Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в феврале 2016 года

Обзор вирусной активности для мобильных Android-устройств в феврале 2016 года

29 февраля 2016 года

Главные тенденции февраля

- Обнаружение многофункциональных троянцев, встраивающихся в системные процессы и предназначенных для выполнения широкого спектра вредоносных действий
- Новые случаи распространения банковских троянцев

«Мобильная» угроза месяца

В феврале специалисты компании «Доктор Веб» обнаружили целый комплект Android-троянцев семейства Android.Loki, работающих совместно друг с другом и предназначенных для выполнения на зараженных мобильных устройствах широкого спектра вредоносных действий. Один из этих троянцев, добавленный в вирусную базу как Android.Loki.3, внедряет библиотеку liblokih.so (Android.Loki.6) в системный процесс, в результате чего другие вредоносные программы из этого набора получают возможность действовать с системными привилегиями. Основные возможности представителей данного семейства:

- установка и удаление приложений;
- включение и отключение приложений, а также их компонентов;
- остановка процессов;
- показ уведомлений;
- регистрация приложений как Accessibility Service (службы, отслеживающей нажатия на экран устройства);
- обновление своих компонентов, а также загрузка плагинов по команде с управляющего сервера;
- сбор подробной технической информации о зараженном устройстве.

Также вредоносные программы передают на управляющий сервер следующие данные:

- список установленных приложений;
- история браузера;

Обзор вирусной активности для мобильных Android-устройств в феврале 2016 года

- список контактов пользователя;
- история звонков;
- текущее местоположение устройства.

Подробнее об этих вредоносных программах рассказано в соответствующей новости на сайте компании «Доктор Веб».

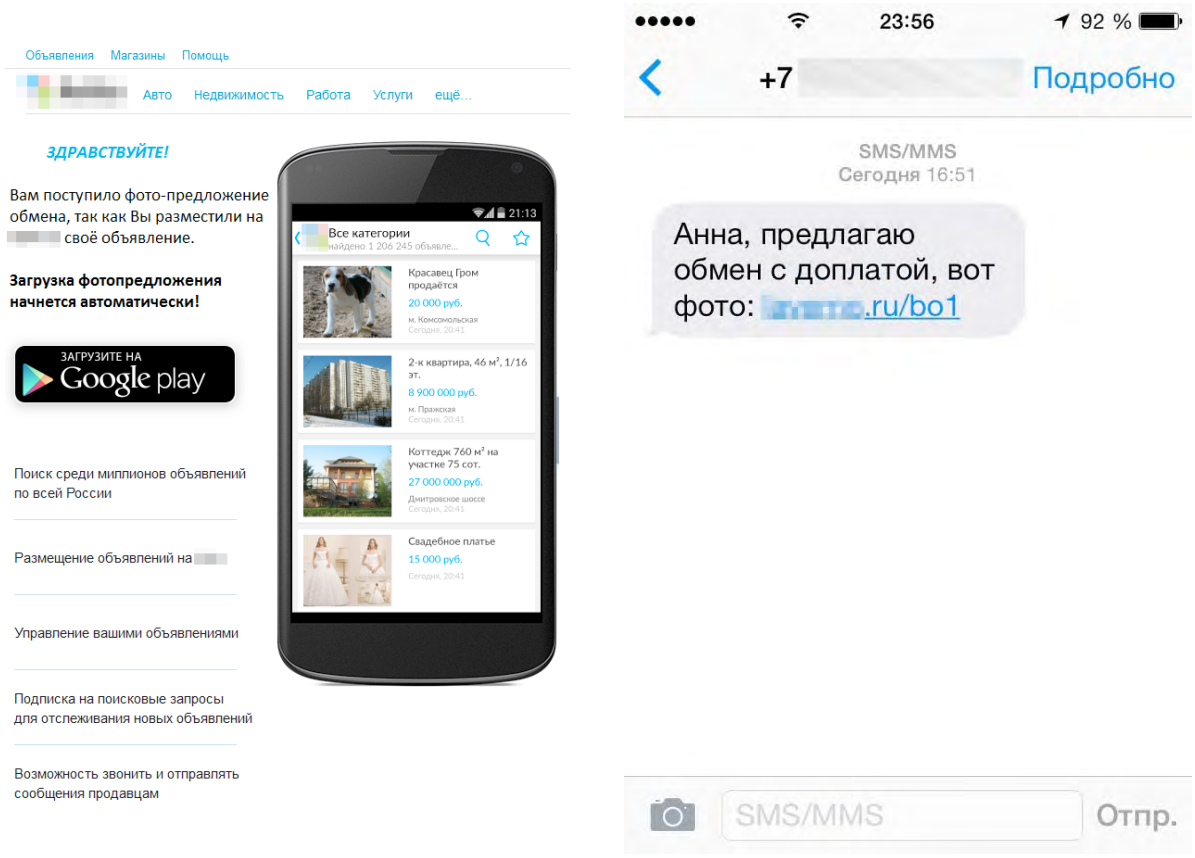
По данным антивирусных продуктов Dr.Web для Android

- **Adware.WalkFree.1.origin**
  Нежелательный программный модуль, встраиваемый в Android-приложения и предназначенный для показа навязчивой рекламы на мобильных устройствах.
- **Android.Xiny.26.origin**
  Троянская программа, предназначенная для загрузки и установки различных приложений, а также показа навязчивой рекламы.
- **Adware.Leadbolt.12.origin**
  Нежелательный программный модуль, встраиваемый в Android-приложения и предназначенный для показа навязчивой рекламы на мобильных устройствах.
- **Adware.Airpush.31.origin**
  Нежелательный программный модуль, встраиваемый в Android-приложения и предназначенный для показа навязчивой рекламы на мобильных устройствах.
- **Android.Backdoor.326.origin**
  Троянская программа, выполняющая различные вредоносные действия по команде злоумышленников.

Обзор вирусной активности для мобильных Android-устройств в феврале 2016 года

Банковские троянцы

Вирусописатели продолжают распространять всевозможных банковских троянцев среди владельцев Android-устройств. Для этого, в частности, киберпреступники не прекращают попыток обмануть пользователей популярных досок объявлений при помощи мошеннических СМС-сообщений. В них потенциальным жертвам, ранее разместившим объявление в Интернете, предлагается «обмен», а также для ознакомления дается ссылка на «фото» товара. Перейдя по указанному в сообщении веб-адресу, пользователи попадают на один из мошеннических интернет-ресурсов, откуда на их мобильные устройства загружается вредоносная программа. Среди распространяемых подобным образом банкеров в минувшем феврале был замечен троянец Android.BankBot.97.origin.



События февраля показали, что злоумышленники по-прежнему заинтересованы в атаках на Android-смартфоны и планшеты. Компания «Доктор Веб» продолжает отслеживать вирусную обстановку в среде мобильных Android-устройств и будет и дальше своевременно информировать пользователей об имеющихся угрозах.

Обзор вирусной активности для мобильных Android-устройств в феврале 2016 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