Компания "Доктор Веб" опубликовала на своем официальном сайте интересную информацию о вирусе из семейства Win32.Rmnet, который «научился» отключать антивирусное ПО.

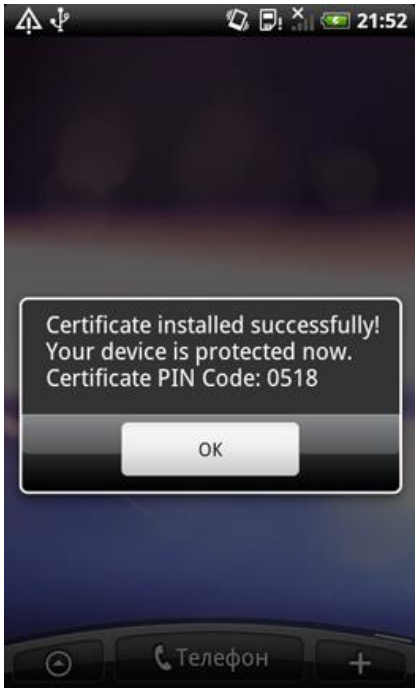
Trojan.Rmnet.19 - модификация известного зловреда Win32.Rmnet. По данным Dr.Web, этим вирусом заражено уже не менее 18 000 компьютеров. Выделяет Trojan.Rmnet.19 из среды себе подобных способность отключать антивирусные программы, эмулируя нажатия мышью на определенные значки. Целью атаки выбраны такие известные и популярные антивирусы, как Avast, Microsoft Security Essential, Norton Antivisus, Eset NOD32, Bitdefender, AVG.

Всего Trojan.Rmnet.19 загружает на зараженный компьютер семь различных модулей:

- новый модуль, позволяющий отключать антивирусные программы;
- модуль для кражи файлов cookies;
- локальный FTP-сервер;
- модуль для выполнения веб-инжектов;
- модуль для кражи паролей от FTP-клиентов;
- новый модуль, позволяющий детектировать наличие виртуальных машин;
- модуль для организации удаленного доступа к инфицированной системе.

По данным антивирусной лаборатории "Доктор Веб", основной мишенью для атаки Trojan.Rmnet.19 стали Великобритания и Ирландия.

Также компания «Доктор Веб» обнаружила новую вредоносную программу для платформы Android, способную перехватывать входящие SMS и перенаправлять их злоумышленникам. Троянец Android.Pincer.2.origin представляет серьезную опасность для пользователей, поскольку в украденных им сообщениях могут находиться в том числе и проверочные mTAN-коды, которые используются различными финансовыми системами типа «Банк-Клиент» для подтверждения денежных операций, а также другая конфиденциальная пользовательская информация.



Троянец, обнаруженный специалистами компании «Доктор Веб» несколько дней назад, является вторым известным представителем семейства Android.Pincer. Как и ее предшественник, обновленная вредоносная программа распространяется под видом сертификата безопасности, который якобы требуется установить на мобильное Android-устройство. В случае если неосторожный пользователь выполнит установку и попытается запустить троянца, Android.Pincer.2.origin продемонстрирует ложное сообщение об успешной установке сертификата, после чего до поры до времени не будет проявлять сколько-нибудь заметной активности. В случае успешного старта при очередном включении мобильного устройства Android.Pincer.2.origin подключается к удаленному серверу злоумышленников и загружает на него ряд сведений о мобильном устройстве. Далее вредоносная программа ждет поступления от злоумышленников управляющего SMS-сообщения. Киберпреступниками предусмотрены следующие директивы: начать перехват сообщений с указанного номера; отправить SMS с указанными параметрами; вывести сообщение на экран мобильного устройства; изменить адрес управляющего сервера; отправить SMS с текстом pong на заранее указанный номер; изменить номер, на который уходит сообщение с текстом pong.

Команда start_sms_forwarding представляет особенный интерес, поскольку позволяет злоумышленникам указывать троянцу, сообщения с какого номера ему необходимо перехватить. Данная функция дает возможность использовать вредоносную программу как инструмент для проведения таргетированных атак и красть, таким образом, специфические SMS-сообщения, например, сообщения от систем «Банк-Клиент», содержащие проверочные mTAN-коды, либо конфиденциальные SMS, предназначенные для самых разных категорий лиц: от простых пользователей до руководителей компаний и государственных структур.