CYBER NOVA

Secure DataFlow Hotspot

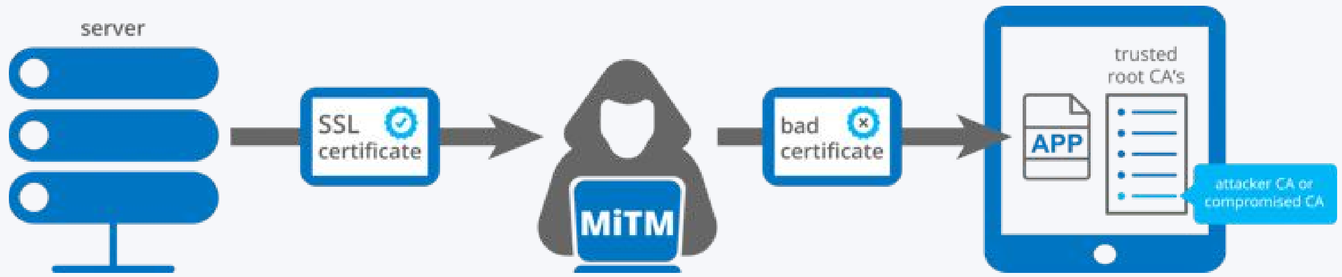
Гарантированная защита трафика привилегированных абонентов в недоверенных Wi-Fi сетях и каналах сотовой связи

Описание проблемы

Владелец публичной Wi-Fi точкой или оператор сотовой связи предоставляют канал связи, безопасность которого невозможно гарантировать.

Кроме того невозможно контролировать достоверность (защиту от модификации) трафика защищаемого абонента и обезопасить его от перехвата критично важной информации.

Неблагонадежные сотрудники оператора сотовой связи, администраторы Wi-Fi сети или злоумышленники имеют возможность реализовать различные атаки как на трафик абонента, так и на самого абонента, в том числе MITM (человек посередине) с целью просмотра, модификации (в том числе удаления) данных канала связи, а так же нарушения его нормального функционирования (частичный или полный обрыв соединения).



Пример из жизни

Атака на представителей власти

В 2014 году, группа злоумышленников, называющая себя «Анонимный интернационал» и специализирующаяся на «сливах» по высшим чиновникам, публиковала переписку, якобы принадлежавшую Аркадию Дворковичу и Евгению Пригожину, взламывала твиттер-аккаунт Дмитрия Медведева, а так же выставляла на аукцион фальшивую переписку его пресс-секретаря Натальи Тимаковой и бывшего главы Роскомнадзора Александра Жарова.

Целями атак данной группы, в том числе, были подразделения и ключевые фигуры высшего политического звена, в частности Управление Президента РФ по внутренней политике и лично заместитель его руководителя Тимур Прокопенко. Его сфальсифицированная переписка опубликована в публичном доступе.

Для проведения вышеперечисленных атак злоумышленники использовали специальное оборудование и програмное обеспечение, позволяющее, в том числе, создавать поддельные Wi-Fi сети и фальш-соты операторов мобильной связи, что дает возможность прослушивать и воздействовать на трафик абонентов, а так же проводить атаки на сами устройства. Переключение зачастую происходит автоматически и без уведомления. В некоторых случаях абонент сам подлючался с недоверенной открытой Wi-Fi сети для получения доступа в ГВС Интернет, предосталяя возможность прослушивать трафик и воздействовать на свое устройство. «Анонимный интернационал» осуществлял атаки "человек по середине" исполнителями, подключенными с «жертвой» в одном публичном Wi-Fi.

Члены группы осуществляли атаки из публичных мест, где в это время находились необходимые им абоненты, прежде всего из Администрации Президента РФ — в частности, в ресторане «Kask», кафе «Шоколадница», ГУМе и др.

Решение проблемы

Secure DataFlow Hotspot позволяет гарантированно защитить канал связи абонента за счет:

- Разделения и шифрования защищаемого трафика;
- Технологии Wi-Fi 6 и других средств повышенной безопасности;
- Улучшенного качества сигнала и скорости передачи данных, что в свою очередь обеспечивает стабильную работу в суровых условиях эксплуатации и сложной оперативной обстановке;
- Нескольких модулей LTE/5G и возможностью "горячей" замены SIM-карт, в сочетании с большим объемом скоростной оперативной и энергонезависимой памяти обеспечивают бесперебойное подключение до 256 устройств;
- Высокопроизводительного процессора ARM Cortext-A53 с основной частотой до 1,3 ГГц, с поддержкой промышленного ввода-вывода.

Как мы гарантируем безопасность соединения конечного пользователя?

Для решения криптографической задачи по дешифрованию исходных данных требуется достаточный объем непрерывного шифртекста.

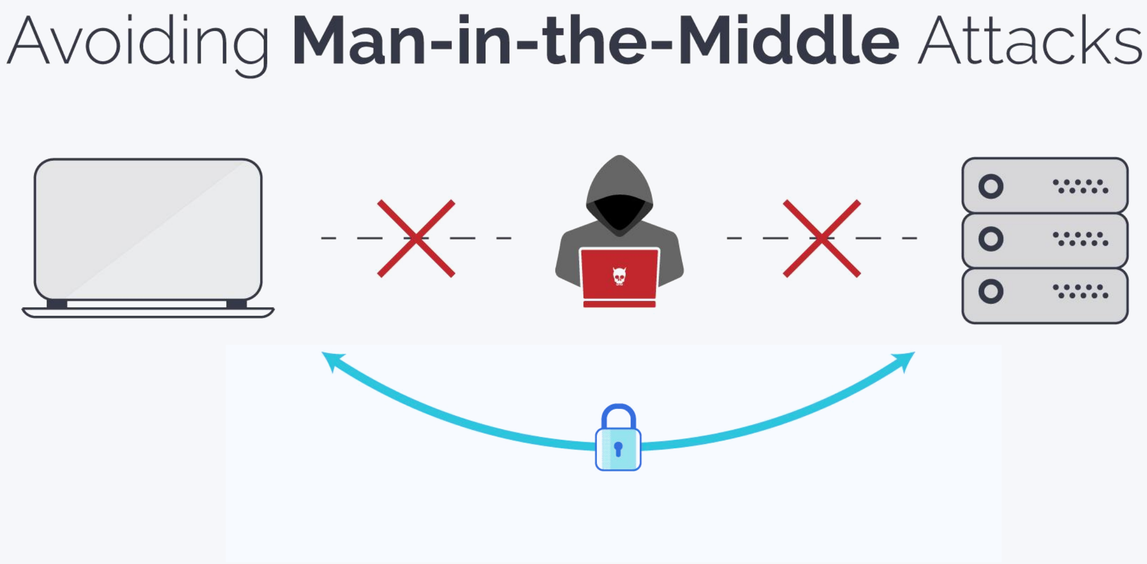
Перед отправкой Secure DataFlow Hotspot дополнительно шифрует трафик, а затем разделяет, перемешивает и передает его через несколько каналов. Основным каналом передачи выступает недоверенная Wi-Fi сеть, остальные каналы организуются с помощью нескольких модемов, подключенных к разным сотовым операторам. Подобная организация передачи данных, совместно с перечисленными выше особенностями устройства сильно усложняет криптоанализ и существенно уменьшает возможности злоумышленников, делая задачу эффективного вредоносного воздействия или дешифрования невыполнимой в обозримое время.

Уникальная технология конвееризации трафика позволяет использовать любой алгоритм шифрования данных по желанию Заказчика, в том числе ГОСТ и уникальные, модифицированные шифр алгоритмы.

Secure DataFlow Hotspot скрывает количество подключенных абонентов и защищает устройства пользователя от атак на уязвимые сервисы по открытым портам.

Минимизация рисков

Трафик Secure DataFlow Hotspot, передаваемый по каналу недоверенной Wi-Fi сети невозможно дешифровать за обозримое время, а его теоретическая модификация или блокировка приводит к перераспределению нагрузки на сотовые каналы со своевременным оповещенем абонента. Данный подход делает атаку вида "человек посередине" неэффективной.



Система обнаружения атак

CYBER NOVA

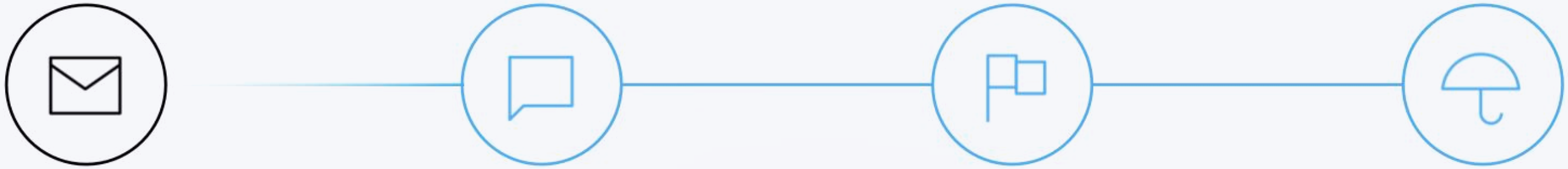
Secure DataFlow Hotspot имеет встроенную систему обнаружения атак “человек посередине” посредством использованием DNS и ARP пакетов.

Кроме того, опционально, существует возможность обнаружения попыток сканирования портов устройства со стороны пользователей Wi-Fi сети с целью выявления внешней вредоносной активности.

Выводы и дальнейшие шаги

CYBER NOVA

Свяжитесь с нами



Мы проведем брифинг, продемонстрируем работу решения и ответим на ваши вопросы

Поможем провести пилотирование решения и выбрать подход к построению сети SD-WAN под ваши задачи

Обеспечим поддержку при внедрении и эксплуатации решения