КОД ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ


# Социальная инженерия – вечная точка входа.

Бочкарев Антон «Третья Сторона»

# 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

# Статистика

- **90%** атак начинаются с фишинговой рассылки.
- За **8 лет** практики, **100%** проектов по социальной инженерии позволили реализовать одну или несколько угроз ИБ.
- В большинстве успешных атак с использованием социальной инженерии не использовались «авторские» или «уникальные» сценарии.
- В большинстве случаев Заказчик был уверен, что не выдержит социо-техническое тестирование на проникновение.

Обучение сотрудников

**VS**

Средства защиты и запреты

# Правило 7%

- Работает на объёмах рассылки от 100 человек.
- Неизменно вне зависимости от проводимых обучения и тестирований.
- В «группу провалившихся» попадают совершенно разные типы сотрудников.

**Не решается обучением.**

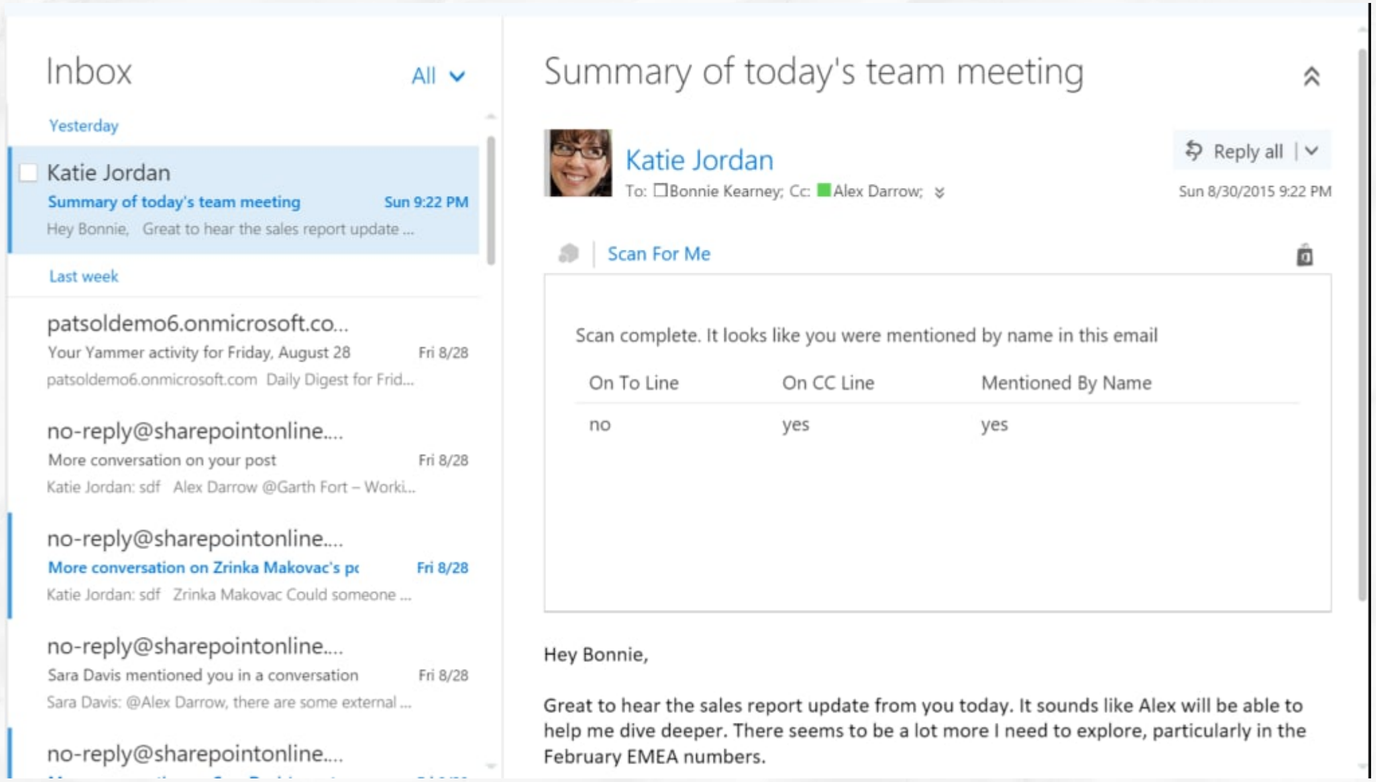
# Личное дело

- Вывод сотрудника из «рабочего» состояния.
- Использование целевых сценариев, адаптированных под потребности жертвы.

**Не решается обучением.**

# Неизменные характеристики

- Использование особенностей характера жертвы.
- Использование недостаточных технический компетенций.




**Не решается обучением.**

# Тактика запретов и блокировок

Что чаще всего используют при социо-технических атаках и как это заблокировать?

- Фишинговые сайты => все недоверенные веб-ресурсы.
- Флешки => все usb-устройства вне белого списка.
- Письма с подменой отправителя => все письма провалившие проверку DMARC.
- Шифрованные архивы => все письма с зашифрованным вложением.
- Макросы и активное содержимое => макросы и powershell.
- И прочее.

**Лишь у небольшого процента компаний все это можно заблокировать для всех пользователей, не нарушив бизнес-процессы.**

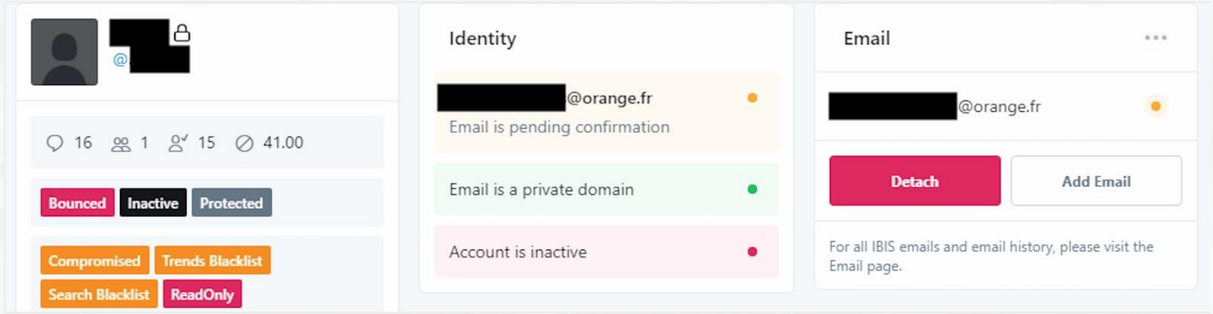
# Обход запретов и блокировок

- Имея контроль над пользователем, возможно обойти бОльшую часть блокировок.
- Жертва, возможно, сама подскажет, как лучше ей переслать файлы или «помочь», ведь она уже встречалась с «подобным» в своей работе.
- Остановить ее могут организационные запреты, которые часто тоже можно обойти с помощью жертвы.

**Способы обойти средства защиты с помощью сотрудников - неискоренимы.**

# Последствия

- Попадание в почту топ-менеджера сложно переоценить.
- Попадание в почту сотрудников техподдержки или низкоуровневого технического персонала, может предоставить злоумышленнику огромные возможности для развития атаки.

# Что же с этим делать?

Комплексно подходить к социо-техническим векторам атак.

- Обучение сотрудников, **совместно** с техническими мерами и средствами защиты.
- Совершенствование процедуры реагирования на инциденты.

Контроль.

- Регулярные социо-технические тестирования на проникновение.
- Red-team для отработки навыков команды реагирования.

- 27 Августа 2022 года в Москве была сожжена машина Евгения Секретарева замначальника управления Генштаба.
- Поджигатель – пенсионерка Елена Белова, выкрикивала экстремистские лозунги рядом с машиной.
- Была уверена, что борется с бандитами и помогает силовым структурам, лозунг – пароль для полиции.
- Под влиянием выполнила **все** инструкции оператора call-центра из Украины.

# Возможности социальной инженерии тяжело переоценить.

# Спасибо за внимание!

# Готов ответить на ваши вопросы.

Бочкарев Антон Дмитриевич
E-mail: adb@3side.org
TG: @bam_hack