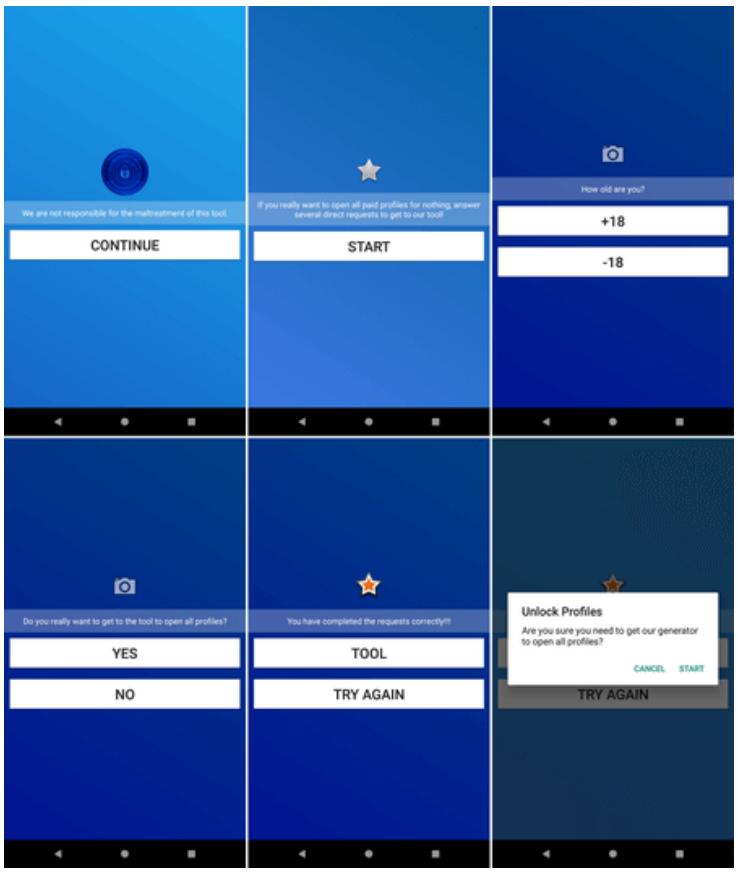


Пользователям предлагалось пройти небольшой опрос, после чего программа загружала мошеннический сайт, на котором имитировался процесс получения доступа. У потенциальных жертв запрашивался адрес электронной почты, после чего им предлагалось выполнить раз-

Угрозы в Google Play

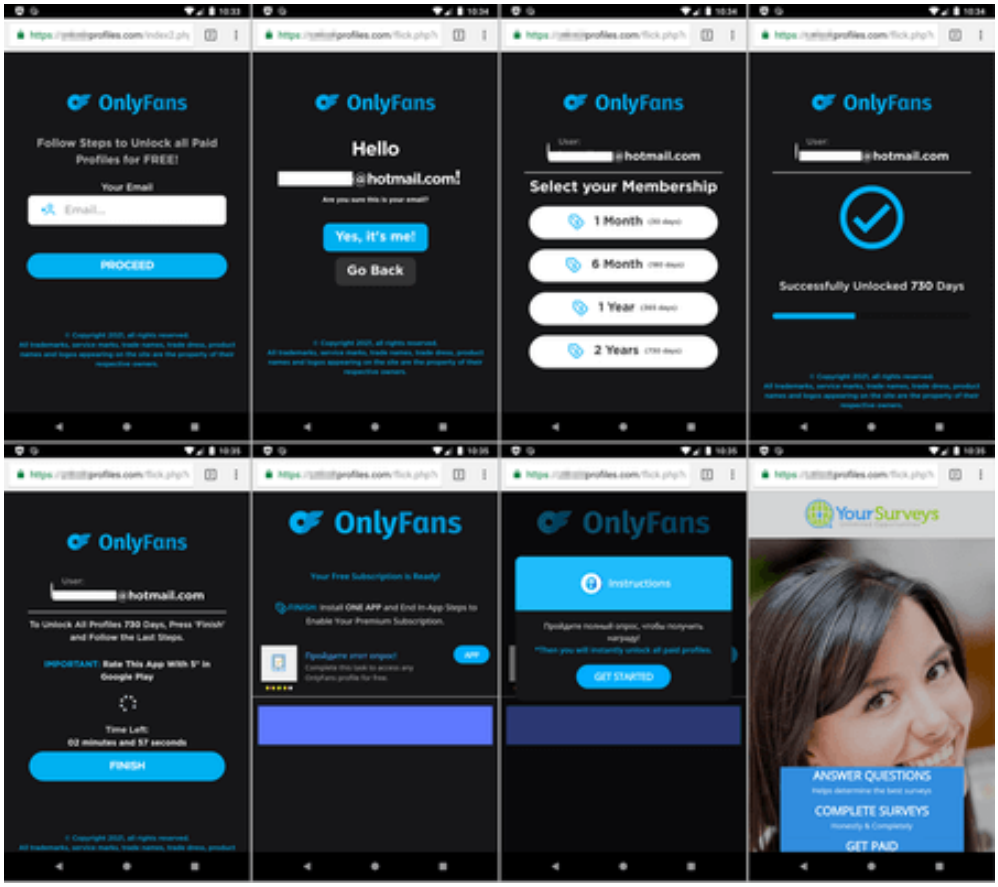
личные задания, например — установить заданные игры и программы или пройти онлайн-опросы. В действительности никакого доступа пользователи не получали, а от успешно выполненных заданий выигрывали сами мошенники — они получали плату от партнерских сервисов. Эта программа-подделка была добавлена в вирусную базу Dr.Web как Android.FakeApp.951.

Опрос в приложении, призванный заманить потенциальную жертву на мошеннический сайт:



Угрозы в Google Play

«Получение» доступа к контенту через мошеннический сайт:



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

Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в мае 2022 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
Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125124, Россия, Москва, 3-я улица Ямского Поля, д.2, корп.12А
www.антивирус.рф | www.drweb.ru | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах

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