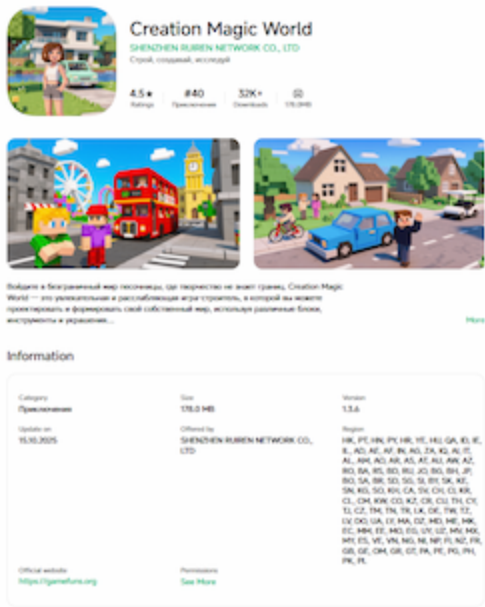


Трояны семейства Android.Phantom проникают в смартфоны вместе с играми и пиратскими модами популярных приложений. Они используют машинное обучение и видеотрансляции для накрутки кликов

 news.drweb.ru/show

January 21, 2026



[Подробнее](#)

Горячая лента угроз | «Горячие» новости | Все новости

21 января 2026 года

Специалисты антивирусной лаборатории «Доктор Веб» обнаружили и исследовали новое семейство троянов с функциональностью кликера. Их объединяет одна особенность: они либо управляются с сервера `hxxps[:]//dllpgd[.]click`, либо загружаются и выполняются по команде с него. Вредоносное ПО данного типа заражает смартфоны на ОС Android.

Один из каналов распространения троянов — официальный каталог приложений для устройств Xiaomi GetApps.



Creation Magic World

SHENZHEN RUIREN NETWORK CO., LTD

Создай, создавай, наслаждайся

4.5★
#40
32K+
176,045




Выборите в бескрайний мир пиксельной, где границы не имеют границ, Creation Magic World — это увлекательная и расширяющаяся игра в строительство, в которой вы можете строить персонажей и формировать свой собственный мир, используя различные блоки, инструменты и украшения.

More

Information

Category Пространство	Size 175.0 MB	Version 1.3.6
Updated on 15.10.2025	Offered by SHENZHEN RUIREN NETWORK CO., LTD	Region HK, PT, HN, PY, HR, YE, HU, GA, RI, BE, S, AD, NE, AF, RI, AG, ZA, KZ, AG, IT, AU, AR, AD, AR, AS, AT, AU, AR, AZ, BG, SA, RS, RO, RU, JO, BH, BH, JP, BG, SA, BR, SD, SO, SI, BY, SK, KT, SN, KG, SG, KH, CA, SV, CH, CL, KR, CL, CM, KM, CO, KZ, CR, CU, TH, CY, TJ, CZ, TM, TN, TR, UA, DE, TW, TZ, UG, DO, UA, UZ, MA, EG, ME, ME, HR, EC, MM, ES, MD, ES, UY, UZ, MA, MA, MY, ES, VE, VN, NG, NE, NP, FI, NZ, FR, GR, GE, OM, GR, GT, PA, PE, PG, PH, PK, PL
Official website https://gamefun.org	Permissions See More	



Theft Auto Mafia

SHENZHEN RUIREN NETWORK CO., LTD

Прямой грабительский мажорский мир

4.5★
#28
60K+
176,045




More

Information

Category Акция	Size 175.0 MB	Version 1.5.5
Updated on 16.10.2025	Offered by SHENZHEN RUIREN NETWORK CO., LTD	Region HK, PT, HN, PY, HR, YE, HU, GA, RI, BE, S, AD, NE, AF, RI, AG, ZA, KZ, AG, IT, AU, AR, AD, AR, AS, AT, AU, AR, AZ, BG, SA, RS, RO, RU, JO, BH, BH, JP, BG, SA, BR, SD, SO, SI, BY, SK, KT, SN, KG, SG, KH, CA, SV, CH, CL, KR, CL, CM, KM, CO, KZ, CR, CU, TH, CY, TJ, CZ, TM, TN, TR, UA, DE, TW, TZ, UG, DO, UA, UZ, MA, EG, ME, ME, HR, EC, MM, ES, MD, ES, UY, UZ, MA, MA, MY, ES, VE, VN, NG, NE, NP, FI, NZ, FR, GR, GE, OM, GR, GT, PA, PE, PG, PH, PK, PL
Official website https://gamefun.org	Permissions See More	

Нам удалось отследить несколько мобильных игр, которые содержат вредоносное ПО: Creation Magic World (более 32 тыс. скачиваний), Cute Pet House (>34 тыс. скачиваний), Amazing Unicorn Party (>13 тыс. скачиваний), Академия мечты Сакура (>4 тыс. скачиваний), Theft Auto Mafia (>61 тыс. скачиваний), Open World Gangsters (>11 тыс. скачиваний). Все зараженные игры выложены от лица одного разработчика, SHENZHEN RUIREN NETWORK CO., LTD., троянцы вшиты в них и запускаются вместе с приложениями.

В первоначальных версиях игр вредоносного ПО не было. 28/29 сентября разработчик публикует обновления для игр, в которые встроен троян [Android.Phantom.2.origin](#). Он работает в двух режимах, которые в коде программы условно называются режим сигнализации (signaling) и фантом (phantom).

В режиме phantom вредоносное ПО использует скрытый от пользователя встроенный браузер на основе виджета WebView. В него по команде с сервера `hxxps[:]//playstations[.]click` загружается целевой сайт для накрутки кликов и файл JavaScript «phantom». Последний содержит в себе сценарий для автоматизации действий на рекламных объявлениях загруженного сайта и фреймворк машинного обучения TensorFlowJS. Модель для этого фреймворка загружается с сервера `hxxps[:]//app-download[.]cn-wlcb[.]ufileos[.]com` в директорию приложения. В сценариях для работы с некоторыми видами рекламы [Android.Pantom.2.origin](#) размещает браузер на виртуальном экране и делает скриншоты. Троян анализирует их с помощью модели для фреймворка TensorFlowJS, а затем кликает по обнаруженным элементам.

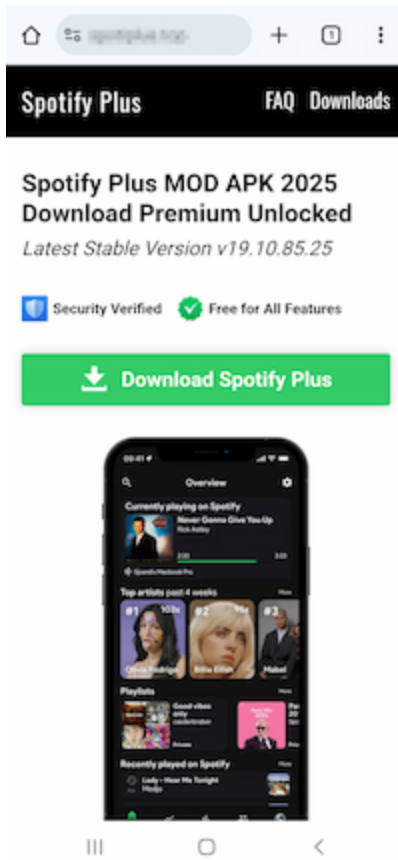
В альтернативном режиме signaling троянец подключается к стороннему серверу при помощи WebRTC. Эта технология позволяет браузерам и приложениям устанавливать прямое соединение для обмена данными, аудио и видео в режиме реального времени без установки дополнительного ПО. В режиме signaling уже упомянутый `hxxps[:]//dllpgd[.]click` выполняет роль сигнального сервера, устанавливающий соединения между узлами WebRTC. Также данный сервер определяет режим работы трояна, phantom или signaling. Задачи с целевыми сайтами приходят от `hxxps[:]//playstations[.]click`.

Далее [Android.Pantom.2.origin](#) тайно от пользователя транслирует злоумышленникам видео виртуального экрана с загруженным в браузер сайтом. Троянец дает возможность подключенному узлу WebRTC удаленно управлять браузером на виртуальном экране: кликать, скроллить, вводить или вставлять текст в форму для ввода.

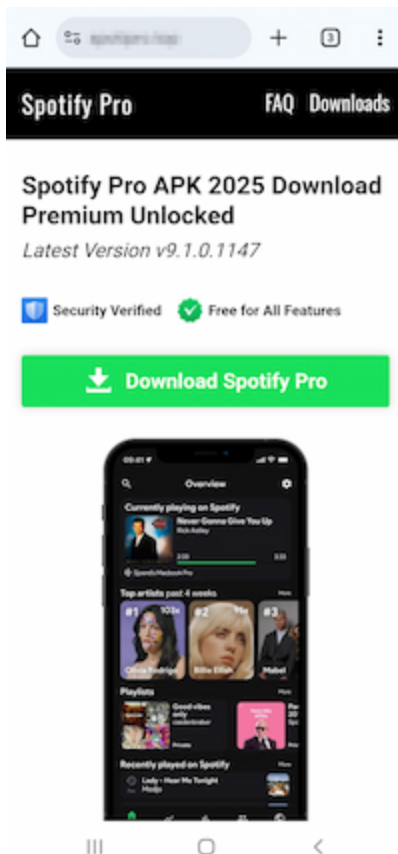
15/16 октября вышеуказанные игры получили еще одно обновление. В дополнение к [Android.Pantom.2.origin](#) в них встроили модуль [Android.Pantom.5](#). Он является дроппером, который содержит внутри себя загрузчик удаленного кода [Android.Pantom.4.origin](#). Эта программа загружает еще несколько троянов, предназначенных для имитации кликов на различных сайтах. Эти модули проще кликера [Android.Pantom.2.origin](#) — они не используют машинное обучение или видеотрансляции, а руководствуются сценариями для кликов, написанных на JavaScript.

Чтобы использовать технологию WebRTC на Android, трояну необходимо подключить специальную библиотеку с Java API, которая не входит в состав стандартной ОС и скачанных приложений. Поэтому поначалу троян работал преимущественно в режиме phantom. С добавлением в приложения [Android.Pantom.5](#), троян [Android.Pantom.2.origin](#) получил возможность использовать загрузчик удаленного кода [Android.Pantom.4.origin](#) для загрузки необходимой библиотеки.

Злоумышленники используют также и другие каналы распространения троянов [Android.Pantom.2.origin](#) и [Android.Pantom.5](#). К примеру, моды музыкального стриминга Spotify с разблокированными premium функциями. Они размещаются на различных сайтах, вот несколько примеров:

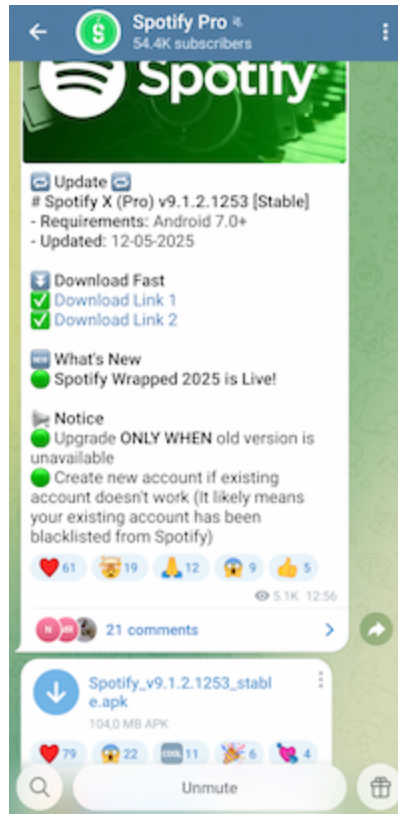


Caŭm Spotify Plus

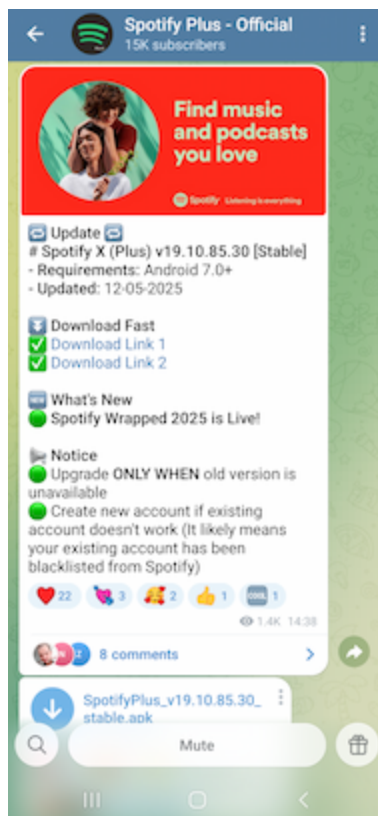


Сайт Spotify Pro

И в специальных телеграм-каналах:



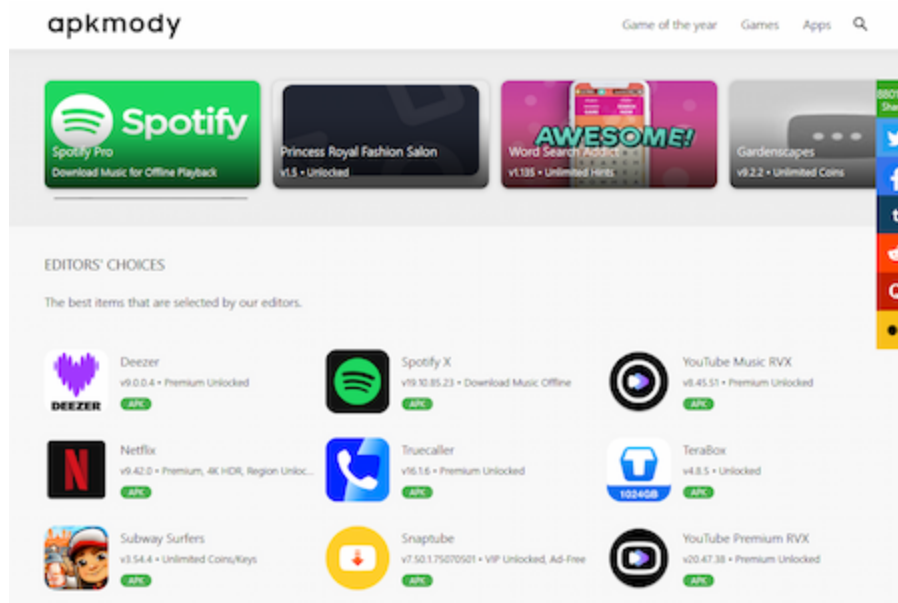
Spotify Pro
(54 400 подписчиков)



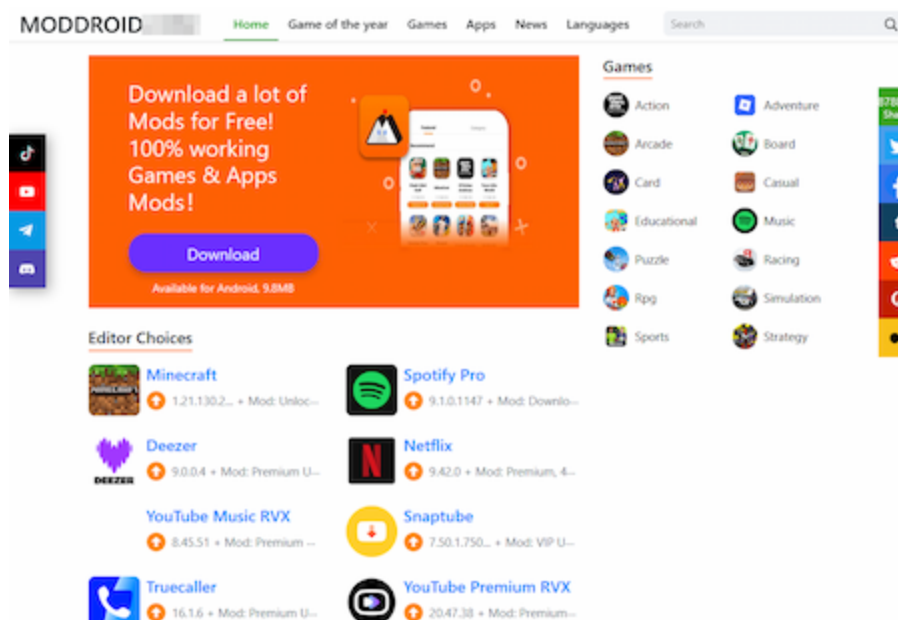
*Spotify Plus – Official
(15 057 подписчиков)*

Моды Spotify, размещенные на сайтах и в указанных на скриншотах телеграм-каналах, содержат [Android.Phantom.2.origin](https://androidphantom2.origin) и библиотеку для организации связи по стандарту WebRTC под Android.

Кроме модов Spotify, злоумышленники вшивают трояны в моды других популярных приложений: YouTube, Deezer, Netflix и др. Они размещены на специальных сайтах с модами:

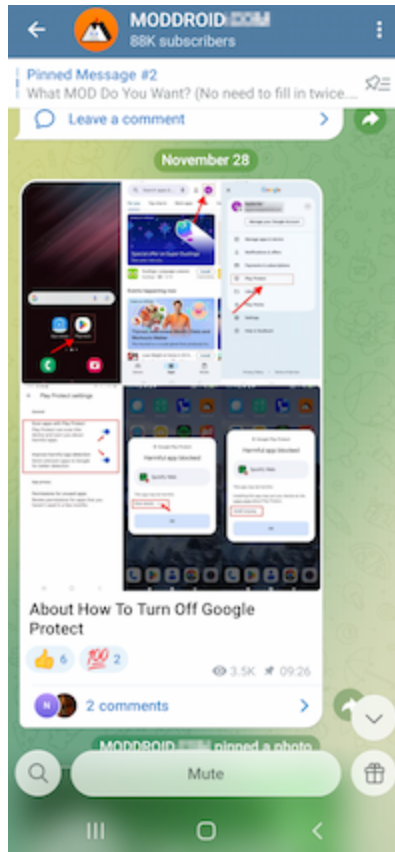


Сайт Apkmody

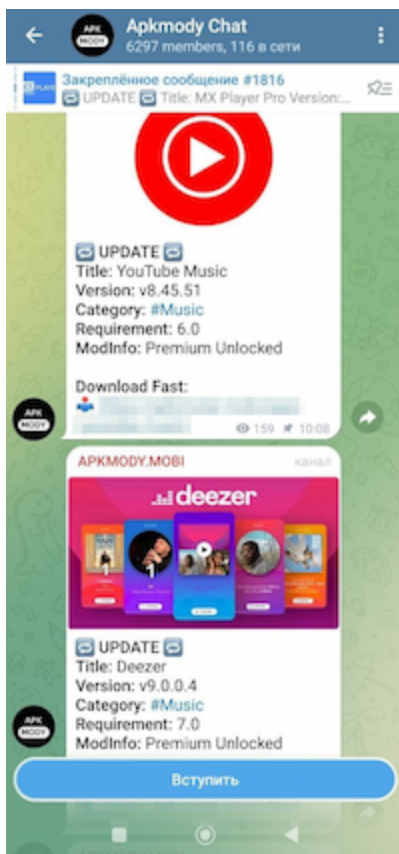


Сайт Moddroid

Сайт Moddroid содержит раздел «Выбор редакции». Из 20 приложений в нем только 4 были чистыми. Остальные 16 содержали трояны семейства **Android.Phantom**. Приложения на этих двух сайтах загружаются с одного CDN-сервера `hxxps[:]//cdn[.]topmongo[.]com`. У этих сайтов есть свои телеграм-каналы, где пользователи скачивают зараженные троянам моды:

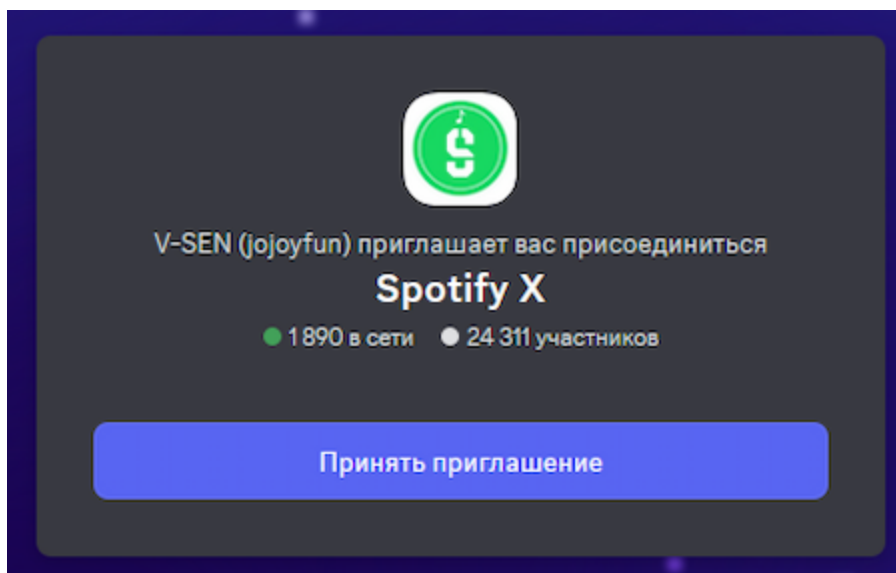


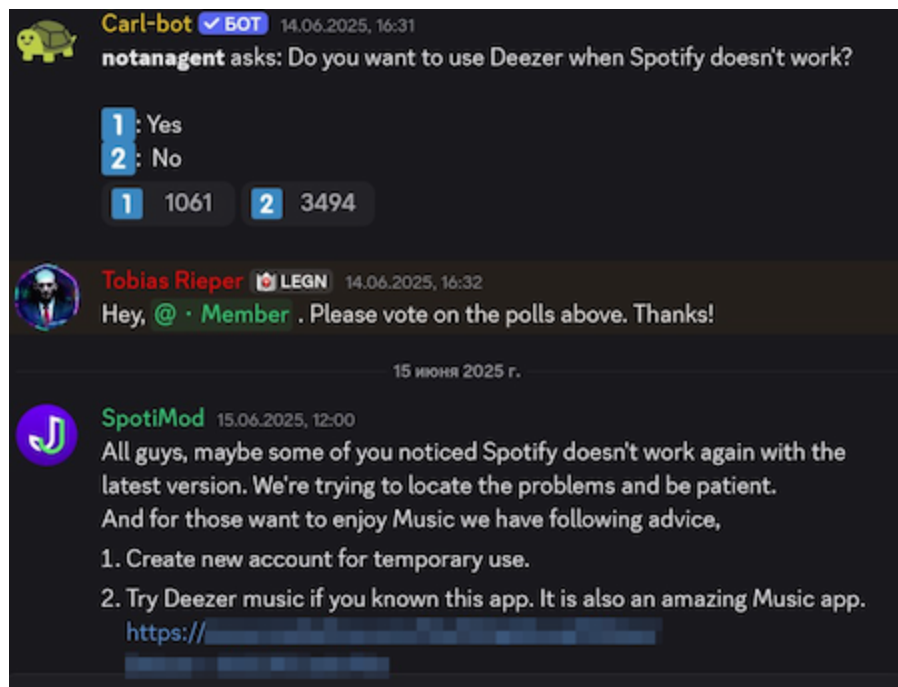
Moddroid.com
(87 653 подписчика)



Apkmody Chat
(6 297 подписчиков)

Также для своих целей преступники используют сервера Discord. Самый большой из них — Spotify X, около 24 тысяч подписчиков.





Администраторы Discord-серверов не стесняются напрямую предлагать зараженные моды. Например, на скриншоте выше администратор от лица сервера предлагает скачать мод музыкального стриминга Deezer вместо Spotify, поскольку последний перестал работать.

По ссылке скачивается рабочий мод. Его код защищен коммерческим упаковщиком, внутри которого скрывается троян [Android.Phantom.1.origin](#). Это загрузчик удаленного кода, по команде с сервера `hxxps[:]//dllpgd[.]click` он загружает уже нам знакомые [Android.Phantom.2.origin](#), [Android.Phantom.5](#) и троян-шпион **Android.Phantom.5.origin**. Последний отправляет информацию об устройстве злоумышленникам, в том числе номер телефона, геолокацию, список установленных приложений.



Этот скриншот с сервера показывает, на каких языках говорят пользователи, которые становятся объектами заражения. Для доступа к чатам на языках, отличных от английского, необходимо поставить реакцию с соответствующим флагом. Больше всего отметились пользователи, говорящие на испанском, французском, немецком, польском и итальянском языках (не считая английского, который является основным языком сервера). Также администраторы сервера не предусмотрели чатов для многих стран Азии.

Трояны могут нанести существенный вред владельцам зараженных устройств. Перечислим несколько возможных исходов:

- **Невольное соучастие.** Смартфон пользователя может быть использован в качестве бота при DDoS-атаке, тем самым делая владельца невольным соучастником киберпреступления.
- **Незаконная активность.** Через устройство злоумышленники могут совершать незаконную онлайн-деятельность, к примеру, использовать смартфон в мошеннических схемах или рассылать спам-сообщения.
- **Повышенное потребление заряда и трафика.** Посторонняя деятельность разряжает аккумулятор и расходует интернет-трафик.
- **Утечка персональных данных.** **Android.Phantom.5.origin** является шпионом и может передавать данные об устройстве и владельце.

Трояны этого семейства представляют угрозу для владельцев мобильных устройств на Android, не защищенных актуальным антивирусным ПО. Российские пользователи испытывают трудности с регистрацией в зарубежных приложениях или оплатой подписок. Ситуация подталкивает искать и использовать альтернативные, зачастую полулегальные, способы получения услуг этих компаний. Эта ситуация на руку вирусописателям, ведь пользователям приходится рисковать и доверять сомнительным вариантам. Особую группу риска составляют дети, которые не думают о правилах цифровой гигиены, желая всего лишь поиграть, послушать музыку или посмотреть видеоклипы.

Мы рекомендуем не скачивать моды на сомнительных сайтах и в каналах. Как правило, проверка источников модов или приложений требует времени, опыта и насмотренности. Поэтому лучший вариант обеспечить себе и своим близким гарантированное спокойствие — использовать Dr.Web Security Space для мобильных устройств. Он защитит не только ваши смартфоны, но и другие умные устройства: игровые консоли, планшеты, smartTV. [Индикаторы компрометации](#)

1

Последние новости [Все новости](#)

Горячая лента угроз

[Читать](#)

«Доктор Веб»: обзор вирусной активности для мобильных устройств за 2025 год

Вирусные обзоры

[Читать](#)

«Доктор Веб»: обзор вирусной активности за 2025 год

Вирусные обзоры

[Читать](#)