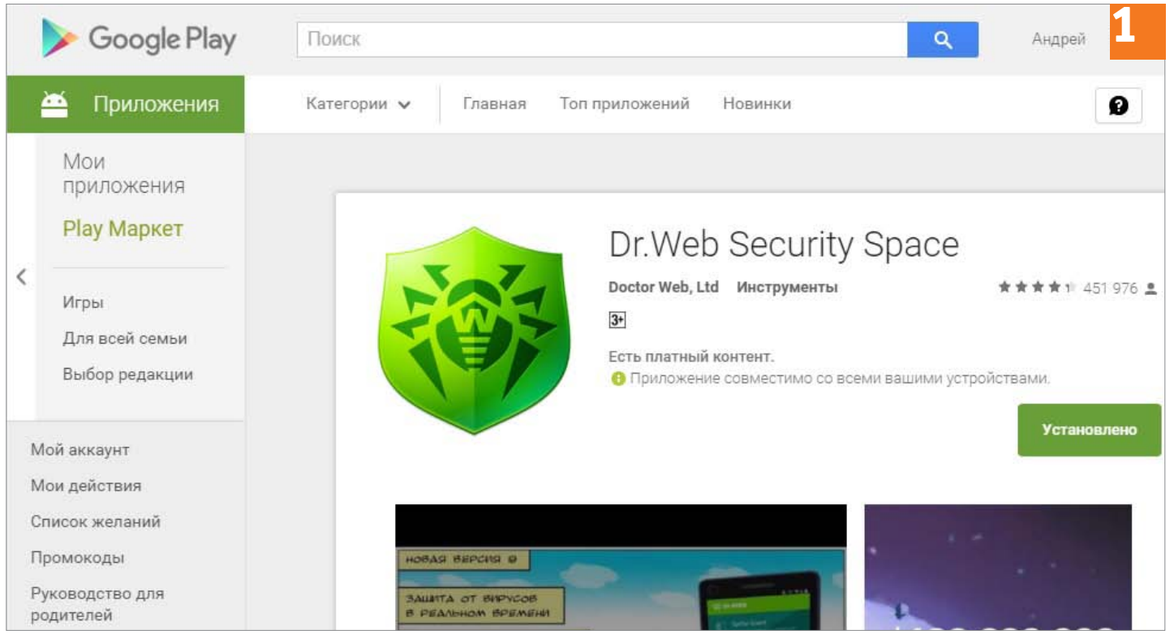


Как обнаружить и удалить руткит со смартфона

Даже если вы осторожны при скачивании новых приложений, это не гарантирует безопасность – при проверке антивирусом можно обнаружить неприятные сюрпризы. CHIP расскажет, как избавить смартфон от троянцев и руткитов.

В конце прошлого года отечественные антивирусные компании забили тревогу: как оказалось, вирус может быть уже изначально интегрирован в заводскую прошивку, поэтому обнаружить и удалить его обычными средствами затруднительно или совсем невозможно. Так, в октябре прошлого года специалисты «Доктор Веб» обнаружили в прошивке Android-смартфона Philips S307 вредоносное программное обеспечение. Руткит под названием Android.Cooee.1 был встроен в графическую оболочку устройства, и его основная цель заключалась в демонстрации пользователю навязчивой рекламы. Также, на смартфон без разрешения владельца загружалось и устанавливалось различное ПО. Можно было бы предположить, что вирус попал на смартфон по вине самих владельцев. Однако, как уверяет программист-исследователь «Доктор Веб» Александр Свириденко, в случае с Philips S307 вирус не предустановился случайно и тем более не устанавливался вручную. По его словам, «Доктор Веб» делал запрос в службу поддержки Philips и получил прошивку с тем же троянцем. Надо отметить, что с такого рода троянцами антивирусные компании ранее уже сталкивалась – на прошивках смартфонов Lenovo и Xiaomi.

Руткиты требуют больше прав

Основной принцип обеспечения безопасности на Android-устройствах состоял в том, что программу можно установить только лишь с согласия пользователя с предварительным ознакомлением требуемых для ее прав. Т.к. многие приложения действительно запрашивали слишком много возможностей, то пользователи стали менее внимательны и соглашались на установку в любом случае. Этим не преминули воспользоваться вирусописатели и стали снабжать безобидные на первый взгляд программы (например, фонарик) троянцами с различными root-эксплойтами. Это давало злоумышленникам неограниченные полномочия на атакуемых смартфонах и планшетах. Современные root-троянцы внедряются в системный каталог Android и, оставаясь в нем скрытыми, продолжают свою работу, даже если установившую их вредоносную программу найдут и удалят.

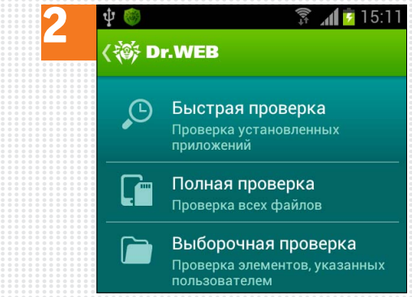
CHIP расскажет, как найти и удалить руткит со смартфона или планшета с помощью антивируса Dr.Web Security Space.

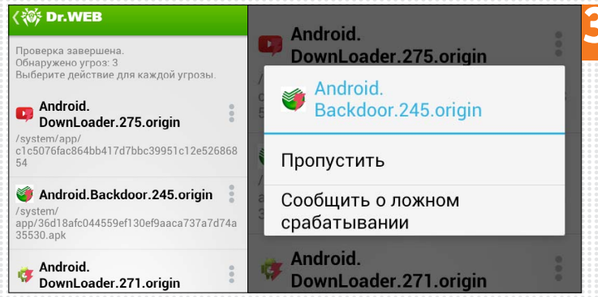
ФОТО: компании-производители;

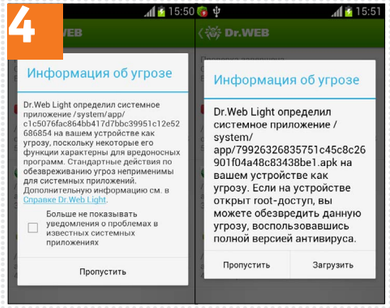
Как это сделать:

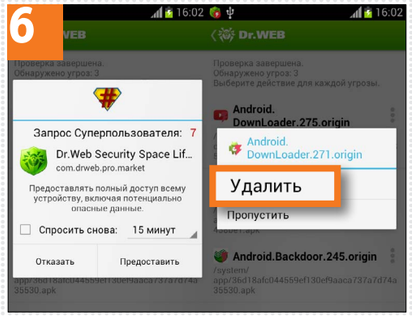
1 Устанавливаем антивирус

Если у вас возникли подозрения, что девайс заражен вирусом или руткитом, скачайте с Google Play бесплатную версию Dr.Web Light. Эта версия способна обнаружить руткит, однако удалить и обезвредить вирус способна только версия Dr.Web Security Space для Android. Впрочем, всем пользователям Dr.Web Security Space для настольных компьютеров она доступна бесплатно.









2 Выполняем полную проверку

После установки приложения зайдите в раздел «Сканер» и кликните по «Полная проверка». Запустится сканирование памяти смартфона и встроенного и внешнего (флешкарта) хранилища файлов.

3 Отправляем вирус на анализ

Если антивирус нашел троянскую программу в системной области, но она не известна как руткит, можно либо пропустить ее, либо отправить на анализ через кнопку «Ложное срабатывание».

4 Удалить или вылечить

Если троян опознан как известный руткит и он находится в жизненно важной части ОС, то не следует торопиться его удалять, т.к. это может привести к повреждению системы и поломке устройства. Возможны два варианта действий.

5 Следуем инструкциям

Если антивирус определил системное приложение на вашем устройстве, как угрозу и сообщил, что некоторые его функции характерны для вредоносных программ, то следует для начала ознакомиться с информацией, изложенной на ресурсе https://drw.sh/xvahqv и выполнить рекомендованные там операции.

6 Удаляем вирус

В случае, если антивирус сообщает, что удаление угрозы безопасно, нажмите кнопку «Удалить» (только в Pro-версии). Однако, это возможно только в случае, если на смартфоне пользователь имеет рут-права.

7 Получаем рут-права

Если смартфон пользователя не рутован, то придется либо выполнить операцию получения рут-прав, либо отказаться от использования устройства. В первом случае вы можете обратиться в техподдержку производителя смартфона или попытаться найти инструкцию по рутованию вашей модели смартфона самостоятельно.

8 Ставим предыдущую прошивку

Если получение рут-прав невозможно, то имеет смысл сначала сделать резервную копию всех пользовательских данных и после этого выполнить операцию сброса настроек до заводских и перепрошивки устройства на более раннюю (предполагается, что она была без вируса). В случае, если у зараженного девайса только одна прошивка, лучше временно отказаться от его использования и обратиться в техподдержку производителя устройства для решения вопроса по обновлению ПО.