Вредоносная программа, использующая уязвимость ОС Android, обнаружена производителем антивирусов Dr. Web, говорится в официальном сообщении компании. Троян, который внесен в вирусную базу под названием Android.Nimefas.1.origin, способен отправлять SMS без ведома пользователя, передавать злоумышленникам конфиденциальную информацию и выполнять ряд команд, полученных с удаленного управляющего узла. Программа заражает смартфоны под управлением ОС Android при установке приложений, используя уязвимость Master Key. Эта уязвимость была недавно обнаружена специалистами компании Bluebox Security. Суть уязвимости — в методе обработки устанавливаемых программ одним из компонентов Android: если в подкаталоге apk—пакета содержатся два файла с одинаковым названием, проверяется цифровая подпись только первого файла, а второй устанавливается без проверки. Android.Nimefas.1.origin как раз является тем самым вторым одноименным dex-файлом, модифицированным киберпреступниками, и уязвимость позволяет легко обходить защиту операционной системы.

Новый троян, запустившись на инфицированном мобильном устройстве, проверяет активность антивирусов и наличие root-доступа. В случае если таковых не обнаружено, Android.Nimefas.1.origin отправляет IMSI (международный идентификатор мобильного абонента) на случайный номер из адресной книги зараженного телефона. Затем вирус рассылает по базе контактов SMS с текстом, загруженным с удаленного узла управления. Сама база контактов в свою очередь передается на сервер злоумышленников. Кроме того, Android.Nimefas.1.origin способен скрывать входящие сообщения от пользователя, используя фильтр по номеру или тексту SMS, также полученный с узла управления. Троян распространяется вместе с приложениями, доступными для загрузки с одного из китайских сайтов-каталогов ПО. Руководство сайта оповещено об угрозе для пользователей, а удаленный сервер, который использовался злоумышленниками для управления Android.Nimefas.1.origin, на данный момент уже не функционирует. Однако техническая легкость, с которой возможен взлом Android через уязвимость Master Key, делает весьма вероятным широкое распространение похожего вредоносного ПО во всем мире в ближайшее время.