Dr.WEB®
с 1992 года

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

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

27 октября 2017 года

В октябре в каталоге Google Play был обнаружен очередной Android-троянец, встроенный в безобидные приложения. Он позволял злоумышленникам использовать зараженные мобильные устройства в качестве прокси-серверов. Кроме того, в прошедшем месяце широкую известность получил троянец-вымогатель, который шифровал файлы на Android-смартфонах и планшетах, менял пароль разблокировки экрана и требовал выкуп.

Главные тенденции окнтября

- Появление в СМИ информации об Android-троянце, который изменял PIN-код разблокировки экрана мобильных устройств и шифровал файлы.
- Обнаружение в Google Play вредоносной программы, превращавшей Android-устройства в прокси-серверы.

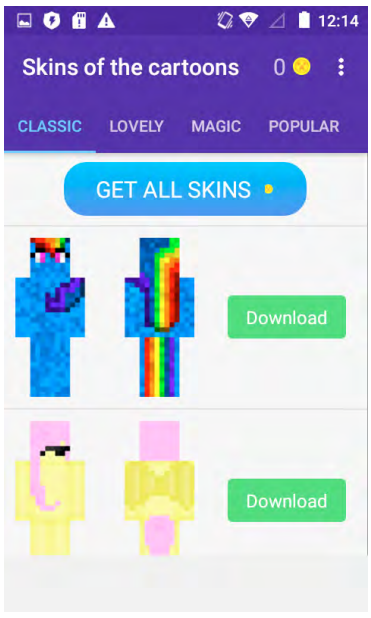
Обзор вирусной активности для мобильных Android-устройств в октябре 2017 года

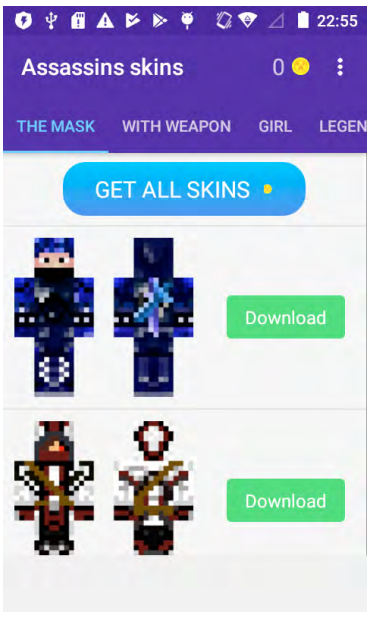
«Мобильная» угроза месяца

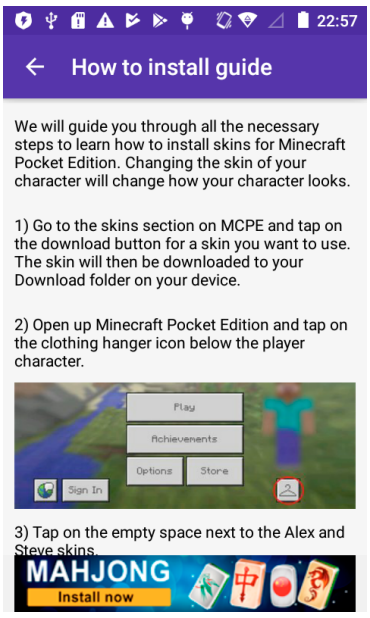
В октябре в каталоге Google Play был выявлен троянец Android.SockBot.5, который был добавлен в вирусную базу Dr.Web еще в июне 2017 года. Злоумышленники встроили его в следующие приложения:

- PvP skins for Minecraft
- Game Skins for Minecraft
- Military Skins for minecraft
- Cartoon skins for Minecraft
- Hot Skins for Minecraft PE
- Skins Herobrine for Minecraft
- Skins FNAF for Minecraft
- Assassins skins for Minecraft

Эти программы позволяли изменять внешний вид персонажей в мобильной версии популярной игры Minecraft.







После запуска троянец незаметно подключался к удаленному командному центру и устанавливал соединение с заданным сетевым адресом, используя протокол SOCKS. В результате киберпреступники превращали смартфоны и планшеты в прокси-серверы и могли пропускать через них сетевой трафик.

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

По данным антивирусных продуктов Dr.Web для Android

- **Android.Click.171.origin**
- **Android.Click.173.origin**
  Троянцы, которые с определенной периодичностью обращаются к заданным веб-сайтам и могут использоваться для накрутки их популярности, а также перехода по рекламным ссылкам.
- **Android.HiddenAds.68.origin**
  Троянец, предназначенный для показа навязчивой рекламы.
- **Android.CallPay.1.origin**
  Вредоносная программа, которая предоставляет владельцам Android-устройств доступ к эротическим материалам, но в качестве оплаты этой «услуги» незаметно совершает звонки на премиум-номера.
- **Android.Sprovider.10**
  Троянец, который загружает на мобильные Android-устройства различные приложения и пытается их установить. Кроме того, он может показывать рекламу.

- **Adware.Jiubang.2**
- **Adware.Fly2tech.2**
- **Adware.SalmonAds.1.origin**
- **Adware.Jiubang.1**
- **Adware.Fly2tech.4**
  Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

Троянец-вымогатель

В прошедшем месяце в СМИ появилась информация о распространении опасного троянца-вымогателя для ОС Android, который изменял PIN-код разблокировки экрана смартфонов и планшетов, шифровал файлы пользователя и требовал выкуп за восстановление работоспособности устройства. Эта вредоносная программа была добавлена в вирусную базу Dr.Web как Android.Banker.184.origin еще в августе 2017 года, поэтому она не представляла опасности для наших пользователей.

После запуска троянец пытается получить доступ к специальным возможностям (Accessibility Service), с использованием которых самостоятельно добавляет себя в список администраторов устройства. Затем он изменяет PIN-код разблокировки экрана, шифрует доступные пользовательские файлы (фотографии, видео, документы, музыку и т. д.) и демонстрирует сообщение с требованием оплаты выкупа. При этом существуют версии вредоносной программы, которые не шифруют файлы размером больше 10 Мбайт.

Несмотря на то что функционал Android.Banker.184.origin в некоторых публикациях называется уникальным, другие троянцы ранее уже использовали аналогичные возможности. Еще в 2014 году компания «Доктор Веб» обнаружила Android-вымогателя Android.Locker.38.origin, который устанавливал собственный код на разблокировку экрана. В том же году появился и первый троянец-энкодер для ОС Android, получивший имя Android.Locker.2.origin. Выполнение же вредоносных действий с использованием функций Accessibility Service (таких, как автоматическое добавление вредоносного приложения в список администраторов) также уже применялось в Android-троянцах, например в Android.BankBot.211.origin.

Злоумышленники по-прежнему пытаются распространять троянцев через официальный каталог Android-приложений Google Play и продолжают совершенствовать вредоносные программы. Для защиты мобильных устройств от потенциального заражения владельцам смартфонов и планшетов необходимо использовать антивирусные продукты Dr.Web для Android.

Обзор вирусной активности для мобильных Android-устройств в октябре 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
125040, 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