ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ*

Как уже снова не получить телефон (почти) любой красотки в Москве, или интересная особенность MT_FREE

ИЗ ПЕСОЧНИЦЫ

cab404 13 марта в 20:27 35,9k

UPD 14.03 8:21 — Телефон больше не получить. Остальные интересные данные пока остались.
UPD 14.03 10:39 — Дабы не очернять ребят из *саппорта* MaximaTelecom: Сообщил о ней я окольными путями, но раз пять переспросил и уточнил, дошло ли моё письмо до адресата — короче говоря, убедился, что оно у эфемерного (имена просили молчать) ответственного за вафли лица в метро. Я признаю, что это тупо, но цепочка "проблема в мосметро" → "у меня уже были связи со всяким мос, надо позвонить им" мне показалась весьма и весьма логичной в момент обнаружения уязвимости.
UPD 14.03 15:40 — Уязвимость была найдена в uid Antxak — суть в том, что в uid лежит md5 телефона без соли. Снова можно искать телефоны.

Пример намайненного телефона

UPD 14.03 18:55 — Уязвимый хэш в uid был заменен на тот же, что и в телефоне. Пока не раскололи последний.

Сеттинг

В Московском метрополитене есть такая замечательная вещь, как бесплатный вайфай.
Единственное, что вам нужно, чтобы войти в него — это ввести свой номер телефона. И так как метро — штука хоть и удобная, но зачастую долгая, бесплатной сетью пользуются практически все. В этом интересном мире нам понравилась девушка за столом напротив.

Небольшая уязвимость

Авторизация в этой сети привязывается по мак-адресу, который всегда можно сменить — например на любой пойманный в воздухе вокруг. Поймать мак-адреса можно, например, утилитой airodump-ng. Иногда даже можно войти в wi-fi не смотря рекламу, если реальный владелец мак-адреса оплатил премиум-доступ.

Слив данных о самом себе

Но если вы не в числе оплативших wi-fi, то вас при подключении поприветствует страничка auth.wi-fi.ru. Помимо рекламы, эта страничка отдает один интересный json, который содержит кучу интересной информации о текущем подключенном пользователе.

Даже если вы оплатили премиум-доступ, эту страничку всегда можно открыть, просто вбив в браузере адрес.

Много интересной информации

Замечу, что номер телефона не закрыт звездочками в реальных данных.

И, собственно, как узнать номер красотки

Я почти уверен, что все вы догадались, как пойдет наш сценарий.

Ева очень хочет узнать телефон Алисы за столом напротив (forbidden love!). Как и большинство людей в Москве, пользуясь телефоном, Алиса так же пользуется и сетью MT_FREE.

Ева следит за Алисой некоторое время, и узнает её MAC с помощью утилиты airodump-ng, широко доступной и работающей практически на любой вафельнице. Узнав его, она следует в метро, меняет свой мак на мак Алисы, открывает страничку auth.wi-fi.ru и получает желанный номер.

Мне лень даже проверять это

Но постой, потенциальная Ева! Чтобы упростить труд перебирания десятков маков из забегаловки в ~~поиске телефона~~ твоем кропотливом исследовании безопасности wi-fi, я сделал небольшой скрипт! Его ты сможешь найти внизу статьи.

To be continued?

Работает получение данных о юзере пока только в метро, т.к удаленно у меня ещё не получилось убедить сервер в том, что мак у меня не 00:00:00:00:00:00. Раньше была возможность

передавать мак в параметре client_mac, но аналога я пока не нашел.

Дисклеймер

Я сообщил об уязвимости (наверняка это делали до меня, эта штука очевидна до нельзя) неделю назад, и так и не получив никакого ответа, решил раскрыть её тут.

Всё описанное выше дисклеймера написано от лица вымышленного персонажа, и является художественной литературой. Его мотивы не совпадают с моими, и я это делаю исключительно в исследовательских целях. И даже не особо понимаю, что мне делать с телефоном красотки, которая мне его не дала.

Я не буду показывать на руководство пользования airodump-ng, чтобы не снизить уровень вхождения совсем до нуля.

Скрипт

Для тех, кому просто посмотреть

Пример работы

Ссылка на скрипт в GitHub Gist

Для работы скрипта из зависимостей нужен только curl, json_pp, и желательно иметь новый oui.txt в /var/lib/ieee-data/ (скачать отсюда)

Если Wi-Fi интерфейс у вас называется не wlp1s0, то смените его в скрипте.

Использование: `./checkmacs.sh [файл с маками на каждой строке]`

Спасибо за прочтение!

UPD: обновил зависимости

Комментарии (77)

Похожие публикации

SIM-карты пассажиров московского метро подвергнутся бесконтактному считыванию

237

Mithgol • 29 июля 2013 в 18:09

Официальный сайт Московского метрополитена затроянили 76

Lux_In_Tenebris • 15 января 2010 в 23:46

Московская подземка обзаведется 3G в 2009 55

Tylerskald • 23 января 2009 в 13:24

Популярное за сутки

Наташа — библиотека для извлечения структурированной информации из текстов на русском языке 14

alexkuku • вчера в 16:12

Unit-тестирование скриншотами: преодолеваем звуковой барьер. Расшифровка доклада 4

lahmatiy • вчера в 13:05

Люди не хотят чего-то действительно нового — они хотят привычное, но сделанное иначе 25

ПЕРЕВОД

Smileek • вчера в 10:32

Руководство по SEO JavaScript-сайтов. Часть 2. Проблемы, эксперименты и рекомендации 2

ПЕРЕВОД

ru_vds • вчера в 12:04

Как адаптировать игру на Unity под iPhone X к апрелю 0

P1CACHU • вчера в 16:13

Лучшее на Geektimes

Стивен Хокинг, автор «Краткой истории времени», умер на 77 году жизни 33

HostingManager • вчера в 13:49

Обзор рынка моноколес 2018 70

lozga • вчера в 06:58

«Битва за Telegram»: 35 пользователей подали в суд на ФСБ 40

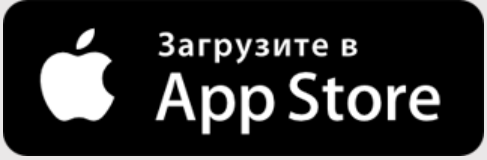
alizar • вчера в 15:14

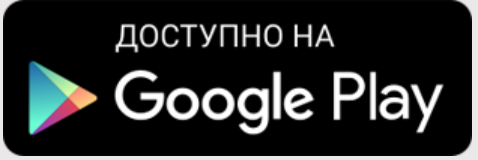
Стивен Хокинг и его работа — что дал ученый человечеству? 8

marks • вчера в 14:46

Sunlike — светодиодный свет нового поколения 17

AlexeyNadezhin • вчера в 20:32





Полная версия