POSITIVE TECHNOLOGIES

ЗАО «ПОЗИТИВ ТЕКНОЛОДЖИЗ»
107061 / МОСКВА / ПРЕОБРАЖЕНСКАЯ ПЛОЩАДЬ / Д. 8
ТЕЛ.: +7 (495) 744 01 44 / ФАКС: +7 (495) 744 01 87 / PT@PTSECURITY.RU
WWW.PTSECURITY.RU / WWW.MAXPATROL.RU / WWW.SECURITYLAB.RU

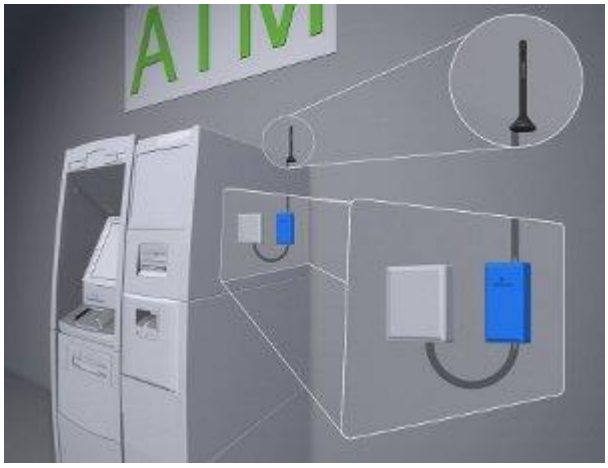
Безопасность 4G: захватываем USB-модем и SIM-карту с помощью SMS

Телеком-операторы активно рекламируют быструю и дешевую 4G-связь. Но насколько она защищена, знают немногие. Экспертам Positive Technologies в процессе исследования безопасности 4G-коммуникаций удалось найти уязвимости в USB-модемах, позволяющие взять под контроль компьютер, к которому подключён модем, а также аккаунт абонента на портале мобильного оператора. Кроме того, атаки на SIM-карту с помощью бинарных SMS позволяют перехватить и расшифровать трафик абонента, либо просто заблокировать заданную "симку".

Доклады по результатам исследования были представлены в ноябре на конференции ZeroNights в Москве (Кирилл Нестеров, Алексей Осипов, Тимур Юнусов) и конференции PacSec в Токио (Сергей Гордейчик, Александр Зайцев). В этой публикации мы резюмируем основные идеи исследования, в котором также участвовали Дмитрий Скляров, Глеб Грицай, Дмитрий Курбатов, Сергей Пузанков и Павел Новиков.

Несколько слов о целях данной работы. Дело касается не только безопасности модных смартфонов, с помощью которых мы читаем свои френдленты в социальных сетях. Цифровая мобильная связь стандарта GSM используется сейчас во многих критических инфраструктурах, включая промышленные системы управления (SCADA). Другой пример из повседневной жизни, с

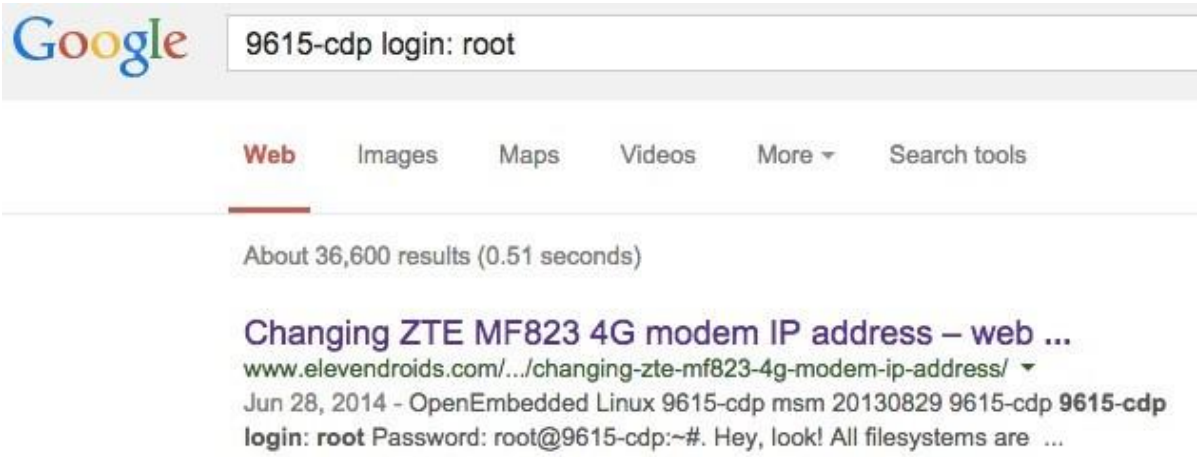
которым никому не хотелось бы встретиться – это кража денег с банковских счетов. Между тем, многие наверняка видели такие маленькие антенны у банкоматов – здесь тоже GSM:



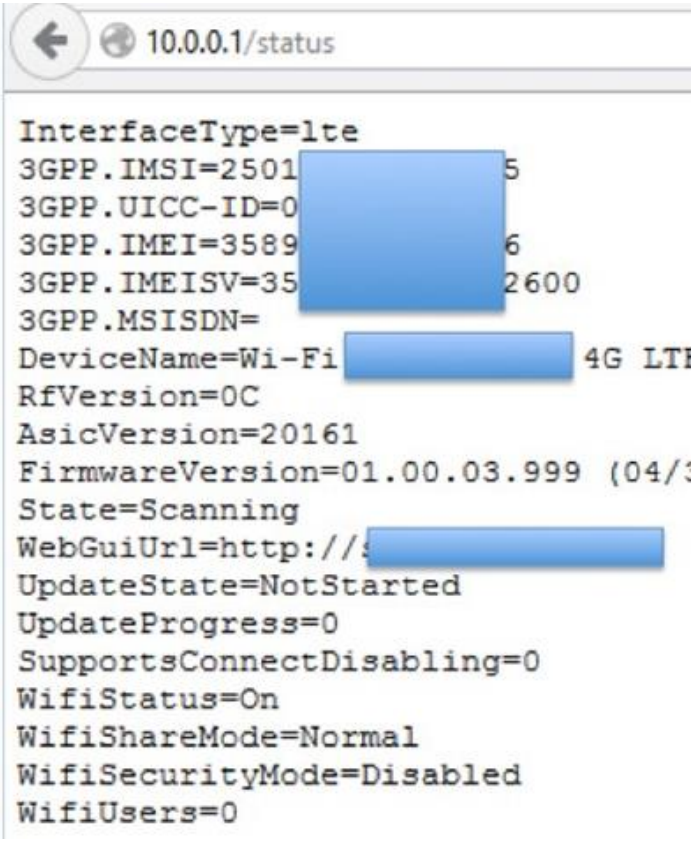
Современный модем для беспроводной связи - это компьютер, на который установлена известная операционная система (обычно Android) и ряд специальных приложений с достаточно широким и возможностями. В этом программном обеспечении и протоколах передачи данных есть уязвимости, которые уже эксплуатировались в последние годы - например, чтобы разлочить модем и отвязать от оператора. Одним из средств защиты от таких взломов стал перенос многих сервисов на Веб - однако это дало лишь новые возможности для атак.

Для нашего исследования мы взяли шесть различных линеек USB-модемов с 30 различными прошивками. Забегая вперёд - не удалось взломать только три прошивки.

Что удалось сделать с остальными? Для начала идентифицируем «железку». В этом нам помогают документация и поисковые системы. В некоторых случаях Google помогает даже больше – можно сразу найти пароль для telnet-доступа:



Однако для внешних коммуникаций нам нужен не telnet, а http. Подключаем модем к компьютеру и изучаем его, как отдельный сетевой узел с веб-приложениями. Находим возможность атаки через браузер (CSRF, XSS, RCE). Таким способом заставляем модем рассказать о себе разные полезные данные:



Помимо раскрытия данных, на атакованном модеме можно:

- поменять настойки DNS (что позволяет перехват трафика)

- поменять настройки SMS-центра (перехват SMS или манипулирование ими)

- сменить пароль на портале самообслуживания через SMS (что позволяет увести деньги со счета, подписавшись на сторонний сервис)

- заблокировать модем путём набора неверных PIN- и PUK-кодов

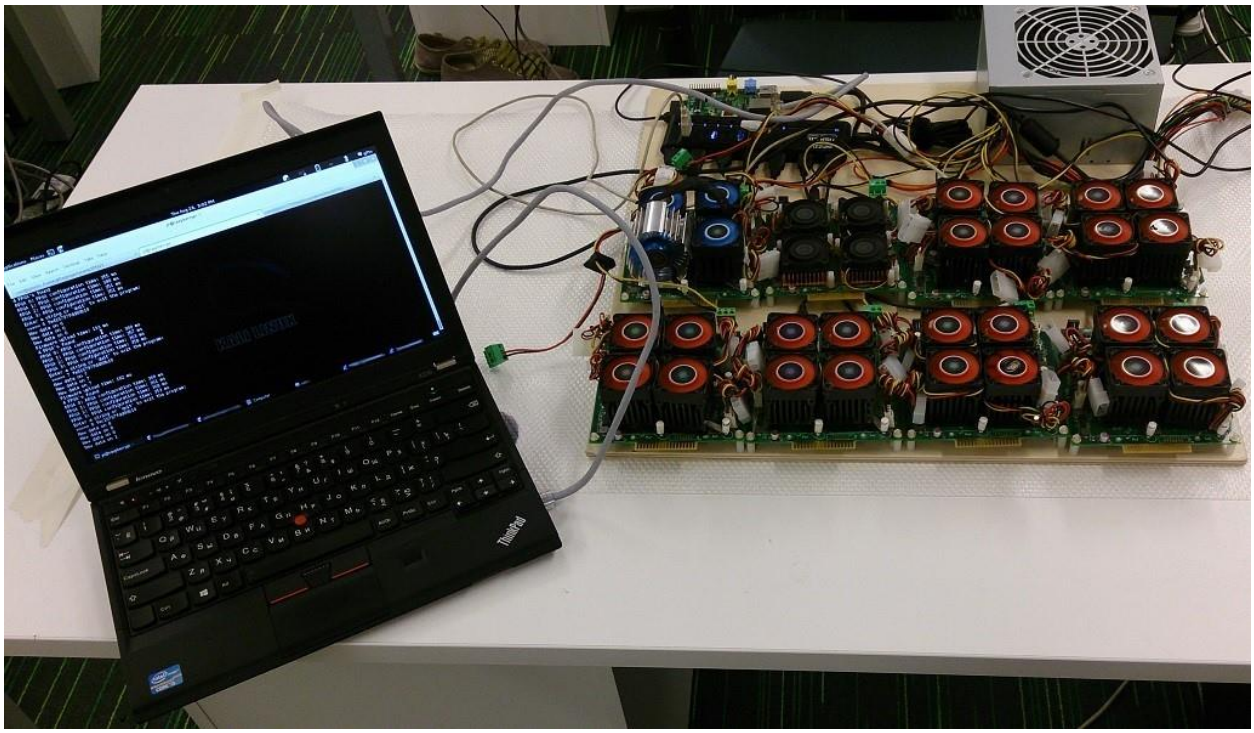
- удаленно «обновить» прошивку модема.

Можно развить атаку и дальше - добраться до компьютера, к которому подключён USB-модем. Один из вариантов такой атаки: на захваченный модем устанавливается драйвер USB-клавиатуры, после чего компьютер воспринимает модем как устройство ввода. С этой "мнимой клавиатуры" на компьютер передаётся команда перезагрузки BIOS с внешнего диска, роль которого играет всё тот же модем. Таким образом на "материнский" компьютер можно установить bootkit, позволяющий дистанционно управлять компьютером. Как это работает, можно посмотреть на видео: http://www.youtube.com/watch?v=6_0tcf-f_II

Лучшее, что может сделать пользователь для защиты от подобных атак - не засовывать что попало в свои USB-порты. Понимая при этом, что к выражению "что попало" относятся даже USB-модемы, которые снаружи кажутся всего лишь маленьким и безобидным устройством связи.

Вторая часть нашего исследования касалась SIM-карт. Тот факт, что сама "симка" тоже является компьютером со своей ОС, файловой системой и многофункциональными приложениями, уже демонстрировали многие другие исследователи. Так, в мае этого года на конференции Positive Hack Days специалист по шифрованию Карстен Ноэль показал, что приложения "симок" (TARS) защищены по-разному. Некоторые можно взломать путём подбора DES-ключей, а некоторые отвечают на внешние команды вообще безо всякой защиты - и рассказывают о себе много лишнего.

Для подбора ключей в нашем исследовании использовался набор программируемых пользователем вентильных матриц (FPGA), которые вошли в моду пару лет назад для майнинга цифровой валюты Bitcoin, а после падения популярности этого развлечения сильно подешевели. Наша плата из восьми модулей *ZTEX 1.15y за 2 тыс. евро считает со скоростью 245.760 Mcrypt/sec, что позволяет подобрать ключ DES за 3 дня.



Hardware	Speed (Mcrypt/sec)	Time for DES (days)	Time for 3DES (part of key is known, days)
Intel CPU (Core i7-2600K)	475	1755,8 (~5 years)	5267,4
Radeon GPU (R290X)	3`000	278	834
Single chip (xs6slx150-2)	7`680	108,6	325,8
ZTEX 1.15y	30`720	27,2	81,6
Our rig (8*ZTEX 1.15y)	**245`760**	**3,4**	**10,2**

После этого мы можем посылать команды известным TAR'ам и управлять ими. В частности, менеджер карты Card manager позволяет нам загрузить на "симку" своё java-приложение.

Другой интересный TAR – это файловая система File system, где хранятся TMSI (идентификатор телефона в мобильной сети) и Kc (ключ шифрования трафика). Доступ к ним позволяет нам с помощью бинарного SMS:

- расшифровать трафик абонента без подбора ключей,

- подменить абонента (получать его звонки и SMS),

- следить за перемещениями абонента.

- при наличии PIN-кода, защищающего файловую систему, можно заблокировать абонента (три неверных PIN-кода и 10 неверных PUK-кодов, после чего карта блокируется).

В заключение - простая статистика. В данном исследовании использовалось более ста SIM-карт различных операторов. Описанным уязвимостям подвержены 20% из них, то есть каждая пятая "симка". При этом едва ли можно дать какие-то советы по защите для конечных пользователей: атаки происходят на довольно низком техническом уровне, поэтому решать вопросы безопасности здесь должны производители SIM-карт и операторы. Западная IT-пресса, кстати, уже описывает данное исследование в новостях про «возможность взлома миллионов SIM-карт и USB-модемов».

PS.

Это было не единственное исследование экспертов Positive Technologies, представленное на ZeroNights'14. На той же конференции Артем Шишкин и Марк Ермолов рассказали о механизмах обхода системы защиты Windows PatchGuard в Windows 8: некоторые детали исследования можно найти здесь, подробности будут в одном из наших следующих постов.

О компании Positive Technologies

Positive Technologies — лидер европейского рынка систем анализа защищенности и соответствия стандартам. Деятельность компании лицензирована ФСТЭК и ФСБ, продукция сертифицирована ФСТЭК, «Газпромом» и Минобороны РФ. Более 1000 организаций в 30 странах мира используют решения Positive Technologies для оценки уровня безопасности своих сетей и приложений, выполнения требований регуляторов и блокирования атак в режиме реального времени. Благодаря многолетним исследованиям специалисты Positive Technologies заслужили репутацию экспертов международного уровня по вопросам защиты SCADA- и ERP-систем, крупнейших банков и телекомов. Согласно исследованиям IDC, в 2013 году компания заняла третье место на российском рынке ПО для безопасности, а также стала лидером по темпам роста на международном рынке систем управления уязвимостями. Подробнее о компании — на сайте ptsecurity.ru.