Dr.WEB®
с 1992 года

«Доктор Веб»: обзор вирусной активности для мобильных устройств в августе 2019 года

Обзор вирусной активности для мобильных устройств в августе 2019 года

9 сентября 2019 года

В последнем летнем месяце вирусные аналитики «Доктор Веб» обнаружили в Google Play троянца-кликера Android.Click.312.origin, встроенного в безобидные приложения. Там же были выявлены и другие вредоносные программы. Среди них — троянец-загрузчик Android.DownLoader.915.origin, рекламные троянцы семейства Android.HiddenAds, которые распространялись под видом полезного ПО, а также банкер Android.Banker.346.origin.

Главные тенденции августа

- Обнаружение новых вредоносных программ в Google Play
- Появление новых нежелательных рекламных модулей

Обзор вирусной активности для мобильных устройств в августе 2019 года

Мобильная угроза месяца

В начале августа компания «Доктор Веб» сообщила о трояне Android.Click.312.origin, обнаруженном в 34 приложениях из Google Play. Он представлял собой вредоносный модуль, который разработчики встраивали в свои программы. В общей сложности ПО с этим троянцем загрузили свыше 101 700 000 пользователей.

Android.Click.312.origin по команде управляющего сервера открывал ссылки в невидимых WebView, мог загружать сайты в браузере и рекламировать приложения в Google Play. Особенности троянца:

- начинал работу через 8 часов после запуска;
- часть функций реализована с использованием рефлексии;
- мог подписывать пользователей на мобильные премиум-услуги через технологию WAP-Click.

Подробнее об Android.Click.312.origin рассказано в новости на нашем сайте.

Обзор вирусной активности для мобильных устройств в августе 2019 года

По данным антивирусных продуктов Dr.Web для Android

Android.HiddenAds.455.origin

Троянец, предназначенный для показа навязчивой рекламы.

Android.Backdoor.682.origin

Троянец, который выполняет команды злоумышленников и позволяет им контролировать зараженные мобильные устройства.

Android.Triada.467.origin

Многофункциональный троянец, выполняющий разнообразные вредоносные действия.

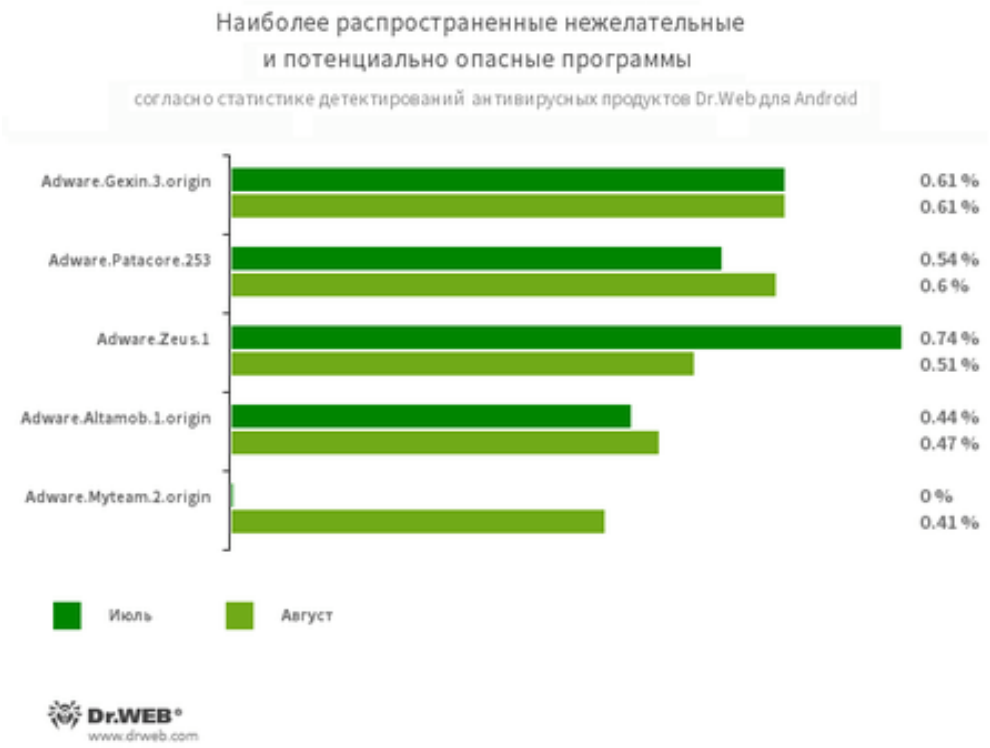
Android.RemoteCode.197.origin

Android.RemoteCode.5564

Вредоносные приложения, предназначенные для загрузки и выполнения произвольного кода.

Обзор вирусной активности для мобильных устройств в августе 2019 года

По данным антивирусных продуктов Dr.Web для Android

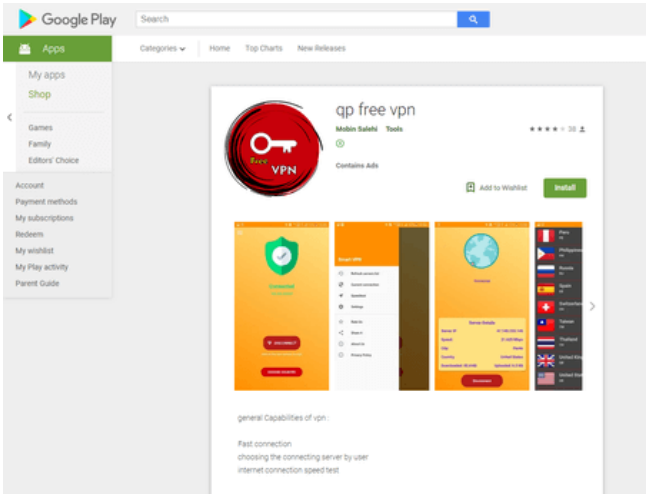


Программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах:

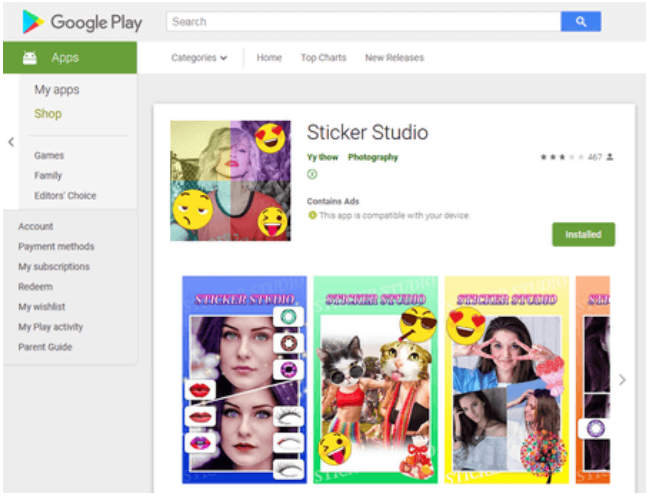
- Adware.Gexin.3.origin
- Adware.Patacore.253
- Adware.Zeus.1
- Adware.Altamob.1.origin
- Adware.Myteam.2.origin (новая угроза)

Угрозы в Google Play

Наряду с кликером Android.Click.312.origin среди обнаруженных в Google Play вредоносных программ был троянец-загрузчик Android.DownLoader.915.origin, который распространялся под видом клиента для подключения к VPN-сетям. Он скачивал и пытался установить приложения, а также загружал заданные злоумышленниками веб-страницы Instagram, Telegram и Google Play и других сервисов.

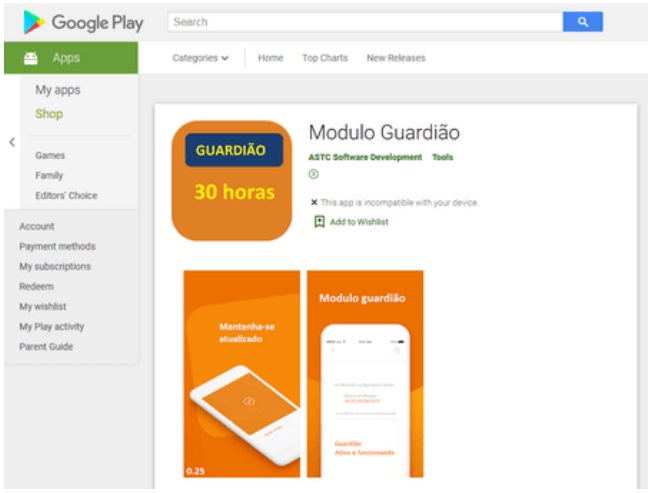


Кроме того, вирусные аналитики выявили новых рекламных троянцев семейства Android.HiddenAds – например, Android.HiddenAds.1598 и Android.HiddenAds.467.origin. Как и другие представители этого семейства, они скрывали значки программ, в которые были встроены, и показывали надоедливую рекламу.



Угрозы в Google Play

В конце августа специалисты «Доктор Веб» обнаружили очередного банковского трояна, атакующего бразильских владельцев Android-устройств. Эта вредоносная программа получила имя Android.Banker.346.origin. Как и другие аналогичные троянцы, о которых наша компания рассказывала ранее (например, в конце 2018 года), Android.Banker.346.origin использует специальные возможности ОС Android (Accessibility Service). С их помощью он крадет информацию из СМС-сообщений, в которых могут быть одноразовые коды и другие конфиденциальные данные. Кроме того, по команде злоумышленников банкер открывает фишинговые страницы.



Для защиты Android-устройств от вредоносных и нежелательных программ пользователям следует установить антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных устройств в августе 2019 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
ВебIQметр | Центр противодействия кибер-мошенничеству

Пресс-центр
Официальная информация | Контакты для прессы | Брошюры | Галерея

Контакты
Центральный офис
125040, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.drweb.ru | www.антивирус.рф | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах