О безопасности сигнальных сетей мобильных операторов РФ

Касымов Дмитрий

dkasymov@ptsecurity.com

Обеспечиваем практическую кибербезопасность

20 лет

опыта
исследований
и разработок

1500+

инженеров по ИБ,
разработчиков,
аналитиков
и других специалистов

¼ эксперты

экспертов в нашем
исследовательском
центре безопасности

200+

обнаруженных
уязвимостей
нулевого дня в год

200+

аудитов безопасности
корпоративных систем
делаем ежегодно

10 лет

проводим самые
крупные в России
и Европе
киберучения

создаем продукты и решения

проводим аудиты безопасности

расследуем инциденты

исследуем угрозы

Ключевые риски

Доступ к голосовой связи, SMS, 2FA, IoT, интернет-банкинг, социальные сети, гос. услуги, как для физических лиц, так и для компаний

Что может злоумышленник?

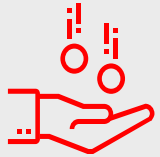
Отказ в обслуживании

MitM

Перехват/перенаправление пользовательского трафика

Данные о местоположении, Трекинг

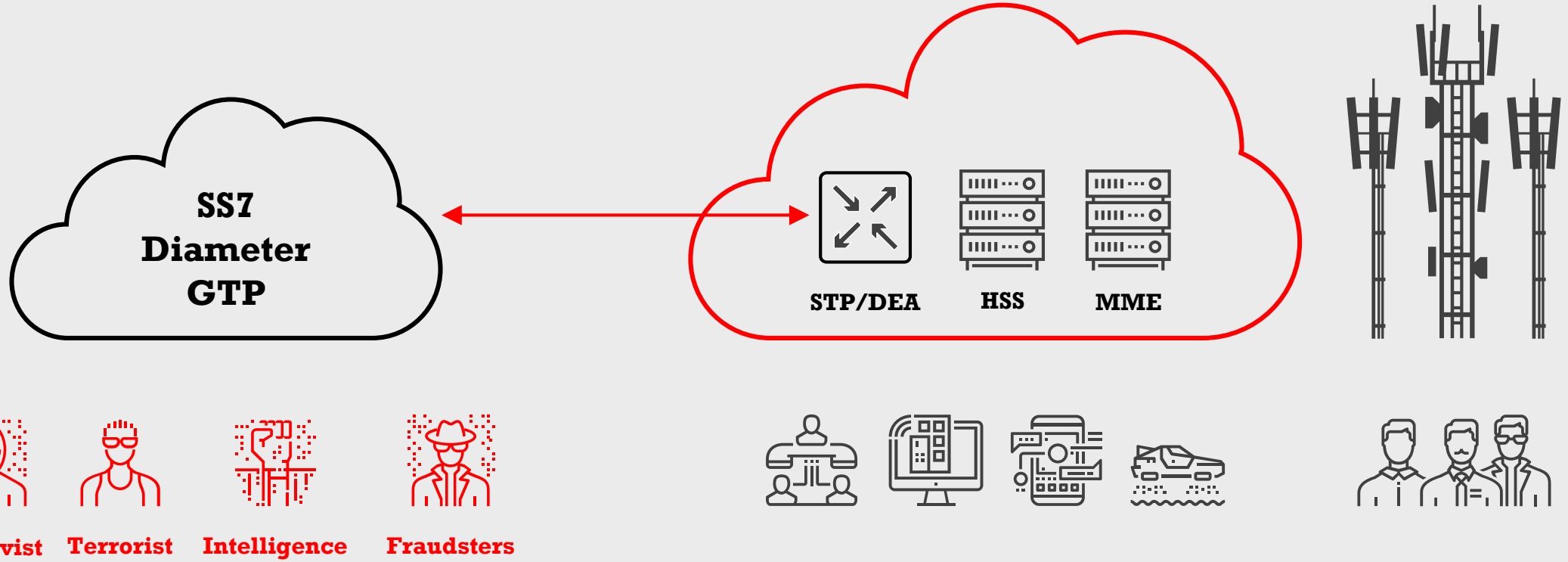
Компрометация персональных данных и «цифровой личности» абонентов, в т.ч. публичных персон и гос. служащих



Кража денег со счетов абонентов и у оператора

Данные о статистики звонков, номера контрагентов и т. д.

Источники угроз



Актуальные угрозы

За последнее время зафиксировано существенное увеличение количества атак со стороны украинских операторов:

- Перенос абонентов в роуминг – **Fake relocation**
- Массовая рассылка **SMS** и обзвон абонентов с призывами к противоправным действиям
- Получение данных о местоположении

Отсутствие адекватного реагирования на возросшие угрозы безопасности может привести к массовой реализации инцидентов, связанных с нарушением работоспособности опорной сети, компрометацией данных абонентов,
а также распространению ложной информации по каналам мобильной связи

Процесс безопасности

Инспектирование

Возможность посмотреть на сигнальную сеть глазами злоумышленника. **Получение информации о потенциальных уязвимостях сигнальной сети**

Детектирование

Постоянное выявление нелегитимного трафика в режиме реального времени имеет важнейшее значение для **обнаружения атак на ранних стадиях и проверки эффективности принятых мер безопасности**

Фильтрация

Активная фильтрация сигнального трафика обеспечивающая полное соответствие рекомендациям GSMA и защиту от актуальных атак сигнальной сети оператора

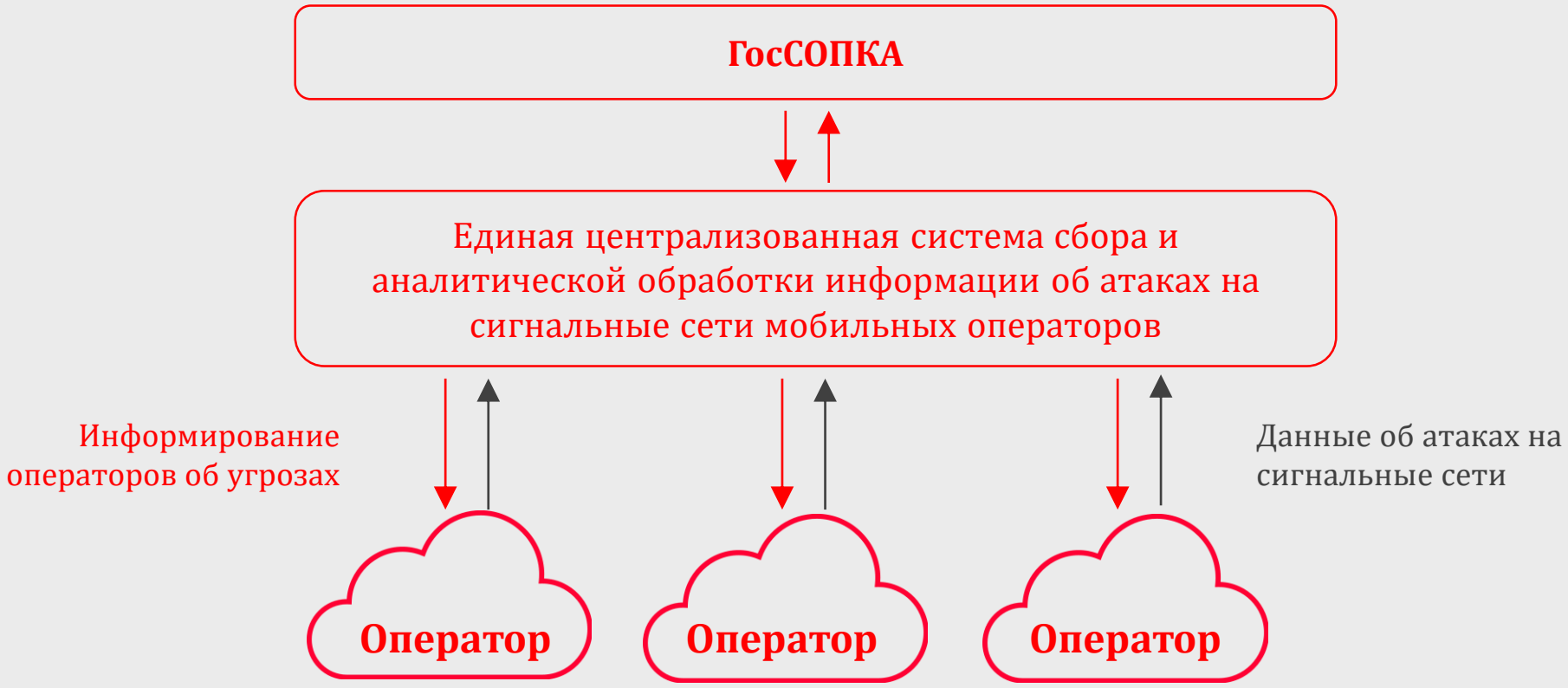
Рекомендации

Для сохранения надлежащего уровня предупреждения, выявления и блокирования атак через сигнальные сети на стороне оператора связи необходимо:

1. Своевременно оценивать эффективность инструментов выявления атак через сигнальные сети SS7 и Diameter, что позволяет своевременно обнаруживать атаки на отдельных абонентов мобильной связи и инфраструктуру оператора
2. Проводить периодические внешние аудиты безопасности сигнальных сетей
3. В случае выявления уязвимых мест, оперативно осуществлять модернизацию настроек телекоммуникационного оборудования, например запрещать сигнальные сообщения, которые не используются для организации связи между операторами, но могут применяться при проведении атак на сети операторов связи
4. Отрабатывать процедуры с применением инструментов безопасности, позволяющих оперативно блокировать атаки через сигнальные сети
5. Регулярно проводить киберучения с целью проверки уровня защищенности сигнальных сетей

Рекомендации

В Российской Федерации необходимо создание нормативной базы и единой системы сбора и аналитической обработки информации об атаках через сигнальные сети на инфраструктуру и абонентов мобильных операторов связи, а также подключение ее к ГосСОПКА



Контакты

Дмитрий Финогенов
Советник генерального директора
Positive Technologies
Моб.: +7(916)509-79-32
Эл. почта: **dfinogenov@ptsecurity.com**

Дмитрий Касымов
Технических менеджер
Моб.: +7(903)105-53-49
Эл. почта: **dkasymov@ptsecurity.com**