УДК 004.22+004.25+004.6

МОБИЛЬНЫЙ ШПИОН " PEGASUS "

Кабиев Назарбек Балабаевич
crazy5naz@gmail.com
Студент 2 курса кафкдры информационной безопасности ЕНУ им. Л. Н. Гумилева,
Нур-Султан, Казахстан
Научный руководитель – А. Б. Оспанова, к.ф.-м.н., и. о. доцента кафедры
информационной безопасности ЕНУ им. Л. Н. Гумилева

Аннотация. В данной статье подробно рассмотрено шпионское ПО «Pegasus». Опасность такого рода программ в том, что их можно незаметно установить на мобильные телефоны и другие устройства, работающие под управлением некоторых версий мобильных операционных систем Apple iOS и Android. “Pegasus” использует неизвестные лазейки, и для защиты от многих из них ещё нет решения. Специалисты называют это уязвимостью нулевого дня. В статье рассказано про способы атаки данного шпионского ПО и подробно описан принцип его работы. А также приведены некоторые рекомендации по уменьшению рисков реализации данной угрозы.

Ключевые слова. Шпионское ПО, Структура смартфона, Процессор приложений, Операционная система, Процессор, Личные данные, Уязвимость, SIM-карта, Сотовый оператор.

1. Введение

Шпионское Программное Обеспечение – это вредоносная программа, которая без согласия пользователя собирает и передает информацию с устройства. Также может именоваться как Spy, SpyWare, Spy-ware, Spy Trojan.

Pegasus — шпионское ПО, которое можно незаметно установить на мобильные телефоны и другие устройства, работающие под управлением некоторых версий мобильных операционных систем Apple iOS и Android. Разработка израильской компании NSO Group.

Pegasus заражает устройства iPhone и Android через SMS, WhatsApp, iMessage и, возможно, другие каналы. Позволяет извлекать сообщения, фотографии и переписку по email,

контакты и данные GPS, а также записывать звонки и незаметно включать микрофон и камеру.

1 – рисунок. «Pegasus»

IT гиганты как Apple, Google, Microsoft тщетно прикладывают большие усилия для устранения уязвимостей, которые удаётся найти, и которые, по различным косвенным оценкам, использует “Pegasus”. Системы, видимо, используют и другие неизвестные самим компаниям лазейки. Такие уязвимости, для устранения которых еще нет эффективных решений, специалисты называют уязвимостью нулевого дня. И борьба с ними в случае с “Pegasus” похожа на «игру с неуловимым грызунами».

Чтобы понять, какая на самом деле бездна кроется за технологий “Pegasus” нужно дать пояснения о самом главном – о структуре смартфонов. Это даст понять не только, почему “Pegasus” настолько опасен, но и то, как любой телефон можно взломать без единого действия со стороны хозяина девайса и вмешательства в устройство, даже без помощи сотовых операторов или админов мессенджеров, которые сотрудничают с людьми. А взломать может пользователь технологий практически любого уровня: и специалист с полномочиями, и продвинутый хакер, и просто мошенники, и даже школьник без глубоких знаний.

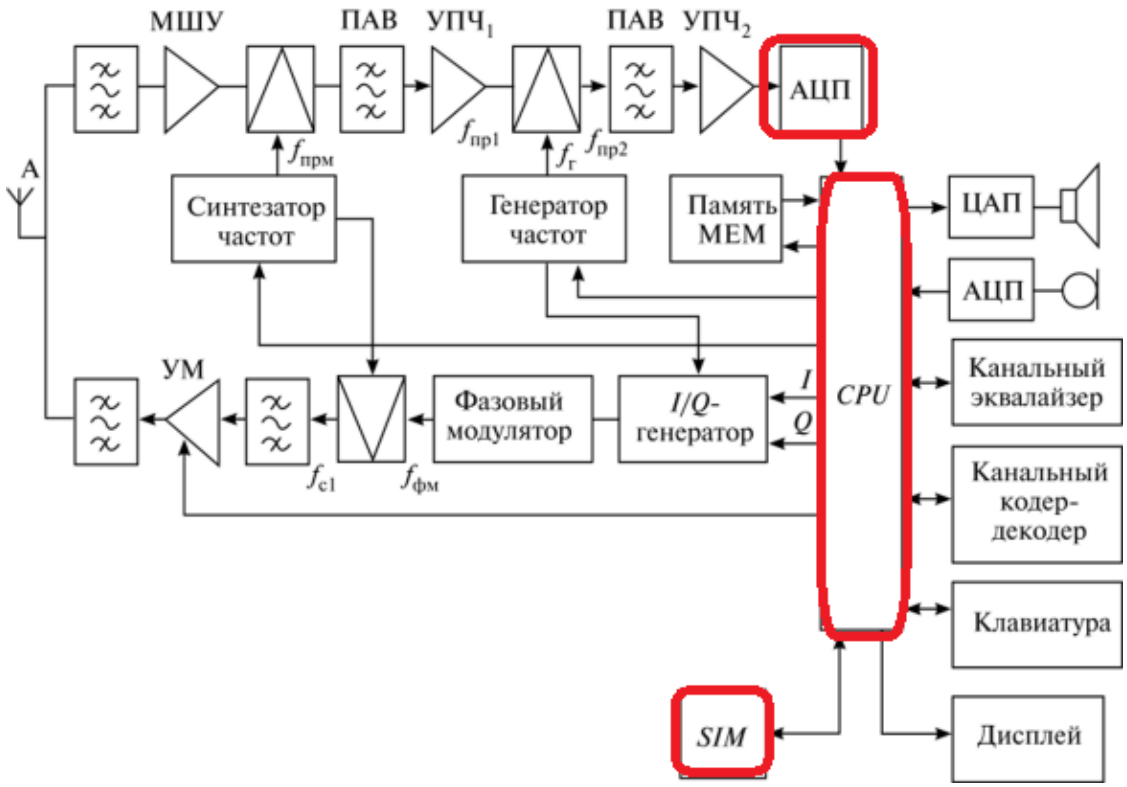
2. Структура смартфона

Типичный смартфон имеет внутри как минимум три независимых компьютерных системы, каждая из которых работает под управлением собственной операционной системы, и каждая из них запрограммирована различным сообществом разработчиков, работающих в разных сегментах отрасли.

1) «Процессор приложений». Это компьютер под управлением Android или iOS. Это та часть, с которой вы взаимодействуете. Это место, где работают ваши приложения. Когда вы думаете о своем смартфоне, вы, вероятно, думаете о процессоре приложений.

2) «Процессор основной полосы частот». Это компьютер, который управляет сотовой частью телефона. И под сотовой связью мы подразумеваем настоящие сотовые технологии, такие как LTE, 5G и т. д., а не Wi-Fi. Этот компьютер подключает и разъединяет телефонные звонки, подключает и разъединяет сеансы сотовой передачи данных, обрабатывает SMS и выполняет другие функции в сотовой сети, включая такие функции, как «управление мобильностью», которые обычно невидимы для вас.

3) SIM-карта. SIM-карта содержит полноценную компьютерную систему (процессор, память и файловая система), работающую под управлением собственной ОС и собственного набора приложений. Когда пользователь устанавливает SIM-карту, она становится неотъемлемой и активной частью его телефона. Структура смартфона представлена на рисунке 2.



2 - рисунок. Структура смартфона

3. Принцип работы “Pegasus”

“Pegasus” имеет много способов получения доступа к устройству. И в этой статье рассмотрен один из способов атаки шпионского ПО “Pegasus”.

Для получения “Pegasus” доступа к мобильному устройству им используется «Процессор основной полосы частот». «Процессор основной полосы частот» обменивается данными с «Процессором приложений» за секунды и делает это на языке восьмидесятых и девяностых, те же протоколы используют допотопные модемы. Процессоры приложение просит, например, просканировать доступные сети, выбрать эту сеть, отправить смс, начать вызов. А «Процессор основной полосы частот» решает эту проблему, но за плотно закрытыми дверями. Процессору приложений недоступны данные ни в каком виде, оно только получает результат. И хотя кажется, что это бронированный черный ящик, но оператор может удаленно отправить ему обновление. Они называются «Over the air», то есть по воздуху, как правило, они доставляют зашифрованные текстовые сообщения, которые вы не увидите, потому что они не будут приняты и обработаны процессором приложений. Его примет лично «Процессор основной полосы частот».

Процесс атаки рассматриваемым шпионским ПО показан на рисунке 3.

3 – рисунок. Способы атаки и доступ к данным

Чтобы получить удаленный доступ к пользовательскому телефону, нужна SIM-карта. Стоит сказать, что как и многие смарт-карты, их можно запрограммировать с помощью амулетов, написанных на Java. “Pegasus” отправляет удаленно обновление с своим амулетом и отправляет сообщение либо SMS, но пользователь даже его не увидит. При его получении начинается передача данных с атакованным устройством пользователя. Этот способ атаки называется «Атака с нулевым щелчком». И таким способом злоумышленники могут получить личные данные, местоположение хозяина устройства, управлять камерой либо другим устройством.

4. Использование

Разработчик заявляет, что предоставляет «уполномоченным правительствам технологии, которые помогают им бороться с терроризмом и преступностью», он опубликовал разделы контрактов, требующих от клиентов использовать Pegasus только в целях уголовной и национальной безопасности. Разработчик также утверждает, что внимательно относится к правам человека.

Apple, Google, Microsoft и с десяток других компаний и организаций, обратилась в Минфин с просьбой ввести санкции против израильской компании и некоторых ее партнеров,

и клиентов. Потому что “Pegasus” использовался не по назначению. В июле 2021 года в прессе появились сообщения о том, что авторитарные режимы используют “Pegasus” для взлома телефонов правозащитников, оппозиционных журналистов и юристов.

В прессу попал список более чем 50 тыс. телефонных номеров людей, предположительно представляющих интерес для клиентов NSO Group. Происхождение списка неизвестно, как и то, подвергались ли эти телефоны взлому с помощью Pegasus. Среди стран — клиентов NSO, чьи правоохранительные органы и спецслужбы вводили номера в систему, значатся Азербайджан, Бахрейн, Венгрия, Индия, Казахстан, Марокко, Мексика, Объединенные Арабские Эмираты, Руанда и Саудовская Аравия. В частности, программу Pegasus использовали для прослушивания телефонов двух женщин, близких к саудовскому журналисту Джамалю Хашогги, убитому в октябре 2018 года. Также в списке были обнаружены номера телефонов принцессы Латифы — опальной дочери правителя Дубая Мохаммеда Аль Мактума и его бывшей жены принцессы Хайи аль-Хусейн.

По имеющимся сведениям, в число жертв Pegasus входит около 600 государственных чиновников из 34 стран, в том числе: президент Ирака Бархам Салех, президент ЮАР Сирил Рамафоса, премьер-министры Пакистана, Египта и Марокко. По данным парижской газеты Le Monde, в 2017 году марокканская разведка определила номер, которым пользуется президент Франции Эммануэль Макрон, что создает опасность заражения Pegasus’ом.

5. Заключение

В данной статье рассмотрено шпионское ПО “Pegasus”, которое очень опасно и может получить личные данные и управление практически любым устройством без особого труда. “Pegasus” опасен настолько, что даже стандартные мероприятия по устранению уязвимостей не дают действенных результатов. Так же на основании анализа множества источников было показано, что оно может принести колоссальный ущерб частным пользователям смартфонов, но также и на уровне государства.

Список использованных источников

1. https://ru.wikipedia.org/wiki/Pegasus_(%D0%9F%D0%9E)
2. https://medium.com/telecom-expert/structure-of-a-smartphone-383575de3eaf
3. https://www.youtube.com/watch?v=0wEjI927sh8
4. https://www.youtube.com/watch?v=fQqv0v14KKY
5. https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcRgHgtlbbagiKy-W11MntD9HmFOy5ZDX5jR_USHhF3DixpD1rjiB128VuY9iop3NohNqdc&usqp=CAU
6. https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcS2wk12Hx4bYUFKc8ovTEpzyQMXlKuWWm7sbw&usqp=CAU