Dr.WEB®
с 1992 года

# «Доктор Веб»: обзор вирусной активности для мобильных устройств в июле 2018 года

# Обзор вирусной активности для мобильных устройств в июле 2018 года

## 31 июля 2018 года

В июле 2018 года злоумышленники вновь распространяли опасный Android-бэкдор Android.Backdoor.554.origin, который известен вирусным аналитикам компании «Доктор Веб» еще с апреля 2017 года. Этот троянец шпионил за пользователями и позволял киберпреступникам дистанционно управлять зараженными смартфонами и планшетами. Android.Backdoor.554.origin скрывал в себе Windows-червя, которого копировал на подключенную к мобильному устройству карту памяти для последующего заражения компьютеров под управлением ОС Windows. Кроме того, в уходящем месяце злоумышленники продолжили атаковать владельцев Android-смартфонов и планшетов с использованием банковских троянцев. Один из них, получивший имя Android.Banker.2746, был доступен для загрузки в Google Play. Ряд других банковских троянцев загружала на мобильные устройства вредоносная программа Android.DownLoader.753.origin, которая также была доступна в официальном каталоге программ ОС Android. Кроме того, в течение июля киберпреступники распространяли прочих банковских троянцев для ОС Android. Среди них был Android.BankBot.279.origin, которого вирусописатели выдавали за полезные приложения. Также в июле вирусные аналитики «Доктор Веб» обнаружили несколько новых коммерческих программ-шпионов, получивших имена Program.Shadspy.1.origin и Program.AppSpy.1.origin.

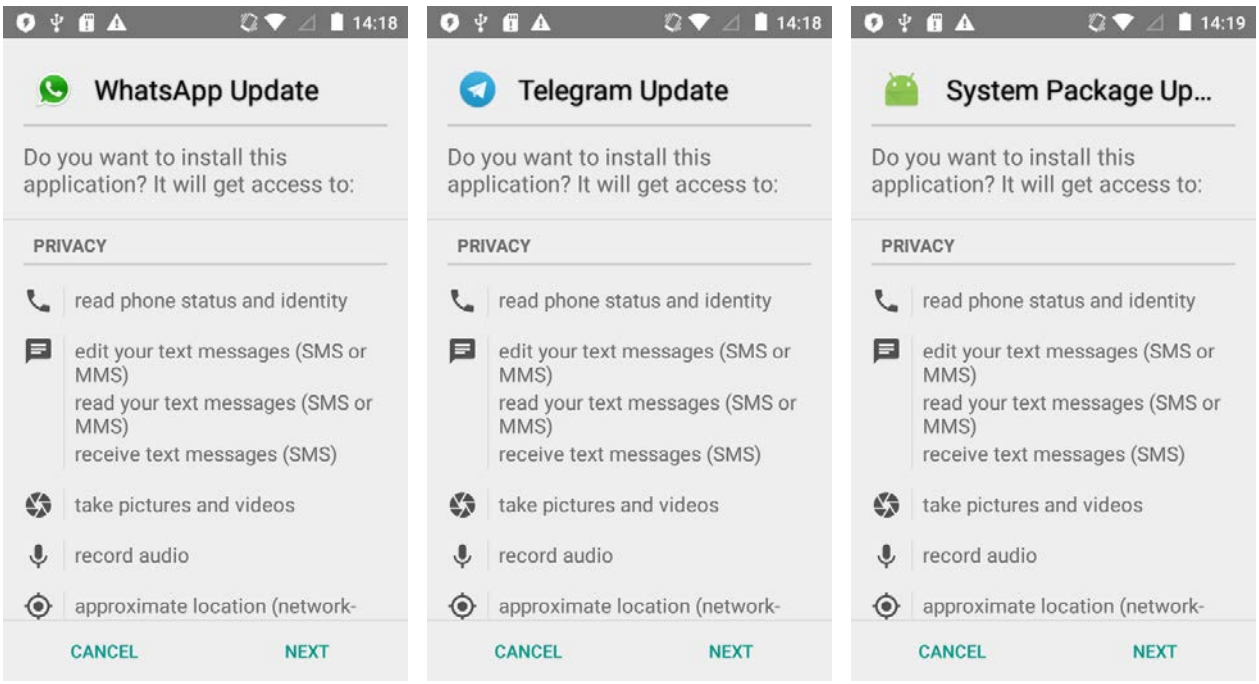
## Главные тенденции июля

- Распространение **Android-бэкдора**, который шпионил за пользователями и помогал злоумышленникам заражать компьютеры под управлением Windows
- Появление в каталоге **Google Play** вредоносных программ
- Распространение банковских троянцев

# Обзор вирусной активности для мобильных устройств в июле 2018 года

## Мобильная угроза месяца

В июле специалисты по информационной безопасности зафиксировали очередную атаку бэкдора Android.Backdoor.**554.origin** на пользователей Android-смартфонов и планшетов. Этот троянец распространялся под видом новых версий известных программ для онлайн-общения, таких как WhatsApp и Telegram, а также системных и других важных обновлений.



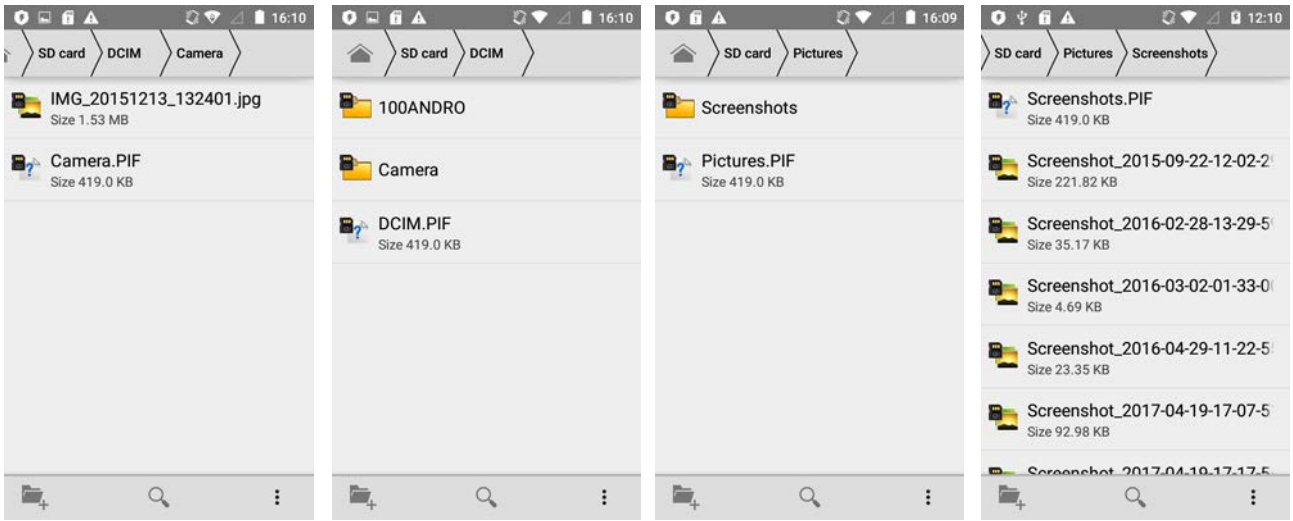

Android.Backdoor.**554.origin** выполнял команды злоумышленников, а также позволял киберпреступникам контролировать зараженное мобильное устройство и шпионить за его владельцем. Троянец отслеживал местоположение Android-смартфона или планшета, перехватывал переписку в популярных программах обмена сообщениями, получал доступ к звонкам и СМС, крал информацию о контактах из телефонной книги и выполнял другие вредоносные действия. Кроме того, этот бэкдор скрывал в своих файловых ресурсах Windows-червя, получившего имя **Win32.HLLW.Siggen.10482**. После заражения мобильного устройства Android.Backdoor.**554.origin** копировал червя на карту памяти, помещая его в каталоги с изображениями. При этом исполняемый файл **Win32.HLLW.Siggen.10482**, имеющий расширение *.pif*, получал имя директории, в которой он размещался. В результате при последующем открытии или копировании этих каталогов на компьютер для просмотра изображений пользователь рисковал запустить червя.

## Мобильная угроза месяца

На следующей иллюстрации показан список директорий, в которые троянец Android.Backdoor.554.origin помещал **Win32.HLLW.Siggen.10482**:

```
SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/DCIM.PIF");
SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/Camera/Camera.PIF");
SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/Facebook/Facebook.PIF");
SpreadPIF(Environment.getExternalStorageDirectory() + "/DCIM/Screenshots/Screenshots.PIF");
SpreadPIF(Environment.getExternalStorageDirectory() + "/Pictures/Pictures.PIF");
SpreadPIF(Environment.getExternalStorageDirectory() + "/Pictures/Screenshots/Screenshots.PIF");
SpreadPIF(Environment.getExternalStorageDirectory() + "/Pictures/Messenger/Messenger.PIF");
```

Примеры успешного копирования исполняемого файла червя в каталоги с изображениями на карте памяти инфицированного Android-устройства:



# Обзор вирусной активности для мобильных устройств в июле 2018 года

## По данным антивирусных продуктов Dr.Web для Android


Android.Altamob.1.origin

Троянская рекламная платформа, которая незаметно загружает и запускает вредоносные модули.

Android.HiddenAds.288.origin

Android.HiddenAds.524

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.Mobifun.4

Троянец, загружающий другие вредоносные приложения.

Android.Xiny.197

Троянец, предназначенный для незаметной загрузки и установки других вредоносных приложений.

# Обзор вирусной активности для мобильных устройств в июле 2018 года

## По данным антивирусных продуктов Dr.Web для Android


Adware.SalmonAds.3.origin

Adware.Altamob.1.origin

Adware.Appalytic.1.origin

Adware.Adtiming.1.origin

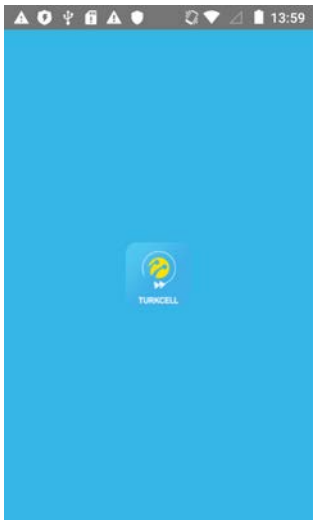
Adware.Jiubang.2

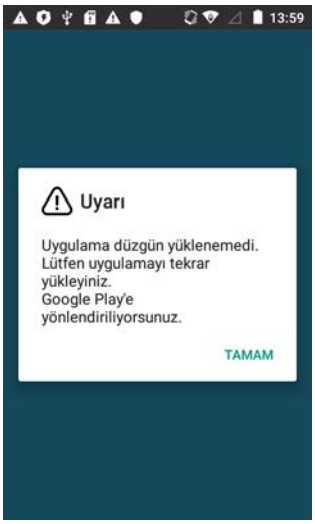
Нежелательные программные модули, встраиваемые в Android-приложения и предназначенные для показа навязчивой рекламы на мобильных устройствах.

## Банковские троянцы

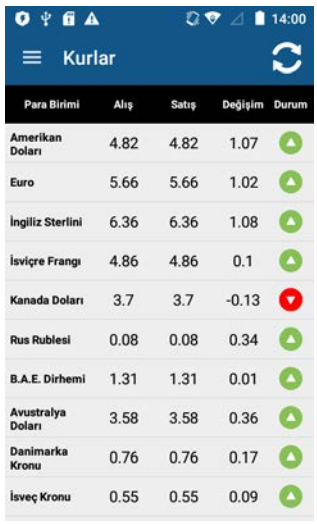
В уходящем месяце специалисты по информационной безопасности обнаружили в каталоге Google Play троянца, по классификации компании «Доктор Веб» получившего имя Android.DownLoader.753.origin. Эта вредоносная программа распространялась под видом финансовых приложений. Некоторые ее модификации действительно выполняли заявленные функции, в то время как остальные были бесполезны и лишь предлагали установить настоящее банковское ПО, загружая его страницы в программе Play Маркет.







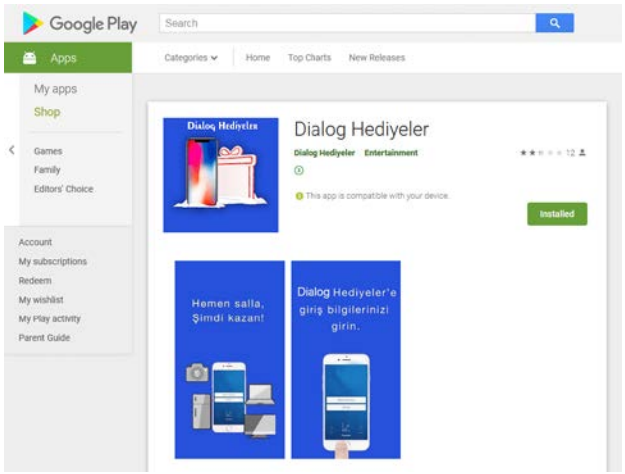




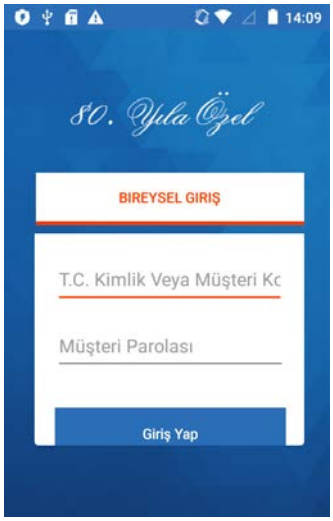

Android.DownLoader.753.origin незаметно скачивал с удаленного сервера одного из банковских троянцев семейства Android.BankBot и пытался установить его, показывая стандартный диалог инсталляции.

## Банковские троянцы

В середине июля специалисты «Доктор Веб» проанализировали Android-банкера, получившего имя Android.Banker.2746. Вирусописатели распространяли этого троянца через каталог Google Play, выдавая вредоносную программу за официальное банковское приложение.




С его помощью они пытались получить доступ к учетным записям клиентов одной из турецких кредитных организаций. Android.Banker.2746 показывал поддельное окно ввода логина и пароля и перехватывал СМС с одноразовыми проверочными кодами.



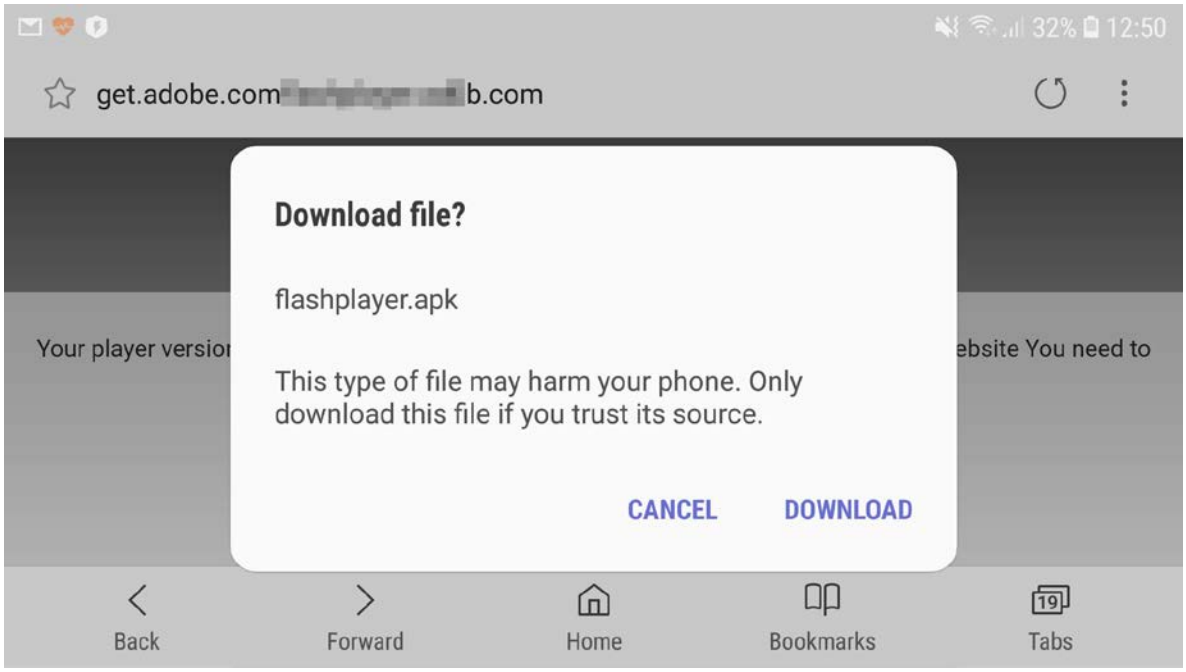

Среди банковских троянцев, атаковавших пользователей в уходящем месяце, была вредоносная программа Android.BankBot.279.origin. Киберпреступники распространяли

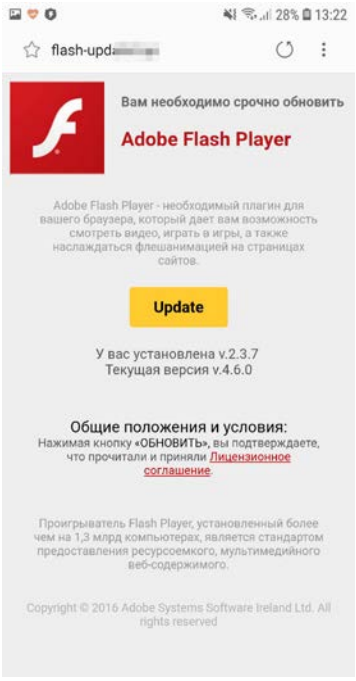
## Банковские троянцы

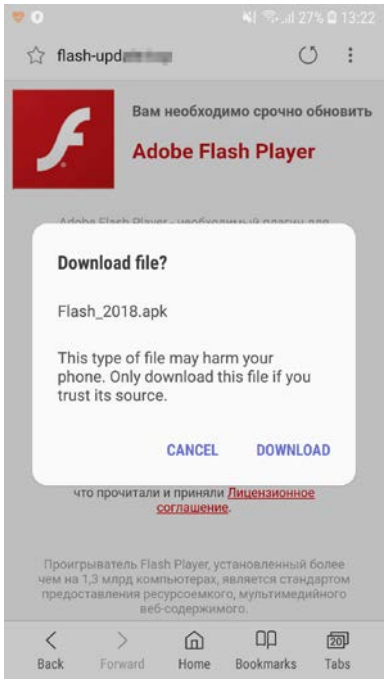
ее с использованием мошеннических веб-сайтов. При посещении одного из них с мобильного устройства троянец загружался под видом безобидных и полезных программ, таких как проигрыватель Adobe Flash Player, программы для онлайн-общения, клиенты для подключения к VPN-сервисам и другое ПО. Android.BankBot.279.origin отслеживал запуск установленных на смартфоне или планшете банковских приложений и показывал поверх их окон фишинговую форму ввода логина и пароля для доступа к учетной записи пользователя. Кроме того, банкер мог менять pin-код разблокировки экрана и блокировать зараженное устройство.
Примеры сайтов, с которых на Android-смартфоны и планшеты скачивался Android.BankBot.279.origin:

# Обзор вирусной активности для мобильных устройств в июле 2018 года

## Банковские троянцы




# Обзор вирусной активности для мобильных устройств в июле 2018 года

## Программы-шпионы

В уходящем месяце специалисты «Доктор Веб» обнаружили несколько новых коммерческих программ-шпионов. Одна из них получила имя Program.AppSpy.1.origin. Она отслеживает местоположение зараженного устройства, прослушивает телефонные звонки и перехватывает СМС-сообщения. Другая программа для кибершпионажа была добавлена в вирусную базу Dr.Web как Program.Shadspy.1.origin. Это приложение обладает обширным функционалом. Program.Shadspy.1.origin отслеживает СМС-переписку, телефонные звонки, местоположение устройства, выполняет запись окружения с использованием встроенного микрофона, копирует историю посещения сайтов из веб-браузера, информацию о запланированных событиях из календаря пользователя, может делать снимки при помощи камеры смартфона или планшета, а также выполнять ряд других действий. Кроме того, при наличии root-полномочий Program.Shadspy.1.origin может перехватывать переписку в программах Facebook и WhatsApp.

Банковские троянцы представляют серьезную опасность для владельцев мобильных устройств. Злоумышленники продолжают распространять эти вредоносные программы не только с помощью мошеннических сайтов, но и через официальный каталог программ Google Play. Для защиты от этих и других Android-троянцев пользователям следует установить антивирусные продукты Dr.Web для Android.

# Обзор вирусной активности для мобильных устройств в июле 2018 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 | free.drweb.ru | www.av-desk.ru
«Доктор Веб» в других странах