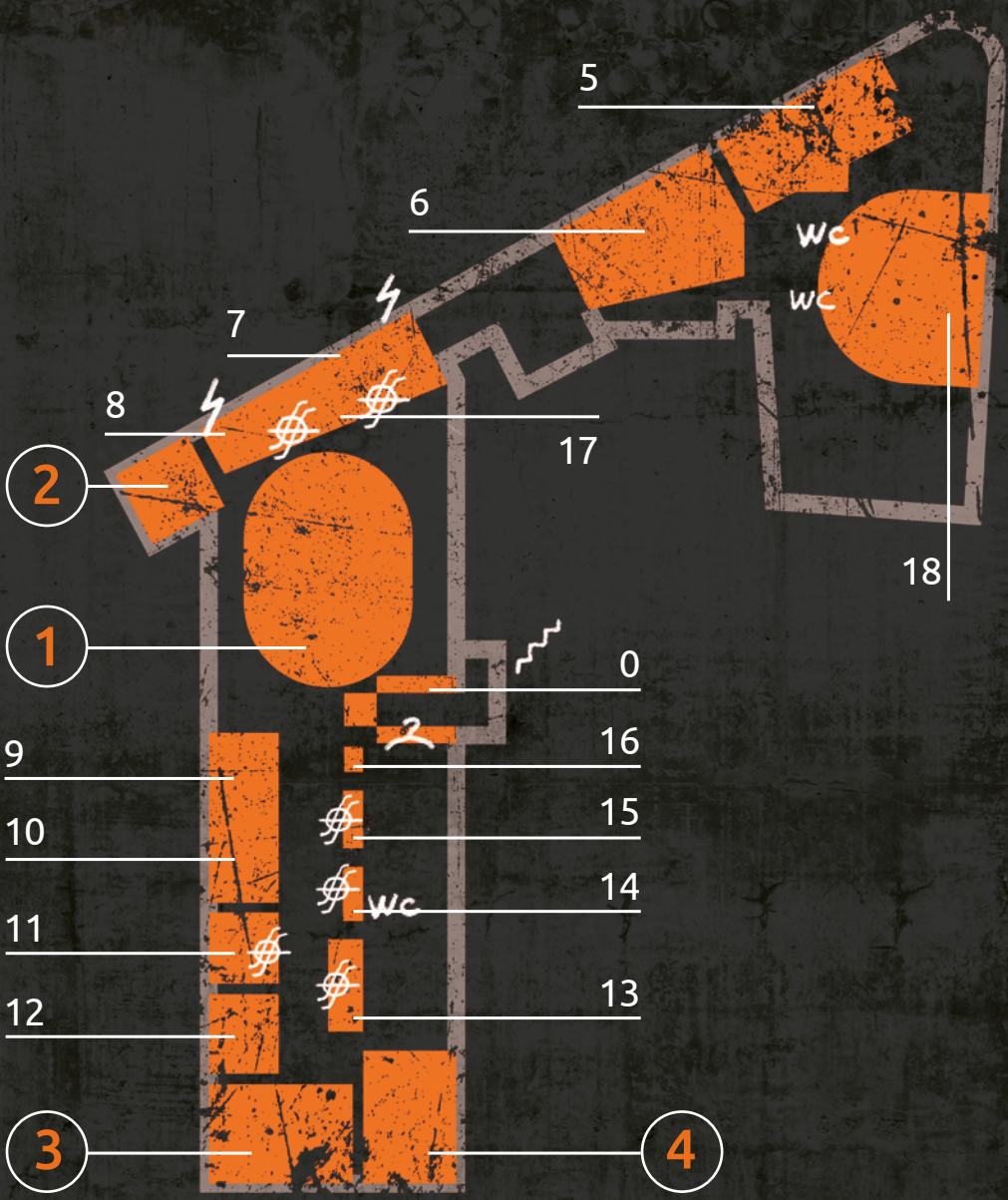
WELCOME TO OFFZONE

15 – 16 ноября 2018

OFF ZONE 2018

Карта мероприятия



0 Регистрация

1 **MAIN TRACK**

2 **HARDWARE.ZONE**

3 **WEB.ZONE / FAST TRACK**

4 **FINANCE.ZONE**

5 Комната спикеров

6 Бар

7 LOUNGE.ZONE

8 Кикер «Зомби против выживших»

9 Qiwi

10 Валарм

11 GAME.ZONE

12 Kaspersky Lab

13 BI.ZONE

14 “Танчики”

15 TATTOO.ZONE

16 Лавка Старьевщика

17 Велотрек

18 CTFZONE

Зарядные станции

Offcoin

15 ноября

MAIN TRACK

11:30 **Открытие**

12:00 **20 лет в ИБ: взгляд со стороны исследователя**
Дмитрий Скляров, Positive Technologies

13:00 **We will charge you. Как пробраться в сеть вендора сквозь EV-зарядку**
Дмитрий Скляр, Kaspersky Lab

14:00

15:00 **Проснись, Нео: детектирование виртуализации при помощи спекулятивного исполнения**
Иннокентий Сенновский, BI.ZONE

16:00 **Уязвимости мобильного OAuth 2.0**
Никита Ступин, Mail.Ru Group

17:00 **Кибергруппировка Lazarus: новые правила игры**
Michal Poslušný и Peter Kálnai, ESET

18:00 **HIDS as a service: деплой и контроль 20 000 инсталляций**
Иван Агарков, Wargaming

19:00

HARDWARE.ZONE

13:00 **Быстрое введение в Software Defined Radio**
Александр Алексеев, Независимый исследователь

14:00 **Знакомство с GnuRadio**
Даниил Погорелов, Независимый исследователь

15:00 **Введение в схемотехнику**
Антон Канышев, Hardware designer

16:00 **Знакомство с микроконтроллерами STM32**
Александр Алексеев, Независимый исследователь

17:00 **DIY для hardware reverse**
Егор Литвинов, GS-Labs

18:00 **Fault Injection-атаки на ARM MK**
Арсений Жгилёв, BI.ZONE

19:00

15 ноября

FINANCE.ZONE

13:00 **Безналичные платежи — как это работает**
Дмитрий Гадарь, Tinkoff.ru

14:00 **Эволюция фрода**
Игорь Митюрин, ПАО Сбербанк

15:00

16:00 **Охота на Android Malware: история о том, как мы ловим преступников**
Борис Иванов, BI.ZONE

17:00 **Антифрод**
Екатерина Блинова, Яндекс.Деньги

18:00

WEB.ZONE

13:00 **Альтернативный обход WAF — Cheat Sheet**
Антон Лопаницын,
Багхантер и исследователь

14:00 **DNS Rebinding в 2k18**
Михаил Фирстов и Андрей Скуратов,
FBK CyberSecurity

15:00

16:00 **HTTP/2**
Магомед Нуров, BI.ZONE

17:00 **Эксплуатация XSS**
Игорь Сак-Саковский, Positive Technologies

18:00 **Атаки на веб-приложения с многослойной архитектурой**
Омар Ганиев, Deteact

19:00

16 ноября

MAIN TRACK

11:00 **Готовы ли мы к массовому внедрению биометрии?**
Никита Вдовушкин и Владислав Лазарев, BI.ZONE

12:00 **Секретики Windows DPAPI**
Константин Евдокимов, M-13

13:00 **Посягательство на самое драгоценное: атаки на менеджеры лицензий**
Сергей Темников и Владимир Дащенко, Kaspersky Lab

14:00

15:00 **Intel ME Manufacturing Mode — скрытая угроза**
Максим Горячий и Марк Ермолов, Positive Technologies

16:00 **Засучим рукава: интерактивное обучение как путь к безопасному программированию**
Anirudh Anand и Mohan Kallepalli, Flipkart

17:00 **Среда Windows: в попытках повысить привилегии**
Теймур Хеирхабаров, Kaspersky Lab

18:00

18:30 **Награждение CTFZONE и закрытие конференции**

HARDWARE.ZONE

11:00 **Side channel атаки**
Иннокентий Сенновский, BI.ZONE

12:00 **Введение в Zigbee**
Егор Литвинов, GS-Labs

13:00 **Как осуществлять перехват и обработку цифровых сигналов на примере nRF24**
Даниил Погорелов, Независимый исследователь

14:00 **Запуск базовой станции GSM на примере Motorolla и USRP**
Даниил Погорелов, Независимый исследователь

15:00 **Физическая безопасность: теория и практика вскрытия замков**
Данила Згонников, Независимый исследователь

16:00 **Изготовление отмычек под разные типы замков**
Данила Згонников, Независимый исследователь

17:00

16 ноября

FINANCE.ZONE

11:00 **Ради денег. Уязвимости платежных устройств**
Тимур Юнусов и Ярослав Бабин, Positive Technologies

12:00

13:00 **Безопасность банкоматов**
Алексей Стенников, Positive Technologies

14:00 **Готов стать пентестером вашего ДБО, или как ломают онлайн-банкинг**
Аркадий Литвиненко, BI.ZONE

FAST TRACK

11:00 **ThingsPro Suite: IIoT-гейтвей от компании Moxa под капотом** Александр Ночвай

11:30 **OAuth2.0@2018– что вы делаете не так?**
Алексей Черных

12:00 **Взламываем телефонные системы ради выгоды и веселья** Himanshu Mehta

12:30

13:00 **Тонкости дебага Cisco ASA**
Илья Костюлин и Сергей Овчинников

13:30 **Забираем Вашу почту без смс и регистрации** Ольга Карелова

14:00 **История одного DevSecOps**
Артем Бачевский, Денис Ратченко, Алексей Гуськов

14:30

15:00 **AppSec as a Code**
Антон Башарин и Юрий Шабалин

15:30

16:00 **Scanner Orchestration Tool: SDLC за один клик** Илья Говорков и Иван Елкин

16:30 **HWallet: простейший аппаратный кошелек для биткоина** Nemanja Nikodijevic

17:00 **IP-репутация: как делать не надо**
Денис Горчаков

17:30 **Что нового в безопасности Android?**
Юрий Шабалин

18:00

Залы

MAIN TRACK

В Main Track о нашумевших низкоуровневых уязвимостях расскажут Максим Горячий и Марк Ермолов (доклад «Intel ME Manufacturing Mode — скрытая угроза»), а также Иннокентий Сенновский («Проснись, Нео: детектирование виртуализации при помощи спекулятивного исполнения»).

Какие типовые методы используют киберпреступники для повышения привилегий в ОС Windows? Как атакуют менеджеры лицензий? Как и с каким инструментарием действовала группировка Lazarus? Достаточно ли развиты биометрические системы для массового использования и как их удается обходить? Это лишь малая часть тем, которые мы подробно рассмотрим в Main Track за два дня конференции.

HARDWARE.ZONE

Если у тебя давно было желание попробовать себя в hardware и для этого нужен был знак, то это он.

Организаторы трека HARDWARE.ZONE доступным языком расскажут про наиболее интересные направления аппаратной безопасности: GnuRadio, введение в схемотехнику, микроконтроллеры STM32, атаки по побочным каналам, перехват и обработку цифровых сигналов на примере nRF24, атаки fault injection на ARM MK и многое-многое другое (трек длится целых два дня). И, конечно же, здесь можно найти всеми любимые отмычки!

Залы

FINANCE.ZONE

На треке FINANCE.ZONE поговорим о том, как на самом деле устроена кибербезопасность в мире финансов.

Начнем с самых основ и разберемся, как работает процессинг, потом перейдем к темам фрода и антифрода с реальными кейсами, рассмотрим проблемы безопасности АТМ и ДБО и под конец погрузимся в технические подробности того, как ломают и защищают сложнейшие финансовые системы и их отдельные компоненты.

WEB.ZONE

В секции WEB.ZONE проанализируем альтернативные способы обхода WAF, рассмотрим, что представляет собой атака DNS Rebinding в 2k18, разберемся, как HTTP/2 работает внутри и какие атаки уже не удастся осуществить, обсудим подходы к анализу приложений с многослойной архитектурой и, конечно, поговорим об эксплуатации XSS.

Да пребудет с тобой веб!

FAST TRACK

Fast Track начнется во второй день конференции (поэтому, чтобы увидеть доклады Fast Track, сразу смотри программу на 16 ноября).

В первой половине дня поговорим о реализации OAuth 2.0, DNS Exfiltration, а также об инструменте для проведения фишинговых кампаний в контексте исследований Red Team. Еще представим исследования о компрометации телефонной системы, а также расскажем и покажем в деталях, что находится под капотом IIoT-гейтвея Things Pro Suite. Доклады второй части мы объединили в Defensive Track: если тебе не безразличны такие слова, как DevSecOps, SDLC, AppSec — добро пожаловать на трек! И не забудьте подготовить интересные вопросы для спикеров.

GAME.ZONE

Совмести приятное с полезным в зоне с игровыми приставками: каждый час здесь проходят турниры, победителям которых начисляются очки OFFCOIN. Поле битвы — популярные игры: Mortal Kombat XL, Worms™ Battlegrounds и TEKKEN 7. И, конечно, мы не забыли о старых добрых приставках Nintendo и SEGA. Заходи в GAME.ZONE порадовать себя любимыми играми!

Задания с бейдж-картой

За умными устройствами далеко ходить не надо: твоя бейдж-карта конференции умеет много крутых вещей. Проверь, на что она способна, и заодно проверь себя:

- испытай навыки программирования, заставив бейдж-карту играть за тебя в «танчики» против компьютера или даже другой карты;
- прояви смекалку, сыграв со своей бейдж-картой в сокобан;
- реши несколько интересных заданий прямо на бейдже!

Больше информации о карте доступно на offzone.moscow/badge

Лавка старьевщика

Сувенирная лавка с продавцом, который расскажет много интересного о постапокалиптической торговле. У старьевщика можно обменять заработанные очки OFFCOIN на сувениры с логотипом конференции (говорят, он охотно принимает и рубли).

Велотрек

Интерактивное соревнование на велотренажерах и машинках на треке. Участники крутят педали на велотренажерах, а их машинки едут к финишу. Кто быстрее крутит, тот приезжает первым и зарабатывает очки OFFCOIN!

Кикер «Зомби против выживших»

Постапокалиптический кикер прибавляет не только адреналина в крови, но и очков OFFCOIN на бейдж-карту. Ты за зомби или за выживших? Приходи потренировать снейк-шоты и пин-шоты — внезапные атаки проводит не только Red Team.

Игра «Тотализатор CTFZONE»

Проверь свою интуицию: попробуй угадать, кто из участников финала соревнований CTFZONE наберет больше очков за определенный интервал времени.Чтобы сделать ставку, найди администратора в зоне BI.ZONE. Он переведет часть очков OFFCOIN с твоей бейдж-карты в телеграм-бот, где ты можешь выбрать свою команду-фаворита. Интуиция сработала? Тот же администратор в зоне BI.ZONE выведет полученные за победу баллы из телеграм-бота обратно на твою бейдж-карту. Подробности об игре — на стойке BI.ZONE.

TATTOO.ZONE

Самое подходящее место для творческих людей, желающих заработать очки OFFCOIN и просто набить тату. Гостям предлагается:

Нанести тату на шкуру бизона. Татуировка — искусство, которому учатся годами. Но здесь приобщиться к нему могут даже те, кто не умеет рисовать. В распоряжении начинающих тату-мастеров будут огромная шкура бизона, заряженная машинка с иглой и краской, а также уникальные трансферные стикеры, по которым несложно сделать свою первую татуировку. Каждый час мы будем выбирать лучшего начинающего тату-мастера и награждать его очками OFFCOIN.

Покрутить барабан и испытать удачу в лотерее. В зоне установлен барабан с капсулами, в которых лежат вкладыши на получение приза. Это может быть татуировка, набор стикеров, очки OFFCOIN — а может быть шанс прокрутить барабан вновь.

Поучаствовать в викторине «Везучий случай». Это самый смелый способ получить татуировку: предстоит пить и стрелять. Если что, стрелять — по плакату с дизайнами татуировок. Но прежде участник должен ответить на три вопроса по разным аспектам кибербезопасности. Все ответы в точку — нальем и пригласим подойти поближе к мишени, были ошибки — придется стрелять с дальней дистанции. В какую тату попадешь из игрушечного пистолета, ту и заберешь. Смельчаки, которые решатся ее набить, получат много очков OFFCOIN.

Набить тату у профессионального татуировщика. Не все же в игры играть, да? Подробности можно узнать у организаторов. И да, за это мы тоже дадим вам много очков OFFCOIN!

Организатор

BI.ZONE
Cybersecurity

Медиа партнеры

Хакер

ANTI-MALWARE

Партнеры

QIWI
Всё проще

валарм

KASPERSKY lab

Комьюнити партнеры

IT SEC

DEFCON NN

RO CREW

DC 8800

КАФЕ И РЕСТОРАНЫ

0 **Progress bar,** Европейская кухня, 500—900 ₽
Берсеневская набережная, 6, строение 3

1 **Сыроварня,** Итальянская, русская, 1500—2000 ₽
Берсеневский переулок, 2, строение 1

2 **Кофейня 1316,** Кофейня, 300—800 ₽
Берсеневская набережная 6с3

3 **Урожай,** Ресторан/Бар, 500-1500 ₽
Берсеневская набережная 6с3

4 **Pita Gyros,** Греческая кухня/Фастфуд, 300—800 ₽
Берсеневская набережная 6с4

5 **ДаблБи,** Кофейня, 500—1000 ₽
Берсеневская набережная 8/1

6 **Silver Panda,** Китайская, азиатская, 300-500 ₽
Берсеневский переулок, 2, строение 1

7 **Bruce Lee,** Китайская кухня, 700—1500 ₽
Болотная набережная д.3/2, стр. 4

8 **Магадан,** Рыба/Морепродукты, 1500—3000 ₽
Берсеневский переулок 3/10с8

9 **Shakti terrace,** Паназиатская кухня, 1000—2000 ₽
Болотная набережная 11с1