Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в июне 2017 года

Обзор вирусной активности для мобильных Android-устройств в июне 2017 года

3 июля 2017 года

В июне вирусные аналитики «Доктор Веб» обнаружили Android-троянца, который шпионил за иранскими владельцами мобильных устройств и выполнял команды злоумышленников. Кроме того, в прошедшем месяце в каталоге Google Play было найдено сразу несколько вредоносных приложений. Одно из них пыталось получить root-доступ, внедрялось в системные библиотеки и могло незаметно устанавливать ПО. Другие – отправляли СМС с премиум-тарификацией и подписывали пользователей на дорогостоящие услуги. Также в Google Play распространялись потенциально опасные программы, работа с которыми могла привести к утечке конфиденциальной информации. Помимо этого в июне был выявлен новый Android-шифровальщик.

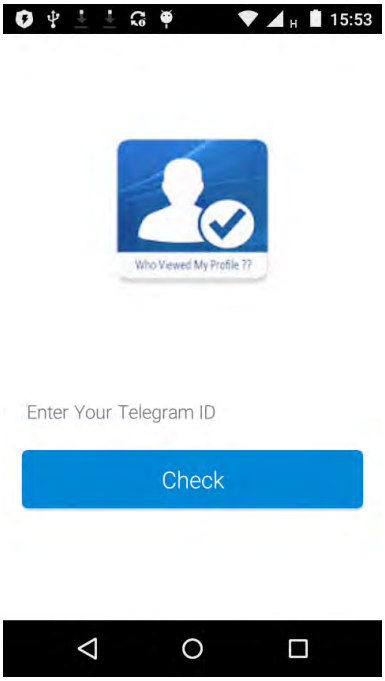
Главные тенденции июня

- Обнаружение Android-троянца, предназначенного для кибершпионажа
- Выявление угроз в каталоге Google Play
- Распространение трояна-шифровальщика для Android

Обзор вирусной активности для мобильных Android-устройств в июне 2017 года

«Мобильная» угроза месяца

В июне вирусные аналитики компании «Доктор Веб» обнаружили Android-троянца Android.Spy.377.origin, который распространялся среди иранских пользователей. Эта вредоносная программа собирала конфиденциальную информацию и передавала ее злоумышленникам. Кроме того, она могла выполнять команды вирусописателей.



Особенности Android.Spy.377.origin:

- распространяется под видом безобидных приложений;
- крадет СМС-переписку, контакты из телефонной книги и данные об учетной записи Google;
- может делать фотографии при помощи фронтальной камеры;
- управляется злоумышленниками через протокол Telegram.

Подробнее об этом троянце рассказано в соответствующей новостной публикации.

Обзор вирусной активности для мобильных Android-устройств в июне 2017 года

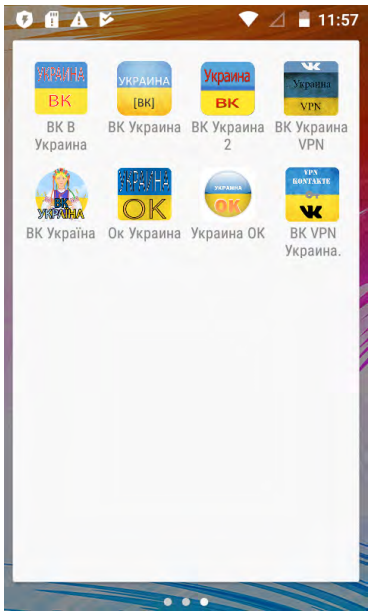
По данным антивирусных продуктов Dr.Web для Android

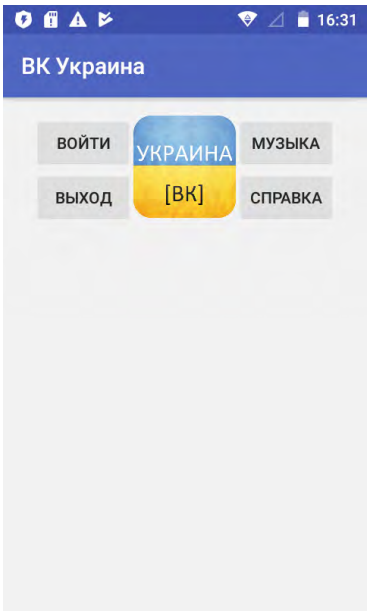
- **Android.HiddenAds.83.origin**
- **Android.HiddenAds.76.origin**
- **Android.HiddenAds.85.origin**
  Троянцы, предназначенные для показа навязчивой рекламы. Распространяются под видом популярных приложений другими вредоносными программами, которые в некоторых случаях незаметно устанавливают их в системный каталог.
- **Android.DownLoader.337.origin**
  Представитель многофункциональных троянцев, выполняющих разнообразные вредоносные действия.
- **Android.Triada.264.origin**
  Представитель многофункциональных троянцев, выполняющих разнообразные вредоносные действия.

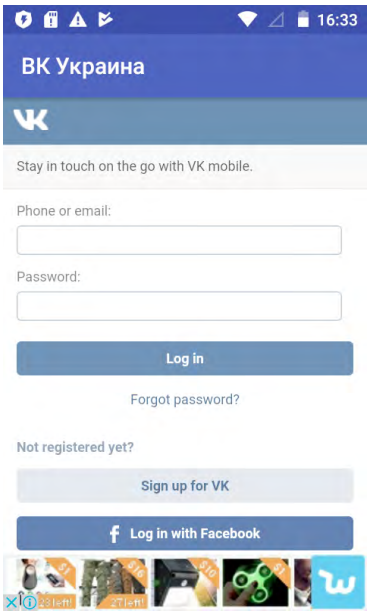
Обзор вирусной активности для мобильных Android-устройств в июне 2017 года

Угрозы в Google Play

В прошедшем месяце специалисты компании «Доктор Веб» обнаружили в каталоге Google Play потенциально опасные программы, которые позволяли работать с заблокированными на территории Украины социальными сетями «ВКонтакте» и «Одноклассники». Эти приложения, добавленные в вирусную базу как Program.PWS.1, задействовали сервер-анонимайзер для обхода ограничения доступа, однако никак не шифровали логин, пароль и другую конфиденциальную информацию пользователей. Более подробно об этом случае рассказано в материале, размещенном на сайте «Доктор Веб».



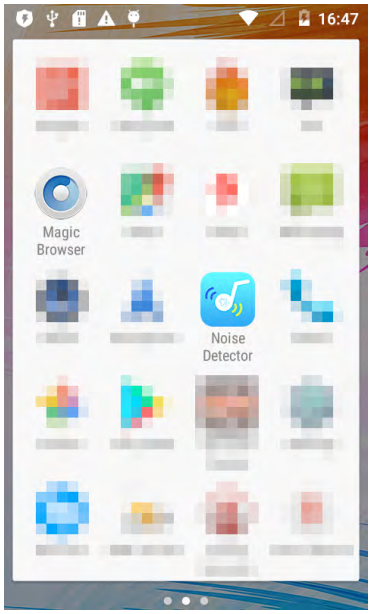


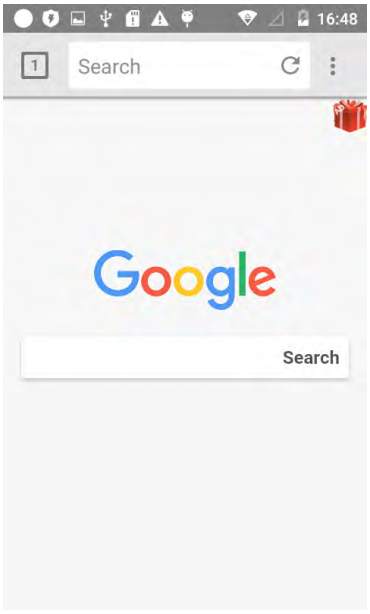


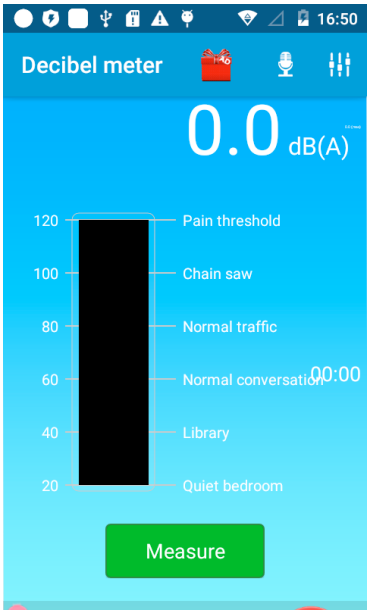
Также в июне в Google Play были выявлены троянцы семейства Android.Dvmap. При запуске эти вредоносные программы пытаются получить на мобильном устройстве root-доступ, после чего заражают некоторые системные библиотеки и устанавливают дополнительные компоненты. Эти троянцы могут выполнять команды злоумышленников, а также загружать и запускать другие приложения без участия пользователя.

Другие Android-троянцы, распространявшиеся через каталог Google Play в июне, были добавлены в вирусную базу Dr.Web как Android.SmsSend.1907.origin и Android.SmsSend.1908.origin. Злоумышленники встроили их в безобидные программы. Эти вредоносные приложения отправляли СМС на платные номера, подписывая абонентов мобильных операторов на дорогостоящие услуги. После этого троянцы начинали удалять все поступающие сообщения, чтобы пользователи не получали уведомлений с информацией об успешном подключении ненужных премиум-сервисов.

Обзор вирусной активности для мобильных Android-устройств в июне 2017 года







Троянец-шифровальщик

В июне был обнаружен троянец-вымогатель Android.Encoder.3.origin, который атаковал китайских пользователей ОС Android и шифровал файлы на SD-карте. Авторы этого энкодера вдохновились нашумевшим троянцем-шифровальщиком WannaCry, в мае 2017 года поразившим сотни тысяч компьютеров по всему миру. Вирусописатели использовали аналогичный стиль оформления сообщения с требованием выкупа за расшифровку.

Обзор вирусной активности для мобильных Android-устройств в июне 2017 года

Злоумышленники требовали у пострадавших выкуп в размере 20 юаней, при этом каждые 3 дня сумма удваивалась. Если через неделю после заражения мобильного устройства киберпреступники не получали деньги, Android.Encoder.3.origin удалял зашифрованные файлы.

Вредоносные и потенциально опасные программы для ОС Android попадают на мобильные устройства не только при загрузке с различных веб-сайтов, но также и при скачивании из каталога Google Play. Владельцам смартфонов и планшетов необходимо с осторожностью устанавливать неизвестные приложения, а также использовать антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в июне 2017 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
125124, Россия, Москва, 3-я улица Ямского поля, вл. 2, корп.12а
www.антивирус.рф | www.drweb.ru | www.mobi.drweb.com | www.av-desk.ru
«Доктор Веб» в других странах