Dr.WEB®
с 1992 года

Обзор вирусной активности для мобильных Android-устройств в июне 2015 года

Обзор вирусной активности для мобильных Android-устройств в июне 2015 года

30 июня 2015 года

Главные тенденции мая

- Активность банковских троянцев
- Появление новых троянцев-загрузчиков
- Появление новых Android-вымогателей
- Рост числа СМС-троянцев

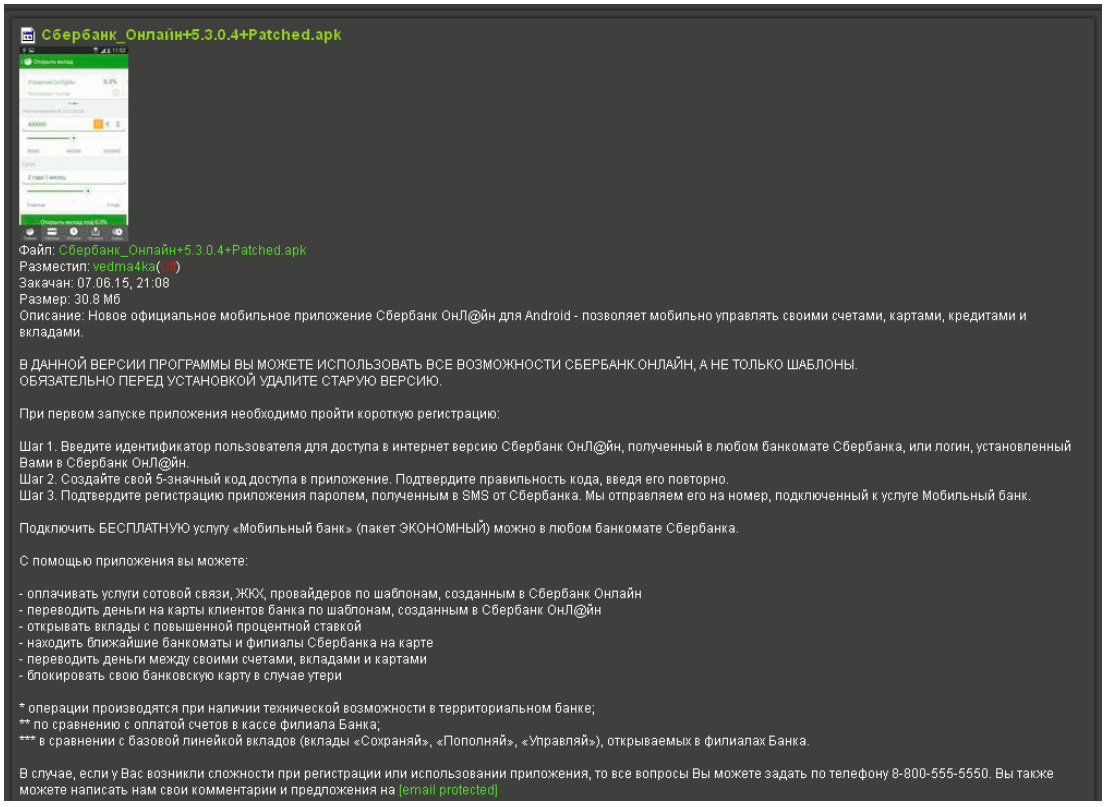
Количество записей для вредоносных и нежелательных программ под ОС Android в вирусной базе Dr.Web

Май 2015	Июнь 2015	Динамика
9155	10 144	+10,8%

Обзор вирусной активности для мобильных Android-устройств в июне 2015 года

«Мобильная» угроза месяца

В прошедшем июне специалисты компании «Доктор Веб» обнаружили и проанализировали весьма любопытного банковского троянца Android.BankBot.65.origin, которого хитроумные злоумышленники внедрили в официальное приложение для доступа к мобильному банкингу от Сбербанка России. Модифицированная вирусописателями программа распространялась ими через популярный веб-сайт, посвященный мобильным устройствам, и предлагалась пользователям для установки в качестве «новой» версии приложения.


Сбербанк_Онлайн+5.3.0.4+Patched.apk

Файл: Сбербанк_Онлайн+5.3.0.4+Patched.apk
Разместил: vedma4ka(ОП)
Закачан: 07.06.15, 21:08
Размер: 30.8 Мб
Описание: Новое официальное мобильное приложение Сбербанк ОнЛ@йн для Android - позволяет мобильно управлять своими счетами, картами, кредитами и вкладами.

В ДАННОЙ ВЕРСИИ ПРОГРАММЫ ВЫ МОЖЕТЕ ИСПОЛЬЗОВАТЬ ВСЕ ВОЗМОЖНОСТИ СБЕРБАНК.ОНЛАЙН, А НЕ ТОЛЬКО ШАБЛОНЫ.
ОБЯЗАТЕЛЬНО ПЕРЕД УСТАНОВКОЙ УДАЛИТЕ СТАРУЮ ВЕРСИЮ.

При первом запуске приложения необходимо пройти короткую регистрацию:

Шаг 1. Введите идентификатор пользователя для доступа в интернет версию Сбербанк ОнЛ@йн, полученный в любом банкомате Сбербанка, или логин, установленный Вами в Сбербанк ОнЛ@йн.
Шаг 2. Создайте свой 5-значный код доступа в приложение. Подтвердите правильность кода, введя его повторно.
Шаг 3. Подтвердите регистрацию приложения паролем, полученным в SMS от Сбербанка. Мы отправляем его на номер, подключенный к услуге Мобильный банк.

Подключить БЕСПЛАТНУЮ услугу «Мобильный банк» (пакет ЭКОНОМНЫЙ) можно в любом банкомате Сбербанка.

С помощью приложения вы можете:

- оплачивать услуги сотовой связи, ЖКХ, провайдеров по шаблонам, созданным в Сбербанк Онлайн
- переводить деньги на карты клиентов банка по шаблонам, созданным в Сбербанк ОнЛ@йн
- открывать вклады с повышенной процентной ставкой
- находить ближайшие банкоматы и филиалы Сбербанка на карте
- переводить деньги между своими счетами, вкладами и картами
- блокировать свою банковскую карту в случае утери

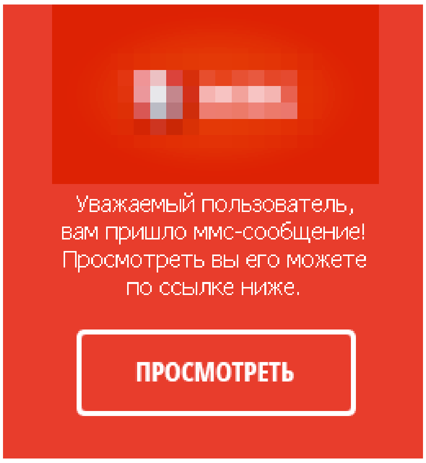
* операции производятся при наличии технической возможности в территориальном банке;
** по сравнению с оплатой счетов в кассе филиала Банка;
*** в сравнении с базовой линейкой вкладов (вклады «Сохраняй», «Пополняй», «Управляй»), открываемых в филиалах Банка.

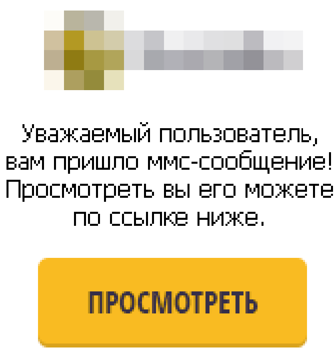
В случае, если у Вас возникли сложности при регистрации или использовании приложения, то все вопросы Вы можете задать по телефону 8-800-555-5550. Вы также можете написать нам свои комментарии и предложения на

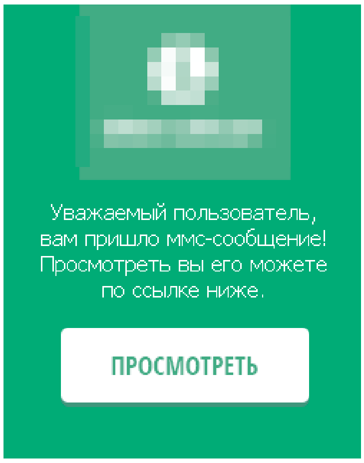
Главная опасность Android.BankBot.65.origin заключается в том, что троянская копия банковского ПО сохраняет все свои оригинальные функции, поэтому после ее установки на мобильное устройство потенциальная жертва не должна заподозрить какой-либо подвох. В действительности же вредоносная программа после своего запуска незаметно для владельца зараженного Android-устройства загружает на удаленный сервер различную конфиденциальную информацию и по команде вирусописателей способна перехватывать и отправлять СМС-сообщения, что может использоваться киберпреступниками для кражи денег с банковских счетов. Подробнее о троянце Android.BankBot.65.origin рассказано в новостной публикации на сайте компании «Доктор Веб».

Android-банкеры

Появляющиеся с завидной регулярностью разнообразные банковские троянцы в настоящее время представляют одну из главных угроз для пользователей ОС Android. Помимо обнаружения опасной вредоносной программы Android.BankBot.65.origin, в минувшем месяце специалисты компании «Доктор Веб» отметили заметную активность других аналогичных троянцев. В частности, злоумышленники из разных стран продолжили распространять Android-банкеры при помощи нежелательных СМС, содержащих ссылку на загрузку вредоносного приложения. Например, в России под видом поступивших MMS-сообщений вновь распространялись различные модификации троянца Android.SmsBot.291.origin.



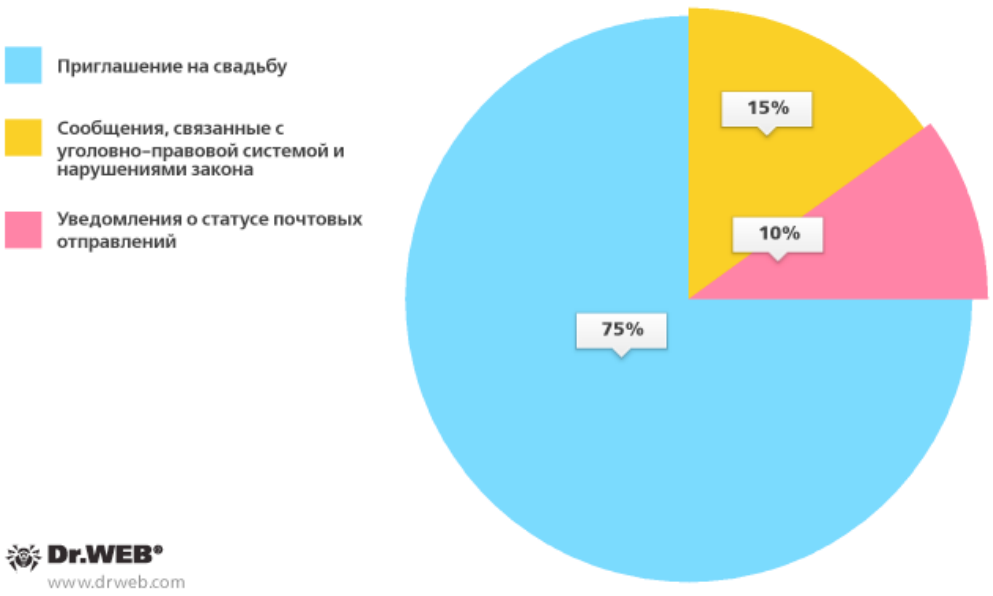




В очередной раз не остались без внимания киберпреступников и пользователи из Южной Кореи: специалисты компании «Доктор Веб» зафиксировали 20 спам-кампаний, организованных южнокорейскими вирусописателями.

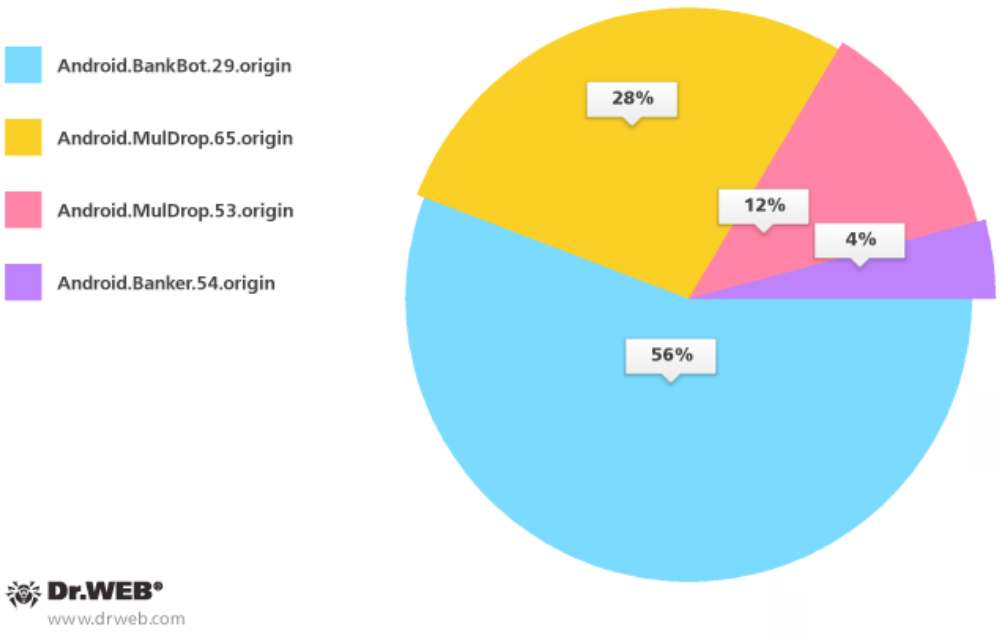
Обзор вирусной активности для мобильных Android-устройств в июне 2015 года

Тематика нежелательных СМС-сообщений, применявшихся при распространении вредоносных программ в Южной Корее



В июне при помощи СМС-спама южнокорейские злоумышленники распространяли следующие вредоносные Android-приложения:

Android-троянцы, распространяемые среди южнокорейских жителей при помощи СМС-спама



Обзор вирусной активности для мобильных Android-устройств в июне 2015 года

Число записей для банковских троянцев **Android.BankBot** в вирусной базе Dr.Web:

Май 2015	Июнь 2015	Динамика
119	122	+2,52%

Число записей для многофункциональных троянцев Android.SmsBot в вирусной базе Dr.Web:

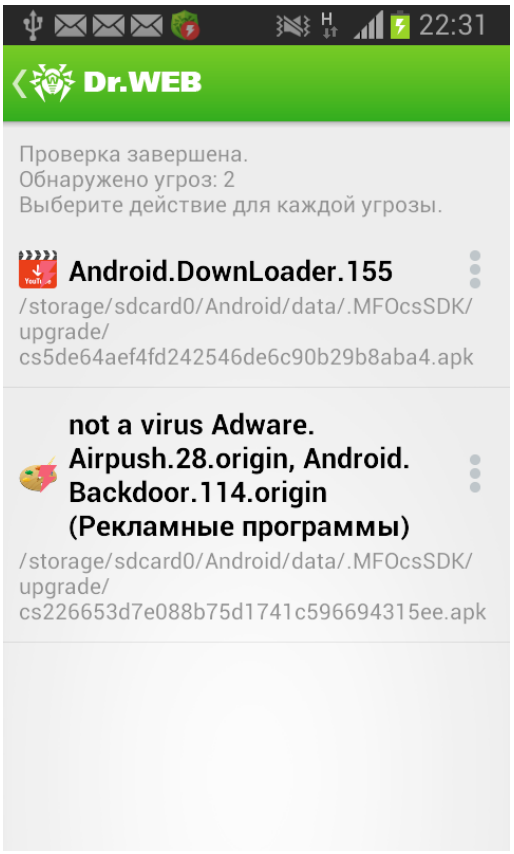
Май 2015	Июнь 2015	Динамика
378	419	+10,85%

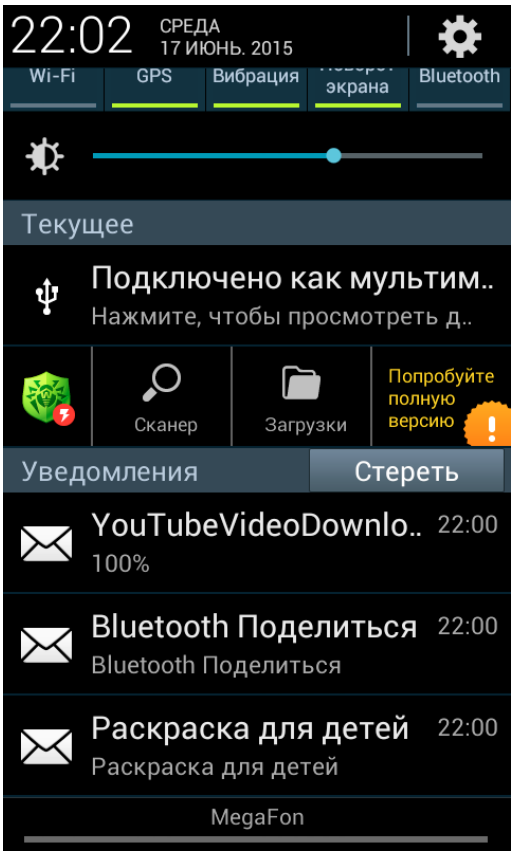
- Android.SmsBot.291
  Банковский троянец, управляемый злоумышленниками удаленно и предназначенный для кражи денежных средств пользователей.
- Android.BankBot.29.origin
  Банковский троянец, крадущий аутентификационные данные у клиентов ряда южнокорейских кредитных организаций. При запуске оригинальных программ интернет-банкинга подменяет их интерфейс своей поддельной копией, в которой запрашиваются все конфиденциальные сведения, необходимые для доступа к управлению банковским счетом. Введенная пользователем информация в дальнейшем передается злоумышленникам. Под видом подписки на некую банковскую услугу пытается установить вредоносную программу Android.Banker.32.origin
- Android.MulDrop.53.origin
  Троянец, предназначенный для распространения и установки на мобильные устройства других вредоносных приложений.
- Android.MulDrop.14.origin
  Троянская программа, предназначенная для распространения и установки на мобильные Android-устройства других вредоносных приложений, в частности, различных банковских троянцев. Распространяется преимущественно среди южнокорейских пользователей.
- Android.BankBot.38.origin
  Android-троянец, предназначенный для кражи денег с банковских счетов владельцев мобильных устройств.
- **Android.BankBot.38.origin**
  Опасный троянец, крадущий различную конфиденциальную информацию и способный выполнять широкий спектр вредоносных действий по команде злоумышленников (в частности, выполнять незаметные звонки, записывать телефонные разговоры, демонстрировать различные сообщения в панели уведомлений и т. п.).

Обзор вирусной активности для мобильных Android-устройств в июне 2015 года

Троянцы-загрузчики

В июне вирусные аналитики «Доктор Веб» обнаружили очередного Android-троянца, предназначенного для загрузки других вредоносных приложений на мобильные устройства пользователей. Эта опасная программа, добавленная в вирусную базу как Android.DownLoader.157.origin, представляет собой внешне безобидную утилиту, которая во время телефонного разговора демонстрирует на экране различную информацию о собеседнике (в частности, страну и регион его проживания, а также название используемого им мобильного оператора). Однако установивших данное приложение пользователей ждет неприятный сюрприз: вскоре после его запуска в информационной панели ОС Android начинают появляться нотификации, внешне похожие на уведомления о входящих сообщениях. Нажатие на эти «сообщения» приводит к загрузке различного ПО, большая часть которого является вредоносным. Более подробная информация о данном троянце приведена в информационной заметке компании «Доктор Веб».





Обзор вирусной активности для мобильных Android-устройств в июне 2015 года

Число записей для троянцев семейства Android.DownLoader в вирусной базе Dr.Web:

Май 2015	Июнь 2015	Динамика
279	310	+11,11%

Android-вымогатели

Серьезную опасность для пользователей мобильных Android-устройств по-прежнему представляют вредоносные программы-вымогатели семейства Android.Locker, блокирующие мобильные устройства под управлением ОС Android и требующие у пользователей выкуп за их разблокировку. В прошедшем месяце вирусная база Dr.Web пополнилась значительным числом новых записей для этих троянцев:

Май 2015	Июнь 2015	Динамика
227	266	+17,2%

СМС-троянцы

В июне было выявлено большое количество новых СМС-троянцев различных семейств. Эти вредоносные приложения незаметно для пользователей отправляют платные СМС-сообщения и подписывают своих жертв на дорогостоящие услуги.

Число записей для СМС-троянцев Android.SmsSend в вирусной базе Dr.Web:

Май 2015	Июнь 2015	Динамика
4204	4745	+12,9%

Защитите ваше Android-устройство с помощью Dr.Web

Обзор вирусной активности для мобильных Android-устройств в июне 2015 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