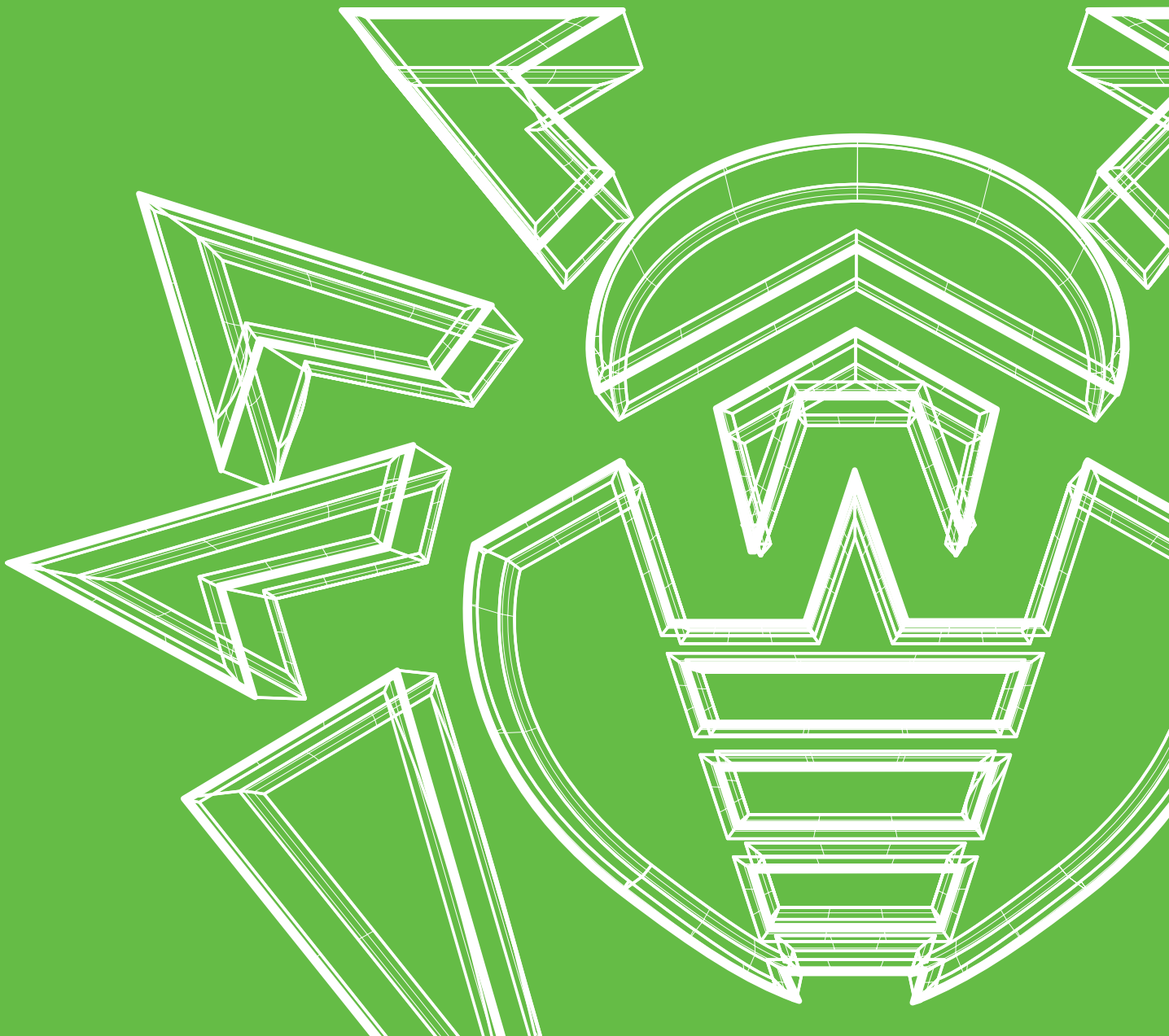
«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 2022 года



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

31 октября 2022 года

Согласно данным статистики детектирований антивируса Dr.Web для Android, в сентябре несколько снизилась активность троянских программ, демонстрирующих рекламу. В то же время на Android-устройствах чаще обнаруживались приложения со встроенными нежелательными рекламными модулями.

Злоумышленники вновь широко применяли специализированные утилиты, позволяющие запускать ПО без его установки. Кроме того, пользователи продолжили сталкиваться с различными шпионскими приложениями.

Троянская программа Android.Spy.4498, которая похищает информацию из уведомлений от других приложений, обнаруживалась на Android-устройствах на 32,72% реже по сравнению с августом. В прошлом месяце на ее долю пришлось чуть более четверти всех детектирований вредоносных приложений.

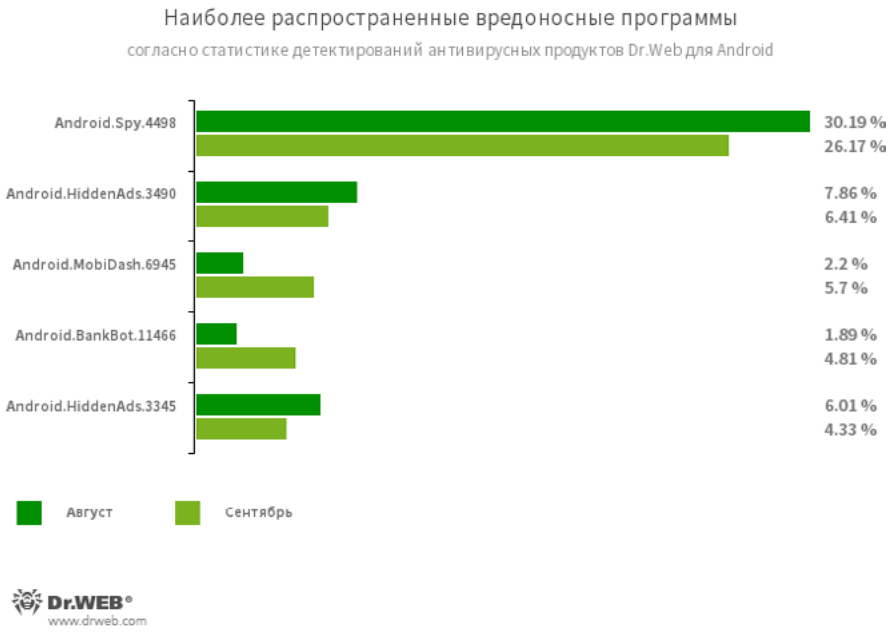
В течение сентября специалисты компании «Доктор Веб» выявили в каталоге Google Play очередные угрозы. Среди них — программы-подделки, применяемые в различных мошеннических схемах, а также рекламное ПО.

ГЛАВНЫЕ ТЕНДЕНЦИИ СЕНТЯБРЯ

- Снижение активности троянской программы Android.Spy.4498
- Снижение активности рекламных троянов
- Увеличение числа детектирований приложений, содержащих нежелательные рекламные модули
- Появление очередных угроз в каталоге Google Play

«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 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.3490
- Android.HiddenAds.3345

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.BankBot.11466

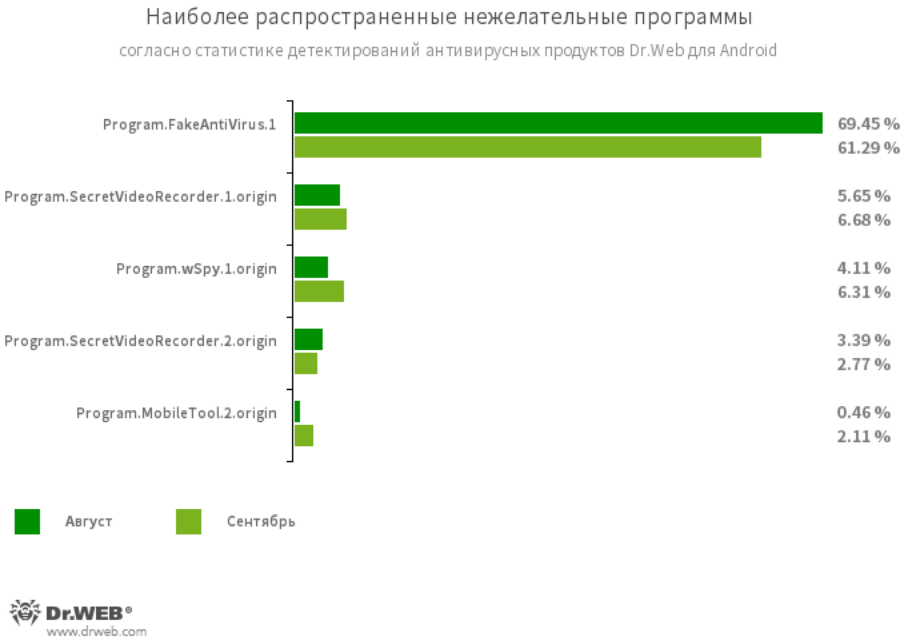
Детектирование вредоносных приложений, защищенных программным упаковщиком ApkProtector. Среди них встречаются банковские трояны, шпионское, а также другое вредоносное ПО.

- Android.MobiDash.6945

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

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

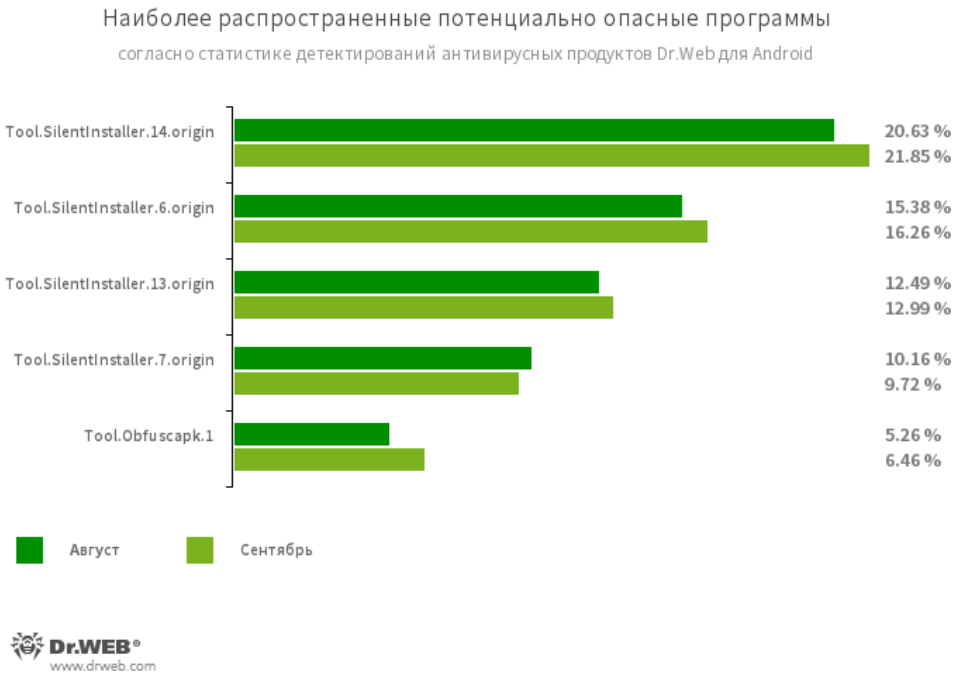
Детектирование различных версий приложения, предназначенного для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Эта программа может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает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

- Program.wSpy.1.origin
- Program.MobileTool.2.origin

Приложения, которые позволяют следить за владельцами Android-устройств и могут использоваться для кибершпионажа. В зависимости от версии и модификации они способны выполнять различные действия. Например, контролировать местоположение устройств, собирать данные об СМС-переписке и беседах в социальных сетях, копировать документы, фотографии и видео, выполнять прослушивание телефонных звонков и окружения и т. п.

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

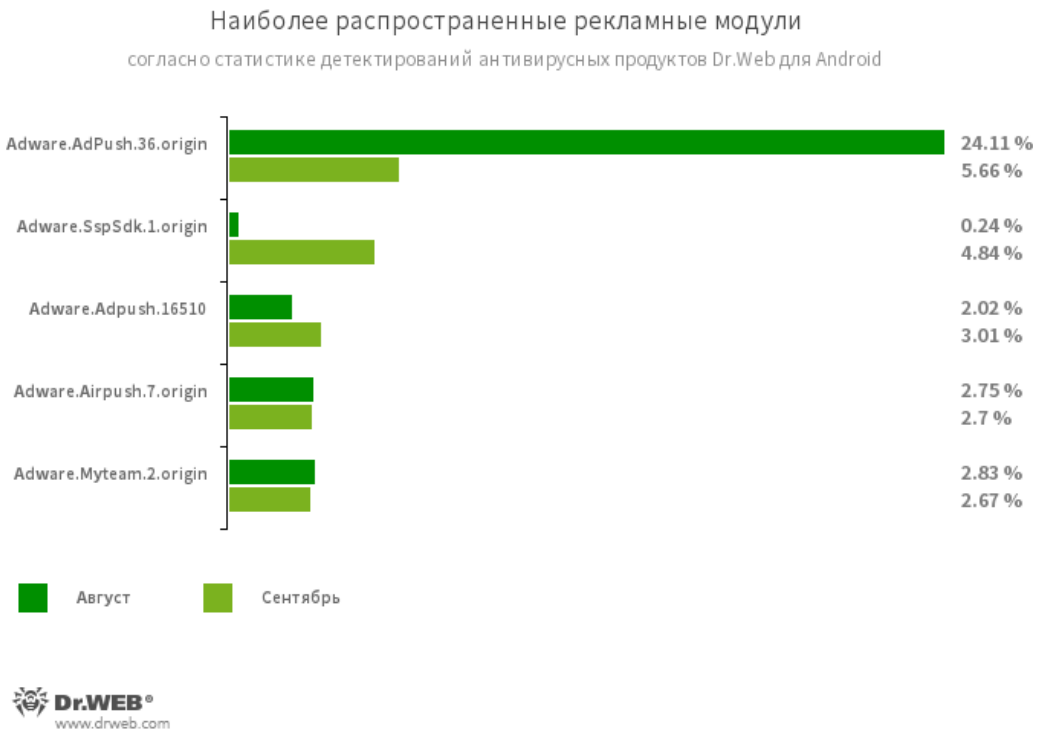
Потенциально опасные программные платформы, которые позволяют приложениям запускать apk-файлы без их установки. Они создают виртуальную среду исполнения, которая не затрагивает основную операционную систему.

- Tool.Obfuscapk.1

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 сентябре 2022 года

По данным антивирусных продуктов Dr.Web для Android



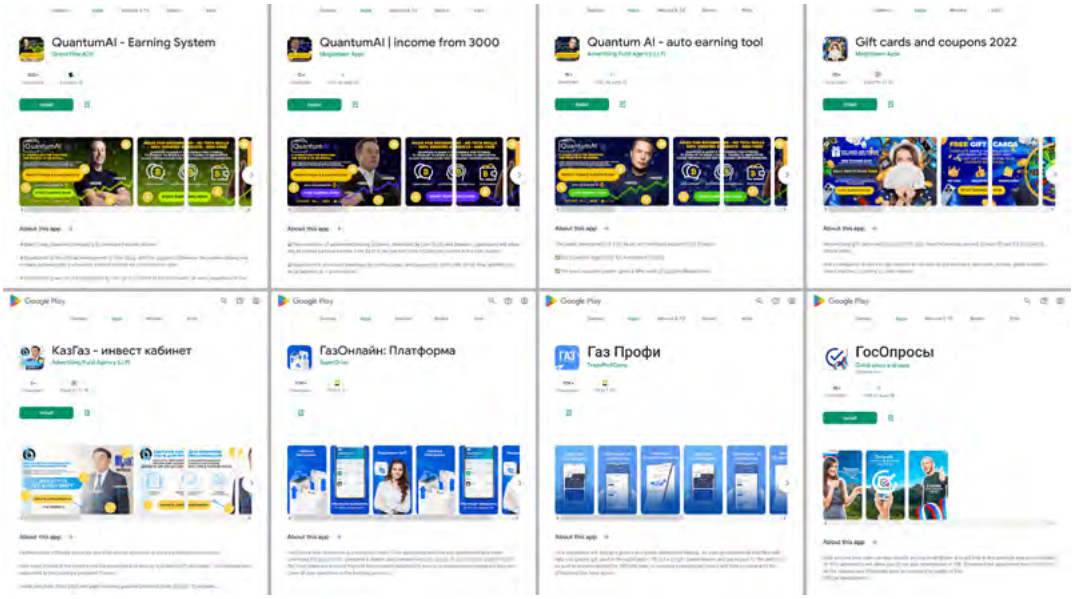
Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах. В зависимости от семейства и модификации они могут демонстрировать рекламу в полноэкранном режиме, блокируя окна других приложений, выводить различные уведомления, создавать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

- Adware.AdPush.36.origin
- Adware.Adpush.16510
- Adware.SspSdk.1.origin
- Adware.Airpush.7.origin
- Adware.Myteam.2.origin

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

Угрозы в Google Play

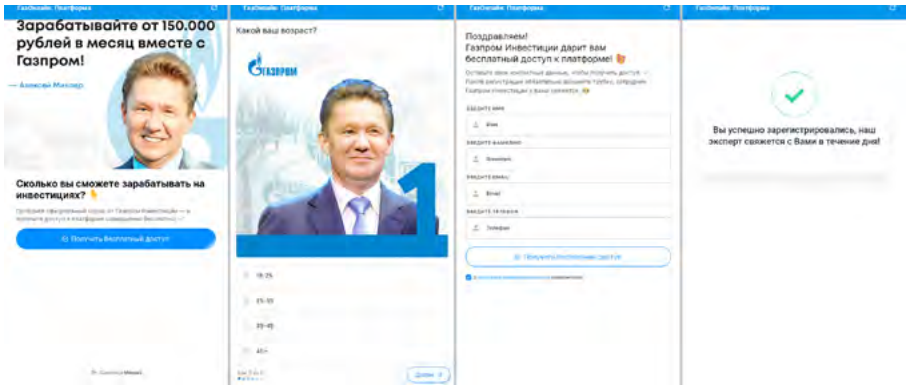
В сентябре в каталоге Google Play были выявлены новые вредоносные программы-подделки, функциональность которых не соответствовала заявленной. Злоумышленники реализовывали через них различные мошеннические схемы и атаковали с их помощью пользователей из разных стран. Так, троянские приложения Android.FakeApp.1005, Android.FakeApp.1007, Android.FakeApp.1011 и Android.FakeApp.1012 распространялись под видом программ, при помощи которых пользователи якобы могли повысить финансовую грамотность, инвестировать в нефтегазовые проекты, получить доступ к автоматизированным торговым системам, а также сервисам онлайн-заработка. Среди них были приложения под названиями QuantumAI | income from 3000, QuantumAI – Earning System, Quantum AI – auto earning tool, «КазГаз – инвест кабинет», «ГосОпросы», «ГазОнлайн: Платформа», а также «Газ Профи» и Gift cards and coupons 2022.

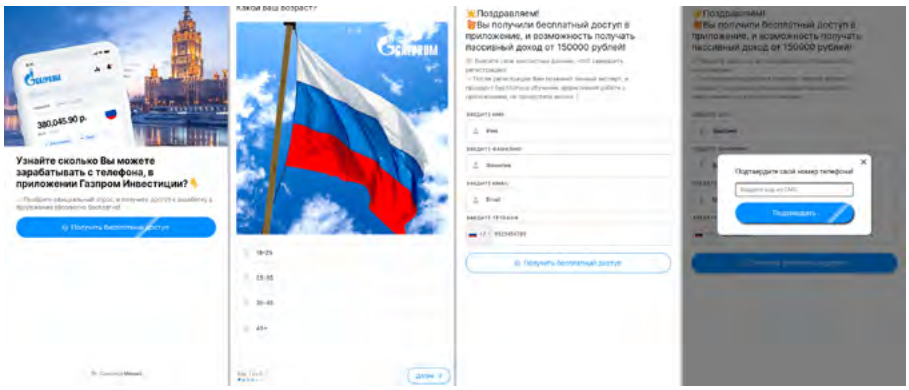


Одни из них были ориентированы на российских пользователей, другие — на русскоговорящих пользователей Казахстана и стран Европейского союза. Трояны загружали мошеннические сайты, на которых потенциальным жертвам предлагалось создать учетную запись для «доступа» к тому или иному сервису. Для этого пользователи должны были указать свои персональные данные: имя, фамилию, адрес электронной почты и номер мобильного телефона. В некоторых случаях от них также требовалось указать одноразовый код, который направлялся им в СМС. После «регистрации» они либо перенаправлялись на другой сомнительный сайт, либо видели сообщение о том, что операция успешно выполнена, и с ними вскоре свяжется «менеджер» или «эксперт». При этом предоставляемая ими информация передавалась неизвестным лицам, которые в дальнейшем могли использовать ее по своему усмотрению. В том числе — для организации фишинг-атак, либо для продажи рекламным агентствам или на черном рынке.

Угрозы в Google Play

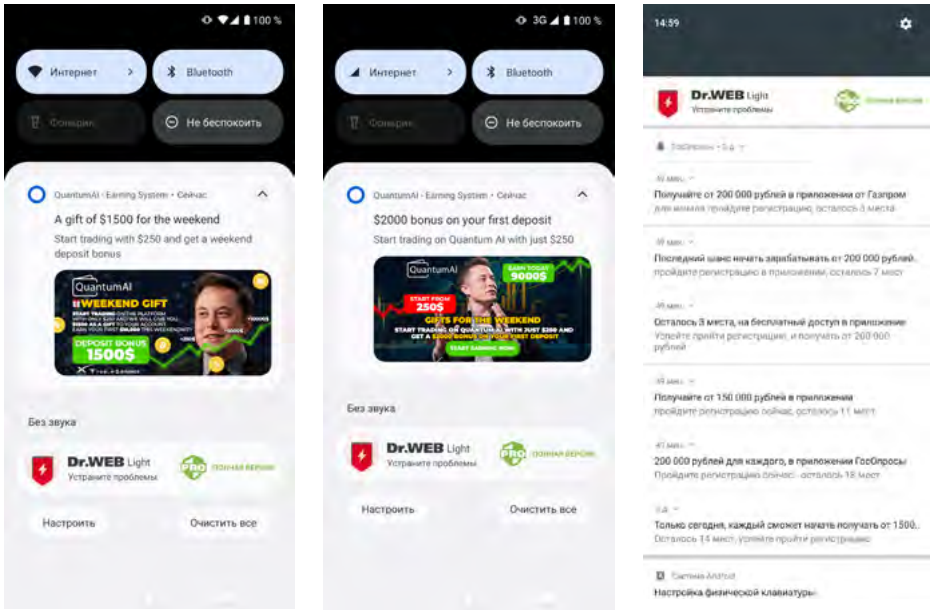
Примеры функционирования таких поддельных приложений:





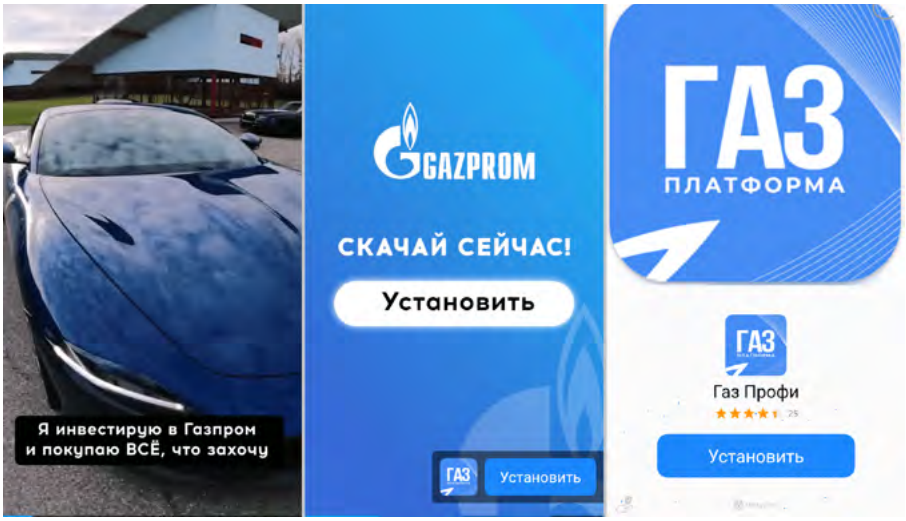
При этом для привлечения внимания пользователей некоторые из этих троянов периодически демонстрировали уведомления с ложными сообщениями. Например, с обещаниями крупного заработка, а также бонусов и подарков клиентам, либо с предупреждениями о якобы ограниченном числе оставшихся для регистрации мест.

Угрозы в Google Play



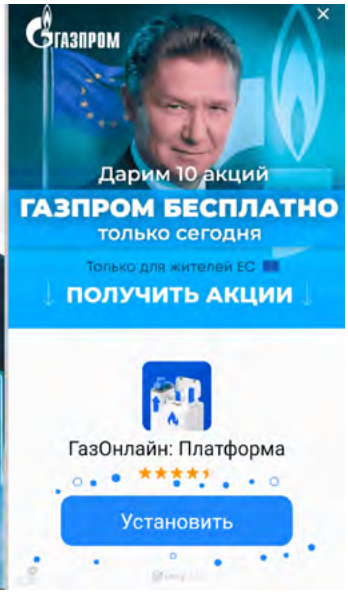
Для охвата большей аудитории киберпреступники рекламировали этих троянов в сторонних приложениях через встроенные в них рекламные системы. При этом реклама в виде полноэкранных баннеров и видеороликов в ряде случаев могла быть таргетированной. Например, нацеленной на русскоговорящих европейских пользователей, которым предлагалось установить приложение, которое якобы позволит бесплатно получить акции крупной российской нефтегазовой компании.

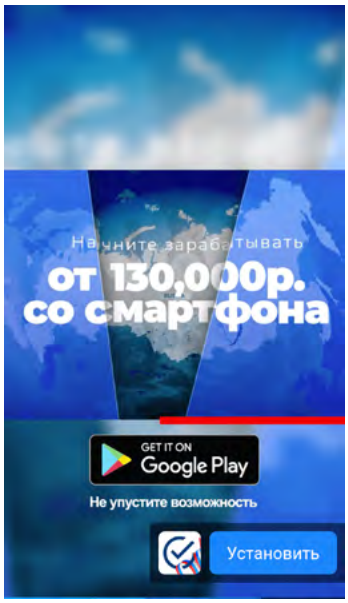
Примеры рекламы, с помощью которой распространялись поддельные программы:

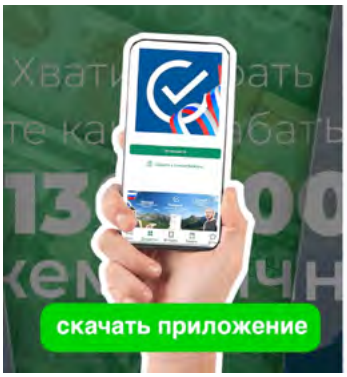


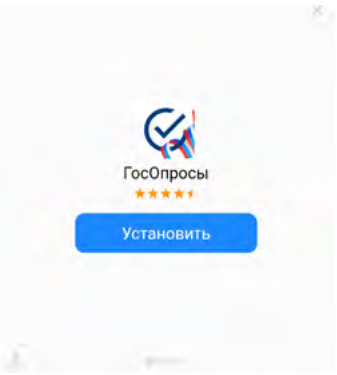
«Доктор Веб»: обзор вирусной активности для мобильных устройств в сентябре 2022 года

Угрозы в Google Play





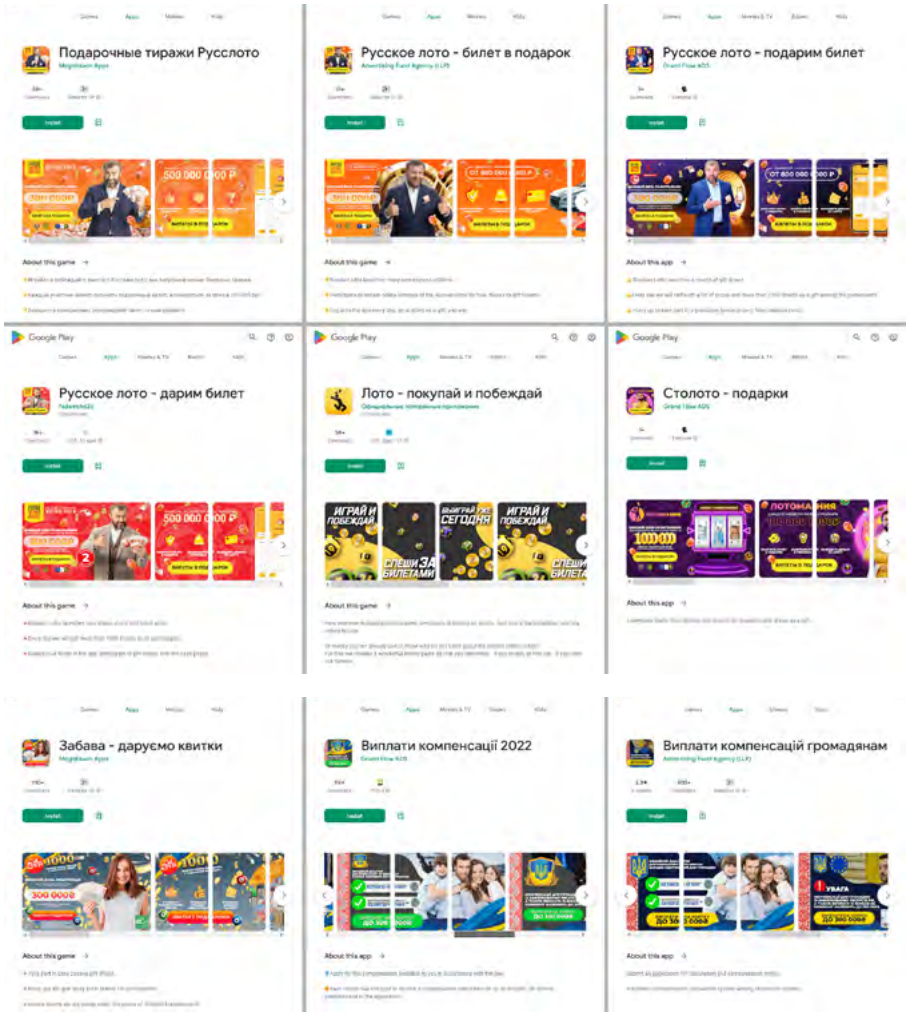




Троянские программы Android.FakeApp.1006, Android.FakeApp.1008, Android.FakeApp.1009, Android.FakeApp.1010, Android.FakeApp.1019, а также некоторые модификации Android.FakeApp.1007 злоумышленники распространяли среди российских и украинских владельцев Android-устройств. С их помощью пользователи якобы могли стать обладателями бесплатных лотерейных билетов и принять участие в розыгрыше призов, либо найти информацию о государственных пособиях и выплатах и оформить их получение.

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

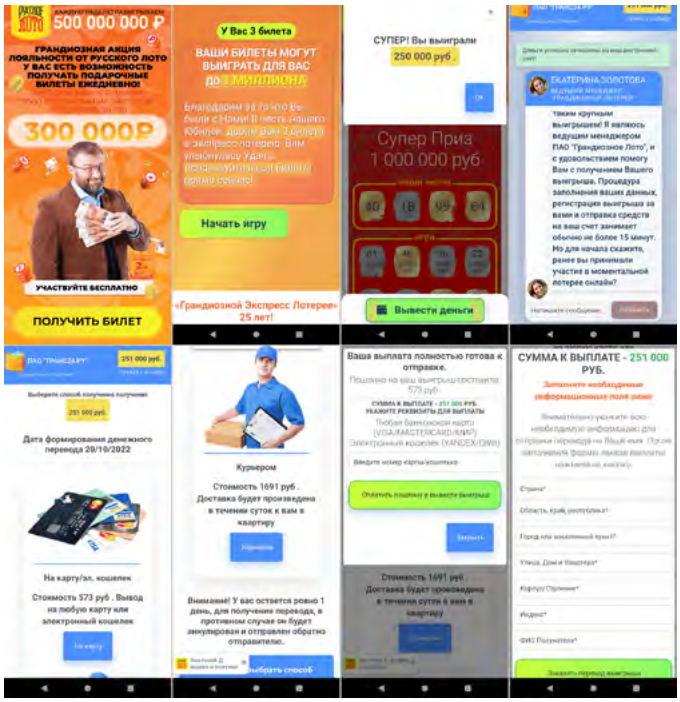
Угрозы в Google Play

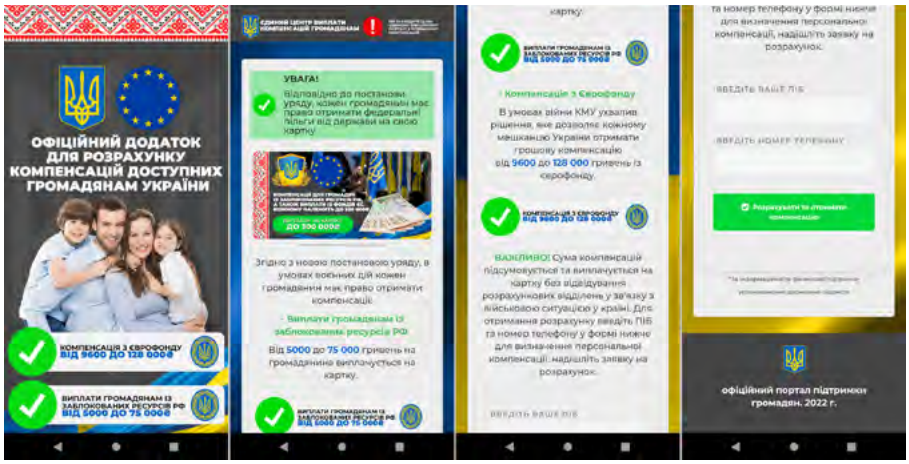


На самом деле трояны загружали мошеннические сайты, содержащие ложную информацию. На них имитировался как розыгрыш лотерей, так и процесс поиска и оформления пособий. Для «получения» выигрышей и государственных выплат потенциальные жертвы мошенников должны были указать свои персональные данные. Кроме того, от них требовалось заплатить комиссию или пошлину за «перевод» средств, либо за «доставку» денег курьером. Предоставленная пользователями информация (в том числе данные банковской карты) и оплата попадали в руки злоумышленников, в то время как сами жертвы обмана не получали никаких обещанных выплат или призов.

Угрозы в Google Play

Примеры работы данных троянских приложений:

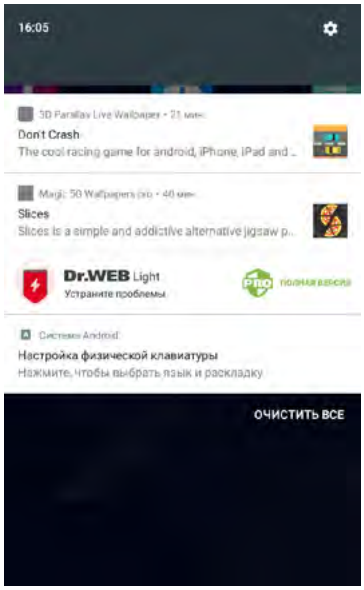




Вместе с тем наши специалисты выявили новые нежелательные рекламные модули, которые по классификации компании «Доктор Веб» получили имена Adware.AdNoty.1 и Adware.AdNoty.2. Эти модули могут быть встроены в различное ПО. Периодически они демонстрируют уведомления с рекламой, например — игр и программ. При нажатии на такие уведомления в браузере Android-устройств загружаются веб-сайты в соответствии со списком рекламных ссылок, заданном в конфигурации модулей.

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

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 сентябре 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