



«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года



«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

8 сентября 2021 года

Согласно статистике детектирования антивирусных продуктов Dr.Web для Android за август, пользователи чаще всего вновь сталкивались с рекламными троянами, а также вредоносными приложениями, способными выполнять произвольный код и загружать другое ПО.

В течение месяца специалисты компании «Доктор Веб» выявили множество угроз в каталоге Google Play. Среди них — программы-подделки семейства [Android.FakeApp](#), загружавшие мошеннические сайты. Кроме того, был обнаружен очередной троян, похищавший логины и пароли от учетных записей Facebook. Также злоумышленники распространяли троянов семейства [Android.Joker](#), которые подписывают жертв на платные мобильные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ АВГУСТА

- Обнаружение вредоносных программ в каталоге Google Play
- Активность рекламных троянов, а также вредоносных программ, загружающих другое ПО и выполняющих произвольный код

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

По данным антивирусных продуктов Dr.Web для Android



[Android.HiddenAds.1994](#)

Троян, предназначенный для показа навязчивой рекламы. Трояны этого семейства часто распространяются под видом безобидных приложений и в некоторых случаях устанавливаются в системный каталог другими вредоносными программами.

[Android.Triada.510.origin](#)

[Android.Triada.4567](#)

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.RemoteCode.284.origin](#)

Вредоносная программа, которая загружает и выполняет произвольный код. В зависимости от модификации трояны этого семейства также могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

[Android.MobiDash.5162](#)

Троянская программа, показывающая надоедливую рекламу. Представляет собой программный модуль, который разработчики ПО встраивают в приложения.

Узнайте больше

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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 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.KeyStroke.1.origin](#)

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

[Program.FreeAndroidSpy.1.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, прослушивать телефонные звонки и окружение и т. п.

[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.

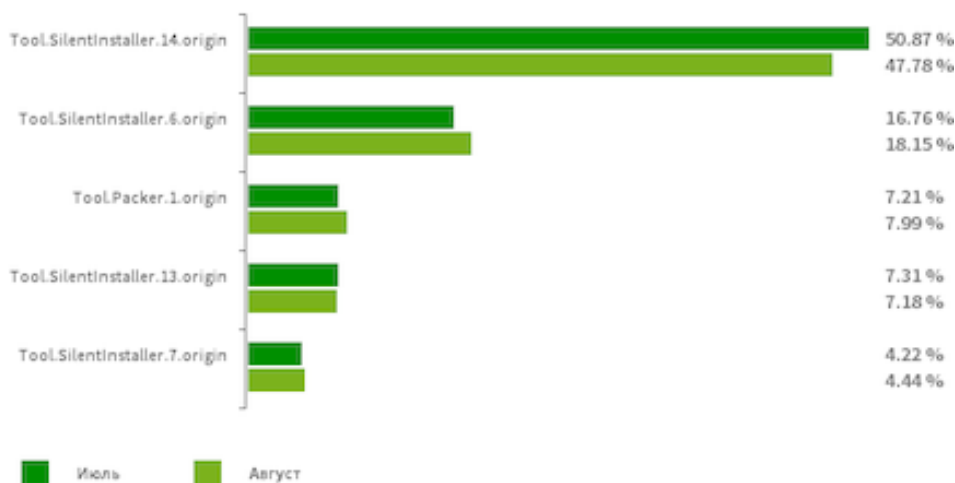
Узнайте больше

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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

По данным антивирусных продуктов Dr.Web для Android

Наиболее распространенные потенциально опасные программы согласно статистике детектирования антивирусных продуктов Dr.Web для Android



[Tool.SilentInstaller.14.origin](#)

[Tool.SilentInstaller.13.origin](#)

[Tool.SilentInstaller.6.origin](#)

[Tool.SilentInstaller.7.origin](#)

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

[Tool.Packer.1.origin](#)

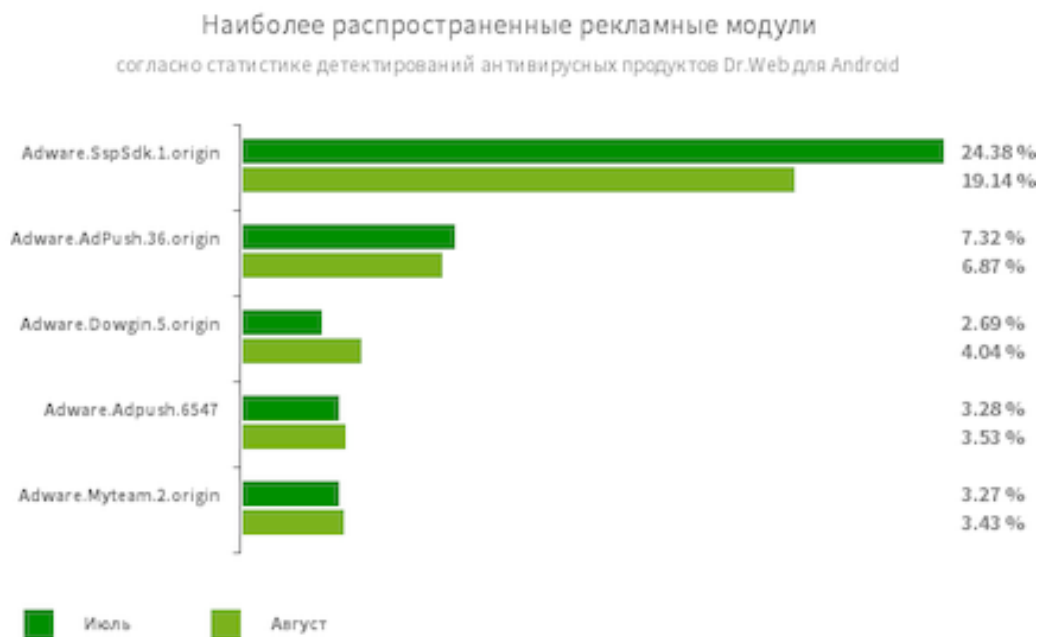
Специализированная утилита-упаковщик, предназначенная для защиты Android-приложений от модификации и обратного инжиниринга. Она не является вредоносной, но может быть использована для защиты как безобидных, так и троянских программ.

Узнайте больше

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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 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.Dowgin.5.origin](#)

[Adware.Myteam.2.origin](#)

[Угрозы в Google Play](#)

Узнайте больше

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

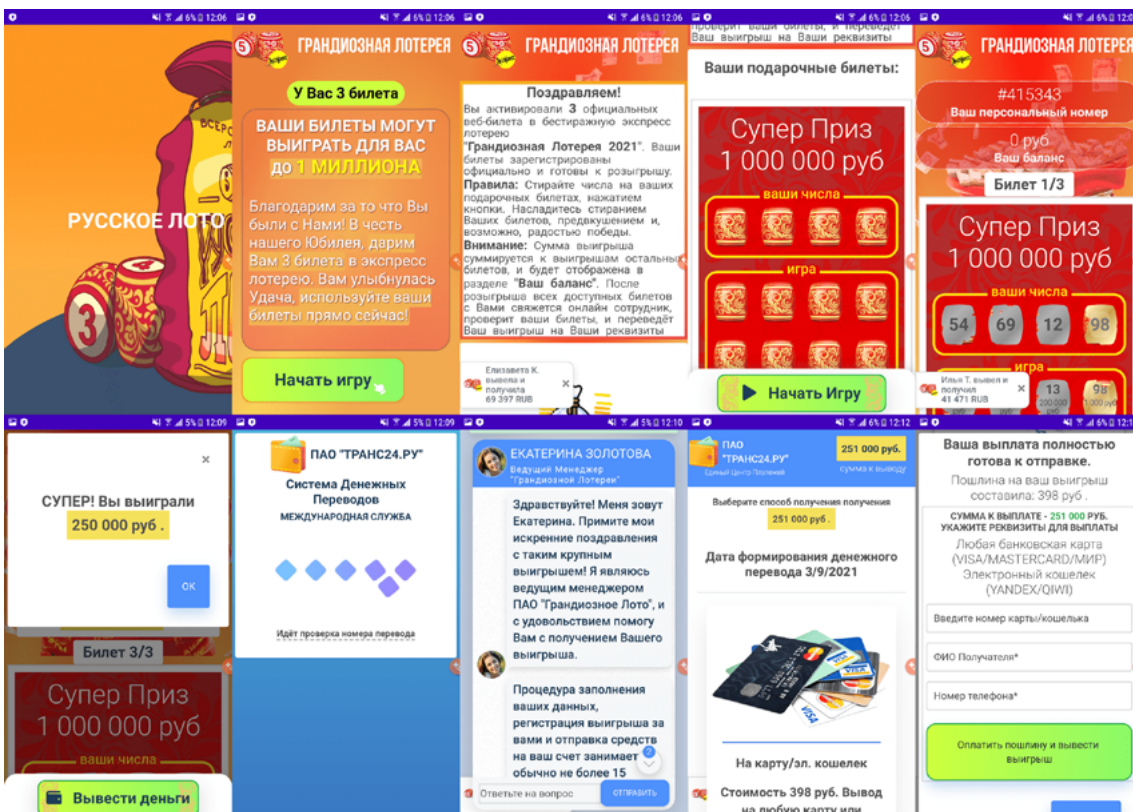
«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play

В августе в каталоге Google Play было обнаружено множество вредоносных программ. Среди них — программы-подделки семейства [Android.FakeApp](#), которые используются в различных мошеннических схемах. Так, часть этих троянов вновь распространялась под видом официальных приложений популярных российских лотерей «Русское лото» и «Гослото», а также их официального дистрибьютора «Столото». Подделки были добавлены в вирусную базу Dr.Web как [Android.FakeApp.307](#), [Android.FakeApp.308](#), [Android.FakeApp.309](#), [Android.FakeApp.310](#), [Android.FakeApp.311](#), [Android.FakeApp.312](#), [Android.FakeApp.325](#), [Android.FakeApp.328](#), [Android.FakeApp.329](#), [Android.FakeApp.330](#), [Android.FakeApp.332](#), [Android.FakeApp.333](#), [Android.FakeApp.334](#), [Android.FakeApp.335](#) и [Android.FakeApp.341](#).

При запуске программы загружали мошеннические сайты, где потенциальным жертвам предлагалось получить бесплатные лотерейные билеты и принять участие в розыгрыше призов. Однако это был обман: игра лишь имитировалась, а для получения «выигрыша» от пользователей требовалось оплатить «комиссию» или «пошлину» — эти деньги оседали в карманах мошенников.

Пример работы одного из таких троянов показан ниже:



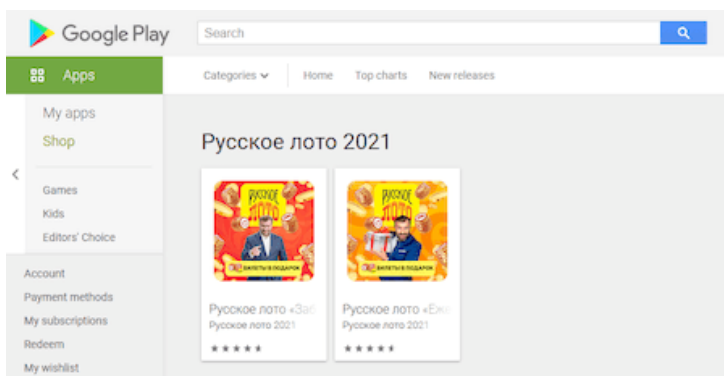
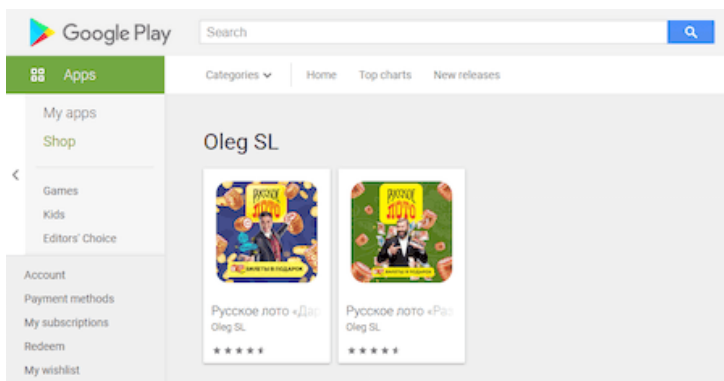
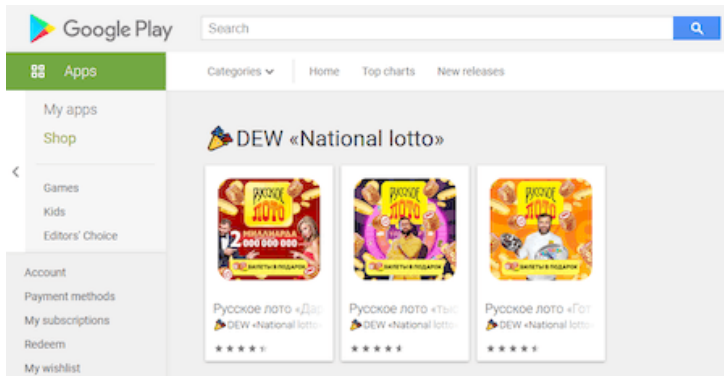
Узнайте больше

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

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

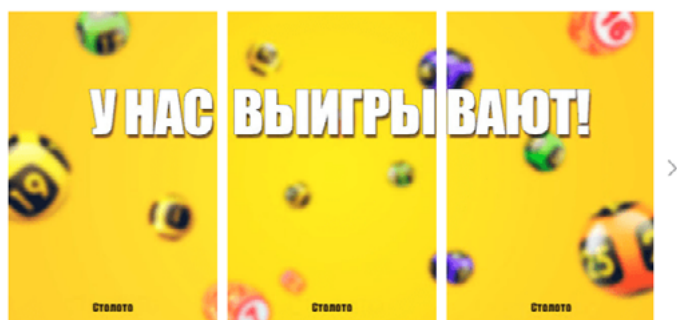
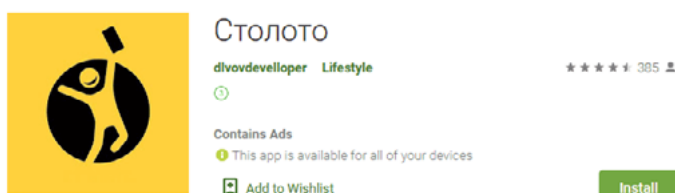
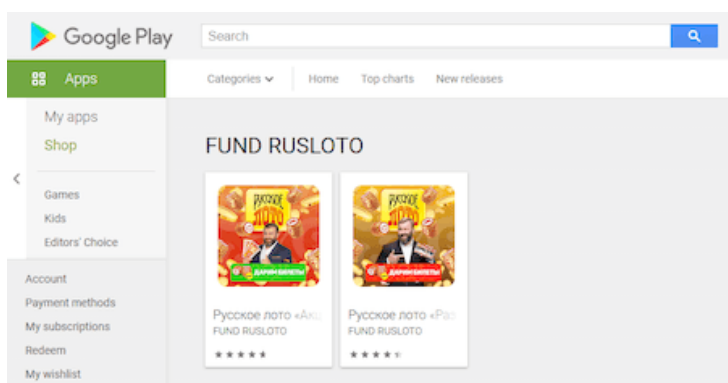
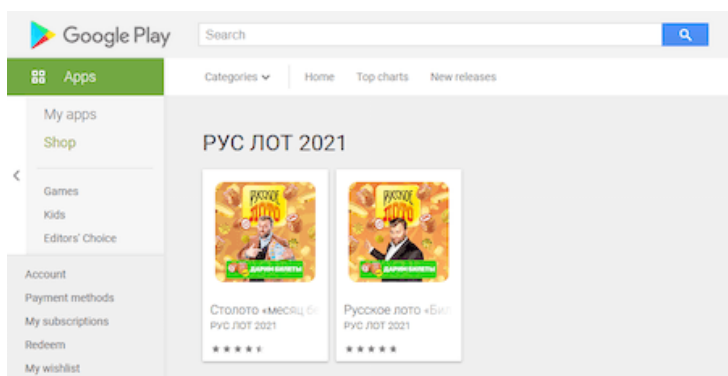
Угрозы в Google Play

Примеры того, как такие подделки выглядят в Google Play:



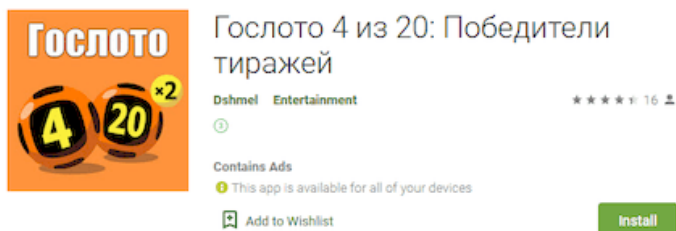
«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play

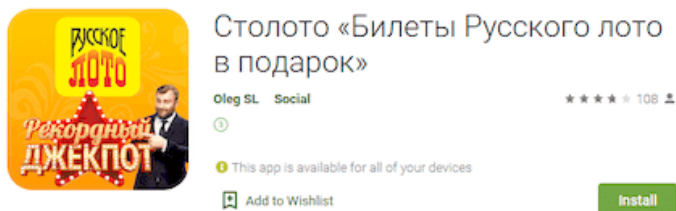


«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play



Гослото
Гослото 4 из 20: Победители тиражей
Dshmel Entertainment ★★★★★ 16 👤
Contains Ads
This app is available for all of your devices
Add to Wishlist Install




Столото
Столото «Билеты Русского лото в подарок»
Oleg SL Social ★★★★★ 108 👤
This app is available for all of your devices
Add to Wishlist Install


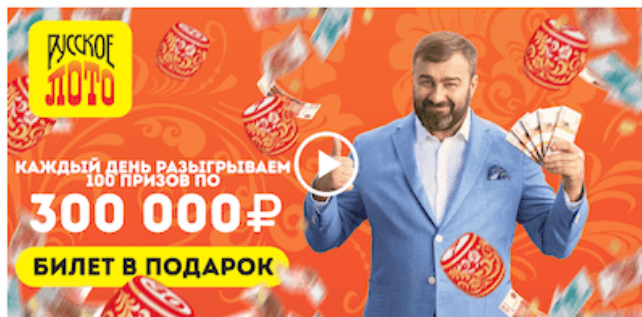


«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play



Русское лото «Дарим Вам билеты на экспресс тиражи»
LLC TK Center «Russian Lotto» Social ★★★★★ 705
This app is available for all of your devices
Add to Wishlist Install



Русское Лото
Deer.tech Casino ★★★★★ 15
Contains Ads
This app is available for all of your devices
Add to Wishlist Install

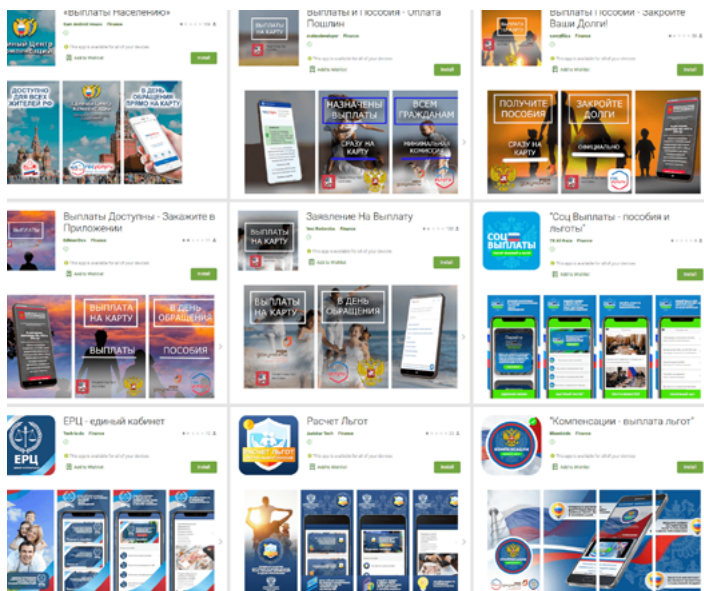


Другими подделками были очередные приложения, с помощью которых российские пользователи якобы могли найти информацию о различных социальных выплатах от государства, а также непосредственно получить эти выплаты на свои банковские карты и счета. Как и в случае со схемой с лотерейными билетами, такие программы лишь загружали мошеннические сайты, на которых для получения «выплат» требовалось оплатить «комиссию».

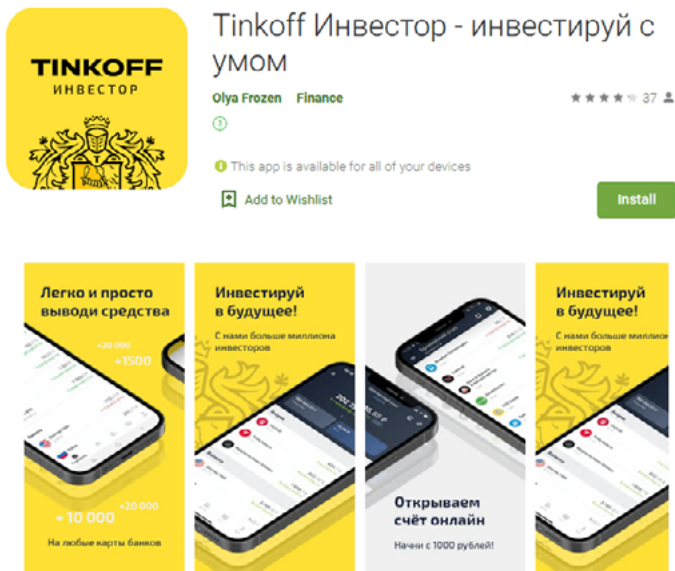
Трояны были доданы в вирусную базу Dr.Web как [Android.FakeApp.306](#), [Android.FakeApp.313](#) и [Android.FakeApp.325](#).

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play



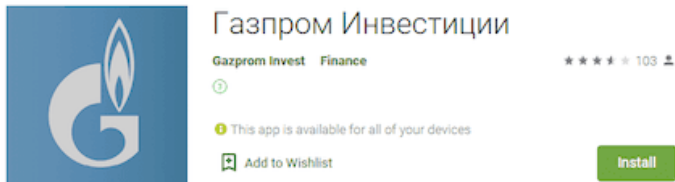
Кроме того, были обнаружены новые мошеннические программы, якобы предназначенные для инвестирования и торговли на финансовом рынке. Некоторые из них злоумышленники распространяли от имени известных компаний.



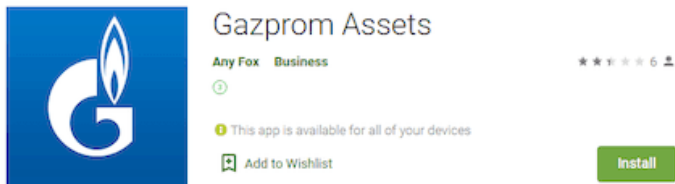
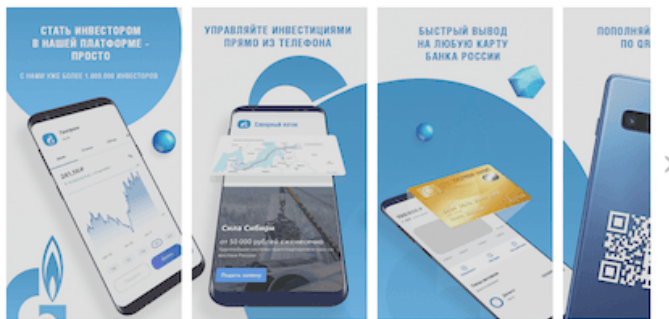
Узнайте больше

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

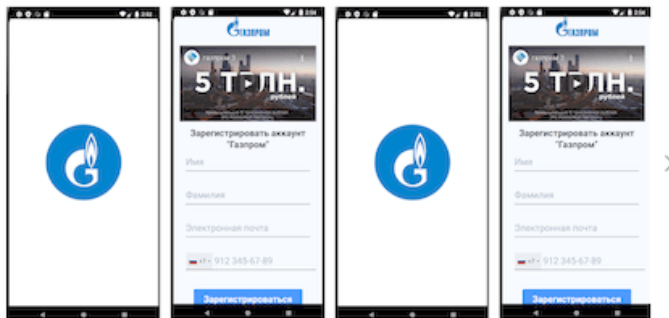
Угрозы в Google Play



Газпром Инвестиции
Gazprom Invest Finance ★★★★★ 103
This app is available for all of your devices
Add to Wishlist **Install**

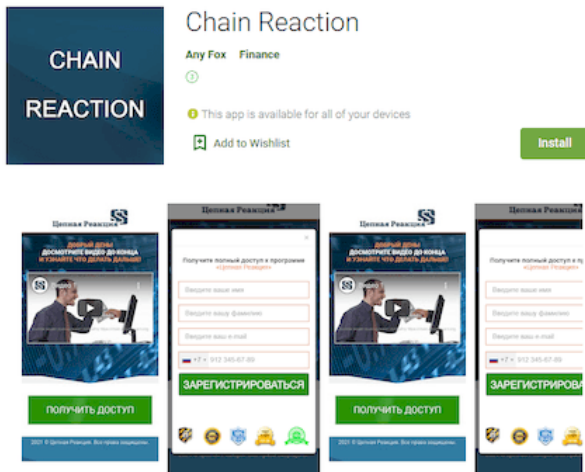


Gazprom Assets
Any Fox Business ★★★★★ 6
This app is available for all of your devices
Add to Wishlist **Install**



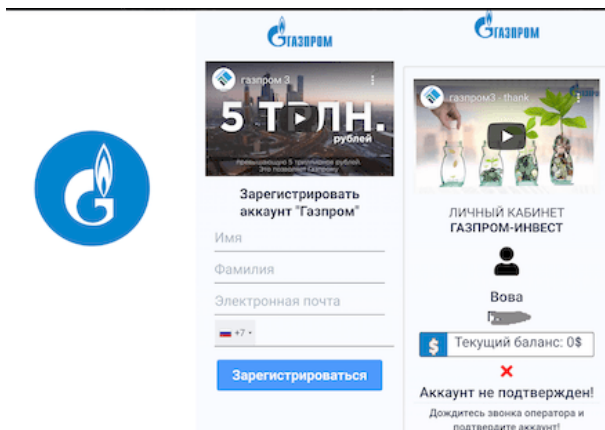
«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play



Эти трояны, получившие имена [Android.FakeApp.305](#), [Android.FakeApp.314](#), [Android.FakeApp.315](#) и [Android.FakeApp.316](#), загружали различные «финансовые» сайты-приманки, где пользователям предлагалось пройти регистрацию, чтобы начать зарабатывать. В некоторых случаях у них запрашивались имя, фамилия, адрес электронной почты и номер мобильного телефона, в других — только телефонный номер. Затем жертвы обмана могли быть перенаправлены на другие мошеннические ресурсы, получить уведомление о том, что мест для новых клиентов якобы не осталось, либо увидеть просьбу дождаться звонка «оператора».

Примеры работы этих троянов:



Узнайте больше

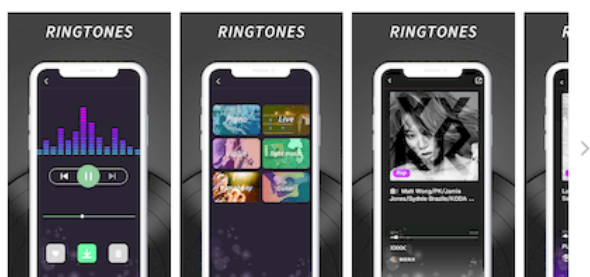
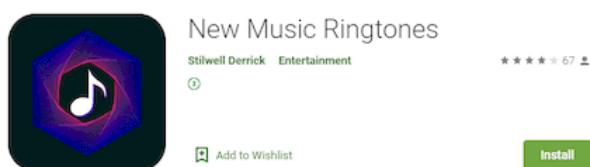
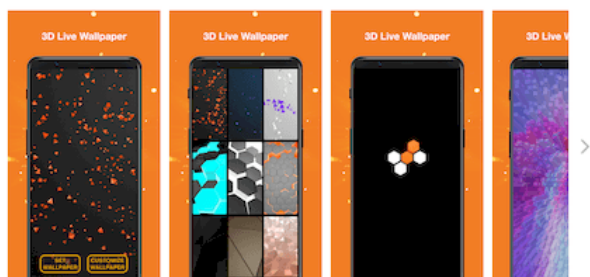
[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play

При помощи таких инвестиционных программ-подделок злоумышленники не только собирают персональную информацию пользователей и могут украсть их деньги, но и способны в дальнейшем вовлечь их в другие мошеннические схемы, в том числе продав полученные данные третьим лицам.

Среди выявленных в Google Play угроз также оказались и новые представители семейства опасных троянов [Android.Joker](#), добавленные в вирусную базу Dr.Web как [Android.Joker.320.origin](#), [Android.Joker.858](#) и [Android.Joker.910](#). Первый распространялся под видом анимированных обоев 3D Live Wallpaper, второй маскировался под музыкальное приложение New Music Ringtones, а третий выдавал себя за приложение Free Text Scanner для сканирования текстов и создания PDF-документов. Все они подписывали владельцев Android-устройств на платные мобильные услуги, а также могли загружать и исполнять произвольный код.

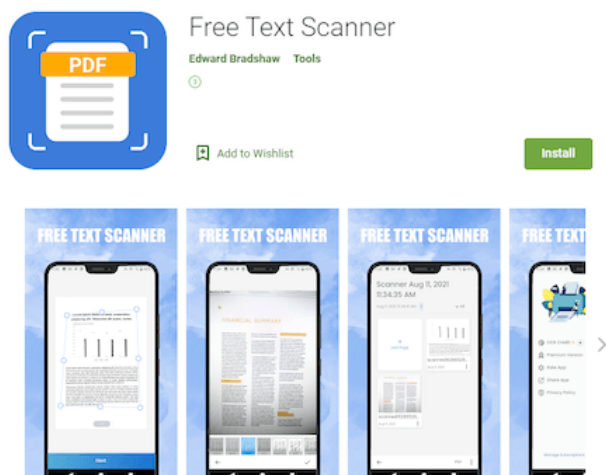


Узнайте больше

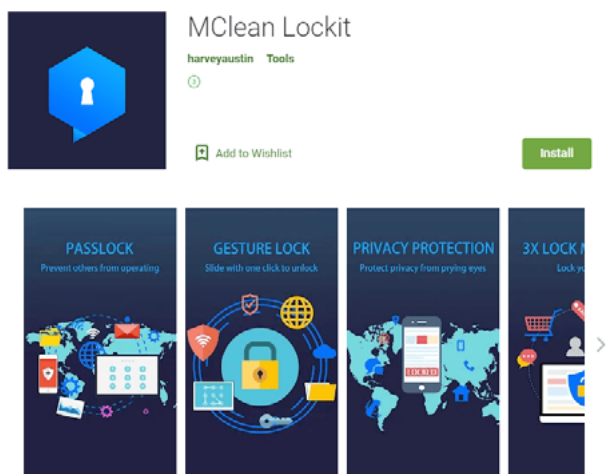
[Лаборатория-live](#) | [Вирусные обзоры](#) | [Горячая лента угроз](#) | [Вирусная библиотека](#)

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2021 года

Угрозы в Google Play



Также наши вирусные аналитики обнаружили нового трояня, предназначенного для кражи логинов и паролей от учетных записей Facebook. Он распространялся под видом программы, позволяющей защитить установленные приложения от несанкционированного доступа. Троян был добавлен в вирусную базу Dr.Web как **Android.PWS.Facebook.34**.



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 августе 2021 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, 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»,
2003-2021

Узнайте больше

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