УДК 004.715

Загребин А.В.
Студент 3 курса ПГУТИ,
г. Самара, РФ
Научный руководитель: Чернова С.В.
с.п. кафедры ПОУТС ПГУТИ,
г. Самара, РФ

НАСКОЛЬКО БЕЗОПАСНЫ БЕСПРОВОДНЫЕ СЕТИ WI-FI?

Аннотация: *в данной статье проанализированы современные уязвимости Wi-Fi сетей и способы защиты от данных типов уязвимостей, приведена статистика, насколько пользователи подвергают себя риску при использовании Wi-Fi сетей.*

Ключевые слова: *снифферы, человек посередине, Wi-Fi адаптер, роутер, социальная инженерия.*

Annotation: *this article analyzes the current vulnerabilities of Wi-Fi networks and ways to protect against these types of vulnerabilities, provides statistics on how users are at risk when using Wi-Fi networks*

Key words: *sniffers, man in the middle, Wi-Fi adapter, router, social engineering.*

В современном мире почти у каждого человека есть смартфон, планшет или ноутбук. Для связи с внешним миром им нужен доступ в интернет. В основном это беспроводные сети, которые находятся абсолютно везде - дома, в кафе или в метро. Беспроводные сети Wi-Fi часто используются хакерами, желающими быстро и без особого риска получить необходимые для себя данные. Взломать сеть Wi-Fi намного проще, поскольку она практически ничем не защищена.

Зачастую пользователи хранят на своих смартфонах, планшетах или ноутбуках множество личной информации: фото, видео, банковские счета и др. При подключении к незащищенной беспроводной Wi-Fi сети и пересылке каких-либо данных, у злоумышленников появляется возможность их перехватить. Заполучить данные пользователей можно при помощи разных видов атак на беспроводные сети Wi-Fi. Подробнее рассмотрим некоторые из них:

Rogue AP — фальшивые беспроводные точки доступа Wi-Fi

Современная техника запоминает название сети Wi-Fi, к которой она подключалась успешно хотя бы один раз, и, если она видит идентичное название сети, то, соответственно, подключается без каких-либо проблем. Данный тип атаки подразумевает создание беспроводной поддельной точки доступа Wi-Fi (rogue AP), к которой гаджет был когда-либо подключен. Используя данную функцию гаджетов, пользователь рискует стать жертвой атаки «человек посередине» (man in the middle). Если все же у гаджета отсутствует функция автоматического подключения, то так же в ход может вступить так называемая “социальная инженерия”. Работает она очень легко, ведь проще всего взломать не машину, а человека. То есть, человек сам подключается к знакомой ему сети, например, в кафе, в то время как злоумышленник, при помощи Wi-Fi jammer (глушилка Wi-Fi), отключает его от Wi-Fi сети. Ничего не понимающий пользователь подключается снова, только уже к Wi-Fi сети злоумышленника. Далее при помощи все той же атаки «человек посередине» (man in the middle), злоумышленник перехватывает трафик и находит нужную информацию.

Сотрудники компании Avast в преддверии международной выставки Mobile World Congress 2016 провели своеобразный эксперимент. За день до открытия в аэропорту Барселоны было развернуто несколько Wi-Fi-точек доступа с SSID-идентификаторами Starbucks, Airport_Free_Wifi_AENA и MWC Free WiFi. Целью Avast была демонстрация того, насколько

пользователи подвергают себя риску при использовании Wi-Fi сетей. Всего за четыре часа специалисты Avast перехватили более 8 млн пакетов данных от более двух тысяч пользователей. Для сохранения приватности пользователей все данные сразу же удалялись. Компании удалось собрать следующую статистику в ходе эксперимента:

50,1 % пользователей использовали устройство Apple, 43,4 % — гаджет под управлением Android, 6,5 % — устройства с Windows Phone;

61,7 % посетителей выставки занимались поиском в Google и проверяли свою почту Gmail;

14,9 % воспользовались поиском Yahoo;

приложение Facebook было установлено на 52,3 % устройств, а Twitter оказался менее популярен — всего 2,4 %

Защититься от данного вида атак можно простым отключением Wi-Fi адаптера при выходе из дома. Так же поможет включение функции «подтверждение подключения» даже к известным сетям. А от “социальной инженерии” существует только один способ защиты - это внимательность пользователя.

Sniffing – анализатор трафика

Так называемый “сниффер” — это программа или устройство для перехвата и анализа сетевого трафика (своего и/или чужого). Сниффер как таковой не является вредоносным и используется в целях обнаружения и устранения отклонений и обеспечения бесперебойной работы. Кроме того, сниффер может быть установлен на любом компьютере, подключенном к локальной сети, без необходимости его обязательной установки на самом устройстве. Иными словами, его невозможно обнаружить на протяжении всего времени подключения.

Чаще всего, злоумышленники устанавливают снифферы в местах с массовым скоплением людей, а так же там, где Wi-Fi менее всего защищен. Например, кафе, отели, аэропорты и т.д. Снифферы маскируют под

устройства, подключенные к сети в рамках спуфинга (это прием, при котором происходит обман сети или пользователя с целью вызвать доверие в надежность источника информации).

Снифферы крайне сложно обнаружить виртуально, обычные пользователи как правило не имеют ни малейшего шанса распознать отслеживание своего сетевого трафика.

Эксплойт KRACK

От всех видов атак, перечисленных выше, можно защититься протоколом шифрования WPA2. Данный же эксплойт использует уязвимости протокола шифрования WPA2 и позволяет прослушивать трафик, проходящий через сеть Wi-Fi. Сам по себе взлом представляет собой классическую атаку «человек посередине» и осуществляет реинсталляцию ключа шифрования. Все устройства, подключенные к одной сети, становятся уязвимыми и могут быть инфицированы вредоносным ПО.

Для взлома с помощью KRACK злоумышленнику необходимо находиться в зоне действия Wi-Fi сети. Таким образом, первой линией защиты является ограничение зоны действия Wi-Fi пределами офиса, жилища и т. д.

Также необходимым является анализ уязвимости сети с помощью профессионального программно-аппаратного комплекса, такого как NETSCOUT AirMagnet Enterprise для обеспечения безопасности и мониторинга сетей Wi-Fi (Wireless IDS/IPS). В данный момент производители оборудования для защиты выпускают много патчей, позволяющие защититься от данной уязвимости.

Общедоступную точку Wi-Fi довольно просто взломать, потому что их не защищают ни в кафе, ни в аэропорту, ни на вокзале. На сайте 3wifi.stascorp.com есть база российских Wi-Fi точек доступа (более 3 миллионов), которые имеют свои проблемы с безопасностью. Данная программа сканирует доступные точки доступа и собирает информацию о них, выявляя незащищенные устройства.

Около 200 тысяч беспроводных сетей не имеют вообще никакой защиты. Еще столько же пользуются устаревшими протоколами безопасности WEP. Это означает, что к ним очень просто подобрать пароль, примерно за 5-10 минут с помощью нужных утилит.

Так же десятки тысяч людей, использующих более новый протокол защиты WPA2, используют попросту ненадежный пароль по типу “12345678” и все виды вариаций этих цифр.

Чтобы не стать жертвой хакеров, для начала необходимо обезопасить свой дом. А для этого нужно:

1) Использовать современные протоколы защиты роутера.

2) Не использовать стандартные или простые пароли от роутера.

3) Обновлять софт роутера.

4) Минимизировать выход покрытия Wi-Fi за пределы контролируемой зоны.

5) Обеспечивать непрерывный мониторинг угроз.

Далее следует подумать о беспроводных точках доступа, которые встречаются в офисе, кафе, аэропорту. Для того, чтобы во время подключения к одной из таких точек доступа данные не были украдены, нужно:

1) Не подключаться к сомнительным точкам доступа.

2) Отключать Wi-Fi адаптер при выходе из дома.

3) Зашифровать всю отправляемую и принимаемую информацию.

4) Сканировать локальную сеть на наличие уязвимостей.

При соблюдении всех этих пунктов, шанс, что персональные данные достанутся злоумышленнику, сводятся к минимуму.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Рассел, Джесси Безопасность в беспроводных самоорганизующихся сетях / Джесси Рассел. - М.: VSD, 2012. - 274 с.

2. Хабрейкен, Джо Домашние беспроводные сети / Джо Хабрейкен. - М.: НТ Пресс, 2014. - 400 с.
3. Шубин, В. И. Беспроводные сети передачи данных / В.И. Шубин, О.С. Красильникова. - М.: Вузовская книга, 2013. - 104 с.