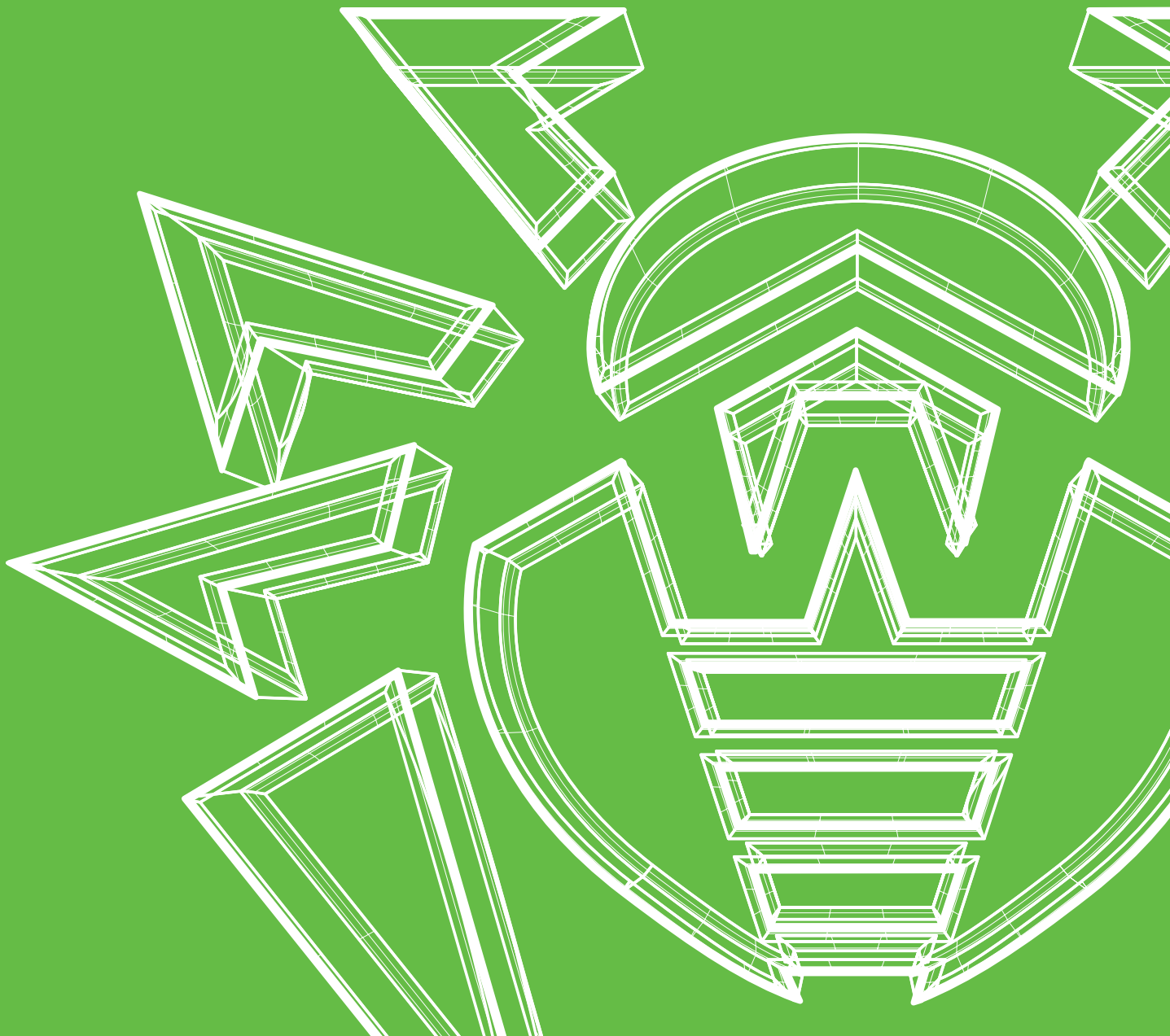
«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 2022 года



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

23 декабря 2022 года

Согласно данным статистики детектирований антивируса Dr.Web для Android, в ноябре незначительно снизилась активность троянских и нежелательных приложений, демонстрирующих рекламу. Тем не менее, они по-прежнему остаются одними из наиболее распространенных Android-угроз. Вместе с тем возросла активность программ, которые могут применяться для кибершпионажа.

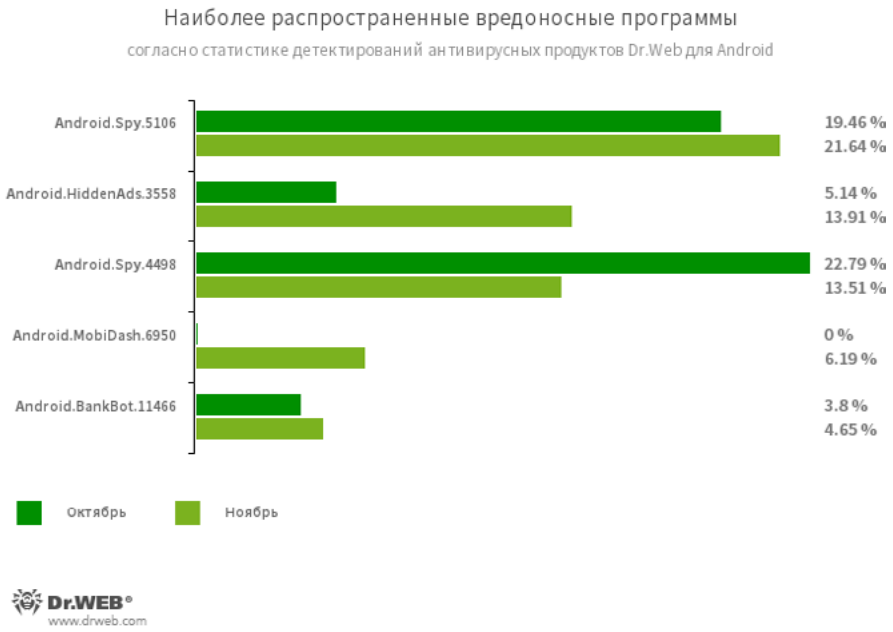
В течение месяца вирусные аналитики компании «Доктор Веб» выявили в каталоге Google Play множество новых вредоносных приложений. Среди них — десятки программ-подделок, которые киберпреступники используют в различных мошеннических схемах, а также трояны, подписывающие жертв на платные услуги.

ГЛАВНЫЕ ТЕНДЕНЦИИ НОЯБРЯ

- Снижение активности вредоносных и нежелательных программ, демонстрирующих рекламу
- Рост активности шпионских приложений
- Обнаружение новых угроз в каталоге Google Play

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

По данным антивирусных продуктов Dr.Web для Android



- Android.Spy.5106
- Android.Spy.4498

Детектирование различных модификаций трояна, который похищает содержимое уведомлений от других приложений. Он также загружает и предлагает пользователям установить другие программы и может демонстрировать диалоговые окна.

- Android.HiddenAds.3558

Троянская программа, предназначенная 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.MobiDash.6950

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

- Android.BankBot.11466

Детектирование вредоносных приложений, защищенных программным упаковщиком ApkProtector. Среди них встречаются банковские трояны, шпионское и другое вредоносное ПО.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в ноябре 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.FakeMoney.3

Программа, якобы позволяющая зарабатывать на просмотре видеороликов и рекламы. Она имитирует начисление вознаграждений за выполненные задания. Для вывода «заработанных» денег пользователи якобы должны накопить определенную сумму, но даже когда им это удается, получить выплаты они не могут.

- Program.wSpy.1.origin

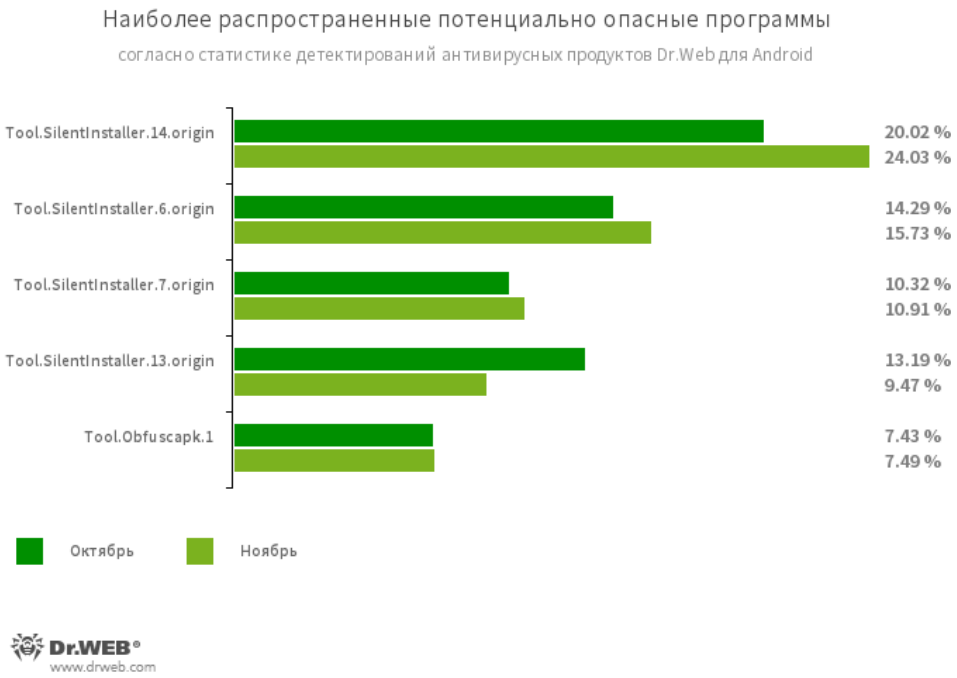
Коммерческая программа-шпион для скрытого наблюдения за владельцами Android-устройств. Она позволяет читать переписку (сообщения в популярных мессенджерах и СМС), прослушивать окружение, отслеживать местоположение устройства, следить за историей веб-браузера, получать доступ к телефонной книге и контактам, фотографиям и видео, делать скриншоты экрана и фотографии через камеру устройства, а также имеет функцию кейлоггера.

- Program.SecretVideoRecorder.1.origin
- Program.SecretVideoRecorder.2.origin

Детектирование различных версий приложения 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.

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

По данным антивирусных продуктов Dr.Web для Android



- Tool.SilentInstaller.14.origin
- Tool.SilentInstaller.6.origin
- Tool.SilentInstaller.7.origin
- Tool.SilentInstaller.13.origin

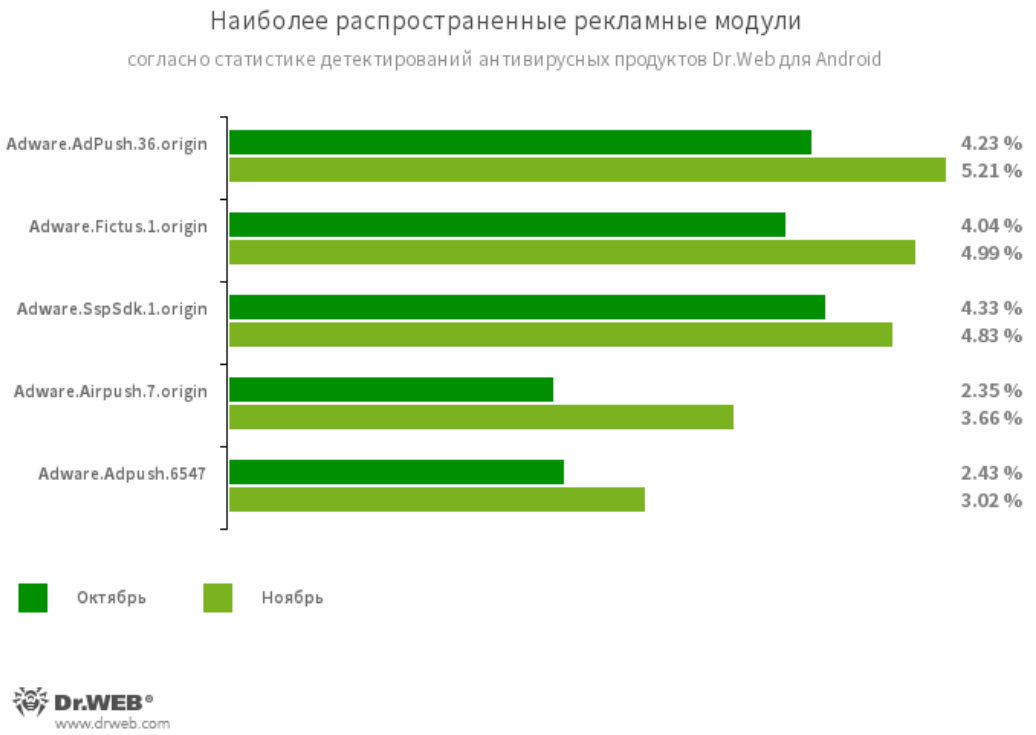
Потенциально опасные программные платформы, которые позволяют приложениям запускать APK-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

- Tool.Obfuscapk.1

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 ноябре 2022 года

По данным антивирусных продуктов Dr.Web для Android



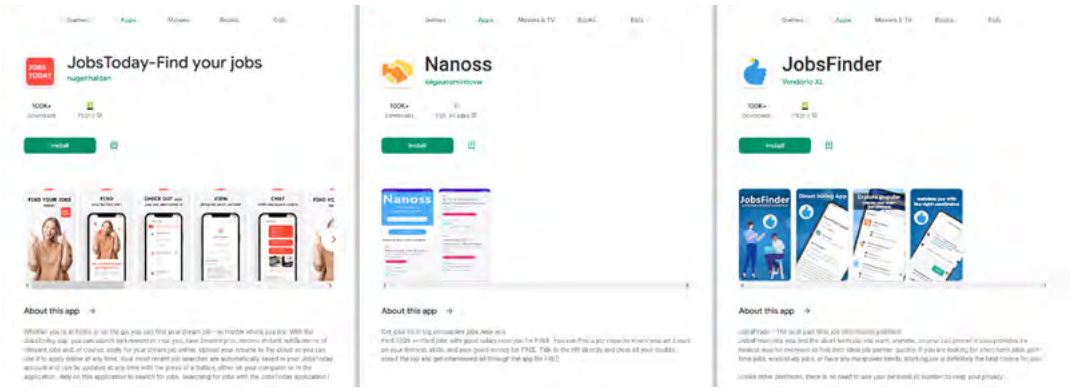
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать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

- Adware.AdPush.36.origin
- Adware.Adpush.6547
- Adware.Fictus.1.origin
- Adware.SspSdk.1.origin
- Adware.Airpush.7.origin

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

Угрозы в Google Play

В ноябре 2022 года вирусные аналитики компании «Доктор Веб» обнаружили более 80 новых вредоносных приложений в каталоге Google Play. Среди них было множество троянских программ из семейства Android.FakeApp — злоумышленники использовали их в различных мошеннических схемах. Например, трояны Android.FakeApp.1036, Android.FakeApp.1039, Android.FakeApp.1041, Android.FakeApp.1045, Android.FakeApp.1046, Android.FakeApp.1047 и Android.FakeApp.1055 распространялись под видом приложений для поиска работы, но на самом деле лишь загружали веб-сайты с поддельными вакансиями.

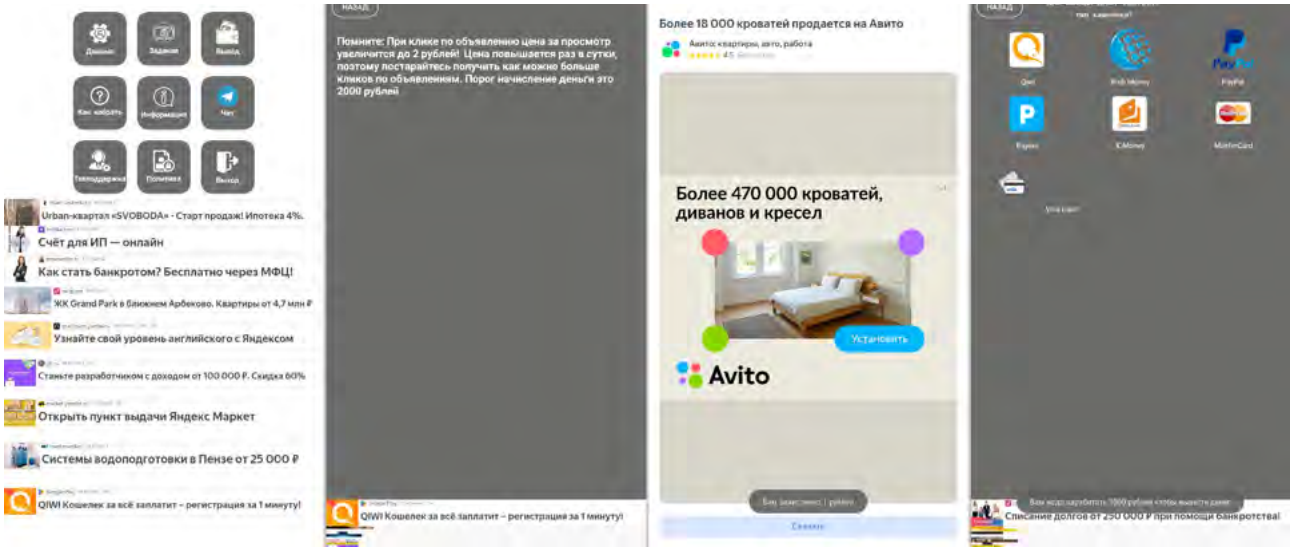


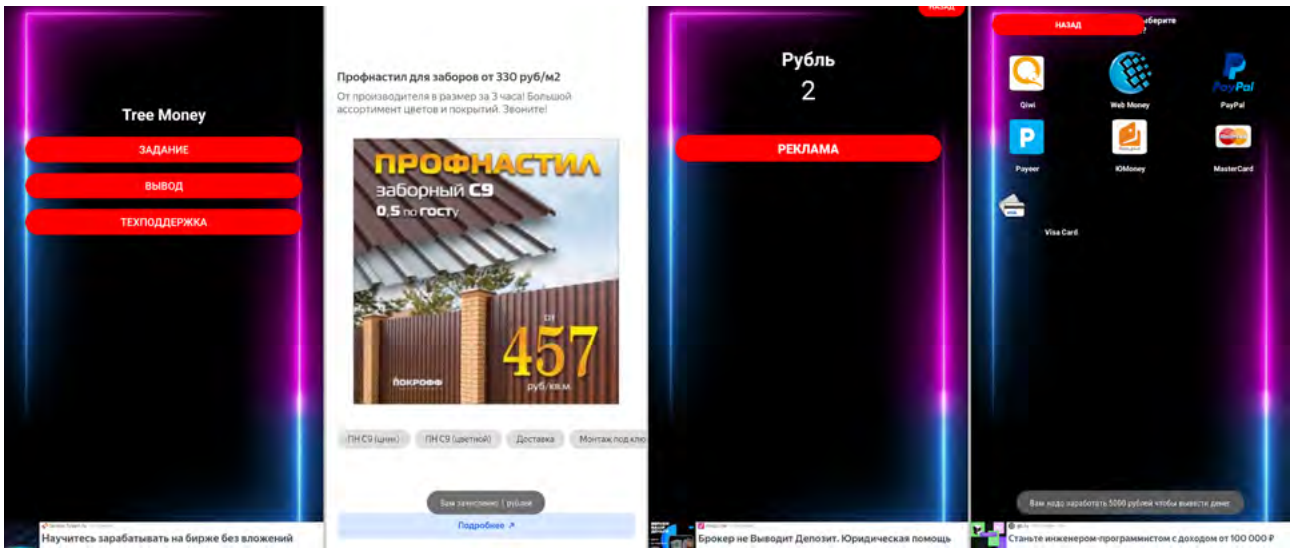
Когда пользователи пытались откликнуться на понравившиеся объявления, у них запрашивалась персональная информация — имя и фамилия, адрес электронной почты и номер мобильного телефона. В дальнейшем эти данные попадали в руки киберпреступников. При этом в ряде случаев потенциальным жертвам мошенников предлагалось связаться с «работодателем» напрямую — например, через мессенджеры WhatsApp и Telegram. Выдавая себя за представителей различных компаний, злоумышленники приглашали пользователей стать участниками сомнительных сервисов онлайн-заработка, после чего пытались выманить у них деньги. Подробнее об этом случае рассказано в материале на нашем сайте.

Троянские приложения, получившие имена Android.FakeApp.1081, Android.FakeApp.1082, Android.FakeApp.1083 и Android.FakeApp.1084, якобы позволяли зарабатывать на просмотре рекламы. Они загружали рекламные видеоролики и баннеры. За каждый успешный просмотр полноэкранной рекламы пользователю «начислялась» награда — 1 рубль. Однако при попытке вывести деньги программы сообщали, что для этого требуется накопить большую сумму — до нескольких тысяч рублей. В данном случае создатели подделок обманывали жертв, чтобы те просматривали как можно больше рекламы и приносили доход злоумышленникам. При этом для увеличения объема рекламного трафика в «справке» некоторых модификаций троянов сообщалось, что при клике по объявлениям вознаграждение якобы увеличится до 2 рублей. Никаких выплат пользователи на самом деле не получали и лишь тратили время.

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

Угрозы в Google Play



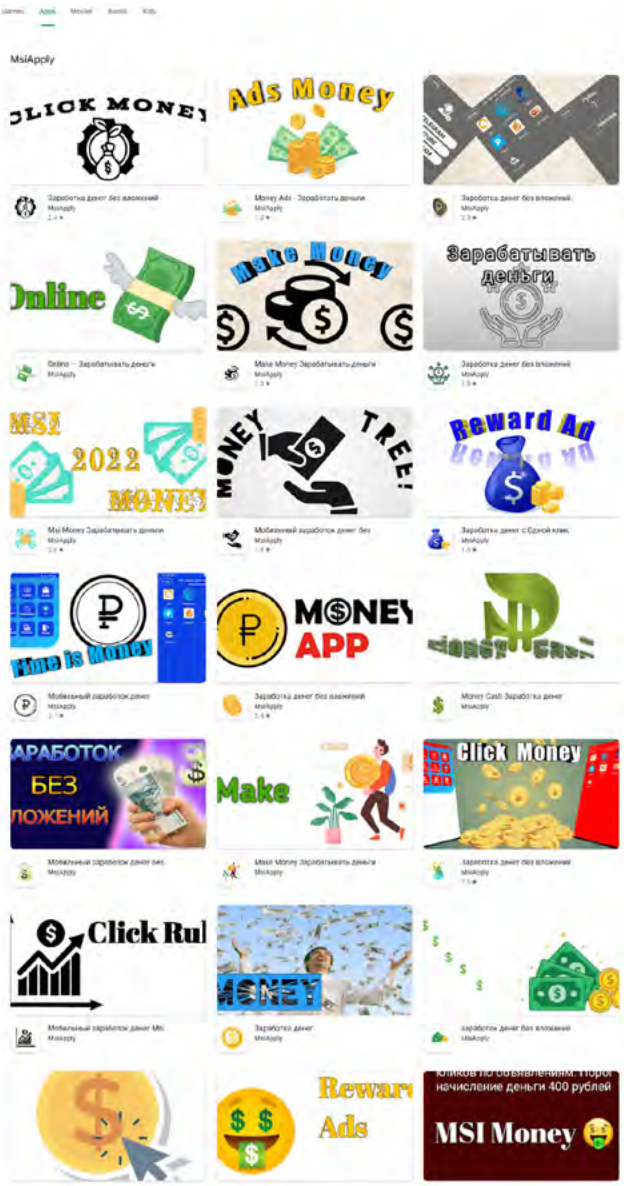


Эти вредоносные приложения были нацелены на русскоязычных пользователей, однако их авторы допустили множество грамматических и лексических ошибок. Среди них — ошибки в названиях программ (например, «Заработка без вложений», «Заработка денег с Одной клик»), а также ошибки в текстах интерфейса (например, «Порог начисление деньги это 2000 рублей», «Вам зачисленно 1 рублей», «Вам надо заработать 3000 рублей чтобы вывести денег»).

Наши специалисты выявили более 20 модификаций этих троянских программ.

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

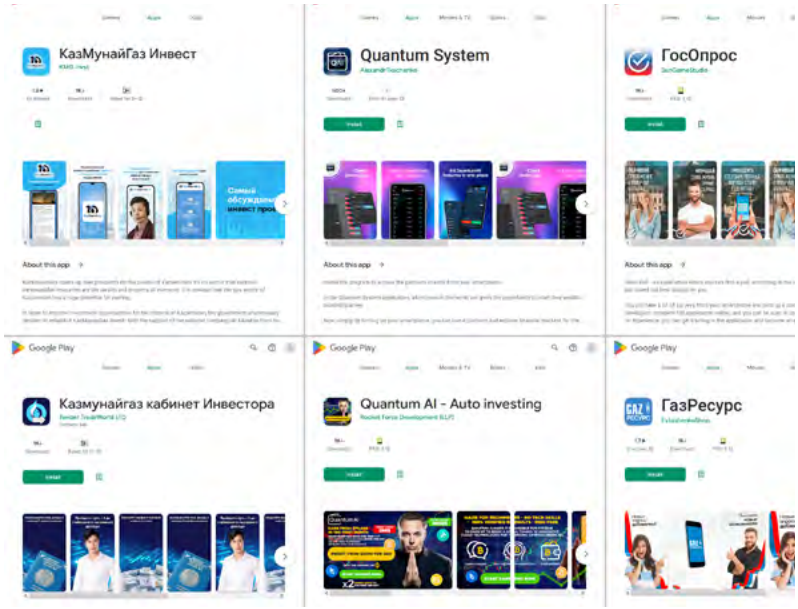
Угрозы в Google Play



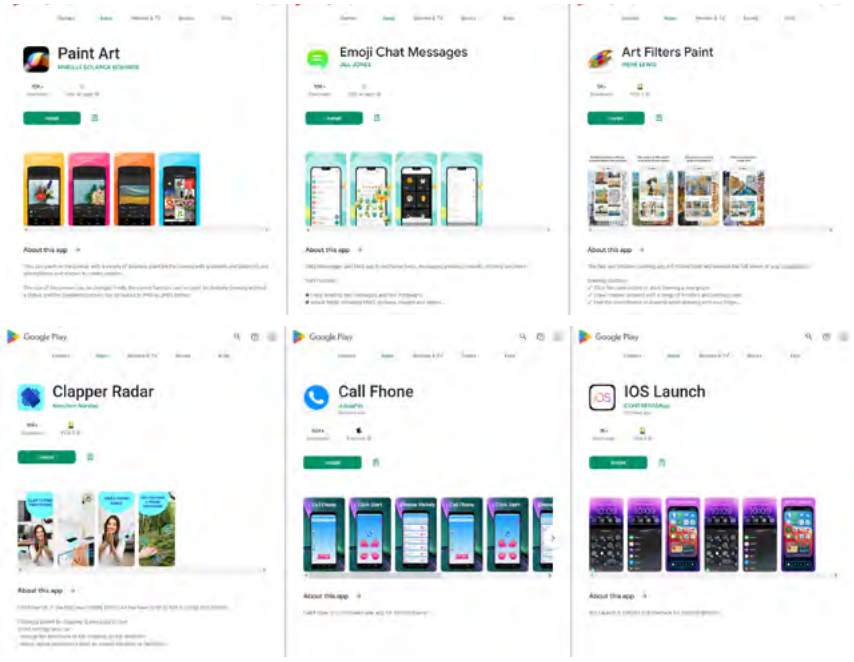
Среди найденных подделок были и очередные троянские приложения, якобы позволяющие зарабатывать на различных инвестициях в криптовалюту и фондовый рынок, а также в торговлю нефтью и газом. Они распространялись под видом всевозможных инструментов, таких как справочники и непосредственно приложения для торговли, и предназначались для пользователей из ряда стран, включая Россию и Казахстан. Эти подделки загружали мошеннические сайты, вводя потенциальных жертв в заблуждение.

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

Угрозы в Google Play



Помимо них, специалисты «Доктор Веб» выявили в каталоге Google Play троянские приложения, подписывающие жертв на платные услуги. Они были внесены в вирусную базу Dr.Web как Android.Joker.1917, Android.Joker.1920 и Android.Joker.1921, а также Android.Subscription.13, Android.Subscription.14 и Android.Subscription.15. Первые три скрывались в программах Paint Art, Emoji Chat Messages и Art Filters Paint. Остальные — в приложениях Call Fhone, IOS Launch и Clapper Radar.



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