ВЫБОР СРЕДСТВ ЗАЩИТЫ: ПОДХОД ОТКРЫТИЯ

В жизни всегда
есть место открытию

open.r
u

открытие | БАНК

ПРОБЛЕМАТИКА

Хотим решить задачу, собираем набор коммерческих решений, и…

На бумаге

- почти любое решение покроет 146% потребностей
- проходило внешнее ревью/сертификацию

На практике

- R&D не успевает за маркетингом
- «У нас “as is”, мы не закладывали эту вашу безопасность»

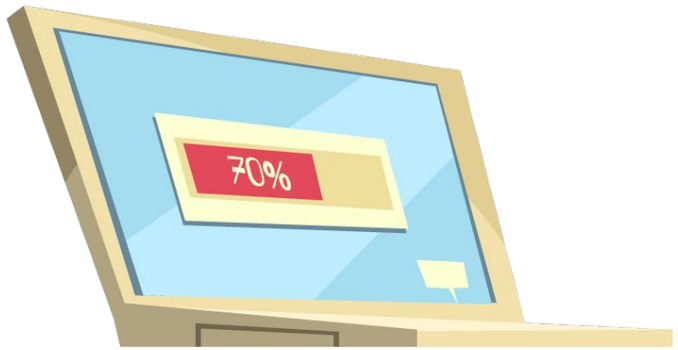
ПОЧЕМУ НАС ЭТО ВОЛНУЕТ?

Заявлено то, чего нет

- Trusteer Rapport – «защита онлайн-банкинга даже на зараженных устройствах»
- <вырезано самоцензурой>

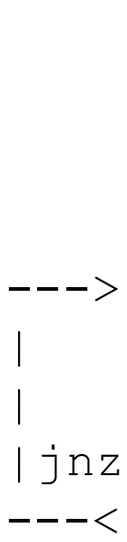
СЗИ забекдорено или уязвимо

- Бекдор в Fortinet (сетевые СЗИ) @2016
- RCE в FireEye (anti-APT) @2015
- LPE в Secret Net (СЗИ от НСД) @2016



THE WHEEL OF PAIN

1. Исследуем рынок в поиске решений, которые *должны* работать
2. составляем шорт-лист
3. Проверяем, работает ли оно
4. Даем фидбек вендору
5. Возвращаемся на шаг 3, пока не заработает
6. Делаем пентест финалиста



ЧТО НА ВЫХОДЕ?

Если работает или имеет потенциал

- Сетевые СЗИ учатся по-настоящему блокировать вредоносный трафик
- «Продвинутые» endpoint-решения учатся блокировать настоящие, а не тестовые атаки
- etc…

Если же нет, то…

- Кто-то уходит и не возвращается
- Или возвращается, но потом

При этом мы:

- Надеемся, что все клиенты вендора получают улучшения
- Открыты для тех, кто придет к нам с вопросами по СЗИ

ЧЬИМИ РУКАМИ?

Условные защитники

- Аналитики
- Инженеры
- Администраторы

Условные нападающие

- Реверсеры
- Пентестеры
- Специалисты по безопасности ПО

НЕ ТОЛЬКО СЗИ

Хорошо, когда secure-by-design

- Все в коробке
- Все работает

Идеальный мир

В любом ПО или ПАК могут быть

- Бекдоры
- Нереализованные на деле функции безопасности
- Уязвимости

Подход аналогичен

Реальность

СПАСИБО!

artem.bychkov@open.ru

В жизни всегда
есть место открытию

open.r
u

открытие | БАНК