КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

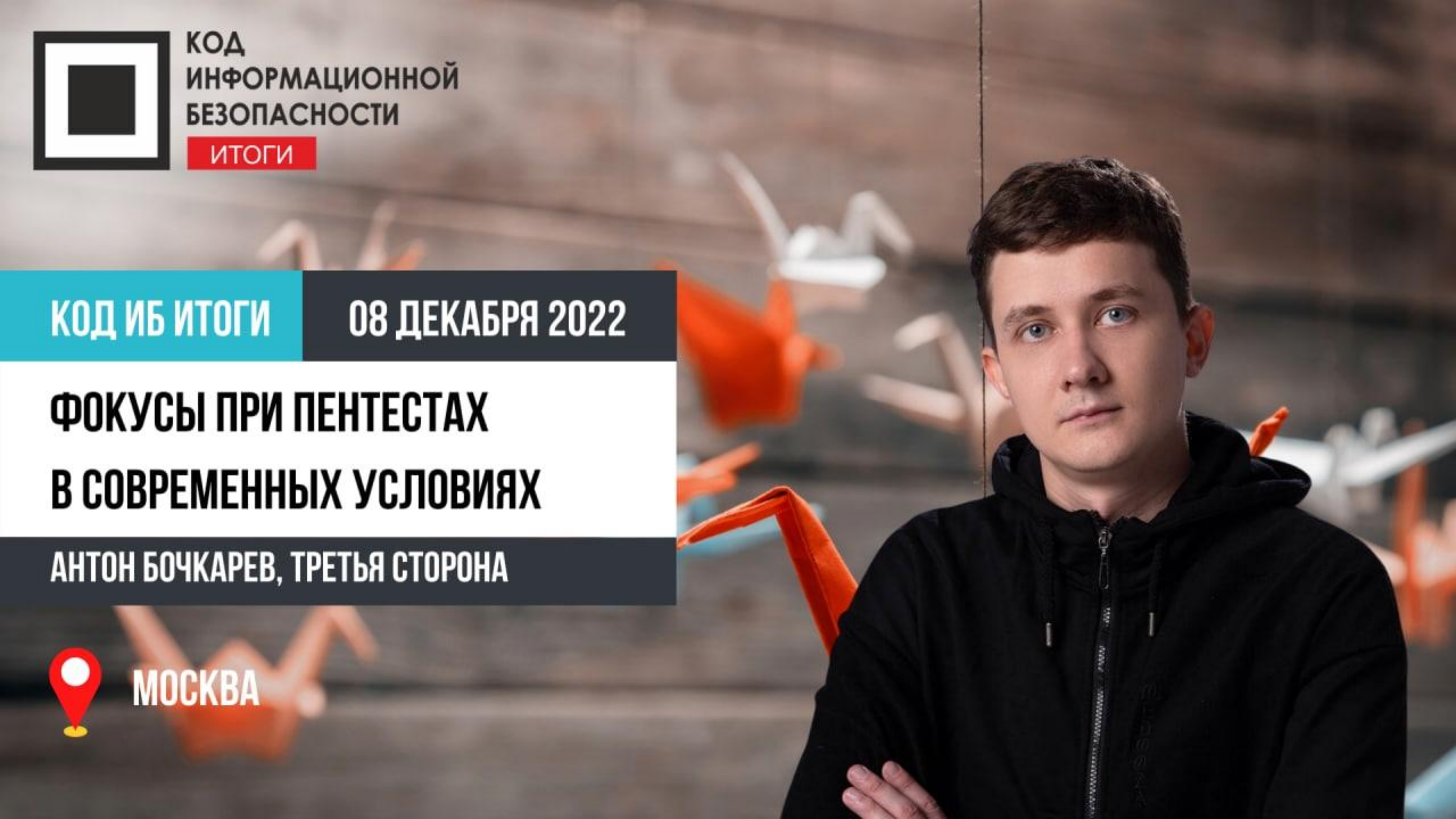
ИТОГИ

КОД ИБ ИТОГИ | 08 ДЕКАБРЯ 2022

ФОКУСЫ ПРИ ПЕНТЕСТАХ В СОВРЕМЕННЫХ УСЛОВИЯХ

АНТОН БОЧКАРЕВ, ТРЕТЬЯ СТОРОНА

МОСКВА



ОБО МНЕ

- 8 лет в Offensive.
- Ex JetInfosystems, Ex Bi.Zone, Ex Red Team Сибур.
- Спикер IT/ИБ конференций.
- Финалист CTF, участник «the Standoff».
- Популяризатор Информационной Безопасности.
- Сооснователь ИБ-стартапа «Третья сторона» 3side.org

Влияние 2022 года

- Кардинально изменилась мотивация атакующих
- За первую половину года, количество атак шифровальщиков выросло на 288%
- Рекордное количество Wipe-malware
- Квалификация атакующих выросла в разы из-за участия ex. пентестеров.
- Появились случаи радикального инсайда

Градус напряжения нарастает (24.02.2022 - ???)

Почему пентесты нужны именно сейчас?

«Нас бы уже взломали»

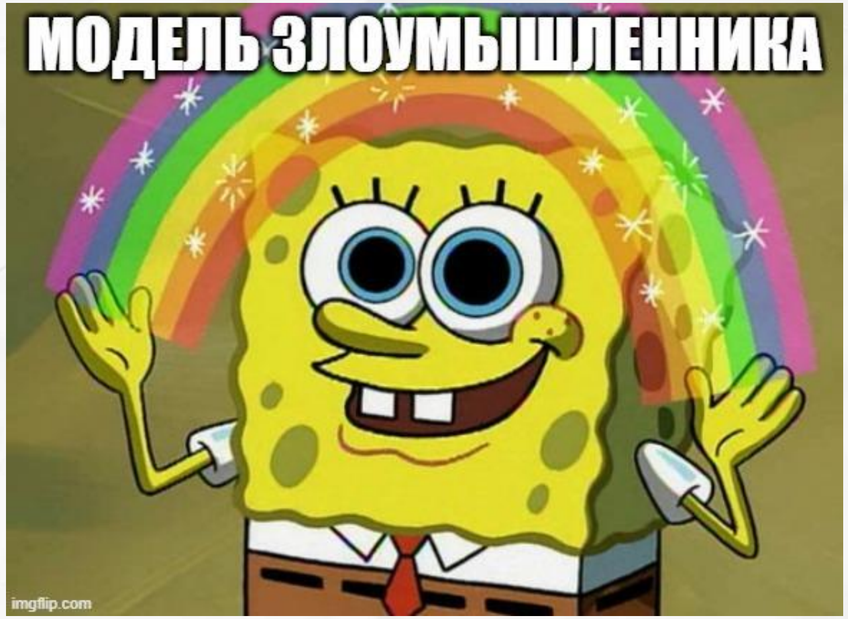
- Активность возросла в разы
- Мотивация изменилась, вы **стали** целью
- Интерпол в рамках конфликта не работает
- Мы уже находили следы компрометации «до нас» у Заказчиков, которые так считали

Может лучше найти уязвимости на пентесте, чем на расследовании?

Модель злоумышленника – краеугольный камень пентеста.

Наиболее актуальны в 2022

- Хактивист
- Взломанный партнер/подрядчик
- Инсайдер/радикальный инсайдер
- Социальный инженер



Нереалистичная модель >> нереалистичный отчет

Хактивист

- Упор на OSINT с обязательным сбором данных из утечек
- В границах работ в первую очередь то, что «на виду»
- В остальном – классический внешний пентест

Иногда из вне «на виду» то, о чем вы уже забыли

Взломанный подрядчик/партнер

- Классический сценарий атак на цепочки поставок, или компрометация внешних сервисов

Основные вопросы:

- Компрометация каких сервисов может затронуть и вас?
- Кто имеет доступ к вашей инфраструктуре?

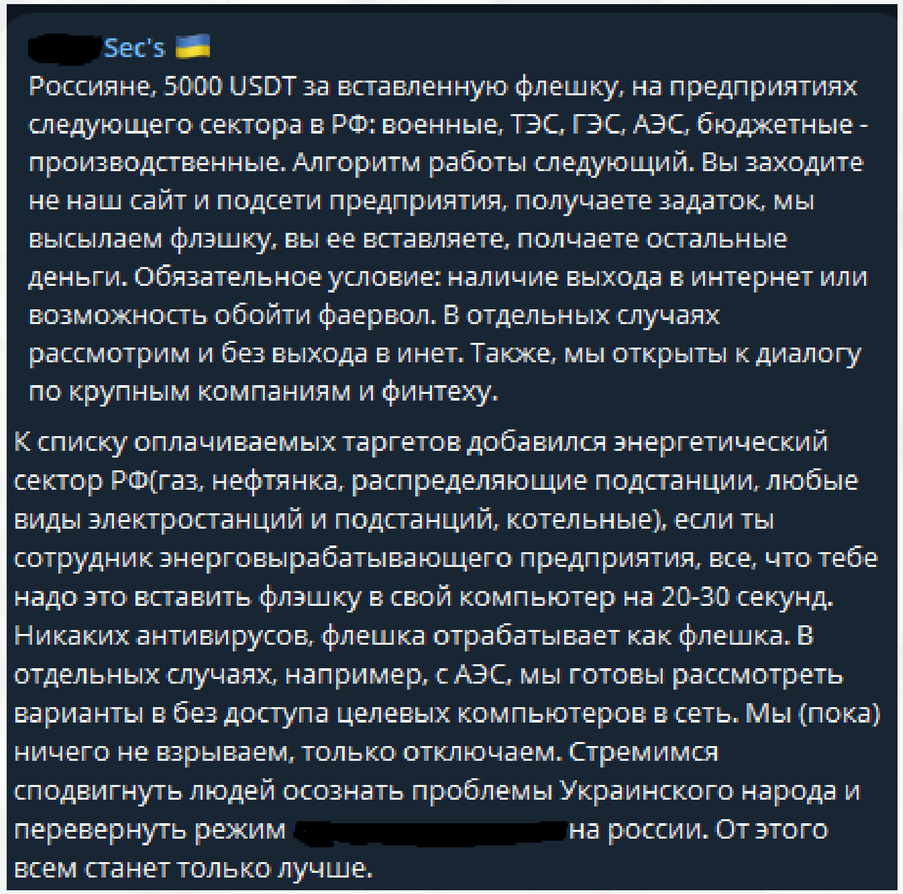
Кому мы доверяем? Никому, конечно же.

Инсайдер/радикальный инсайдер

- **Обязательный** сценарий в текущих условиях
- Классический внутренний пентест из самого массового и IT-сегментов

Причины:

- Алчность
- Политически мотивированная иммиграция



Билеты уже куплены, задержать виновника никто не успеет.

Социальный инженер

- Классический фишинг был и остается на первом месте
- Телефонный фишинг становится **обязательным** сценарием в текущих условиях

Примеры успешных манипуляций в этом году:

- Сожжена машина сотрудника генерального штаба
- Сожжено отделение Сбера в Санкт-Петербурге
- Сотрудник ЦБ перевел 1.6 миллионов кредитных средств мошенникам

Если ваш сотрудник поддался на манипуляцию, он сделает все что ему скажут.

На что еще стоит обратить внимание?

Противодействие и вариативность

- Проведите хотя бы один полноценный проект в формате Redteam
- Подумайте о проведении «скоростного сценария», для оценки скорости реагирования

- Закажите работы у разных команд, свежий взгляд и креативная составляющая часто помогают увидеть значительно больше

Зачем скрываться, если можно все успеть за одну ночь?

Прогноз на 2023

- Стремительный рост Ransomware
- Политически мотивированные APT и хактивисты будут действовать еще эффективнее и организованнее
- Атаки на цепочки поставок будут еще более актуальны
- Границы «этики» взломов будут окончательно стерты
- DDoS вернется разовыми разрушительными атаками

Изменение политической обстановки может повлиять на прогноз исключительно в худшую сторону

Спасибо за внимание!

Готов ответить на ваши вопросы.

Бочкарев Антон Дмитриевич

Все наши контакты на баннерах синего цвета с надписью «3side.org»