

Анализ потребления ресурсов для детектирования вредоносной активности в мобильном окружении

Али Абдулмаджидов, Эмиль Шарифуллин

17.01.17

Сегодня мобильные устройства стали очень популярны и их "экспансия" растет. В добавок к смартфонам, у нас есть интернет вещей, который часто работает под управлением мобильных операционных систем (iWatch, Samsung Gear). В результате пользователи доверяют очень важную информацию (доступ к банковскому счету и.т.д) этим девайсам, что делает их очень сладкой целью для злоумышленников. Судя по отчету McAfee в 2016 году обнаруживалось в среднем от 1000 до 6000 вирусов в час.

Уже существуют множество способов обнаружения вредоносных програм. Некоторые из исследователей предложили искать вирусы по потреблению энергии. В нашей работе, мы пошли немного дальше и попытались доказать или опровергнуть возможность обнаружения вредоносной активности в перепакованных приложениях на основе потребления ресурсов.