Опыт fu... ошибок SOC

Владимир Дрюков,

Директор центра реагирования и мониторинга Solar JSOC

Ростелеком
Солар

#whoarewe

190+
сотрудников
Solar JSOC

№1
на рынке SOC
в России

7 лет
бесценного
опыта

100+
клиентов,
с которыми
мы стали лучше

История 1 – сказ о потерянном антивирусе

Вводные

- Заказчик – крупная региональная банковская сеть
- Внутренние KPI на покрытие антивирусной защитой
- Выполнение KPI – 98,5%
- «Контроль антивирусной защиты не нужен, сами смотрим»

Три месяца спустя:

- Отстуки на свежий C&C с одной из машин
- Хост – АРМ оператора регионального АРМ КБР
- Первые итоги анализа – ВПО на машине в течение 1,5 лет

Результат

Мораль – доверяй, но проверяй

История 2 – общество мертвых художников

Ростелеком
Солар

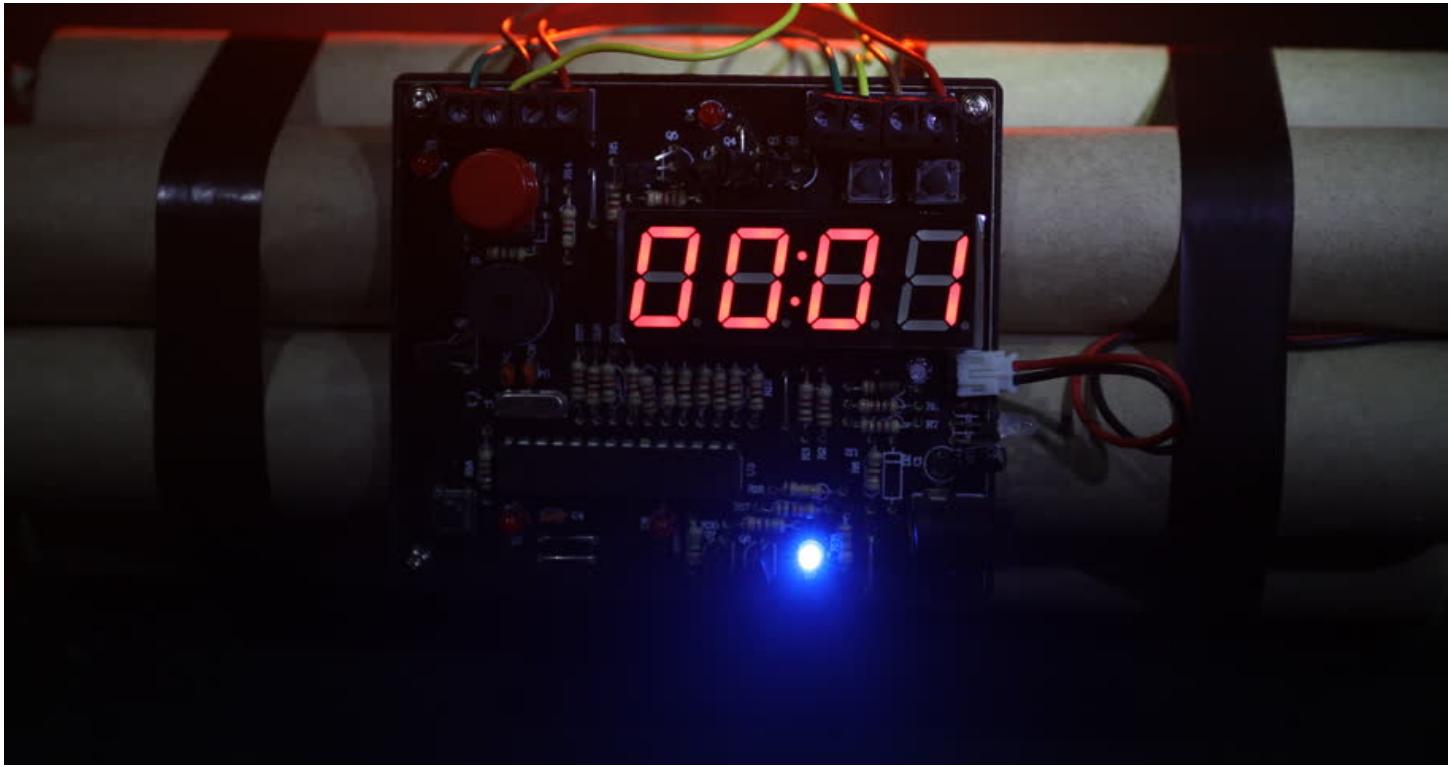
Вводные

- Заказчик – подключены только периметральные средства защиты, цель – выявление сетевых IoC
- 2 коммерческие базы фидов, обновляются на регулярной основе
- Сбой в обновлении одной из них, пришлось чистить «старье» руками

Полтора месяца спустя:

- Странные отстуки и сетевые активности в районе местного SAP
- Ручной анализ логов – попытки общения с мертвыми художниками
- Древняя версия ВПО, принесенная на флешке, приехала и поползла…
- Антивирус – Microsoft Essentials

Результат



Выводы – информация не бывает старой, но бывает устаревшей

Кейс 3 – особенности голубиной почты MDR

Вводные

- Multi-tenant инсталляция SIEM
- Общие учетки для работы в SIEM со всеми заказчиками, контент разделен фильтрами и тэгами
- Два заказчика на одном SIEM с общей адресацией
- У обоих заказчиков отключен резолвинг DNS

Полтора месяца спустя:

- К расследованному инциденту надо приложить отчет
- Сбойнул фильтр при поиске сырых событий по заказчику
- Какой-то отчет большой получился...

Результат

Результат – 2

Выводы – не бывает много защиты от дурака