Dr.WEB®
с 1992 года

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

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

1 октября 2015 года

Главные тенденции сентября

- Серьезная компрометация каталога iOS-приложений App Store
- Обнаружение в каталоге Google Play большого числа троянских программ
- Новые случаи внедрения Android-троянцев в прошивки мобильных устройств
- Появление новых опасных троянцев-вымогателей для ОС Android
- Новые атаки с использованием банковских троянцев

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

Август 2015	Сентябрь 2015	Динамика
12 504	14 033	+12,23%

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

«Мобильная» угроза месяца

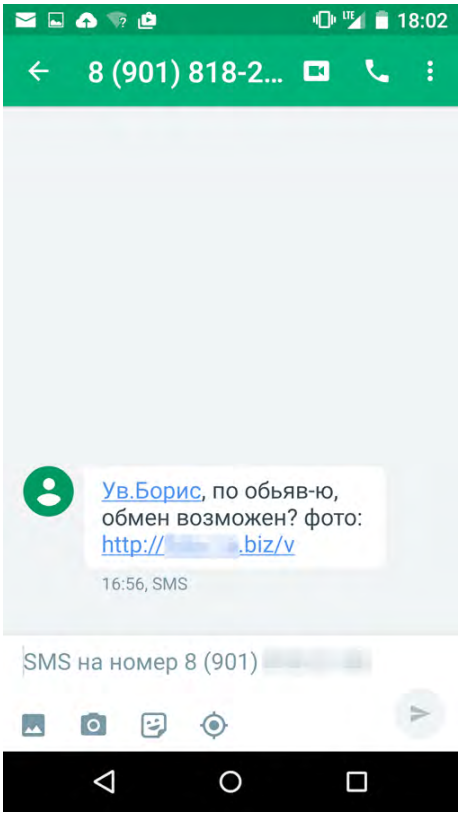
В сентябре одним из самых заметных событий мобильной вирусной тематики стало вскрытие факта массового проникновения опасного троянца IPhoneOS.Trojan.XcodeGhost в официальный магазин iOS-приложений App Store, до этого времени считавшийся наиболее надежным источником программ для владельцев мобильных устройств, работающих под управлением iOS. Это произошло благодаря тому, что изобретательные киберпреступники модифицировали одну из официальных версий среды разработки приложений Xcode, которая незаметно для использующих ее программистов встраивала троянца в создаваемые приложения на этапе их сборки. В результате «зараженные» таким образом изначально безобидные игры и программы успешно прошли предварительную проверку компании Apple и беспрепятственно попали в каталог App Store. Примечательно, что вирусописатели распространяли измененную версию Xcode среди китайских разработчиков, поэтому большинство пострадавших от IPhoneOS.Trojan.XcodeGhost – именно китайские владельцы мобильных устройств под управлением iOS. Однако пользователи из других стран также могли стать жертвами злоумышленников, если загрузили соответствующие троянские версии программ.

После запуска содержащего IPhoneOS.Trojan.XcodeGhost приложения троянец собирает информацию о зараженном мобильном устройстве, включая его тип, название модели и UUID-идентификатор, используемый в настоящее время язык системы, а также данные о сети и отправляет эти сведения на управляющий сервер. Однако главная опасность IPhoneOS.Trojan.XcodeGhost заключается в том, что он способен отображать поддельные диалоговые окна с целью проведения фишинг-атак, открывать заданные злоумышленниками ссылки и даже в ряде случаев красть пароли из буфера обмена.

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

Банковские троянцы

В прошедшем месяце пользователи Android-устройств вновь оказались под прицелом киберпреступников, охотившихся за их деньгами. Так, в начале месяца специалисты компании «Доктор Веб» зафиксировали очередную спам-рассылку СМС-сообщений в адрес пользователей, ранее разместивших те или иные объявления на бесплатных онлайн-сервисах. В распространяемых СМС потенциальным жертвам от имени заинтересованного в объявлении человека предлагалось открыть некую ссылку для получения более подробной информации, при этом в некоторых случаях злоумышленники обращались к пользователям по имени, что могло легко заставить их поверить в обман. В действительности при переходе по указанному веб-адресу на мобильное устройство загружался банковский троянец Android.SmsBot.459.origin, предназначенный для хищения денег со счетов владельцев мобильных Android-устройств. Подробнее об этом инциденте рассказано в соответствующей новостной публикации на нашем сайте.



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

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

Август 2015	Сентябрь 2015	Динамика
495	520	+5%

Троянцы в прошивках

В середине сентября специалисты компании «Доктор Веб» зафиксировали очередной случай заражения троянцем одной из Android-прошивок. Вредоносная программа Android.Backdoor.114.origin, обнаруженная на планшете Oysters T104 HVi 3G, была внедрена злоумышленниками в системный каталог ОС, поэтому ее удаление стандартными методами представляется невозможным и требует либо получения root-полномочий, либо обновления образа операционной системы на заведомо чистую версию. Эта вредоносная программа опасна тем, что способна выполнять незаметную загрузку, установку и удаление приложений по команде с управляющего сервера, при этом она также может самостоятельно активировать отключенную опцию установки ПО из непроверенных источников. Ко всему прочему, троянец собирает и отправляет на удаленный сервер очень обширную информацию о зараженном устройстве. Более подробно об Android.Backdoor.114.origin изложено в материале, опубликованном на сайте компании «Доктор Веб».

Android-вымогатели

В сентябре некоторые производители антивирусных средств сообщили об обнаружении троянца-вымогателя для ОС Android (Android.Locker.148.origin по классификации Dr.Web), использующего якобы новые технические приемы для получения доступа к функциям администратора мобильного устройства, а также блокировки атакуемых смартфонов и планшетов путем установки собственного пароля на разблокировку их экрана. Однако подобный функционал был ранее реализован в других вредоносных программах, в частности, в троянцах Android.Locker.38.origin и Android.BankBot.29.origin, которые известны специалистам «Доктор Веб» еще с 2014 года.

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

Как типичный представитель своего семейства, Android.Locker.148.origin после запуска пытается получить доступ к функциям администратора мобильного устройства, чтобы в полной мере выполнить вредоносные действия, а также осложнить свое удаление в дальнейшем. При этом троянец использует специальный обманный механизм, показывая поверх стандартного системного диалога собственное окно, в котором предлагается установить некое обновление. В действительности же, соглашаясь на установку этого «обновления», пользователь предоставляет троянцу доступ к расширенным системным функциям, после чего тот уже беспрепятственно блокирует атакованный смартфон или планшет, устанавливая пароль на разблокировку экрана, и требует выкуп у своей жертвы.

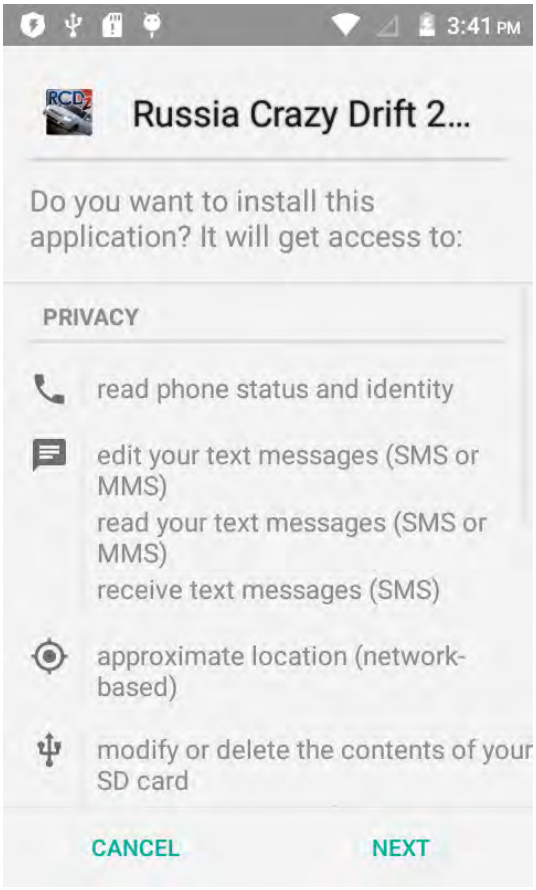
Число записей для Android-вымогателей в вирусной базе Dr.Web:

Август 2015	Сентябрь 2015	Динамика
431	490	+13,7%

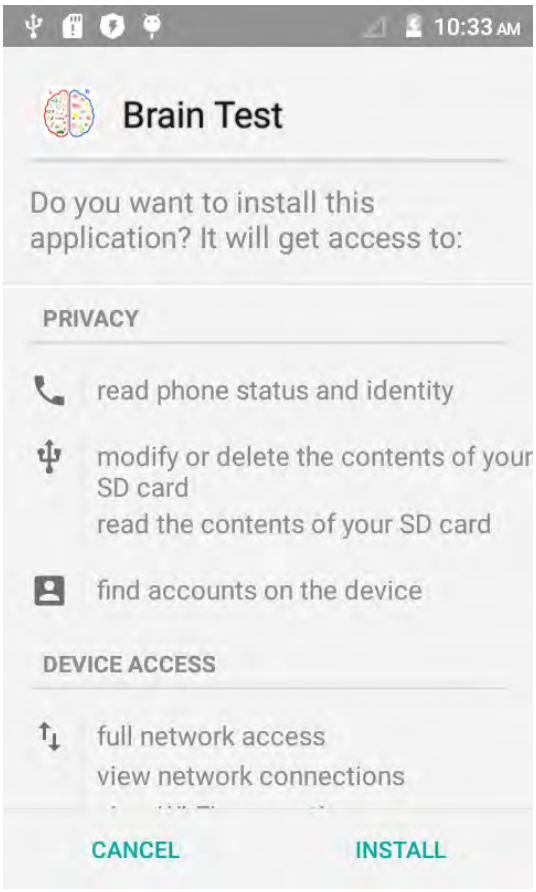
Троянцы в Google Play

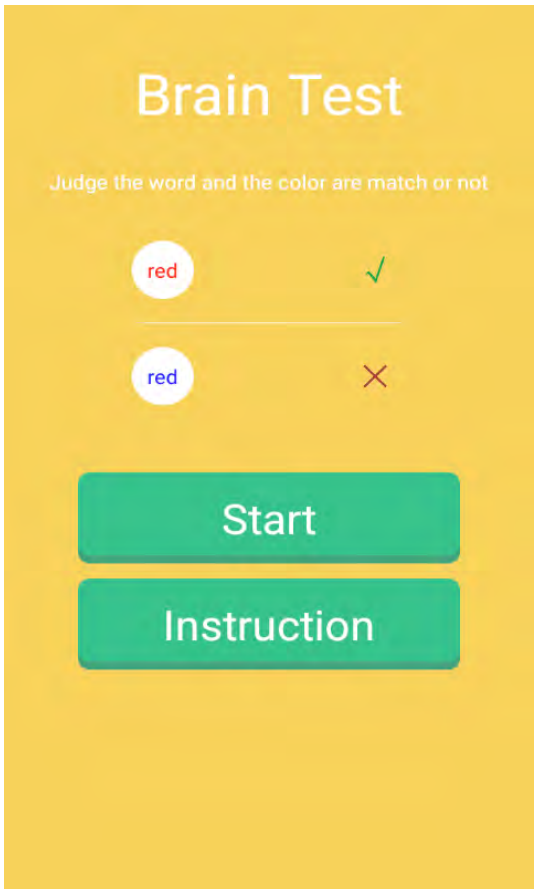
Несмотря на все усилия компании Google, направленные на обеспечение безопасности ее официального каталога приложений для ОС Android, злоумышленники продолжают с успехом внедрять в него различные вредоносные программы. Так, в прошедшем сентябре специалисты по информационной безопасности вновь выявили в Google Play сразу нескольких троянцев. Один из них – Android.MKcap.1.origin – скрывался внутри различных игр и обладал весьма примечательным вредоносным функционалом. В частности, вирусописатели использовали этого троянца для выполнения автоматической подписки на различные платные сервисы. Для этого Android.MKcap.1.origin получал с управляющего сервера определенную ссылку на страницу сайта с премиум-контентом, после чего копировал оттуда проверочное изображение CAPTCHA и загружал его на веб-портал популярного сервиса по распознаванию подобных кодов подтверждения. Как только содержимое изображения расшифровывалось, троянец автоматически передавал полученный результат на исходный веб-сайт с платным сервисом, чтобы завершить регистрацию. При этом в случае если при подписке на услугу сервис высылал дополнительные СМС-сообщения с кодами подтверждений, Android.MKcap.1.origin также автоматически обрабатывал их и передавал сайту необходимые коды.

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



Еще одним троянцем, обнаруженным в каталоге Google Play в сентябре, стал опасный бэкдор Android.Backdoor.273.origin, скрывавшийся внутри приложения с именем Brain Test. Эта вредоносная программа примечательна тем, что использовала ступенчатый алгоритм заражения целевых мобильных устройств. В частности, сам троянец практически не содержит основного вредоносного функционала, необходимого киберпреступникам, и в своей работе полагается на вспомогательные компоненты, которые загружает с удаленного узла. После запуска на инфицированном смартфоне или планшете Android.Backdoor.273.origin поочередно скачивает с управляющего сервера и пытается выполнить несколько эксплойтов, предназначенных для получения root-доступа на Android-устройствах. В случае успеха троянец загружает с сервера свой второй вредоносный компонент (детектируется как Android.DownLoader.173), который незаметно устанавливается в системный каталог и в дальнейшем используется злоумышленниками для загрузки и скрытной инсталляции других вредоносных приложений.





Особенности троянца Android.Backdoor.273.origin:

- после запуска проверяет IP-адрес домена, через который в данный момент осуществляется сетевое подключение на мобильном устройстве, и, в случае обнаружения соответствия адресам компании Google, завершает свою работу (таким образом злоумышленники пытаются обойти антивирусную фильтрацию Bouncer каталога Google Play);
- в зависимости от модификации, вредоносная программа может быть как защищена специальным упаковщиком, шифрующим ее код, так и распространяться без подобной защиты;
- пытается получить root-доступ на зараженном мобильном устройстве при помощи четырех эксплойтов, которые поочередно загружаются с управляющего сервера;
- инсталлирует еще одного троянца, который незаметно загружает и устанавливает различные программы по команде вирусописателей;
- инсталлирует два вспомогательных троянских компонента, которые контролируют целостность друг друга и, в случае удаления одного из них, а также самого Android.Backdoor.273.origin, снова загружают необходимые файлы и повторно инфицируют мобильное устройство.

Также в прошедшем месяце в каталоге Google Play были найден еще один троянец,

замаскированный под безобидные игры и добавленный в вирусную базу Dr.Web как Android.MulDrop.67. В зависимости от модификации, после своего запуска Android.MulDrop.67 может приступить как к немедленному выполнению вредоносных действий, так и выждать 24 часа, чтобы усыпить бдительность потенциальной жертвы. В обоих случаях вредоносная программа извлекает скрытого внутри нее троянца Android.DownLoader.217.origin, которого тут же пытается установить. При этом Android.DownLoader.217.origin запрашивает у пользователя доступ к функциям администратора мобильного устройства, чтобы в дальнейшем уменьшить риск своего удаления. Основное предназначение данных вредоносных приложений – показ рекламы, а также загрузка и установка других троянцев.

Обзор вирусной активности для мобильных Android-устройств в сентябре 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