1. Введение

В столице нашей необъятной Родины идет беспрецедентный по масштабу проект внедрения технологии Gpon от компании МГТС под эгидой борьбы против медных проводов и за доступную интернетизацию населения. Число абонентов МГТС по городу Москва превышает 3.5 миллиона человек, предполагается, что охвачены будут все.

Идея замечательная – оптика в каждую квартиру, высокоскоростной интернет, бесплатное подключение и Wi-Fi роутер в подарок (правда официально без права его перенастройки, но об этом далее). Реализация же такого масштабного проекта (подобное устройство ставится в каждую квартиру, где есть хотя бы городской телефон от МГТС) как обычно не обошлась без дыр в планировании, которые могут дорого обойтись конечному пользователю. Наша компания заинтересовалась вопросами информационной безопасности клиентов столь масштабного проекта и провела экспресс-исследование, результаты которого мы и предлагаем общественности для информирования о существующих угрозах и мерах борьбы с ними в домашних условиях.

2. Жизнь на ладони

Угрозы оказались вовсе не иллюзорными и малозначительными, а системными и потенциал риска трудно переоценить. Я хочу предостеречь счастливых абонентов МГТС от угрозы их приватности, таящейся не только в роутере ZTE ZXA10 F660, любезно принудительно подаренном провайдером (впрочем, менее уязвимый Huawei HG8245, также устанавливаемый абонентам все равно никак не защищен от «настроек по-умолчанию»), но и в самой организации подключения абонентов к новым линиям связи. Вот так выглядят варианты устанавливаемого оператором оборудования:

Менее опасный **Huawei HG8245**

Куда более «дырявый» **ZTE ZXA10 F660**

Проблем тут несколько разной степени опасности, какие-то решить можно своими силами, на какие-то можно лишь обратить внимание. Давайте перечислим основные моменты, которые помогут злоумышленнику взломать вашу домашнюю сеть (при условии, что вы таки являетесь абонентом МГТС по услуге Интернет):

-

Пароль на WiFi – это ваш номер телефона (в ходе исследования встречались ленивые монтажники, которые оставляли паролем MAC-адрес роутера без первых 4-х знаков).

Это означает, что взломать Wi-Fi техникой перебора хэндшейка по маске 495?d?d?d?d?d?d?d не потребует много времени, речь идет о считанных минутах и для этого вовсе не обязательно все время находиться возле объекта взлома. Достаточно перехватить момент соединения беспроводного устройства абонента(смартфона, планшета, ноутбука) с роутером, а остальное уже можно спокойно сделать на домашнем компьютере. Этот просчет оператора на уровне организации подключения — зияющая дыра, открывающая домашние сети миллионов абонентов для атаки злоумышленников. Эту проблему можно решить только локально — самостоятельно поменяв пароль точки доступа на более безопасный, однако следующая уязвимость куда серьезнее, так как на нее эффективно повлиять абонент самостоятельно просто не в силах.

-

Речь идет об уязвимости технологии беспроводной настройки WPS, которая включена по-умолчанию на роутерах ZTE ZXA 10 F660. И если в случае с организационным просчетом, подставившим сети пользователей на уровне паролей злоумышленник не может массово взламывать абонентов, занимаясь каждым по-отдельности, то при эксплуатации WPS-уязвимости роутера этой модели взлом сетей может быть поставлен на поток. Технология работает следующим образом — для WPS-соединения используется пин-код, состоящий из 8 цифр. При получении правильного пинкода роутер отдает реальный Wi-Fi пароль. Мало того, что этот пин-код может быть взломан с использованием известного инструмента Reaver куда эффективнее и быстрее сложного WPA2 пароля, но главная проблема — он единый для всех роутеров ZTE ZXA10 F660! Более того, его легко можно найти за 10 минут в интернете. Повторяю — зная этот пин-код(который нельзя ни поменять, ни выключить) в течении 3 секунд получается реальный Wi-Fi пароль любой сложности и типа шифрования, либо производится прямое подключение к сети абонента. Таким образом «счастливые» обладатели именно этой модели оборудования (а их у оператора всего 2, так что шанс 50/50) даже установив невозможный ко взлому пароль на беспроводную сеть все равно из-за несовершенства технологии будут взломаны менее, чем за 5 секунд.

3. Чем чреват для владельца взлом WiFi?

Опустим банальности вроде «бесплатного интернета», сейчас не 90-е и на интернет людям с гаджетами обычно хватает. Так что за угрозы? Перечислим самые очевидные:

- Перехват траффика абонента, кража паролей от почтовых служб, социальных сетей, программ обмена сообщениями и других конфиденциальных данных
- Атака на компьютеры владельца точки с целью получения доступа к файлам пользователя, просмотра веб-камер, установки вирусов и шпионских программ (как правило домашние ПК куда более уязвимы для атак изнутри, чем корпоративные машины, здесь и традиционно слабые пароли и нерегулярные обновления и открытые ресурсы)
- Прослушка телефонных разговоров. (Да, с переходом на незащищенный sip это стало проще, чем когда-либо). Теперь не только спецслужбы, но и любопытный сосед (а может и не сосед) может записывать ваши разговоры по городскому номеру ввиду того, что новая технология телефонии работает по незащищенному протоколу SIP. Для оперативного перехвата и записи разговоров которого давно существуют в открытом доступе все необходимые инструменты.
- Кража телефонного номера — незначительно изменив программное обеспечение роутера злоумышленник может выяснить пароль от SIP-аккаунта и использовать его для звонков от лица взломанного абонента. Это не только потенциал прямого убытка владельцу номера, но и возможность нанесения куда более серьезного ущерба путем использования номера ничего не подозревающего гражданина для шантажа, террористических контактов или же с целью подставить владельца — например с этого номера сообщив в полицию о заложенной бомбе
- Создание большого ботнета (число абонентов МГТС в г. Москва — 3 504 874) с потенциалом каждого соединения в 100мбитс. Да, для этого потребуется армия леммингов, но как всем хорошо известно – на разного рода «чанах» постоянно обитают орды биологических ботов, которых регулярно привлекают заинтересованные лица к разнообразным интернет-акциям, как правило вредительского толка.
- Использование случайной (или не случайной) сети для анонимной загрузки в Интернет запрещенных материалов (Догадываетесь, в чью дверь постучат?).

4. Меры защиты

Что можно предпринять, как защитить свою приватность в такой ситуации? Сделать самому можно немного, но это обязательные действия для каждого, кто не хочет стать жертвой плохо продуманной кампании оператора. Нам понадобятся пароли от роутера, которые легко гуглятся в Интернете, записывайте:

- Доступ к вэбинтерфейсу роутера ZTE ZXA10 F660 – login: **mgts**, Password: **mtsoao**
- Доступ к консоли по протоколу Telnet – login: **root**, password: **root**
- для Huawei HG8245:
  адрес по умолчанию — **192.168.100.1**
  login: **telecomadmin**, password: **admintelecom**
- Через вэбинтерфейс обязательно меняем пароль на точку доступа и ее имя (MAC-адрес все равно выдаст принадлежность к клиентам МГТС, но переименование точки снизит вероятность сопоставления конкретного Wi-Fi сигнала конкретной квартире)
- Владельцам ZTE ZXA F660 следует отключить Wi-Fi функционал кнопкой на

устройстве. На данный момент это единственный способ защититься от WPS-взлома.

К сожалению в лучшем случае этими мерами воспользуются считанные проценты от 3.5 миллионов пользователей, большинство никогда не узнает об этой статье и останется уязвимым перед лицом реальной угрозы на долгое время, до тех пор, пока что-то или кто-то не заставит оператора потратить кучу денег и принять централизованные меры по исправлению технических и организационных недостатков проекта.

5. Вывод

Какие выводы можно сделать из всего вышесказанного? Самые неутешительные – масштабнейший проект внедрения GPON(повторюсь – речь идет о 3.5 миллионах абонентов!) обошелся без консультаций со специалистами по информационной безопасности, либо эти консультации были полностью проигнорированы в ходе самого внедрения. Пароли-телефоны, не отключаемый WPS с единым ключом, незащищенная SIP-телефония, извлекаемые из WEB-интерфейса пароли — есть результат слабой организационной составляющей и полного игнорирования элементарных норм информационной безопасности. Уверен, МГТС далеко не уникальны в подобных просчетах, многие более мелкие операторы сетевых услуг попадают в такие же ситуации в области защиты данных своих абонентов, но масштаб проблемы на этот раз превосходит все мыслимые границы

6. Официальная реакция ОАО МГТС

Мы, как добропорядочные исследователи безопасности, заинтересованы в скорейшем решении озвученных выше проблем. К сожалению наше беспокойство не нашло отклик в сердцах сотрудников пресс-службы ОАО МГТС, на которых мы пытались выйти, используя все имеющиеся каналы. Отзыв получили лишь один — через Facebook, сотрудник пресс-лужбы заверил нас, что мы можем с чистой совестью опубликовать имеющийся материал, а они потом отвечая на вопросы прессы заверят всех в том, что абоненты в безопасности, а данные их — конфиденциальны. Тэги: как
,
по
,
от
,
под
,
новые

,
без
,
проекта
,
мгтс
,
квартиру
,
gpon
,
борьбы
,
масштабного
,
каждую
,
телефон