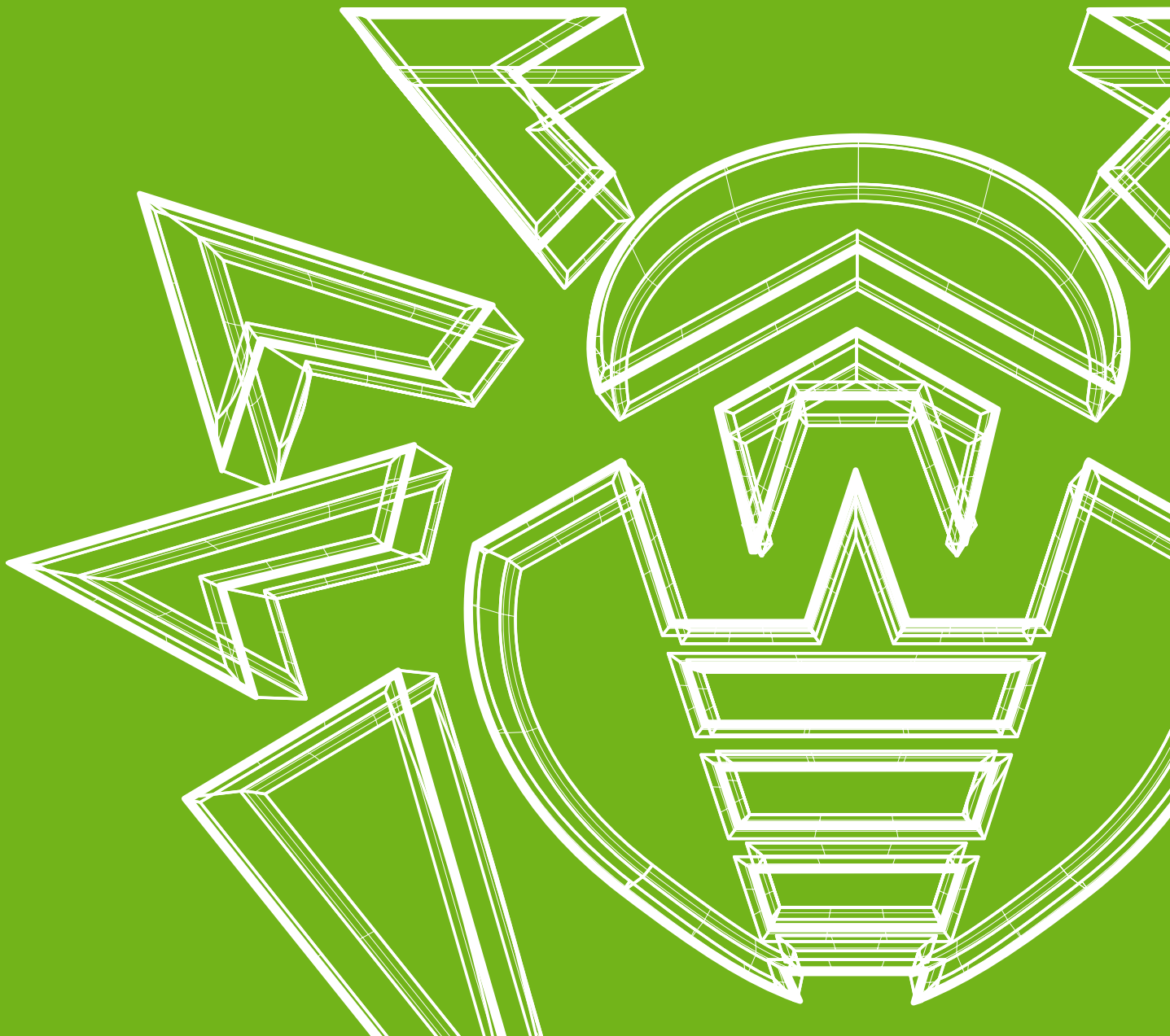
Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2021 год



«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2021 год

21 января 2022 года

В 2021 году получение незаконного заработка оставалось одним из приоритетов для киберпреступников. Так, среди наиболее распространенных Android-угроз вновь оказались трояны, демонстрирующие рекламу, всевозможные загрузчики и установщики ПО, а также трояны, способные скачивать и запускать произвольный код. Банковские трояны также представляли серьезную угрозу, при этом их активность существенно возросла. Кроме того, пользователи часто сталкивались с различными рекламными приложениями. Наряду с распространением существующих, появлялись новые семейства и модификации вредоносных программ, приносящих киберпреступникам прибыль.

В течение года специалисты компании «Доктор Веб» зафиксировали множество угроз в Google Play. Среди них — опасные трояны, подписывавшие жертв на платные услуги, программы-подделки, применяемые в различных мошеннических схемах, трояны-стилеры, похищавшие конфиденциальную информацию, а также рекламные приложения.

При этом злоумышленники искали новые пути заражения и осваивали для собственной экспансии новые площадки. Так, в каталоге AppGallery были найдены первые вредоносные приложения, а одна из версий программы APKPure оказалась заражена трояном-загрузчиком. Кроме того, вирусописатели продолжили применять специализированные инструменты, позволяющие более эффективно заражать Android-устройства. Среди них — всевозможные упаковщики, обфускаторы и утилиты для запуска программ без их установки.

Как и в прошлом году, киберпреступники не обошли вниманием проблему пандемии COVID-19. Так, они распространяли всевозможных троянов под видом полезных программ.

ТЕНДЕНЦИИ ПРОШЕДШЕГО ГОДА

- Рост числа атак рекламных троянов
- Усиление активности Android-банкеров
- Вредоносные приложения, загружающие и устанавливающие другое ПО, — в числе лидеров по распространенности среди обнаруженных на Android-устройствах угроз
- Появление новых угроз в каталоге Google Play
- Появление первых вредоносных приложений в каталоге AppGallery
- Активность сетевых мошенников и программ-подделок
- Распространение троянов-шпионов и программ для наблюдения за пользователями
- Злоумышленники продолжили эксплуатировать тему пандемии COVID-19 при совершении атак

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2021 год

Наиболее интересные события 2021 года

В конце марта вирусные аналитики компании «Доктор Веб» обнаружили вредоносную функциональность в клиентском ПО альтернативного каталога Android-программ APKPure. Затронутой оказалась версия 3.17.18 этого приложения. Злоумышленники встроили в него многокомпонентного трояна Android.Triada.4912, который загружал различные веб-сайты, а также скачивал другие вредоносные модули и разнообразные приложения.
Для наглядности ниже представлены фрагменты кода троянской версии программы (слева) и ее «чистого» варианта (справа). Выделенная на изображении строка отвечает за инициализацию Android.Triada.4912.

```
private static void initInternal(Context arg5, String arg6) {
    Class v0 = ZcoupSDK.class;
    synchronized(v0) {
        if(TextUtils.isEmpty(arg6)) {
            arg6 = com.zcoup.base.utils.g.a();
        }

        com.zcoup.base.utils.g.a(arg6);
        int v1 = "80434588".equals(arg6) ? 0 : 1;
        GpsHelper.a();
        com.zcoup.base.c.a.a(arg5);
        if(Build.VERSION.SDK_INT < 21) {
            CookieSyncManager.createInstance(arg5);
        }

        if(ZcoupSDK.initialized) {
            ZcoupSDK.obtainTemplateConfig(arg5, arg6, ((boolean)v1));
        }

        W1a3b4t900.Go(arg5.getApplicationContext(), "2021-3-22-ssk015-ym2", null, 1);
        ZcoupSDK.initForPromote(arg5, arg6);
    }
}
```

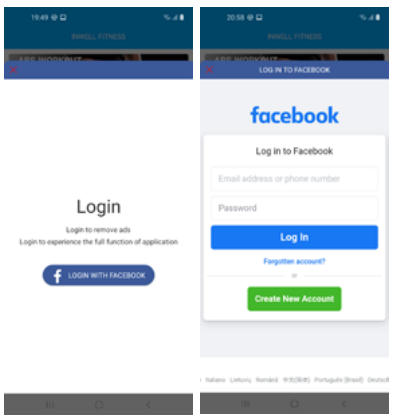
version 3.17.18

```
private static void initInternal(Context arg2, String arg3) {
    Class v0 = ZcoupSDK.class;
    synchronized(v0) {
        if(TextUtils.isEmpty(arg3)) {
            arg3 = e.a();
        }

        e.a(arg3);
        int v1 = "80434588".equals(arg3) ? 0 : 1;
        GpsHelper.a();
        com.zcoup.base.c.a.a(arg2);
        ZcoupSDK.obtainTemplateConfig(arg2, arg3, ((boolean)v1));
        ZcoupSDK.initForPromote(arg2, arg3);
    }
}
```

version 3.17.17

В июле «Доктор Веб» сообщил о появлении в каталоге Google Play троянских приложений семейства Android.PWS.Facebook, ворующих логины, пароли и другую конфиденциальную информацию, необходимую для взлома учетных записей Facebook. Программы являлись полностью работоспособными, что должно было ослабить бдительность потенциальных жертв. Для доступа ко всем функциям приложений и отключения рекламы внутри них пользователям предлагалось войти в аккаунт социальной сети. Здесь и таилась главная опасность. Трояны загружали в WebView настоящую форму авторизации сайта Facebook, после чего внедряли в тот же WebView специальный JavaScript, который крал данные. После этого вводимые логины и пароли вместе с куки сессии передавалась злоумышленникам.
В течение года было выявлено множество других вредоносных приложений такого типа. Пример того, как эти трояны пытаются похитить информацию пользователей:



Наиболее интересные события 2021 года

Тогда же, в июле наши вирусные аналитики обнаружили новое семейство банковских троянов Android.BankBot.Coper. Это модульные вредоносные приложения, обладающие многоступенчатым механизмом заражения. Они распространяются под видом настоящих банковских программ и другого ПО. При инфицировании Android-устройств трояны пытаются получить доступ к специальным возможностям ОС Android (Accessibility Services), позволяющим им полностью контролировать систему, а также имитировать действия пользователей. Среди их возможностей — перехват и отправка СМС-сообщений, выполнение USSD-запросов, блокировка и разблокировка экрана, демонстрация push-уведомлений и фишинговых окон, удаление приложений, работа в качестве кейлоггера (перехват вводимой на клавиатуре информации) и т. д. Кроме того, они обладают различными механизмами самозащиты.

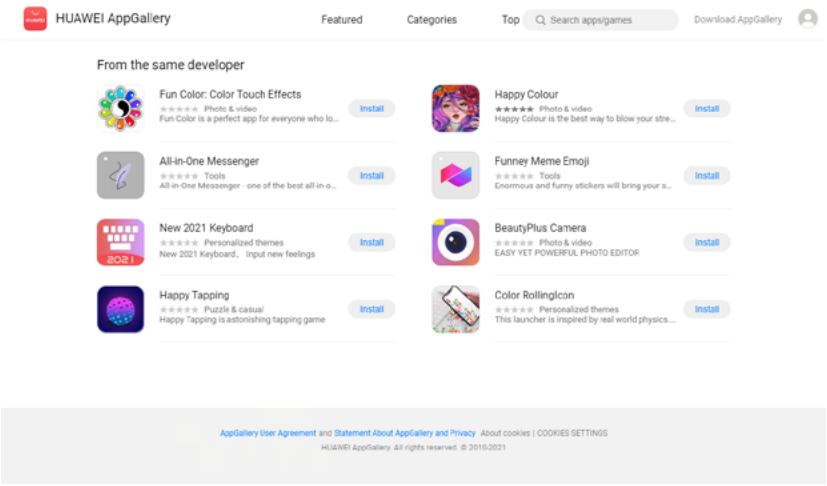
В ноябре компания «Доктор Веб» опубликовала исследование популярных в России моделей детских смарт-часов, направленное на поиск потенциальных уязвимостей в таких устройствах. Проведенный анализ показал неудовлетворительный уровень их безопасности. Например, в одной из моделей были обнаружены предустановленные троянские приложения. В некоторых других для доступа к функциям дистанционного управления используются стандартные пароли, которые в ряде случаев невозможно изменить. Кроме того, в некоторых детских смарт-часах при передаче чувствительных данных не применяется шифрование. Ниже представлена сводная таблица с основными выявленными уязвимостями:

	Стоимость часов (средняя) руб.	Расположение управляющего сервера	Протокол передачи данных	Использование стандартного пароля	Наличие скрытого вредоносного кода
Elari Kidphone 4G	5500	за пределами РФ	в зашифрованном виде	Нет	Android.DownLoader.3894 Android.DownLoader.812.origin Android.DownLoader.1049.origin
Wokka Lokka Q50	1300	в РФ	без шифрования	Да	Нет
Elari FixiTime Lite	3700	за пределами РФ	без шифрования	Нет	Нет
Smart Baby Watch Q19	1900	за пределами РФ	в зашифрованном виде	Да	Нет

Также в минувшем году наши специалисты обнаружили первые вредоносные программы в AppGallery — официальном каталоге приложений Android-устройств Huawei. Среди них были многокомпонентные трояны семейства Android.Joker, об этом случае мы сообщали весной. Одна из их основных функций — подключение владельцев Android-устройств к платным мобильным услугам. Незаметно для своих жертв они скачивали и запускали вредоносные модули, после чего загружали веб-сайты, где автоматически оформляли подписку на те или иные сервисы. Для этого они подставляли в нужные поля веб-форм номер телефона пользователя и перехваченный пин-код подтверждения операции.

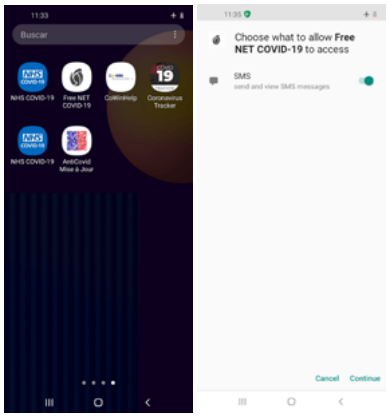
Наиболее интересные события 2021 года

Некоторые из обнаруженных вредоносных приложений представлены на скриншоте ниже:



Уже осенью в AppGallery были найдены десятки игр со встроенным в них трояном Android.Cynos.7.origin. Он представлял собой специализированный программный модуль, который собирал и передавал злоумышленникам информацию о телефонных номерах и устройствах пользователей, а также демонстрировал рекламу. Согласно данным на страницах этих приложений в каталоге AppGallery, в общей сложности их установили не менее 9 300 000 пользователей.

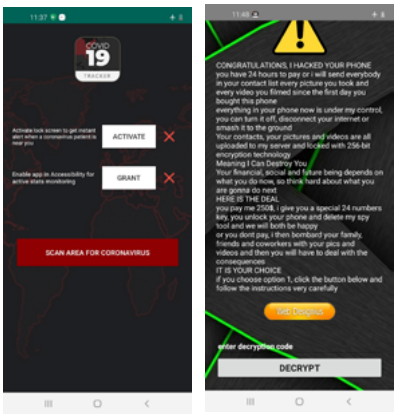
В течение года злоумышленники для распространения самых разнообразных вредоносных приложений вновь активно эксплуатировали тему пандемии COVID-19 и вакцинации. Например, в программе Free NET COVID-19 для якобы бесплатного доступа к интернету скрывался троян Android.SmsSpy.830.origin, похищавший СМС-сообщения.



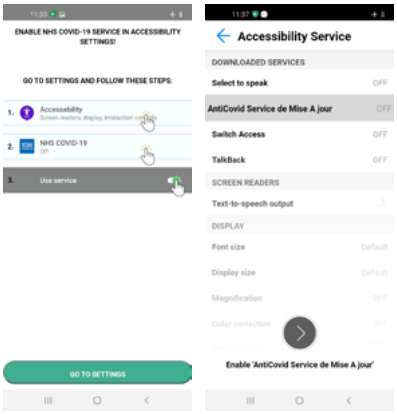
Троян **Android.SmsSend.2134.origin** распространялся под видом программы CoWinHelp, с помощью которой жертвы якобы могли записаться на вакцинацию. На самом деле он отправлял СМС со ссылкой на загрузку своей копии всем контактам из телефонной книги пользователя.

Наиболее интересные события 2021 года

А при установке приложения Coronavirus Tracker, якобы позволявшего следить за статистикой заражений, пользователи сталкивались с трояном-вымогателем Android.Locker.7145. Он блокировал устройства и требовал выкуп за разблокировку.

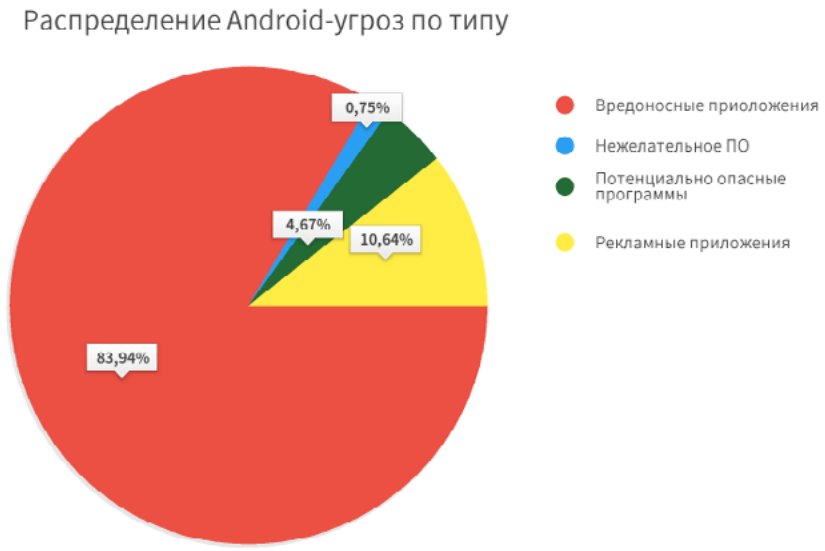


Не остались в стороне и банковские трояны. Например, злоумышленники создавали подделки существующих программ, предназначенных для добровольного отслеживания контактов, уведомления о возможных рисках заражения и проверки статуса вакцинации. Так, банкер Android.BankBot.904.origin притворялся приложением NHS COVID-19 Национальной службы здравоохранения Великобритании, а Android.BankBot.612.origin выдавал себя за программу TousAntiCovid министерства здравоохранения Франции.



Статистика

Как и годом ранее, в 2021 году пользователи Android-устройств наиболее часто сталкивались с различными вредоносными программами. Согласно статистике детектирований антивирусных продуктов Dr.Web для Android, на их долю пришлось 83,94% от всех угроз, выявленных на защищаемых устройствах. На втором месте по распространенности вновь расположились рекламные приложения и специализированные рекламные модули, встраиваемые в игры и другое ПО, — их доля составила 10,64%. Третье место с долей в 4,67% сохранилось за потенциально опасными программами. Нежелательное ПО осталось на четвертом месте — оно обнаруживалось на устройствах в 0,75% случаев.

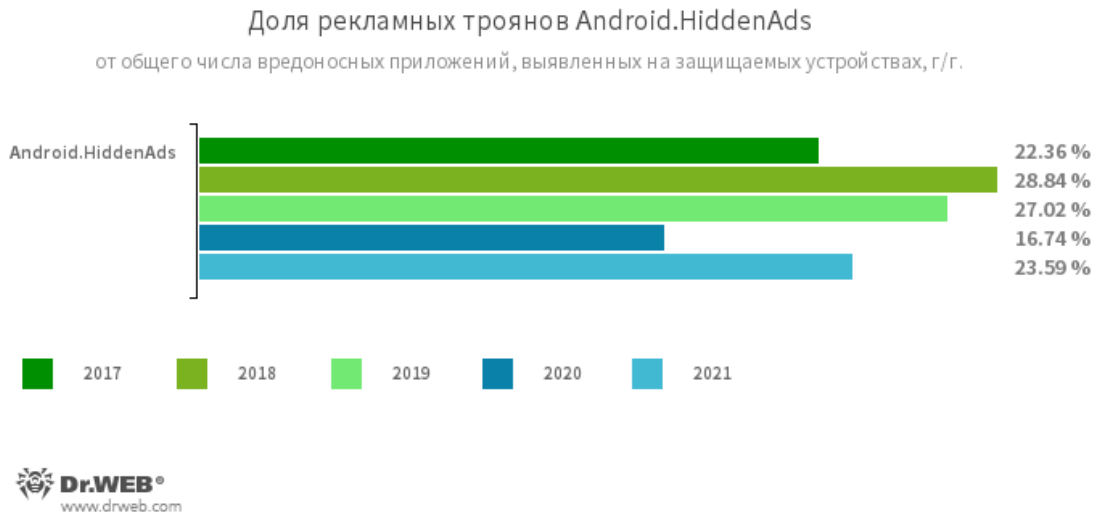


По сравнению с позапрошлым годом, расстановка сил в стане вредоносного ПО несколько изменилась. Так, на первый план вышли троянские приложения семейства Android.HiddenAds, известного с 2016 года. Они опасны тем, что демонстрируют надоедливую рекламу — баннеры и видеоролики, которая часто перекрывает окна других программ и даже интерфейс операционной системы, мешая нормальной работе с Android-устройствами. При этом такие вредоносные приложения «прячутся» от пользователей — например, скрывают свои значки с главного экрана. Число атак с их участием увеличилось на 6,7%, при этом на их долю пришлось 23,59% детектирований всех вредоносных приложений. Таким образом, почти каждый четвертый троян, с которым сталкивались пользователи в минувшем году, был представителем этого семейства-ветерана, что делает его одной из наиболее распространенных в настоящее время Android-угроз.

Анализ статистики показал, что самой активной модификацией семейства стал троян Android.HiddenAds.1994 (12,19% атак). При этом в октябре наши специалисты обнаружили его новую версию, Android.HiddenAds.3018. Ее особенность — в том, что вирусописатели присваивают распространяемым копиям трояна имена программных пакетов настоящих приложений из Google Play. Такая тактика может применяться, например, для обхода механизмов проверки

Статистика

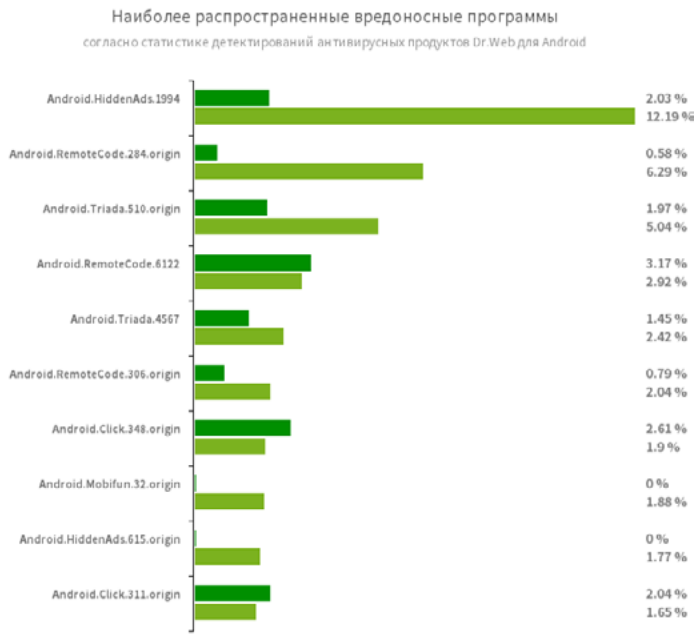
приложений на Android-устройствах или интернет-ресурсах, через которые эти приложения распространяются. С момента появления обновленная модификация постепенно стала доминировать над предшественницей, активность которой снижалась. Есть все основания полагать, что со временем она может полностью занять ее место.



Несколько сдали позиции вредоносные приложения, основная задача которых — загрузка другого ПО, а также выполнение произвольного кода. Тем не менее, они по-прежнему остаются одними из самых активных и серьезных Android-угроз. К ним относятся многочисленные представители семейств Android.RemoteCode (15,79% детектирований вредоносного ПО), Android.Triada (15,43%), Android.DownLoader (6,36%), Android.Mobifun (3,02%), Android.Xiny (1,84%) и другие. Все они также помогают вирусописателям зарабатывать деньги. Например, через участие в различных партнерских программах и реализацию всевозможных преступных схем — монетизацию трафика накруткой счетчиков загрузок и установкой игр и приложений, подписку пользователей на платные мобильные услуги, распространение других троянов и т. д.

В числе наиболее распространенных вредоносных приложений остались и трояны-кликеры из семейства Android.Click (10,52% детектирований), которые также являются инструментами нелегального заработка. Они способны имитировать действия пользователей — например, загружать сайты с рекламой, нажимать на баннеры, переходить по ссылкам, автоматически подписывать на платные сервисы и выполнять другие вредоносные действия.

Статистика



Android.HiddenAds.1994

Android.HiddenAds.615.origin

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.RemoteCode.284.origin

Android.RemoteCode.6122

Android.RemoteCode.306.origin

Вредоносные программы, которые загружают и выполняют произвольный код. В зависимости от модификации они также могут загружать различные веб-сайты, переходить по ссылкам, нажимать на рекламные баннеры, подписывать пользователей на платные услуги и выполнять другие действия.

Android.Triada.510.origin

Android.Triada.4567.origin

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

Статистика

их модификации могут эксплуатировать уязвимости, чтобы получить доступ к защищенным системным файлам и директориям.

Android.Click.348.origin

Android.Click.311.origin

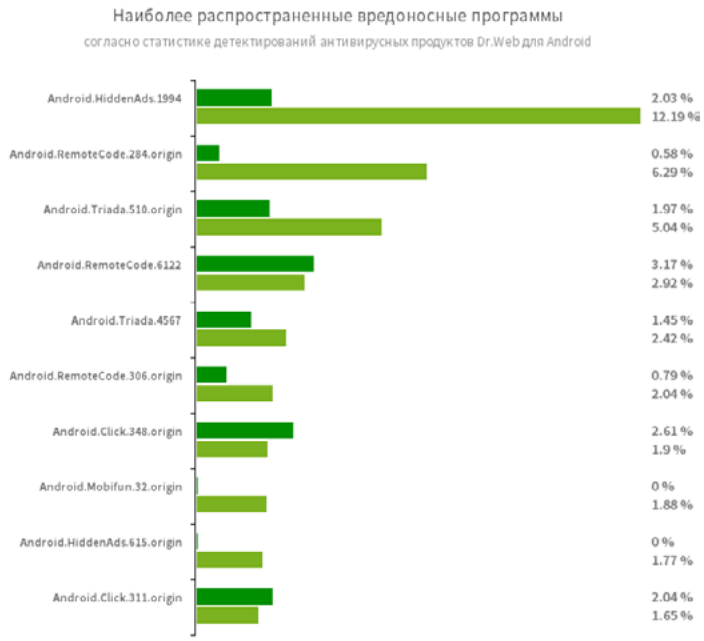
Вредоносные приложения, которые самостоятельно загружают веб-сайты, нажимают на рекламные баннеры и переходят по ссылкам. Могут распространяться под видом безобидных программ, не вызывая подозрений у пользователей.

Android.Mobifun.32.origin

Дроппер, распространяющий трояна Android.Mobifun.29.origin. Последний сам является дроппером и выступает промежуточным звеном в цепочке доставки полезной нагрузки (других вредоносных программ) на Android-устройства.

В 2021 году больше половины (55,71%) выявленных на Android-устройствах нежелательных приложений составили программы семейства Program.FakeAntiVirus. Это почти в 3,5 раза больше, чем годом ранее. Такие программы имитируют работу антивирусов, обнаруживают несуществующие угрозы и предлагают купить свои полные версии — якобы для лечения заражения и исправления проблем.

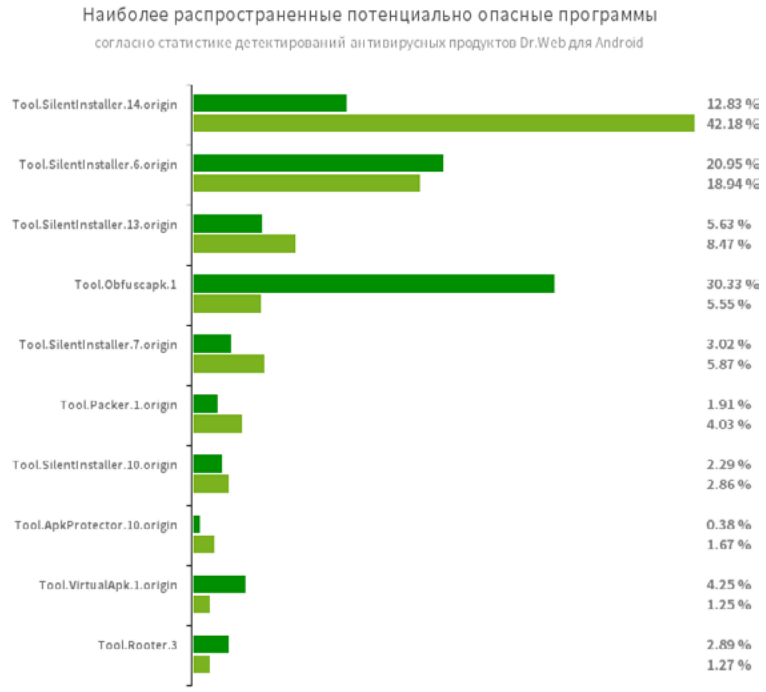
Кроме того, антивирусные продукты Dr.Web для Android вновь детектировали множество специализированных программ, позволяющих контролировать активность пользователей, собирать информацию о них, а также дистанционно управлять устройствами.



Статистика

Program.FakeAntiVirus.1
Program.FakeAntiVirus.2.origin
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.FreeAndroidSpy.1.origin
Program.SecretVideoRecorder.1.origin
Program.Mrecorder.1.origin
Program.Reptilicus.7.origin
Program.NeoSpy.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.WapSniff.1.origin
Программа для перехвата сообщений в мессенджере WhatsApp.
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.
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.
Наиболее распространенными потенциально опасными программами снова стали специализированные утилиты, позволяющие запускать Android-приложения без их установки. Среди них — различные представители семейства Tool.SilentInstaller. Они уверенно заняли первое место по числу обнаружений на устройствах пользователей с результатом в 79,51% от общего выявленных программ, несущих потенциальный риск. Это на 53,28% больше, чем годом ранее.
Кроме того, актуальным остается использование злоумышленниками всевозможных обфускаторов и программ-упаковщиков. С их помощью вирусописатели пытаются защитить вредоносные приложения от анализа специалистами по информационной безопасности и детектирования антивирусами. Приложения, защищенные такими утилитами, обнаруживались на Android-устройствах в 14,16% случаев.
Третьими по числу обнаружений стали утилиты, позволяющие получать root-полномочия. Такие инструменты могут работать в связке с троянскими приложениями, позволяя им, например, заражать системный каталог Android-устройств. На долю таких утилит пришлось 2,59% детектирований потенциально опасного ПО.

Статистика



Tool.SilentInstaller.6.origin
Tool.SilentInstaller.7.origin
Tool.SilentInstaller.10.origin
Tool.SilentInstaller.13.origin
Tool.SilentInstaller.14.origin
Tool.VirtualApk.1.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.

Tool.ApkProtector.10.origin

Детектирование Android-приложений, защищенных программным упаковщиком ApkProtector. Этот упаковщик не является вредоносным, однако злоумышленники могут использовать его при создании троянских и нежелательных программ, чтобы антивирусам было сложнее их обнаружить.

Статистика

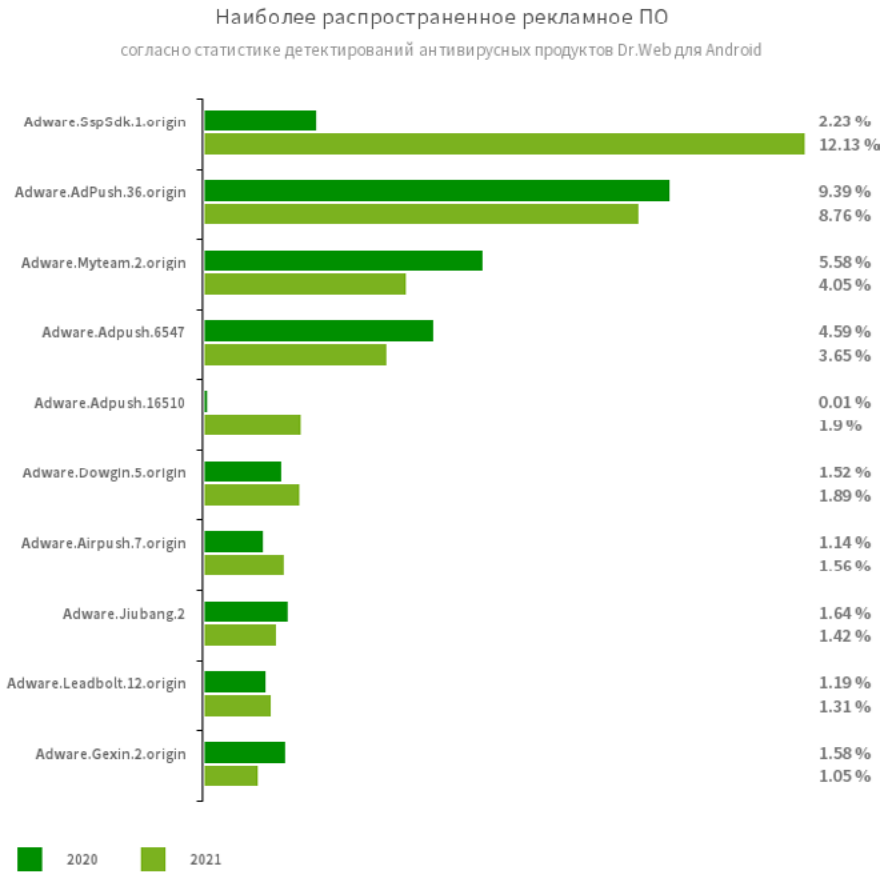
Tool.Packer.1.origin

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

Tool.Rooter.3

Утилита для получения root-полномочий на Android-устройствах, которая задействует различные эксплойты. Наряду с владельцами Android-устройств ее могут применять злоумышленники и вредоносные программы.

Среди рекламного ПО наиболее часто на устройствах пользователей детектировались приложения с модулями, которые демонстрировали уведомления и диалоговые окна, а также загружали и предлагали пользователям установить различные игры и программы. Кроме того, распространенными вновь стали встроенные в приложения модули, которые демонстрировали баннеры с рекламой вне этих программ.



Статистика

Adware.SspSdk.1.origin
Adware.AdPush.36.origin
Adware.Adpush.6547
Adware.Adpush.16510
Adware.MyTeam.2.origin
Adware.Dowgin.5.origin
Adware.Airpush.7.origin
Adware.Jiubang.2
Adware.Leadbolt.12.origin
Adware.Gexin.2.origin

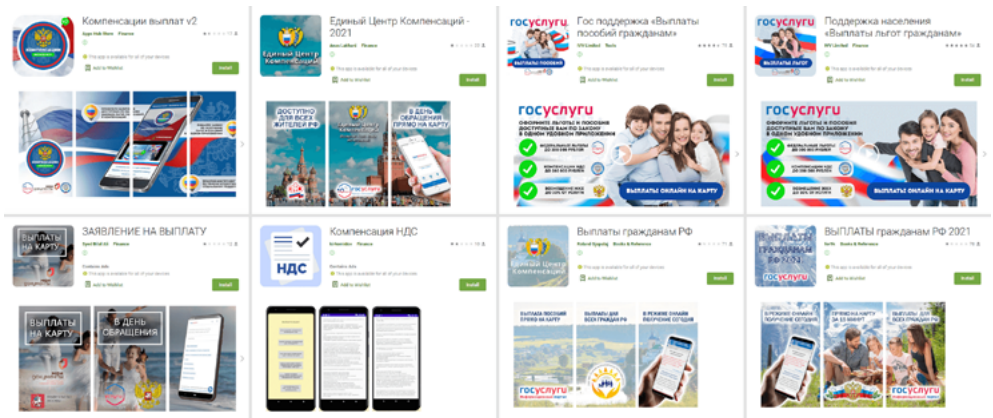
Рекламные модули, которые разработчики встраивают в свои приложения для их монетизации. Такие модули показывают надоедливые уведомления, баннеры и видеорекламу, которые мешают работе с устройствами, загружают веб-сайты, а некоторые — скачивают и предлагают установить приложения. Кроме того, они могут собирать конфиденциальную информацию и передавать ее на удаленный сервер.

Угрозы в Google Play

Среди угроз, выявленных в каталоге Google Play в 2021 году, было множество троянов, принадлежащих к семейству Android.Joker. Они опасны тем, что способны загружать и исполнять произвольный код, также автоматически подписывать пользователей на платные мобильные услуги. Эти трояны распространялись под видом самых разных приложений — фото- и видеоредакторов, музыкальных плееров, мессенджеров, программ для работы с документами и заботы о здоровье, переводчиков, утилит для оптимизации работы системы и других. При этом они выполняли заявленные функции, чтобы потенциальные жертвы не заподозрили в них угрозу. В течение года вирусные аналитики «Доктор Веб» выявили в Google Play более 40 неизвестных ранее модификаций таких вредоносных приложений, число установок которых превысило 1 250 000.

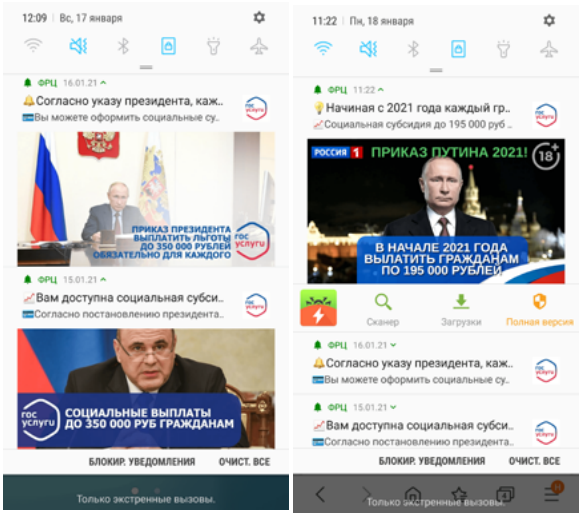
Другой массированной угрозой стали вредоносные приложения-подделки из семейства Android.FakeApp, которые злоумышленники используют в различных мошеннических схемах. Такие трояны тоже распространяются под видом полезных и безобидных программ, но на самом деле не выполняют заявленных функций. Основные задачи большинства из них — обмануть пользователей и заманить их на мошеннические сайты, а также выудить как можно больше конфиденциальных данных. Наши специалисты обнаружили сотни таких троянов, которые загрузили свыше 1 700 000 пользователей.

Как и годом ранее, одной из популярных схем с применением этих вредоносных приложений стала эксплуатация темы государственной социальной поддержки населения в России. Для этого многие трояны Android.FakeApp распространялись под видом программ для поиска информации о выплатах пособий и льгот, «компенсации» НДС и т. п., а также непосредственного получения выплат. Однако они лишь загружали мошеннические сайты, где каждому посетителю сулились многотысячные выплаты. За «начисление» обещанных средств от жертв требовалось оплатить «государственную пошлину» или «комиссию банка» в размере от нескольких сотен до нескольких тысяч рублей. Никаких выплат жертвы мошенников на самом деле не получали — вместо этого они переводили собственные средства злоумышленникам, а также предоставляли им свои персональные данные.



Угрозы в Google Play

Некоторые модификации троянов периодически демонстрировали уведомления с сообщениями о якобы доступных выплатах и компенсациях. Таким образом киберпреступники пытались привлечь дополнительное внимание потенциальных жертв, чтобы те чаще переходили на мошеннические сайты. Примеры таких уведомлений:

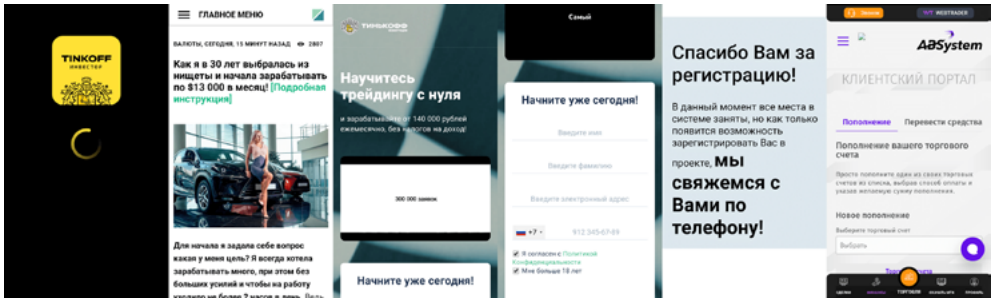


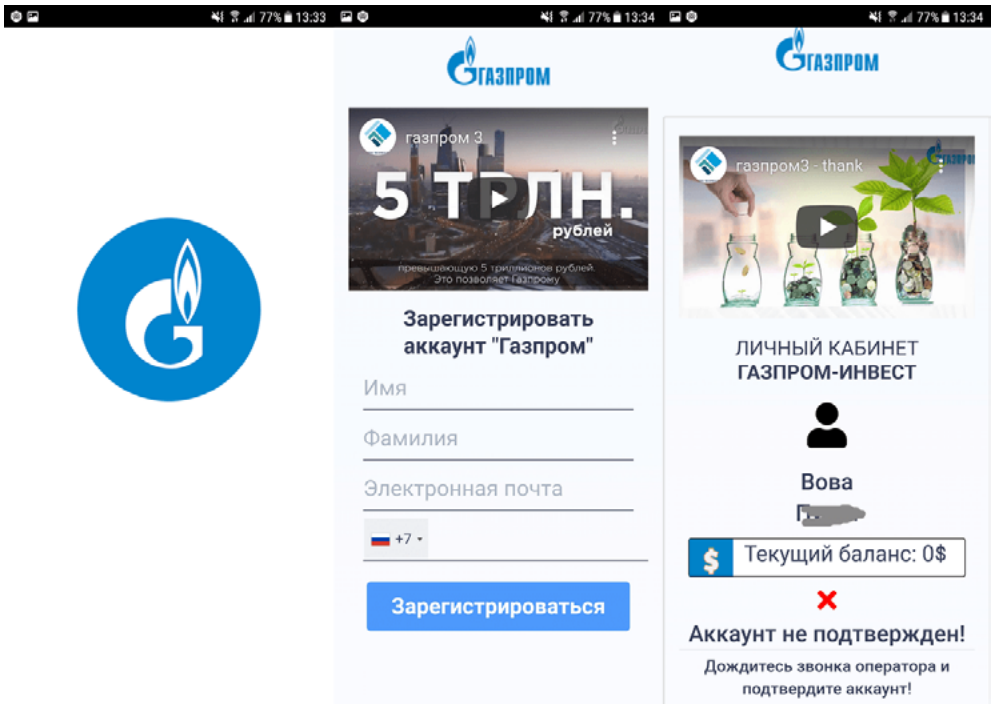
Другой популярной схемой стали предложения инвестиций и заработка на торговле криптовалютами, нефтью, газом и другими активами. Подобные схемы уже несколько лет применяются при атаках на владельцев компьютеров. Однако в минувшем году они стали более активно продвигаться и среди пользователей мобильных устройств, для чего создавались соответствующие программы-подделки. С их помощью пользователи якобы могли получать пассивный доход от инвестиций, не имея ни опыта, ни специальных экономических знаний. Для большей привлекательности такие трояны часто распространялись под видом официального ПО известных компаний или оформлялись в стиле существующих финансовых приложений.

Угрозы в Google Play

На загружаемых многими из них сайтах владельцам Android-устройств предлагалось зарегистрировать учетную запись, указав персональную информацию, и дождаться звонка «оператора». Предоставленные при регистрации данные — имена, фамилии, адреса электронной почты и номера телефонов — злоумышленники могли самостоятельно использовать для дальнейшего обмана пользователей или же продать на черном рынке.

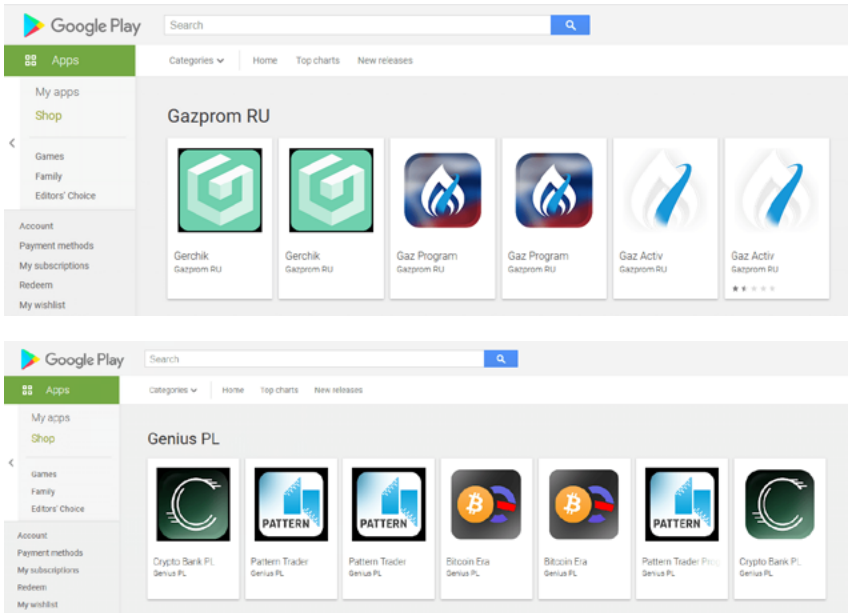
Примеры работы таких троянов:





При этом финансовые программы-подделки «охотились» не только на российских, но и на иностранных пользователей, которые также рисковали оказаться на поддельных сайтах и попасть в сети мошенников.

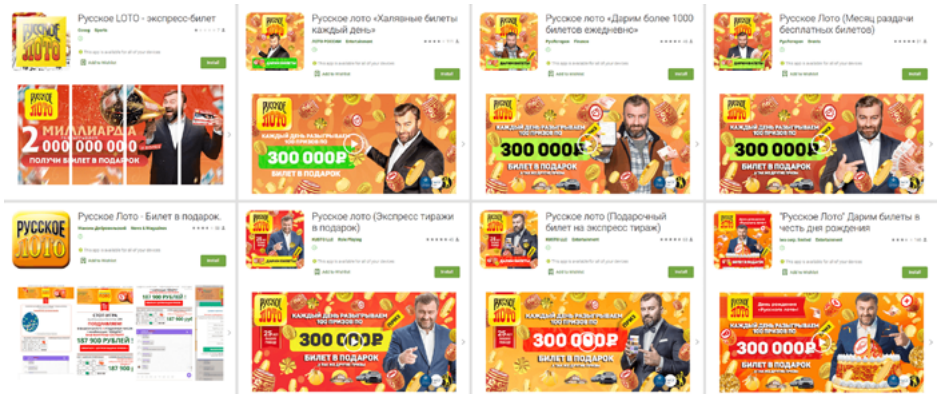
Угрозы в Google Play



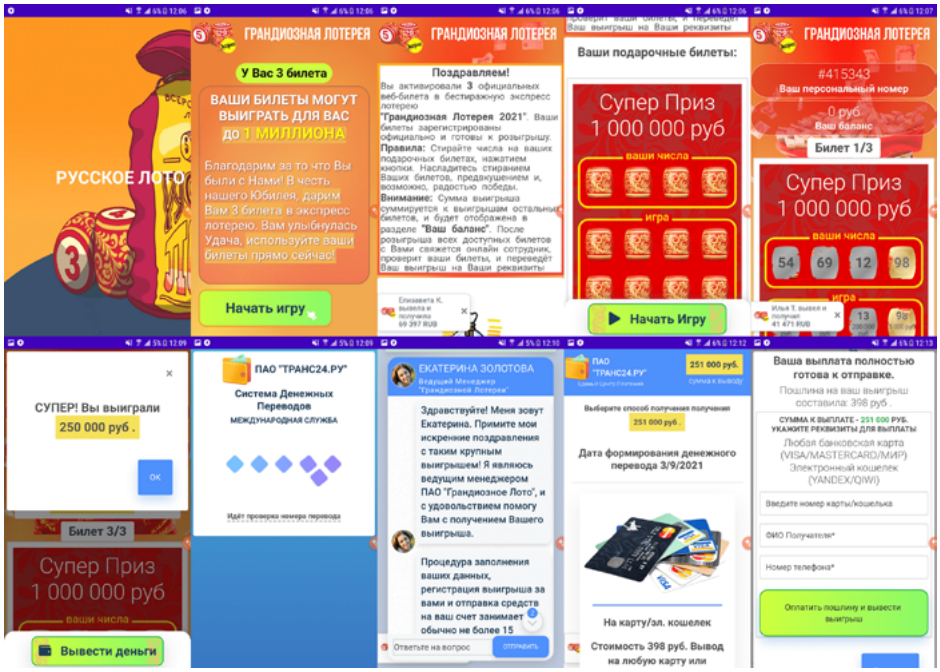
Один из таких троянов, Android.FakeApp.277, даже распространялся под видом инвестиционной программы от Илона Маска. В ней потенциальным жертвам предлагалось «удвоить» объем имеющейся у них криптовалюты, отправив ее якобы на криптокошельки компании Tesla. Никакого отношения ни к известной компании, ни к ее владельцу эта подделка не имела, и обманутые пользователи переводили криптовалюту мошенникам.

Угрозы в Google Play

Другая группа троянов этого семейства активно распространялась под видом официальных приложений популярных российских лотерей. С их помощью пользователи якобы могли получить бесплатные лотерейные билеты и принять участие в розыгрыше призов. На самом деле билеты были ненастоящие, а игра лишь имитировалась — всегда с неизменной победой «счастливчика». При этом для получения «выигрыша» от жертв требовалось оплатить «комиссию» или «пошлину» — эти деньги оседали в карманах мошенников.



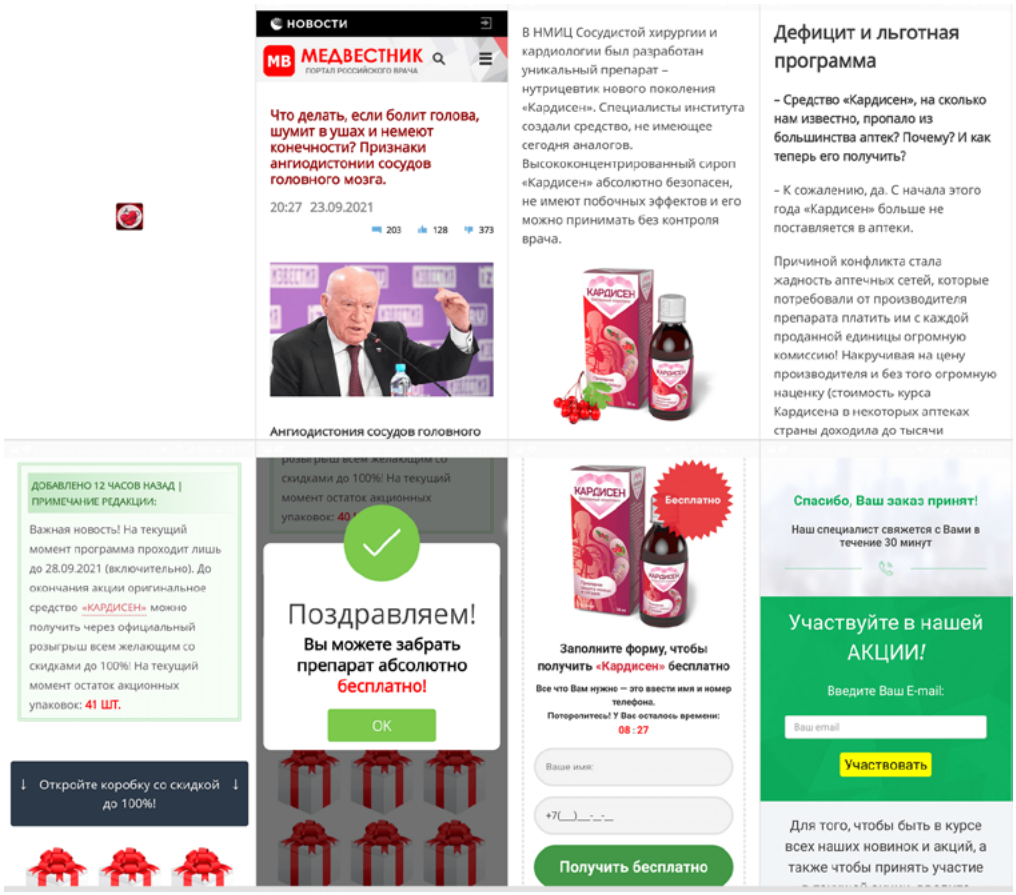
Пример того, как эти трояны обманывают пользователей:



Применялись и другие схемы. Например, некоторые трояны Android.FakeApp распространялись под видом приложений, которые злоумышленники выдавали за безобидные программы разнообразной тематики. Среди них — справочники о моде, животных, природе, различные гороско-

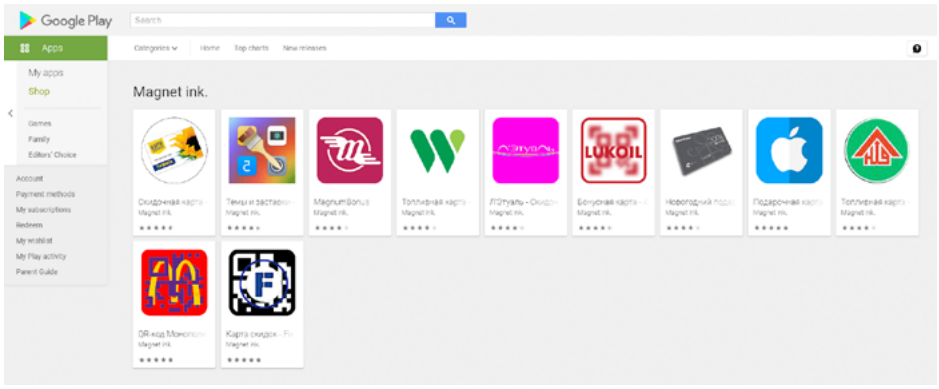
Угрозы в Google Play

пы. Другие распространялись под видом ПО с информацией о болезнях и способах их лечения. В первом случае мошенники даже не старались скрыть признаки подделки. При запуске программ потенциальные жертвы неожиданно попадали на сомнительные и откровенно мошеннические сайты «онлайн-знакомств», где для привлечения внимания часто имитировалось общение с реальными людьми, а пользователям предлагалось пройти регистрацию, иногда платную. Во втором случае жертвы попадали на сайты, рекламирующие некие чудо-лекарства, которые им «посчастливилось» застать в наличии и приобрести якобы по очень выгодной цене.

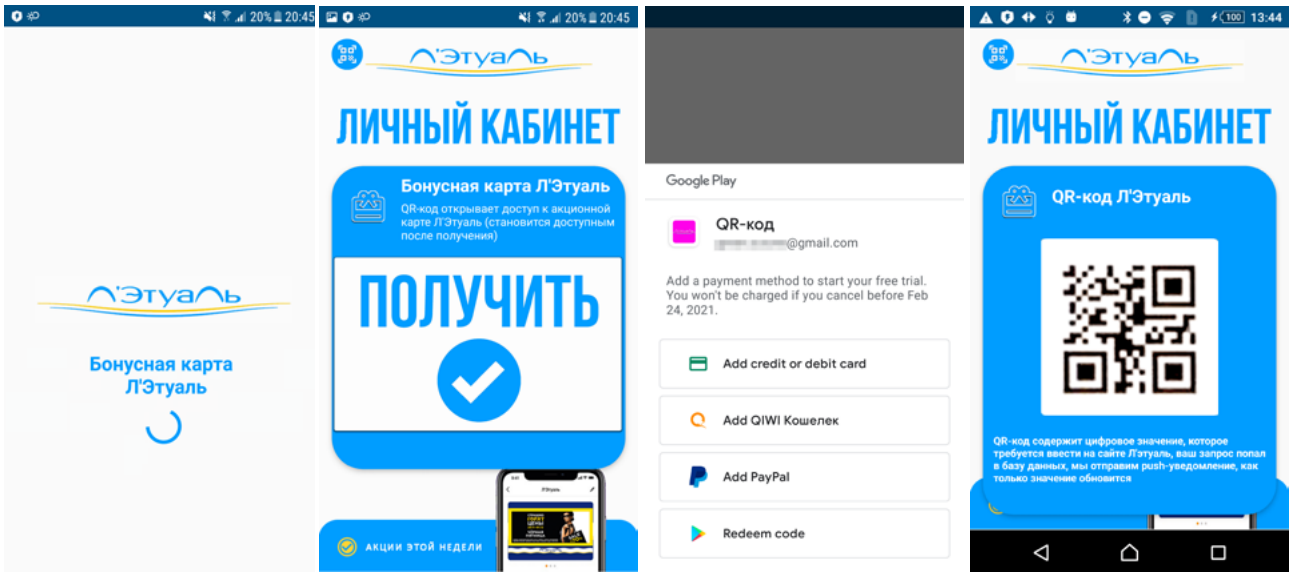


Распространялись приложения-подделки и под видом программ, якобы предоставлявших доступ к скидкам, акционным и бонусным картам, а также подаркам от известных магазинов и компаний. Для большей убедительности в них использовалась символика и названия соответствующих брендов — производителей электроники, АЗС и торговых сетей.

Угрозы в Google Play



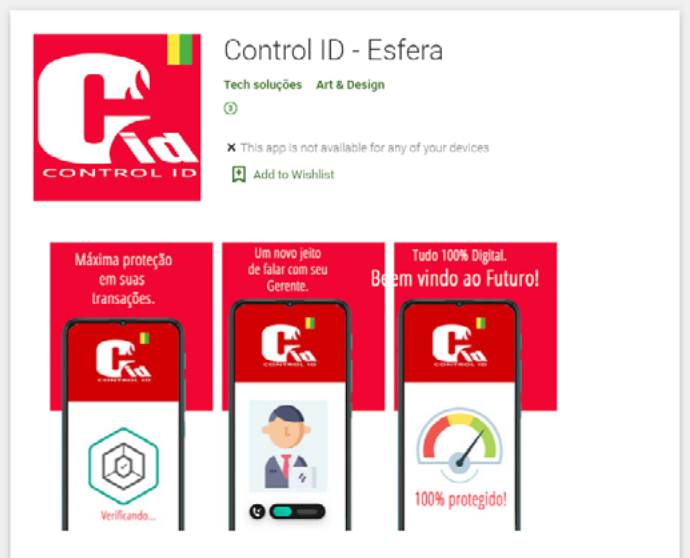
В зависимости от модификации троянов, при их запуске потенциальным жертвам предлагалось оформить платную подписку стоимостью от 400 рублей и выше в день или неделю — якобы чтобы воспользоваться всеми функциями приложений и получить обещанные бонусы. Однако в результате они получали лишь бесполезные штрих- или QR-коды. В течение 3 дней с начала активации подписки пользователи могли от нее отказаться. Но в данном случае злоумышленники рассчитывали, что жертвы либо забудут об этих программах и подключенных через них услугах, либо просто не обратят внимания, что активировали дорогостоящий сервис с периодической оплатой.



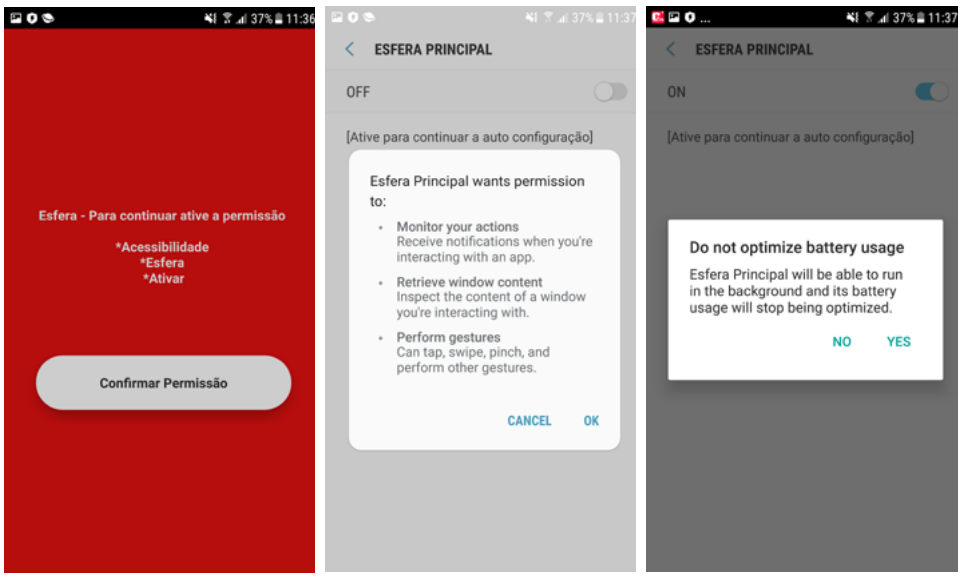
Среди выявленных в Google Play угроз были и другие типы вредоносных приложений. Например, трояны семейства Android.Proxy, превращающие зараженные устройства в прокси-серверы, через которые злоумышленники переадресовывали интернет-трафик. Также наши специалисты выявили новые модификации рекламных троянов Android.HiddenAds.

Угрозы в Google Play

Кроме того, в официальном каталоге приложений появлялись банковские трояны. Один из них, Android.Banker.3679, распространялся под видом приложения для работы с бонусной программой Esfera банка Santander и предназначался для бразильских пользователей.

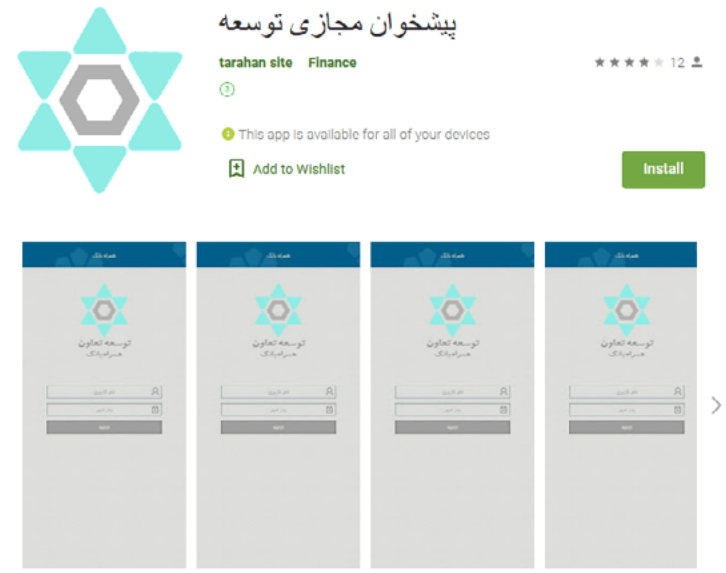


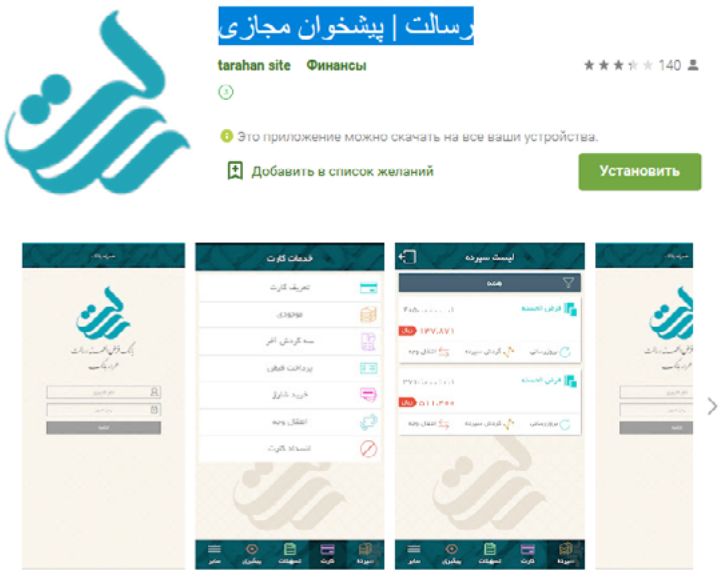
Его основными функциями были фишинг и кража конфиденциальных данных, а главной целью — банковское приложение Santander Empresas. Троян запрашивал доступ к специальным возможностям ОС Android, с помощью которых получал контроль над устройством и мог самостоятельно нажимать на различные элементы меню и кнопки и считывать содержимое окон приложений.



Угрозы в Google Play

Другой троян, Android.Banker.4919, распространялся под видом банковских приложений Resalat Bank и Tose'e Ta'avon Bank и атаковал иранских пользователей. Он загружал фишинговые сайты, а также имел функциональность для кражи СМС-сообщений, однако не мог этого сделать из-за отсутствия необходимых системных разрешений.





Угрозы в Google Play

Пример одного из сайтов, которые загружала эта вредоносная программа:

Также наши специалисты обнаружили приложения со встроенными рекламными модулями семейства Adware.NewDich, которые по команде управляющего сервера загружали различные веб-сайты в браузере Android-устройств. Чтобы не вызвать подозрений в неправомерных действиях, загрузка сайтов происходила, когда пользователи не работали с этими программами.

Модули Adware.NewDich часто загружают страницы различных партнерских и рекламных сервисов, которые перенаправляют пользователей на разделы размещенных в Google Play программ. Одной из них было приложение, которое оказалось банковским трояном и получило имя Android.Banker.3684. Этот троян перехватывал вводимые логины, пароли, одноразовые проверочные коды, а также содержимое поступающих уведомлений, для чего запрашивал соответствующее системное разрешение. Еще одно рекламируемое приложение содержало рекламный модуль Adware.Overlay.1.origin, который загружал веб-страницы и демонстрировал их поверх окон других программ.

Банковские трояны

В 2021 число обнаруженных на Android-устройствах банковских троянов увеличилось на 43,74% по сравнению с предыдущим годом. На их многочисленные модификации пришлось 5,4% детектирований всех вредоносных программ. Пик распространения Android-банкеров пришелся на начало весны, после чего интенсивность их атак постепенно снижалась с небольшим повышением активности в августе и сентябре.

Возросшая активность этих вредоносных приложений во многом обусловлена появлением множества новых семейств. Например, в начале января стал распространяться банковский троян Oscorp (Android.BankBot.792.origin), а в июле в вирусную базу Dr.Web были добавлены записи для детектирования трояна S.O.V.A. (Android.BankBot.842.origin). Тогда же стало известно о семействах Coper и Abere (Android.BankBot.Abere.1.origin). Последний интересен тем, что управляется через Telegram-боты. Уже в октябре пользователям стали угрожать различные модификации трояна SharkBot (Android.BankBot.904.origin).

Кроме того, злоумышленники распространяли банкеров Anatsa (Android.BankBot.779.origin) и Flubot (Android.BankBot.780.origin, Android.BankBot.828.origin). Несмотря на то, что их первые модификации появились в конце 2020 года, основная их активность пришлась именно на последние 12 месяцев.

Вместе с тем оставались активными и старые семейства, такие как Anubis (Android.BankBot.518.origin, Android.BankBot.670.origin, Android.BankBot.822.origin и другие модификации), Ginp (Android.BankBot.703.origin), Gustuff (Android.BankBot.657.origin, Android.BankBot.738.origin), Medusa (Android.BankBot.830.origin), Hydra (Android.BankBot.563.origin), BRATA (Android.BankBot.915.origin), Alien (Android.BankBot.687.origin, Android.BankBot.745.origin) и Cerberus (Android.BankBot.612.origin, Android.BankBot.8705). При этом появлялись и новые «потомки» трояна Cerberus, основанные на его исходном коде, который попал в открытый доступ в конце лета 2020 года. Одним из них был банкер ERMAC (Android.BankBot.870.origin), начавший свои атаки в июле.

Перспективы и тенденции

Извлечение прибыли остается одной из главных целей вирусописателей, поэтому в будущем году следует ожидать появления новых троянских и нежелательных приложений, позволяющих зарабатывать деньги. Поскольку реклама — это надежный и относительно простой источник дохода, сохранится актуальность рекламных троянов. Также вероятно увеличение числа вредоносных программ, предназначенных для загрузки и установки различного ПО.

Продолжат появляться новые банковские трояны, многие из которых будут сочетать в себе широкую функциональность. Они будут не только красть деньги со счетов пользователей, но и выполнять другие задачи.

Сохранится угроза со стороны мошенников и всевозможных программ-подделок, которые те будут распространять. Кроме того, возможны новые атаки с применением троянов, крадущих конфиденциальную информацию, а также рост числа случаев использования шпионских программ.

Также следует ожидать, что для защиты вредоносных программ все больше киберпреступников станут использовать всевозможные обфускаторы и упаковщики.

Со своей стороны компания «Доктор Веб» продолжит отслеживать активность злоумышленников и выявлять самые актуальные угрозы, предоставляя надежную защиту для наших пользователей. Для защиты от Android-угроз рекомендуется применять антивирусные средства Dr.Web для Android, а также устанавливать все актуальные обновления операционной системы и используемых программ.

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2021 год

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