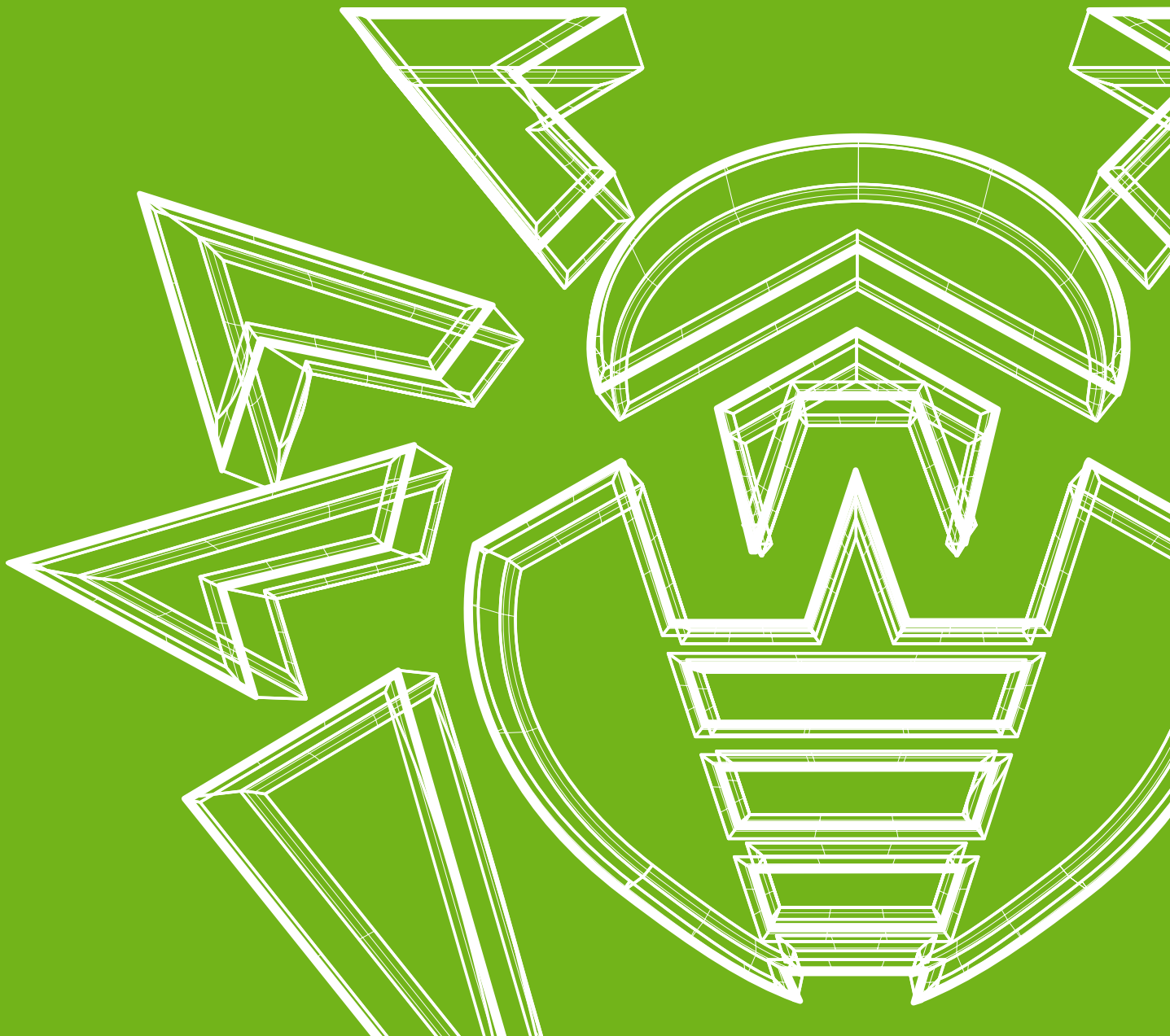
Dr.WEB®
с 1992 года

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



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

28 января 2022 года

Согласно статистике детектирований антивирусных продуктов Dr.Web для Android, в декабре наиболее активными Android-угрозами вновь стали различные рекламные трояны. Кроме того, на защищаемых Android-устройствах часто обнаруживались вредоносные приложения, загружающие другие программы.

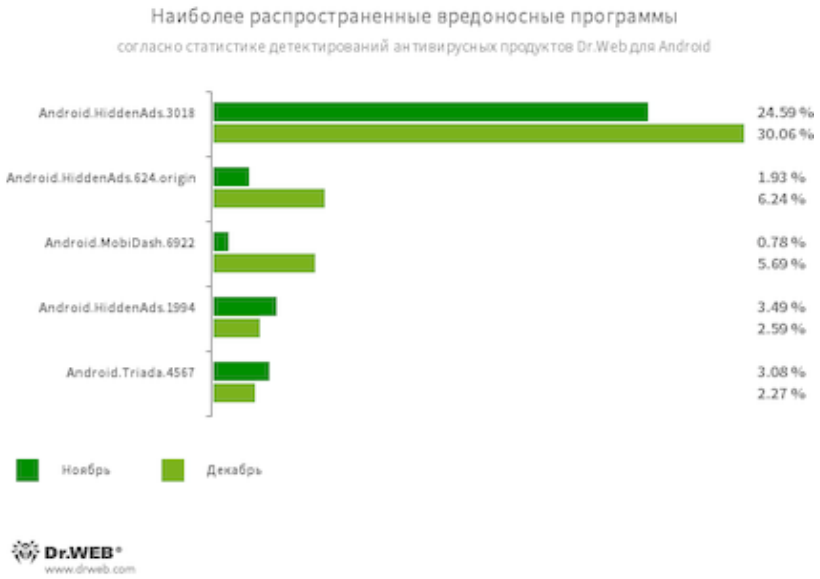
В каталоге Google Play были выявлены очередные угрозы. Среди них — всевозможные вредоносные программы-подделки семейства Android.FakeApp, применяемые в различных мошеннических схемах, трояны семейства Android.Joker, подписывающие пользователей на платные мобильные услуги, и другие вредоносные приложения.

ГЛАВНЫЕ ТЕНДЕНЦИИ ДЕКАБРЯ

- Рекламные трояны по-прежнему занимают лидирующие позиции среди угроз, выявляемых на Android-устройствах
- Появление новых троянов в каталоге Google Play

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

По данным антивирусных продуктов Dr.Web для Android



Android.HiddenAds.3018

Android.HiddenAds.624.origin

Android.HiddenAds.1994

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.HiddenAds.3018 является новой версией трояна Android.HiddenAds.1994.

Android.MobiDash.6922

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

Android.Triada.4567

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 декабре 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.SecretVideoRecorder.1.origin

Приложение, предназначенное для фоновой фото- и видеосъемки через встроенные камеры Android-устройств. Оно может работать незаметно, позволяя отключить уведомления о записи, а также изменять значок и описание приложения на фальшивые. Такая функциональность делает данную программу потенциально опасной.

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 телефонных разговоров.

Program.Gemius.1.origin

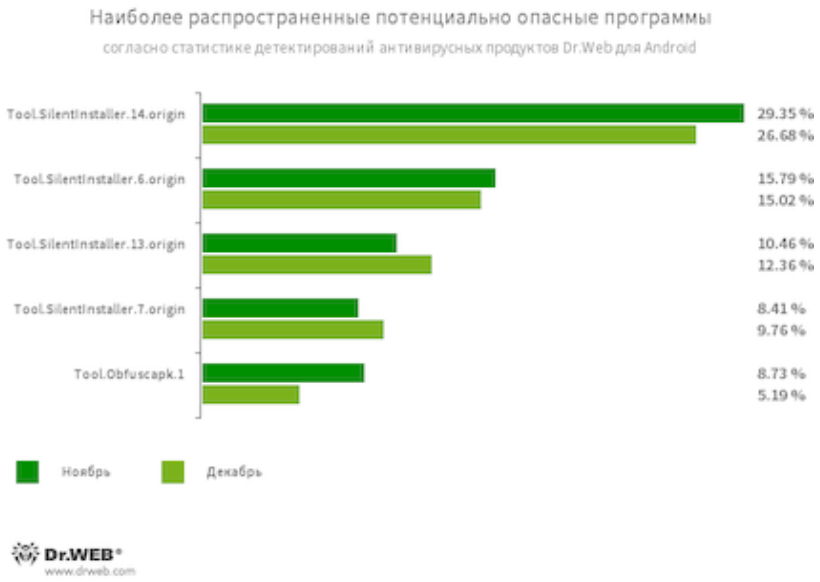
Программа, собирающая информацию о мобильных Android-устройствах и о том, как они используются. Вместе с техническими данными она собирает конфиденциальные сведения — информацию о местоположении устройства, сохраненных в браузере закладках, истории посещения сайтов, а также о вводимых интернет-адресах.

Program.WapSniff.1.origin

Программа для перехвата сообщений в мессенджере WhatsApp.

«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2021 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 декабре 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.16510

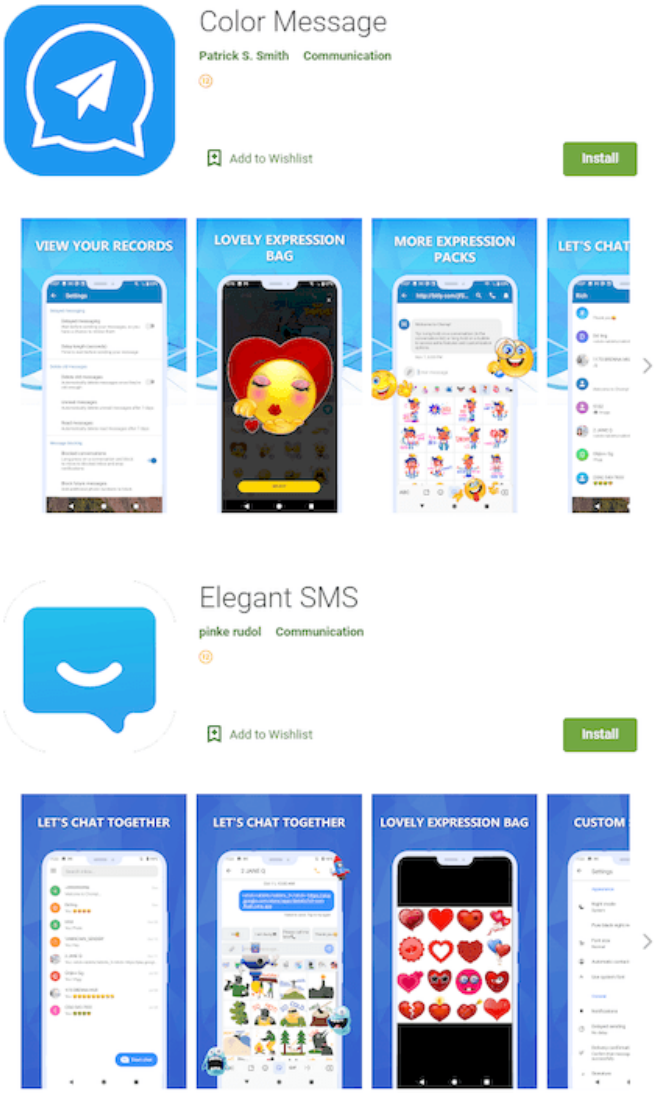
Adware.Adpush.6547

Adware.Myteam.2.origin

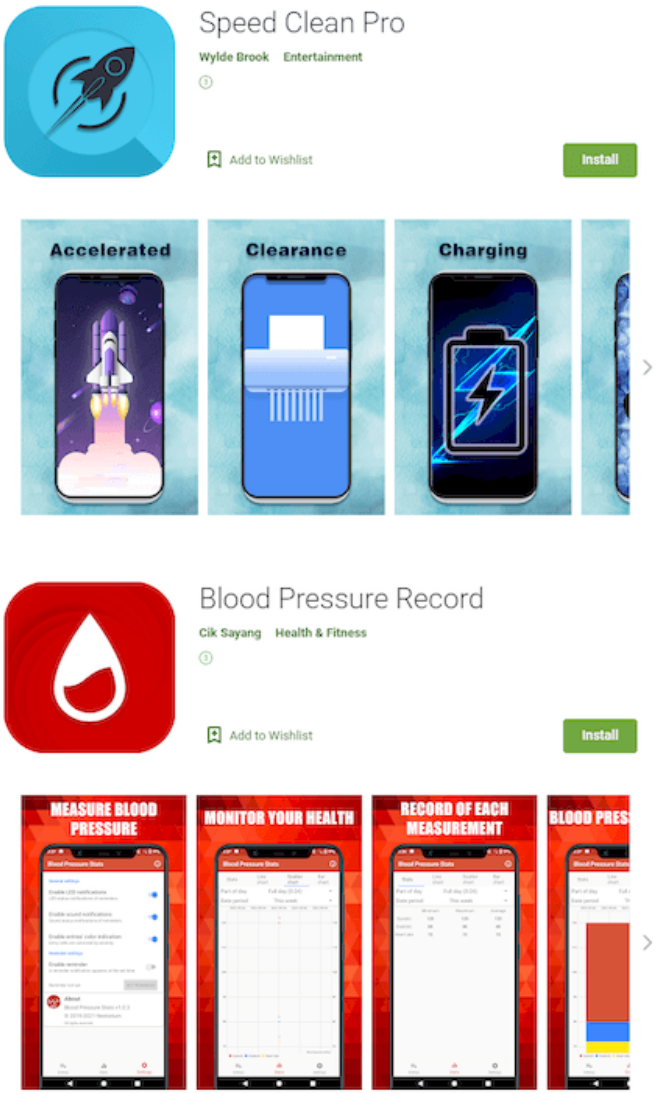
«Доктор Веб»: обзор вирусной активности для мобильных устройств в декабре 2021 года

Угрозы в Google Play

В декабре 2021 года в каталоге Google Play были обнаружены новые вредоносные приложения семейства Android.Joker, которые загружают и исполняют произвольный код и подписывают пользователей на платные мобильные сервисы. Например, трояны Android.Joker.1097 и Android.Joker.1126 скрывались в мессенджерах Color Message и Elegant SMS, а Android.Joker.1129 распространялся под видом утилиты Speed Clean Pro для оптимизации работы Android-устройств. Трояна Android.Joker.1157 злоумышленники выдавали за программу PDF Camera Scanner для создания PDF-документов, а Android.Joker.1160 — за приложение Blood Pressure Record для контроля кровяного давления.

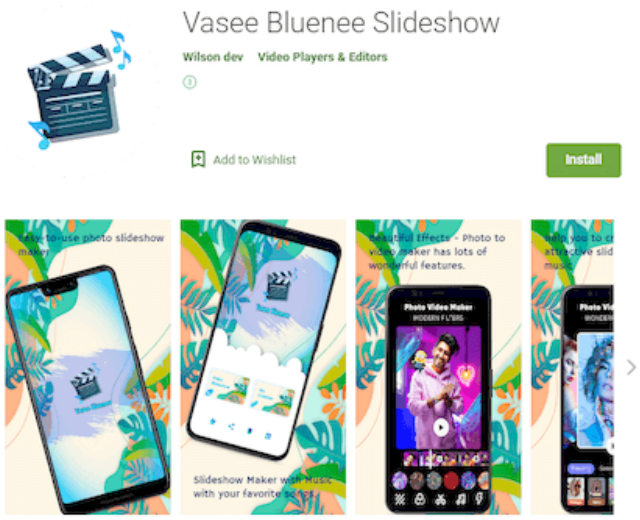


Статистика

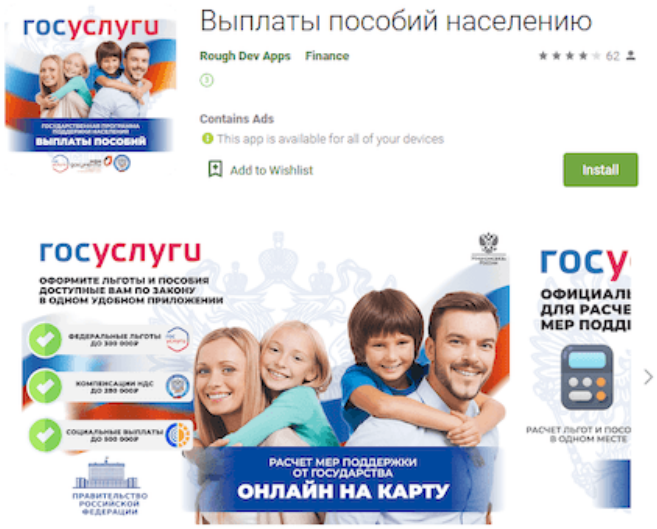


Наши вирусные аналитики также обнаружили очередного трояна из семейства Android.PWS.Facebook. Такие вредоносные приложения крадут логины, пароли и другую информацию, необходимую для взлома учетных записей Facebook. Новый представитель этого семейства распространялся под видом приложения Vasee Bluenee Slideshow для создания слайд-шоу и видеороликов. Его компоненты были добавлены в вирусную базу Dr.Web как Android.PWS.Facebook.101 и Android.PWS.Facebook.102.

Статистика



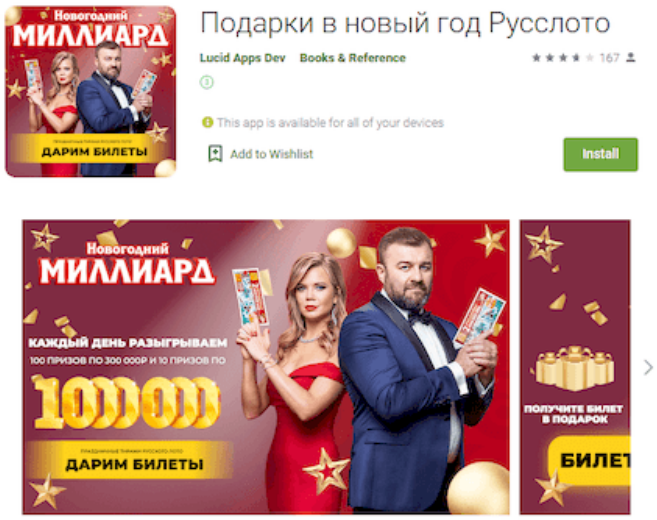
Кроме того, в Google Play были найдены программы-подделки, которые использовались в различных мошеннических схемах. Некоторые из них, такие как Android.FakeApp.721 («Выплаты пособий населению») и Android.FakeApp.724 («ФРП РУ Выплаты»), злоумышленники вновь распространяли под видом приложений с информацией о мерах социальной поддержки в России. С их помощью пользователи также якобы могли получить выплаты и компенсации. Однако трояны лишь загружали мошеннические сайты, где жертвам предлагалось указать персональные данные и оплатить «комиссию» или «пошлину» для «перевода» денег на их банковский счет.



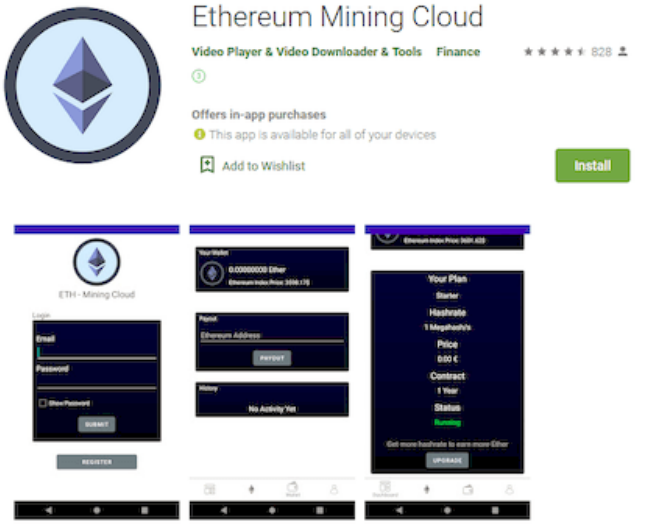
Статистика

Аналогичная функциональность была и у троянов, получивших имена Android.FakeApp.722 и Android.FakeApp.723. Вирусописатели выдавали их за программы для получения бесплатных лотерейных билетов. Эти вредоносные программы загружали сайты, на которых для «получения» билетов и выигрышей пользователи должны были оплатить «комиссию».

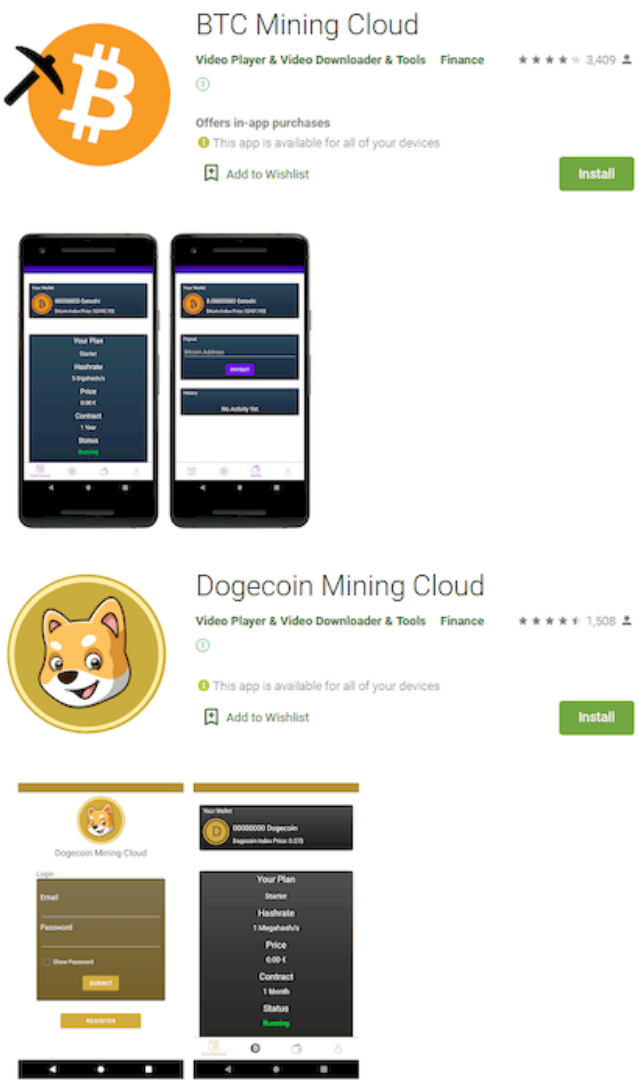
Статистика



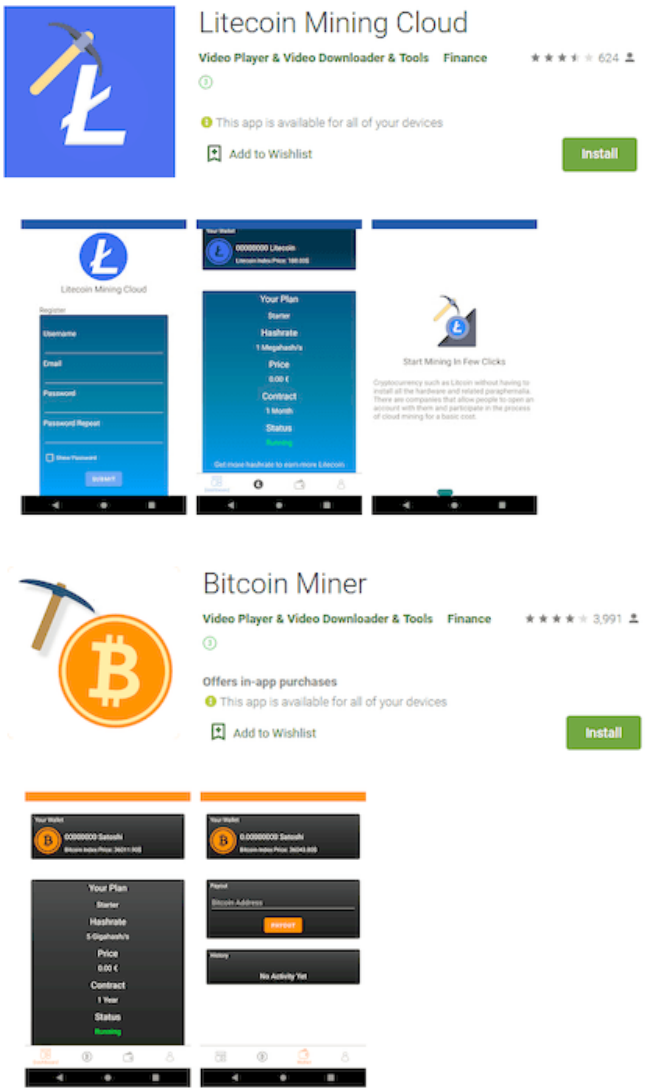
А трояны Android.FakeApp.727 и Android.FakeApp.729 распространялись под видом приложений для майнинга криптовалют. Они скрывались в таких программах как Dogecoin Mining Cloud, Litecoin Mining Cloud, Bitcoin Miner, Ethereum Mining Cloud и BTC Mining Cloud. Установившим их пользователям предлагалось получать криптовалюту при помощи облачного сервиса, а для увеличения скорости добычи — оплатить премиальные тарифные планы.



Статистика


BTC Mining Cloud
Video Player & Video Downloader & Tools
Finance
3,409
Offers in-app purchases
This app is available for all of your devices
Add to Wishlist
Install
Dogecoin Mining Cloud
Video Player & Video Downloader & Tools
Finance
1,508
This app is available for all of your devices
Add to Wishlist
Install
Dogecoin Mining Cloud
Email
Password
Your Plan
Hashrate
Price
Contract
Status

Статистика



Это не первые троянские приложения такого типа. Например, ещё в августе 2021 года вирусные аналитики компании «Доктор Веб» обнаружили аналогичную вредоносную программу с именем Multimine - BTC Cloud Mining. Она была добавлена в вирусную базу Dr.Web как Android.FakeApp.336.

Статистика

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 декабре 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 Ямского поля улица, д.2, к.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