Продемонстрированный немецкими специалистами метод позволяет взламывать SIM-карты и устанавливать на них Java-апплеты, открывающие широкий простор для действий злоумышленников.

Исследователи из немецкой лаборатории Security Research Labs продемонстрировали способ установки в SIM-карту мобильного телефона вредоносного кода. Метод основан на уязвимости в SIM-карте. Специалисты утверждают, что под угрозой находятся миллионы владельцев мобильных аппаратов.

Взлом осуществляется с помощью технологии Over-the-air (OTA), которая позволяет устанавливать на телефон программное обеспечение «по воздуху», то есть через сети сотовой и беспроводной связи. Данная технология, в том числе, позволяет устанавливать Java-апплеты в SIM-карту.

Команды OTA представляют собой закодированные SMS-сообщения, при этом для шифрования сообщений используется устаревший стандарт DES (Data Encryption Standard), разработанный в 70-х годах.

Для того чтобы взломать SIM-карту, на первом этапе необходимо получить ключ шифрования DES. Делается это следующим образом: атакующий посредством OTA отправляет на мобильный телефон SMS-сообщение с произвольным бинарным кодом. Телефон, получив неправильную команду, в ответ отправляет аналогичное бинарное сообщение об ошибке, в котором содержится ключ шифрования. Далее с помощью радужных таблиц данный 56-битный ключ расшифровывается на обычном персональном компьютере за 2 минуты.

На втором этапе атакующий снова отправляет на телефон SMS-сообщение с бинарным кодом, которое, благодаря раскрытию ключа шифрования, имеет подлинный вид и принимается телефоном. Данное сообщение содержит в себе Java-апплет, который успешно устанавливается на SIM-карту. Такой апплет может без согласия и ведома пользователя отправлять SMS-сообщения, изменять номера голосовых ящиков, передавать информацию для определения местоположения телефона и пр.

Помимо прочего, Java-апплет может передавать платежные данные пользователя, которые в некоторых случаях хранятся на SIM-картах, добавляют исследователи в своем блоге. «Перед хакерами открывается масса возможностей для совершения преступлений», - считают эксперты.

Существует несколько методов защиты от описанной выше атаки. Например, можно использовать более современные стандарты шифрования, такие как AES, или установить в телефон брандмауэр, который защитит пользователя от SMS-сообщений из неизвестных источников.

Исследователи лаборатории Security Research Labs планируют представить описанный выше метод взлома SIM-карт на конференции BlackHat 31 июля и 3 августа на хакерском фестивале OHM.

Добавим, что это не первый случай, когда уязвимость находят в базовых технологиях сотовой связи. В 2011 г. эксперты этой же немецкой лаборатории уже предупреждали о том, что в операторы используют достаточно простые механизмы защиты, что открывает широкий просто для действий злоумышленников. В 2010 г. специалист по информационной безопасности
Крис Пейджет
(Chris Paget)
продемонстрировал
, как любой желающий может перехватывать телефонные звонки, используя оборудование за $1,5 тыс.

Источник

родемонстрированный немецкими специалистами метод позволяет взламывать SIM-карты и устанавливать на них Java-апплеты, открывающие широкий простор для действий злоумышленников.

Подробнее: http://www.cnews.ru/top/2013/07/22/naydena_uyazvimost_v_simkartah_pod_ugrozoy_milliony_mobilnikov_536222